# 374: Lecture 25: Poly reductions and NP and other stuff 11/17/22

polynomial time reductions

$$\boxed{X} \xrightarrow{R} \boxed{Y}$$

$I_X$ is YES $\overset{R}{\Longleftrightarrow} I_Y = R(I_X)$ is YES

R runs in poly time.

---

CLIQUE $\overset{P}{\Longleftrightarrow}$ Independent set $\overset{P}{\Longleftrightarrow}$ Vertex Cover

$\langle G, k\rangle$ $\langle G, k\rangle$ $\langle G, k\rangle$

SAT 3SAT

CNF formula $\bigwedge_{i=1}^{m} C_i$ $C_i = \bigvee_{j=1}^{t} l_{ij}$

$l_{ij}$ is a literal variable or its negation.

$$f(x_1, x_2, \dots, x_n) = (\overline{x_7} \vee x_2 \vee x_{13} \vee \overline{x_{55}}) \wedge x_{11} \wedge (x_{12} \vee x_7)$$

$2^n$

---

3SAT $(x_1 \vee \overline{x_2} \vee x_3) \wedge (x_1 \vee \overline{x_7} \vee x_{19}) \dots$

3CNF

---

3SAT $\leq_p$ SAT

---

**SAT $\leq_p$ 3SAT**

F CNF $\Longrightarrow$ F' 3CNF

F is satisifiable if and only if F' is satistiable.

$\overline{x_1} \Longrightarrow (\overline{x_1} \vee y \vee z) \wedge (\overline{x_1} \vee \overline{y} \vee z) \wedge (\overline{x_1} \vee y \vee \overline{z})$
$\wedge (\overline{x_1} \vee \overline{y} \vee \overline{z})$

clause of F

$y = 1$ $z = 0$

$(\overline{x_1} \vee \overline{y} \vee z) = \overline{x_1}$

Long clauses

$x \vee y \vee z \vee w$ $(x \vee y \vee \alpha) \wedge (z \vee w \vee \overline{\alpha})$

$x \vee y \vee z \vee w \vee u \vee v$

---

Conclusion There is poly time reduction from SAT to 3SAT.

SAT $\overset{P}{\Longleftrightarrow}$ 3SAT.

---

Certificate is a short proof that a given instance of a decision problem is a YES instance.

short: polynomial size in the size of the instance

proof: string for a program that verifies it.

---

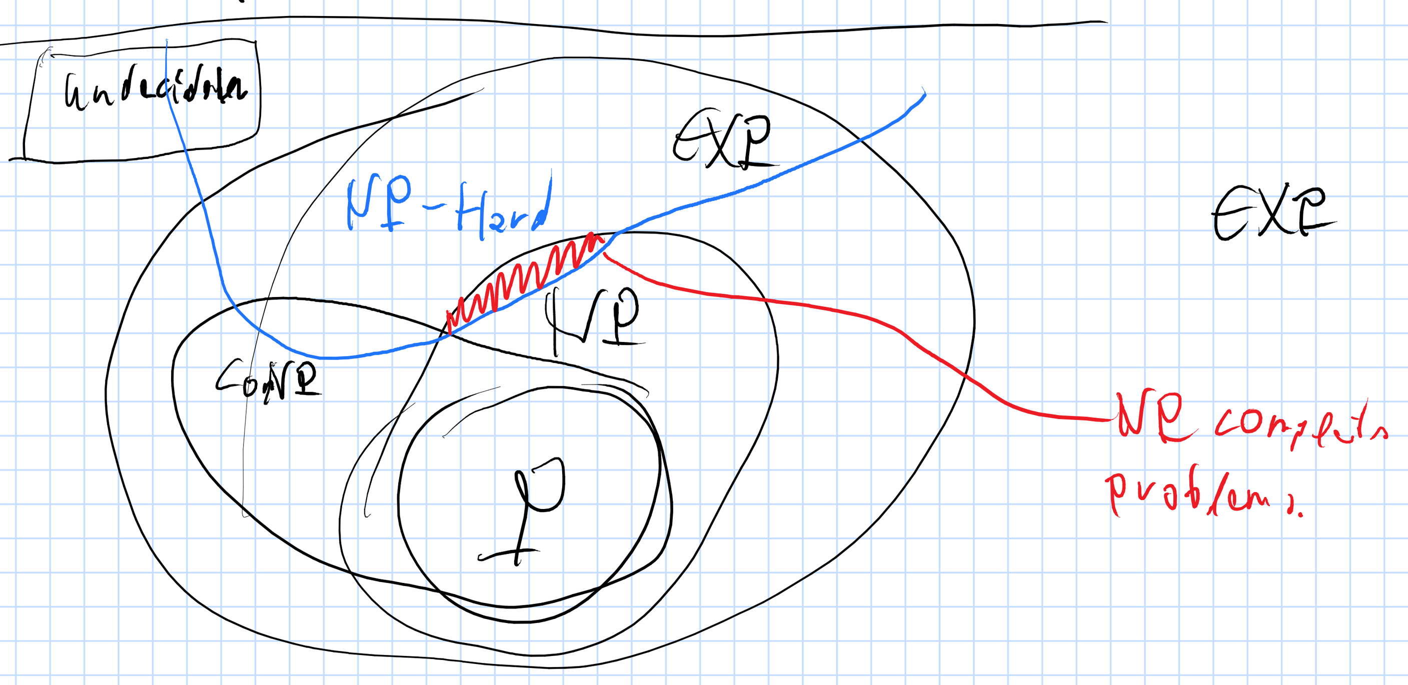
certifier/verifier for a decision problem X is a poly time alg($I_X$, proof):

- $I_X$ instance of the problem
- <proof>: |<proof>| bounded by a polynomial $p(|I_X|)$

The alg runs in polnomial time, s.t.

- $I_X$ is a no in NO instance, then certifier rejects,
- $I_X$ is a YES instance, then $\exists$<proof> s.t. certifier accepts.

---




EXP $2^{O(p(n))}$

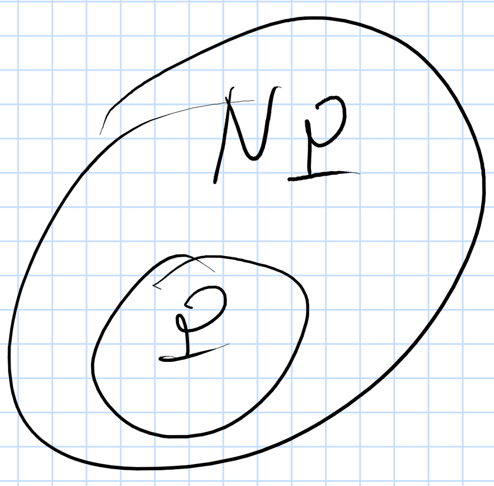
$2^n$ $2^{n^2}$

P = polynomial time

NP = Nondeterministic Polynomial.

$= \{X$ decision problem $|$ X has an efficient certifier (only for YES instances)$\}$

---




---

Composite Give number x return two integers s.t. $x = \alpha \cdot \beta$. $\alpha, \beta > 1$

---

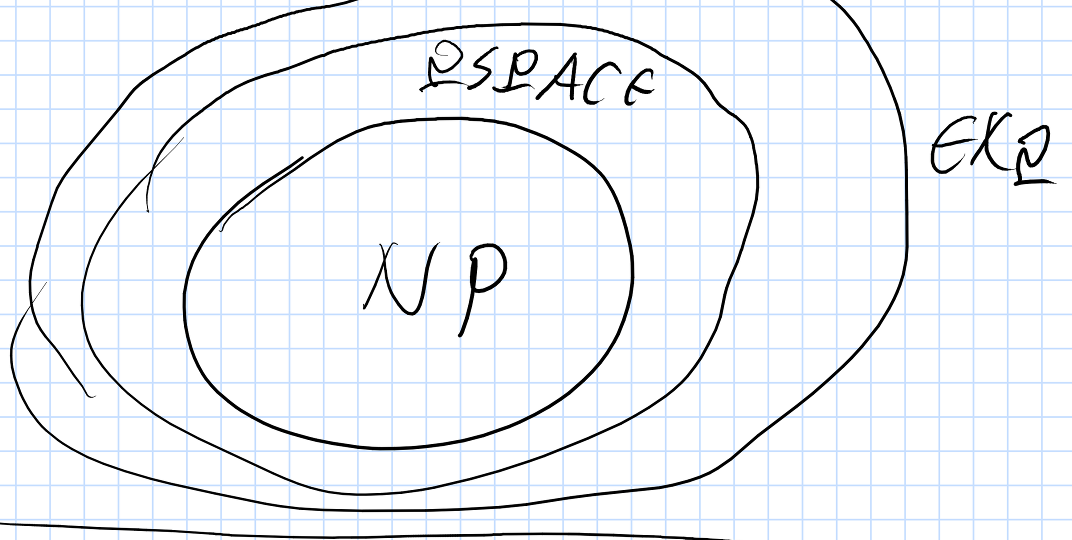
NPC = NP Complete

A decision problem is NPC if:

- it is in NP
- if we can solve it in polynomial time then all problems in NP can be solved in polynomial time P = NP.

---

PSPACE all problems that can be solved using polynomial space




---

Post Correspondence problem

S: set of strings $\subseteq \Sigma^*$

T: set of strings.

$S = \{\alpha_1, \alpha_2, \dots, \alpha_t\}$ $T = \{\beta_1, \beta_2, \dots, \beta_t\}$

$\exists\, i_1, i_2, \dots, i_k$

$$\alpha_{i_1} \alpha_{i_2} \cdots \alpha_{i_k} \overset{?}{=} \beta_{i_1} \beta_{i_2} \cdots \beta_{i_k}$$

Undecidable