Homework for Computational Complexity
Spring 2019, UPC Barcelona
Instructor: Albert Atserias

Created: 24/05/2019
Last modified: 24/05/2019

Homework 3

Exercise: IPs with deterministic verifiers Prove that dIP = NP. [1]

[1] Let dIP be defined like IP except that the verifier is deterministic instead of probabilistic: A language L is in dIP if and only if there exists a polynomial-time computable function $V : \Sigma^* \times \Sigma^* \to \Sigma^* \cup \{0, 1\}$ and a polynomial p such that for every $x \in \Sigma^*$ and for $t = p(|x|)$ the following hold:

1. if $x \in L$, then there exists a p-bounded prover P such that $(V \leftrightarrow_t P)(x) = 1$,
2. if $x \notin L$, then for every p-bounded prover P we have $(V \leftrightarrow_t P)(x) = 0$.

Recall that a p-bounded prover is a function $P : \Sigma^* \times \Sigma^* \to \Sigma^*$ satisfying $|P(x, \langle m_1, \ldots, m_r\rangle)| \leq p(|x|)$ for every $x \in \Sigma^*$ and $m_1, \ldots, m_r \in \Sigma^*$, and that $(V \leftrightarrow_t P)(x)$ denotes the output of the $2t$-round iteraction between V and P on input x; i.e., $(V \leftrightarrow_t P)(x) = V(x, \langle m_1, \ldots, m_{2t}\rangle)$ where $m_{2i-1} = V(x, \langle m_1, \ldots, m_{2i-2}\rangle)$ and $m_{2i} = P(x, \langle m_1, \ldots, m_{2i-1}\rangle)$ for $i = 1, \ldots, t$.