COL 351 Lecture 34 2023/04/10

Topic : Polynomial-time Verification,

$\mathbb{P}$ and $\mathbb{NP}$

Recap:

On input $G = (V, E)$, k:

VC : Does G have a vertex cover of size $\leq k$?

IND : Does G have an ind. set of size $\geq k$?

CLIQUE: Does G have a clique of size $\geq k$?

VC-search: On input G and k, if G has a vertex cover of size $\leq k$, find one such vertex cover. Otherwise return "NO".

Claim : VC-opt $\leq_{Cook}$ VC-search $\leq_{Cook}$ VC

$T(n) = cn^2 + T(n-1)$

$T(n) = O(n^3)$

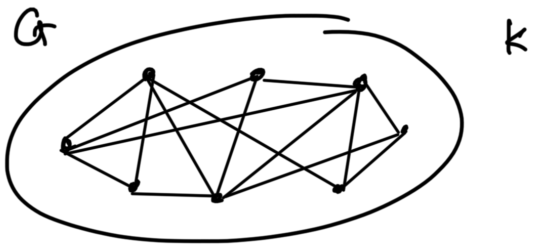
Definition: We say that a decision problem Q is in the complexity class $\mathbb{P}$ if Q has a polynomial-time algorithm.

Examples

- Given (bipartite) G, does G have a perfect matching?
- Given G, does G have a VC of size $\leq 10^{100}$?

Open problems: $VC \overset{?}{\in} \mathbb{P}$ $\quad$ $IND \overset{?}{\in} \mathbb{P}$ $\quad$ $CLIQUE \overset{?}{\in} \mathbb{P}$

But we know either all of VC, IND, CLIQUE are in $\mathbb{P}$, or none of them is in $\mathbb{P}$.



(Prover) Pramsu

(Verifier) Vedant

Does G have a VC of size $\leq k$?

Yes, G has a VC of size $\leq k$

Prove your claim.

Gives a subset C of vertices.

Checks whether C is a VC of G and $|C| \leq k$.
If yes, accepts
no, rejects.

Another possibility:

Prover: Gives a list

(e_1, v_1) (e_2, v_2). (e_m, v_m)

Verifier: Checks whether

- $\{e_1, \ldots, e_m\}$ is the edge set of v
- $\forall i$ v_i is an endpoint of e_i
- $\{v_1, \ldots, v_m\}$ is a set of $\leq k$ (distinct) vertices.

Definition: Let Q be a decision problem. A polynomial-time verifier for Q is a polynomial-time algorithm V that takes two inputs:

- x — an instance of Q of size poly$(|x|)$
- y — an additional bit-string a.k.a. "proof"

and returns YES or NO with the following guarantee.

$\forall x$:

- If x is a YES instance of Q, then $\exists y$ of size poly$(|x|)$ such that $V(x, y)$ returns YES.
- If x is a NO instance of Q, then $\forall y$ of size poly$(|x|)$ $V(x, y)$ returns NO.

Definition: A decision problem Q is said to be in the complexity class $\mathbb{NP}$ if Q has a polynomial-time verifier.

e.g. VC, IND, CLIQUE.

Claim: $\mathbb{P} \subseteq \mathbb{NP}$.

Proof: A poly-time decision algorithm is also a poly-time verifier (that ignores the proof.)

Million Dollar Open problem: $\mathbb{P} \stackrel{?}{=} \mathbb{NP}$.