CS 40: Computational Complexity

Sair Shaikh

November 6, 2025

Problem 1. Prove that $\text{IP}_{0:\frac{2}{3}} = \text{NP}$.

Solution. First, we handle the easy direction. Note that NP = $\exists$P (by Problem 1), i.e. languages in NP are precisely those where, for each string, there exists a polynomial-sized witness that can be verified in polynomial time if and only if that string is in the language. Thus, we can come up with an verifier-prover protocol, where the prover produces this witness string (using their infinite powers), and the verifier runs the polynomial time computation to verify it (without the need for randomness). If the instance was not in the language, no such witness string would exist to pass the polynomial time computation. Thus, $\text{NP} \subseteq \text{IP}_{0:1} \subseteq \text{IP}_{0:\frac{2}{3}}$, where the last containment follows as we are weakening the error bounds on the complexity class.

Next, we need to show that $\text{IP}_{0:\frac{2}{3}} \subseteq \text{NP}$. We recall the definition of NP = $\exists P$,

$$\exists P = \{\{x \in \Sigma^* : \exists y \in \Sigma^* \text{ with } |y| = \text{poly}(|x|) \text{ such that } \langle x, y\rangle \in L_0\} : L_0 \in P\}$$

Let $L \in \text{IP}_{0:\frac{2}{3}}$. It suffices to construct a language $L_0 \in \text{P}$ such that:

$$x \in L \iff \exists y_x : |y_x| \in \text{poly}(|x|) \wedge \langle x, y_x\rangle \in L_0 \in P$$

Note that if $x \in L$, then there exists a prover P such that:

$$\mathbf{Pr}_r[V * P(x, r) = 1] \geq \frac{2}{3}$$

Note that since this probability is positive, there exists some r' such that $V * P(x, r') = 1$. We pick as y_x the transcript of all messages up to the last verification by the verifier, call it T, as well as the r', i.e. $y_x = \langle T, r'\rangle$. Next, we need to show that $|y_x| \in \text{poly}(|x|)$ and that there exists a polynomial time turing machine that accepts $\langle x, y_x\rangle$.

Note that $\text{IP}_{0:\frac{2}{3}}$ involves only a polynomial round of interactions. In each round of interactions, the messages sent are also at most polynomial in length, as the polynomial-time bounded verifier needs to send and read them. Thus, the entire transcript is polynomial length in $|x|$. Moreover, the randomness uses by the verifier is also polynomial length by the same argument. Thus, $y_x \in \text{poly}(|x|)$.

Moreover, we have the following algorithm A that accepts $\langle x, T, r' \rangle$.

1. Simulate the verifier on input x to verify the transcript. Run each of the computations that the verifier would have run, given the previous prover message. Check your own output against what the verifier sent in the transcript, reject if there's a discrepancy. Use the randomness from r' in these computations.
2. Simulate the final computation by the verifier using the remanining randomness from r'. Accept if the verifier would have accepted, reject otherwise.

This clearly runs in polynomial time as it is simulating a polynomial-time bounded verifier for a polynomial number of rounds of interaction. In fact, it is even polynomial in $|x|$, which is a part of the input.

Thus, we have shown that:

$$x \in L \implies \exists y_x : |y_x| \in \text{poly}(|x|) \wedge \langle x, y_x \rangle \in L_0 \in \text{P}$$

For the other direction, fix some x and assume that there exists y_x such that $|y_x| \in \text{poly}(|x|)$ and A accepts $\langle x, y_x \rangle$. Since A verifies that y_x consists of a valid transcript and at least one choice of randomness to make the verifier accept, we note that there must exist a prover (that generates responses in accordance with this transcript) such that the probabilitiy that the verifier accepts is non-zero (probabilistic method). That is,

$$\exists y_x : |y_x| \in \text{poly}(|x|) \wedge \langle x, y_x \rangle \in L_0 \in \text{P} \implies \exists P : \mathbf{Pr}_r[V * P(x, r) = 1] > 0$$

But then this implies that $x \in L$ by the definition of $\text{IP}_{0:\frac{2}{3}}$ (i.e. this implication is the contrapositive of the $x \notin L$ case of the IP definition). Thus, we have shown that:

$$x \in L \iff \exists y_x : |y_x| \in \text{poly}(|x|) \wedge \langle x, y_x \rangle \in L_0 \in P$$

Thus, $L \in \exists \text{P} = \text{NP}$. That shows that $\text{IP}_{0:\frac{2}{3}} = \text{NP}$.