Efficient verification (book: certification)

Dec 2

Q: Is $w \in Y$?

Eg: Y is IS

$w = G; k$

↳ A certificate/witness is a string that supports the claim that $w \in Y$

Def: B is an efficient verifier for Y if

(1) B takes as input w, t & output $B(w,t) \in \{0,1\}$

(w: input, t: witness)

(2) B runs in time poly $(|w|)$

(3) $w \in Y \iff \exists$ a string/witness t s.t (i) $|t| \leq$ poly $(|w|)$ AND (ii) $B(w,t) = 1$

Eg. $Y = IS$ i/p: $w = G; k$

Witness: $S \subseteq V$ of size $|S| = k$

Q: $\exists$ an efficient verifier

Claim: $\exists$ an efficient verifier for IS with witness

Verifier $B(w, t)$ (w: $G; k$, t: S)

Intuition: If G has an IS of size $\geq k$ $\Rightarrow \exists$ an IS S^* of size $= k$

Intuition: $B(G; k, S) = 1$ if S is an IS $= k$

0. If $|S| \neq k$ return 0
1. If $\forall\, u \neq v \in S$ it is the case that $(u,v) \notin E$ return 1 else return 0

$O(k^2)$, poly(n)

Claim 2: G has an IS of size $\geq k \iff \exists$ a witness $S \subseteq V$ s.t $B(G; k, S) = 1$

DEF: $Y \in NP$ if $\exists$ an efficient verifier B for Y

(Unpack the def a bit):

$Y \in NP$ iff for all inputs w:

(i) $w \in Y \Rightarrow \exists$ a witness t s.t. $|t| \le \text{poly}(|w|)$, $B(w,t) = 1$

(ii) $w \notin Y \Rightarrow \forall$ witness t s.t. $|t| \le \text{poly}(|w|)$, $B(w,t) = 0$

$IS \in NP$ Ex: $VC \in NP$

Big Q: $P \stackrel{?}{=} NP$

Claim 3: $P \subseteq NP$

Pf: $Y \in P$ (. . . goal: $Y \in NP$)

$\Rightarrow \exists$ an algo A s.t. $A(w) = 1 \iff w \in Y$

Show: Efficient verifier
$B(w,t)$
return $A(w)$
} poly time

$\Rightarrow \forall$ witnesses t, $B(w,t) = A(w)$ ✓

$\Rightarrow Y \in NP$ ∎

Def: X is NP-complete if

① $X \in NP$

② $\forall Y \in NP$, $Y \le_p X$

Claim 4: Let X be NP complete.

If $X \in P \Rightarrow P = NP$

THM: VC, IS is NP-complete

Get back:

THM: (1) $IS \leq_p VC$ (2) $VC \leq_p IS$

Crucial Lemma: Let $G = (V, E)$

S is an IS $\iff$ $V \setminus S$ is a VC

Prove (1) $IS \leq_p VC$

Pf: given G, k for IS

$(G, k) \xrightarrow{G, n-k}$ [Algo for VC] $\xrightarrow{T/F}$ use same answer for IS

$\Rightarrow$ G has IS of size $\geq k$ $\iff$ G has a VC of size $\leq n-k$

$\rightarrow$ Pf of $VC \leq_p IS$ ↗

Pf (idea) of crucial lemma:

S is an IS $\Rightarrow V \setminus S$ is a VC.

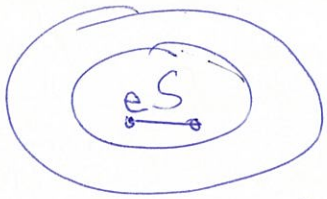
Pf by contradiction

Let S ~~is~~ be an IS

& assume $V \setminus S$ is not a VC

$\Rightarrow$ e ~~is~~ completely in S

$\Rightarrow$ S is not an IS ☑



Pf of $\Leftarrow$ is similar (Ex.)

Satisfiability / SAT problem

General: SAT formula

↳ AND of clauses

↳ OR of literals

↳ $x_i, \bar{x}_i$

OR ↓ AND ↓

$$(x_1 \vee \bar{x}_2) \wedge (\bar{x}_1 \vee \bar{x}_3) \wedge (x_2 \vee \bar{x}_3)$$

generally: $C_1 \wedge C_2 \wedge \cdots \wedge C_m$ $\quad C_i$: clause

$\equiv C_1, C_2, \cdots, C_m$

Clause: OR of literals : $t_1 \vee t_2 \vee \cdots \vee t_e$

each $t_i \in \{ x_1, \cdots, x_n, \bar{x}_1, \cdots, \bar{x}_n \}$