Problems in P

→ $\{(G, s, t) \mid G$ is a graph, $s, t \in V(G)$, $\exists$ a path from s to t in $G\}$

→ Given n linear equations in n unknowns, determine if there exists a soln.

→ Given 2 positive integers, determine if there are coprime.

a, b are coprime if $\gcd(a, b) = 1$

NP

A language $L \in \Sigma^*$ is in NP if there exists a polynomial $p : \mathbb{N} \to \mathbb{N}$ and a polynomial time DTM M s.t. $\forall x \in \Sigma^*$,

$$x \in L \iff \exists u \in \Sigma^{p(|x|)} \text{ s.t. } M(x,u) \text{ accepts.}$$

u: witness / certificate for x

Examples

→ Linear Programming [EP, Karmarkar]

Given a list of m linear inequalities over n variables

(coefficients: rationals) $a_1 u_1 + a_2 u_2 + \cdots + a_n u_n \leq b$

is there an assignment of rational nos to $u_1, u_2, \ldots, u_n$ satisfying the inequalities?

certificate for a "yes" instance is an assignment satisfying the inequalities

→ Is a given integer n composite? [CP, AKS]

certificate for n being composite consists of a non-trivial (other than 1/n) factor of n.

→ Graph Isomorphism

Given 2 graphs $G_1 = (V_1, E_1)$, $G_2 = (V_2, E_2)$,

is G_1 isomorphic to G_2

↓

$|V_1| = |V_2|$ & $\exists$ a 1-1 map $f : V_1 \to V_2$ s.t.

$\{u, v\} \in E_1$ iff $\{f(u), f(v)\} \in E_2$.

certificate : 1-1 map between V_1 & V_2

→ Independent Set Problem

Given graph G & an integer k, determine if $\exists$ an independent set in G of size k.

independent set: subset $S \subseteq V(G)$ s.t. no 2 vertices in S are connected by an edge.

certificate: an independent set in G of size k

Alternate definition of NP

NTIME $(T(n))$

A language $L \in$ NTIME$(T(n))$ if $\exists$ a $O(T(n))$-time non-deterministic Turing machine (NDTM) M s.t. $\forall x \in \Sigma^*$, $x \in L$ iff M accepts x

An NDTM M runs in time $T(n)$ if for every i/p x, every branch is the computation tree of M is of length $\leq T(|x|)$ i.e., M halts within $T(|x|)$ steps irrespective of the non-deterministic choices it makes.

$$NP = \bigcup_{c \in \mathbb{N}} NTIME(n^c)$$

① $NP \subseteq \bigcup_{c \in \mathbb{N}} NTIME(n^c)$

$L \in NP$. $\exists$ DTM M and p s.t. $\forall x$, $x \in L \Leftrightarrow \exists u$ s.t. $M(x,y)=1$ & $|u| = p(|x|)$

Let N be a NDTM that on i/p x guesses a string of length $p(|x|)$ & accepts if $M(x,u)=1$.

N is poly-time since M is poly-time & p is a polynomial.

$L(N) = L.$

$\therefore \quad NP \subseteq \bigcup_{c \in \mathbb{N}} NTIME(n^c)$

(2) $\bigcup_{c \in \mathbb{N}} NTIME(n^c) \subseteq NP$

$L \in \bigcup_{c \in \mathbb{N}} NTIME(n^c)$

$\exists$ poly-time NDTM N that accepts L.

The certificate for a "yes" instance x of L, would be the sequence of choices that N makes on i/p x.

Since N is poly-time, certificate will have size polynomial in input size ($|x|$).

$$EXP = \bigcup_{c \geq 1} DTIME\left(2^{n^c}\right) \qquad NEXP = \bigcup_{c \geq 1} NTIME\left(2^{n^c}\right)$$

captures infeasible computation (inefficient)

$$P \subseteq NP \subseteq EXP \subseteq NEXP$$

Is $P = NP$?

Is $EXP = NEXP$?

Polynomial-Time Reducibility

$(A \subseteq \Sigma^*, B \subseteq \Gamma^*)$

A is polynomial-time (or Karp) reducible to B, denoted $A \leq_p B$, if $\exists$ a polynomial time computable function $f : \Sigma^* \to \Gamma^*$ s.t. $\forall x \in \Sigma^*$

$$x \in A \quad \text{iff} \quad f(x) \in B$$

$f(x)$ is computable in time polynomial in $|x|$.

Defining Hardness for NP

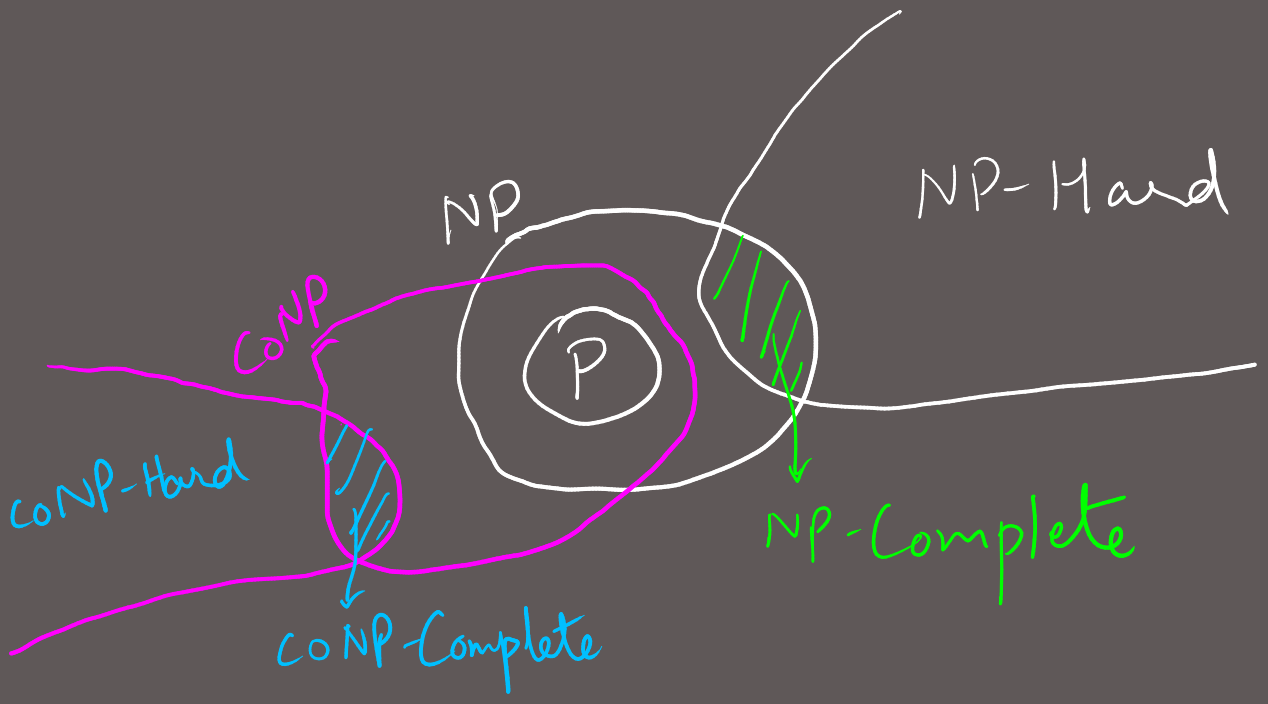
What are the hardest problems in NP?

A language B is NP-hard if for every $A \in NP$, $A \leq_p B$. [e.g.: Independent Set, HP]

Completeness for NP

Completeness - motivated by the question $P \stackrel{?}{=} NP$

A language B is NP-Complete if B is NP-hard & $B \in NP$.



Thm:

1. $\leq_p$ is transitive (exercise: show this!)
2. A is NP-hard $\Rightarrow$ $A \in P \Rightarrow P = NP$
3. A is NP-complete $\Rightarrow$ $A \in P$ iff $P = NP$.