Homework for Computational Complexity
Spring 2020, UPC Barcelona
Instructor: Albert Atserias

Created: 11/06/2020
Last modified: 12/06/2020

Homework 3 - Solutions

Exercise 1 The inclusion $\mathrm{BPP} \subseteq \mathrm{BPP}^{\mathrm{BPP}}$ is obvious since the given access to the oracle can be simply ignored. To prove $\mathrm{BPP}^{\mathrm{BPP}} \subseteq \mathrm{BPP}$ fix a language $A \in \mathrm{BPP}^{\mathrm{BPP}}$ and we show that it is also in BPP. Let M be a polynomial-time non-deterministic oracle Turing machine and let $B \in \mathrm{BPP}$ be such that M^B decides A with error bounded by $1/4$. Let $p(n) = n^k$ be a polynomial that bounds the running time of M^B on inputs of length n. Let M' be the polynomial-time non-deterministic Turing machine that works as follows: On input x of length n, simulate the computation of M^B on input x but replace each query "$y \in B$?" by $2n^{k+1} + 1$ many executions of the BPP algorithm that decides B on input y, and take the majority vote as the answer to the query. By the same analysis as in the error reduction theorem, the probability that any one of the majority votes gives a wrong answer is, for large enough n, at most 2^{-n^k}. Since each computation path makes at most n^k queries, the probability that M' gets a wrong answer in one of the majority votes or a wrong answer in the end is at most $n^k 2^{-n^k} + 1/4$, which is less than $1/3$, for large enough n. This shows that M' decides A with error at most $1/3$, for large enough n. By table look-up we can make it decide A with error at most $1/3$ on all input lengths and still run in polynomial time. Error reduction applied to M' to reduce this error to $1/4$ shows that A is in BPP.

Exercise 2 By what we did "in class", it suffices to show that if $\Sigma_i^{\mathrm{P}} = \Pi_i^{\mathrm{P}}$, then $\Sigma_{i+1}^{\mathrm{P}} \subseteq \Sigma_i^{\mathrm{P}}$. Assume then that $\Sigma_i^{\mathrm{P}} = \Pi_i^{\mathrm{P}}$ and let A be a language in $\Sigma_{i+1}^{\mathrm{P}}$, say

$$A = \{x : (\exists y, |y| \leq |x|^k)(\langle x, y\rangle \in B)\}$$

where $B \in \Pi_i^{\mathrm{P}}$ and $k \geq 1$ is a constant. By assumption we also have $B \in \Sigma_i^{\mathrm{P}}$ hence $A \in \Sigma_i^{\mathrm{P}}$ by collapsing the leading existential quantifier in the Σ_i^{P}-expression for B with the existential quantifier $\exists y$ in A.

Exercise 3 Assume $\mathrm{NP} \subseteq \mathrm{P/poly}$. This implies $\mathrm{NP}^{\mathrm{SAT}} \subseteq \mathrm{NP/poly}$: give the advices for the polynomially many input lengths that are potentially queried in the $\mathrm{NP}^{\mathrm{SAT}}$ machine as advice. It follows that $\mathrm{NP}^{\mathrm{NP}} \subseteq \mathrm{NP}^{\mathrm{SAT}} \subseteq \mathrm{NP/poly} \subseteq (\mathrm{P/poly})/\mathrm{poly} \subseteq \mathrm{P/poly}$. For Karp-Lipton, assume that $\mathrm{NP} \subseteq \mathrm{P/poly}$, so SAT has polynomial size circuits. By self-reducibility of SAT, for every formula-size m there is a circuit C_m of size at most m^q for some constant $q \geq 1$ such that, given a Boolean formula F of size m, the circuit $C_m(F)$ outputs a satisfying assignment of F if there is one, i.e., $F(C(F)) = 1$ if and only if F is satisfiable. Now, fix $A \in \Pi_2^{\mathrm{P}}$ say

$$A = \{x : (\forall y_1, |y_1| \leq |x|^k)(\exists y_2, |y_2| \leq |x|^k)(\langle x, y_1, y_2\rangle \in B\}$$

where $B \in \mathrm{P}$ and $k \geq 1$ is a constant. The language

$$C := \{\langle x, y_1\rangle : (\exists y_2, |y_2| \leq |x|^k)(|y_1| \leq |x|^k \wedge \langle x, y_1, y_2\rangle \in B)\}$$

is in NP. By the Cook-Levin Theorem there is a polynomial time computable function F such that, for every x and y_1 we have $\langle x, y_1 \rangle \in C$ if and only if $F(\langle x, y_1 \rangle)$ is a satisfiable formula, i.e., if and only if $F(\langle x, y_1 \rangle)(C_m(F(\langle x, y_1 \rangle))) = 1$, where m is the length of $F(\langle x, y_1 \rangle)$. Suppose the length m of $F(\langle x, y_1 \rangle)$ is bounded by $|x|^r$ when $|y_1| \leq |x|^k$. Then

$$A = \{x : (\exists C, |C| \leq |x|^{rq})(\forall y_1, |y_1| \leq |x|^k)(F(\langle x, y_1 \rangle)(C(F(\langle x, y_1 \rangle))) = 1)\}.$$

This shows that $A \in \Sigma_2^{\mathrm{P}}$ and we have shown $\Pi_2^{\mathrm{P}} \subseteq \Sigma_2^{\mathrm{P}}$. By symmetry we also have $\Sigma_2^{\mathrm{P}} \subseteq \Pi_2^{\mathrm{P}}$, hence $\Sigma_2^{\mathrm{P}} = \Pi_2^{\mathrm{P}}$ and the polynomial time hierarchy collapses to $\Sigma_2^{\mathrm{P}} = \Pi_2^{\mathrm{P}}$.