Thursday, February 24, 2022 1:27 PM

Goals

- Understand NP Definition

<u>NP</u>

Let $L \subseteq \{0,1\}^*$. Then $L \in NP$ if $\exists$ a polynomial $p: \mathbb{N} \to \mathbb{N}$ and a polytime TM M s.t. $\forall x \in \{0,1\}^*$

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

If $x \in L$, then $\exists\, u \in \{0,1\}^{p(n)}$ s.t. $M(x,u)=1$

If $x \notin L$, then $\underline{\forall\, u} \in \{0,1\}^{p(n)}$, $\underline{M(x,u)=0}$

Terminology:

- $M \Rightarrow$ Verifier
- $u \Rightarrow$ witness or certifate

$m \times m$ grid $O(m^2)$

ex:

$L = \{\langle x \rangle : x$ is a solvable sudoku grid$\}$

u? fill of the rest of the grid

M? checks each row + col