P, NP, and all that

Monday, November 4, 2019 11:24 AM

Julian
– PG

We come to a central definition in Complexity theory — P

$$P = \bigcup_k \mathrm{TIME}(n^k)$$

Class of languages that can be decided in polynomial time.

i.e. $\exists k \in \mathbb{N}$ s.t. $L \in \mathrm{TIME}(n^k)$.

$n = |x|$ length of input.

k is fixed, independent of n.

E.g. $\{\langle G \rangle : G$ is a connected graph$\}$

$\{\langle s_1, s_2, k \rangle :$ the edit distance between s_1 & s_2 is at most $k\}$

A_1 & A_2 is at most k }

$$NP = \bigcup_k NTIME(n^k)$$

$L \in NP$: $\exists k$, $\exists$ NTM M s.t. $\forall x$, $|x| = n$

if $x \in L$ M has an accepting path of length $\leq n^k$.

$\boxed{\text{Nondeterministic polynomial time}}$.

$\exists$ "short" proof of membership

$x \in L$ has a certificate of length $\leq n^k$.

e.g. $\{ \langle G \rangle :$ G is Hamiltonian $\}$

$\{ \langle G, k \rangle :$ G has a clique of size $k \}$

$\{ \langle a_1, a_2, \ldots a_k \rangle :$ $\exists$ partition A_1, A_2

... integers s.t.

$\{ \langle a_1, a_2, \dots a_k \rangle$

integers

of these integers s.t.

$$\sum_{i \in A_1} a_i = \sum_{i \in A_2} a_i \quad \}$$

Clearly, $P \subseteq NP$.

$$\text{Co-NP} = \bigcup_{k} \{ L : \exists \text{TM that accepts } x \in \bar{L} \text{ in } NTIME(n^k) \}$$

$$L \in NP \iff \bar{L} \in \text{Co-NP}$$

$x \in L$ has short proof $=$ $x \notin \bar{L}$ has short proof.

---

e.g. $\{ \langle G \rangle$: G is not Hamiltonian$\}$

$\{ \langle G, k \rangle$: G does not have a clique of size $k \}$.

Thm. $P \subseteq NP \cap \text{Co-}NP$.

Open problem:

$P = NP$?

E.g. – CLIQUE

– INDEPENDENT SET

$= \{ \langle G, k \rangle :$ G has an ind. set of size $k \}$

– HAM

– VERTEX COVER

$= \{ \langle G, k \rangle :$ G has a subset S of vertices s.t. every edge has at least one end point in S $\}$

– ILP

$= \{ \langle A, b \rangle :$ $Ax \leq b$ has an integer solution x $\}$

$= \{ \langle A, b \rangle :$ $Ax = b$ has integer solution $x \}$

- SAT:

  $= \{ \langle F \rangle :$ Boolean formula s.t. $\exists x \in \{T/F\}^n$ and $F(x) = T \}$