Miguel Alcón Doganoc
Computational Complexity
May 28, 2019

Homework 3

1 Exercise: IPs with deterministic verifiers

1.1 dIP $\supseteq$ NP

As we know, a language $L \subseteq \{0,1\}^*$ is in **NP** if there exists a polynomial $p : \mathbb{N} \to \mathbb{N}$ and a poly-time TM M (the *verifier* for L) s.t. for every $x \in \{0,1\}^*$,

$$x \in L \Leftrightarrow \exists u \in \{0,1\}^{p(|x|)} \text{ s.t. } M(x,u) = 1$$

If $x \in L$ and $u \in \{0,1\}^{p(|x|)}$ satisfy $M(x,u) = 1$, we call u a *certificate* for x.

So, if $L \in \mathbf{NP}$, then we can let the prover P provide the *certificate* of the input in the first round of the deterministic prove system, and also let the verifier V behave like M. Hence, $L \in \mathbf{dIP}$.

1.2 dIP $\subseteq$ NP

Starting from $L \in \mathbf{dIP}$, let V, P be the verifier and prover for L. A *certificate* that an input x is in L is a transcript $(m_1, m_2, ..., m_{2t})$ causing V to accept. We can verify the transcript checking that

$$V(x) = m_1, V(x, \langle m_1, m_2\rangle) = m_3, ..., \text{ and } V(x, \langle m_1, m_2, ..., m_{2t}\rangle) = 1$$

We know the transcript exists since $L \in \mathbf{dIP}$. So, we can define P to satisfy

$$P(x, \langle m_1\rangle) = m_2, P(x, \langle m_1, m_2, m_3\rangle) = m_4, ..., P(x, \langle m_1, ..., m_{2t-1}\rangle) = m_{2t}$$

With this, we can clearly see that $(V \leftrightarrow_t P)(x) = V(x, \langle m_1, m_2, ..., m_{2t}\rangle) = 1$, hence $x \in L$. Then $L \in \mathbf{NP}$. $\square$