NP-Completeness

Yu Ren

Note Title 9/30/2015

Clique: Does G have a clique of size $\geq K$?

Ind. Set: ———— an Ind. Set ————?

Vertex Cover: ———— a V.C. of size $\leq K$?

HAM: ———— a Hamiltonian cycle?

ILP: A, b : $\exists x \in \mathbb{Z}^n$ s.t. $Ax \leq b$?

SAT: $\exists x$: $F(x) = 1$?

⋮

all in NP

$\boxed{P = NP?}$

short proofs of membership ("certificates")

How hard are these problems?

Are some harder than others?

Which ones are the <u>hardest</u>?

<u>REDUCTION</u> from decision problem A

to decision problem B

is an algorithm to solve A using

a procedure to solve B.

$A \hookrightarrow B$ is a polytime reduction if the algorithm makes only a polynomial number of calls to B, each on inputs of size poly(n), and uses polynomial additional time. $n = |x|$

$$x \in L_A \longrightarrow \begin{array}{l} y_1 \in L_B \\ y_2 \in L_B \\ \vdots \\ y_m \in L_B \end{array}$$

$|y_i| \le \text{poly}(n)$

$m \le \text{poly}(n)$.

This is a COOK reduction.

A Karp reduction is a 1-1 map between strings in the languages:

$A \hookrightarrow B$: $x \in L_A \iff y \in L_B$

y is constructed from x in polytime.

E.g.

Clique $\rightarrow$ I.S.

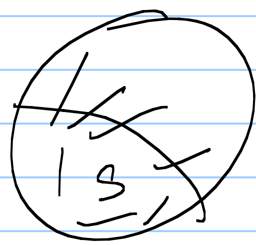
$\exists$ k-clique in $G \iff \exists$ k-Ind. set in $\overline{G}$

$\overline{G} = (V, \overline{E})$

Clique $\to$ Ind. set

Ind. set $\to$ clique.

V.C. $\to$ Ind. Set



$V \setminus S$ is an ind. set.

G has a V.C. of size $\leq K$

$\iff$ G has an Ind. set of size $\geq n-K$.

SAT $\to$ I.L.P.

CNFSAT: $F = (x_1 \vee x_2 \vee \bar{x}_3 \ldots) \wedge (x_2 \vee x_3 \vee \bar{x}_4) \wedge \ldots$

ANDs of ORs.

$$x_1 + x_2 + 1 - x_3 + \ldots \geq 1$$

$$x_2 + x_3 + 1 - x_4 \geq 1$$

$$\left.\begin{array}{l} 0 \leq x \leq 1 \\ x \in \mathbb{Z}^n \end{array}\right\} x_i \in \{0,1\}$$

A language L is NP-complete if

(1) $L \in NP$

(2) $\forall A \in NP$ $\exists$ polytime reduction $A \to L$.

L is the "hardest" language in NP.

If $L \in P \implies NP \subseteq P \implies P = NP$.

$\exists$ NP-Complete language? YES! Lots of them.

Thm. SAT is NP-Complete [Cook/Levin]

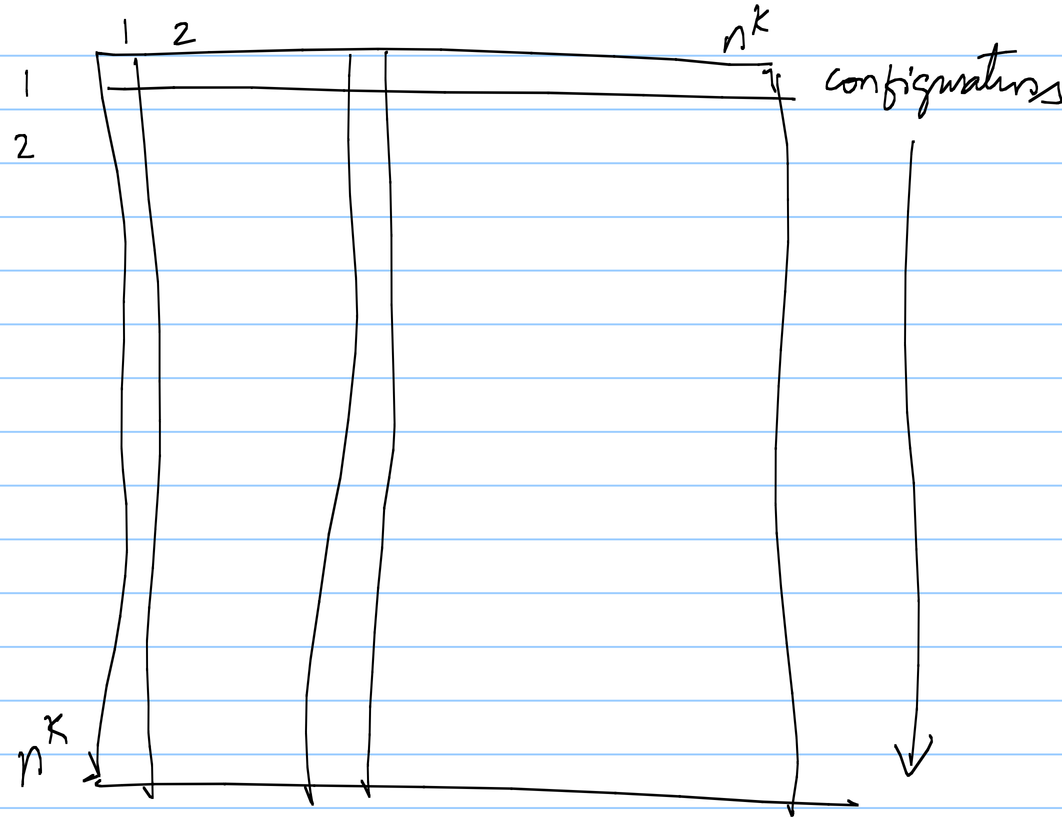
Pf. Take a language L in NP. We need to decide L given a procedure to decide SAT.

$L \in NP$. So $\exists$ TM M that accepts any $x \in L$ in $\leq n^k$ steps for some fixed k.

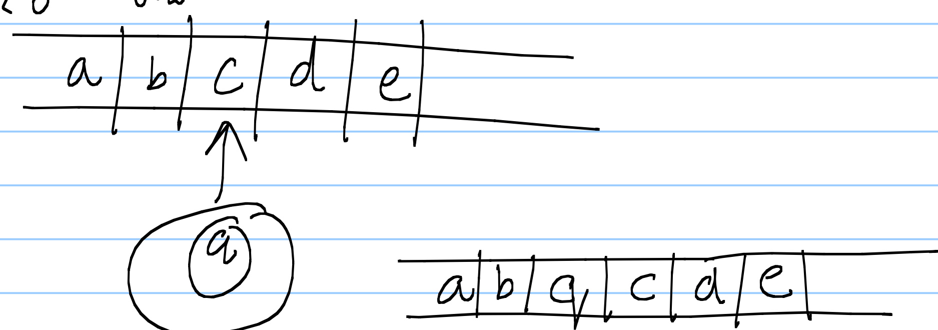
$\exists$ a sequence of $\leq n^k$ configurations from a starting configuration to q_{accept} if $x \in L$. How can we check this using SAT?

Can we write the existence of such an accepting path as a poly-sized SAT formula?

YES. Variables $X_{i,j,s}$



$$X_{i,j,s} = \begin{cases} 1 & \text{if } i^{th} \text{ step has } j^{th} \text{ entry} = s. \\ 0 & \text{o.w.} \end{cases}$$



$s \in \Gamma \cup Q$

$\forall i\, j \quad X_{i,j,s} = 1$ for exactly one value of s.

$\left(\bigvee_{s} X_{i,j,s}\right)$ ensures atleast one s.

How to get exactly one?

For 2 variables $(X_1 \vee X_2) \wedge (\bar{X}_1 \vee \bar{X}_2)$

atleast one is True

atleast one is false

for K variables

$$(x_1 \vee x_2 \dots \vee x_k) \wedge [(\bar{x}_1 \vee \bar{x}_2) \wedge (\bar{x}_1 \vee \bar{x}_3) \dots\dots]$$

$$(x_1 \vee x_2 \dots \vee x_k) \wedge \Big(\bigwedge_{i \neq j} (\bar{x}_i \vee \bar{x}_j)\Big)$$

In our case

$$\Big(\bigvee_{s} x_{i,j,s}\Big) \wedge \Big(\bigwedge_{s,t} \big(\overline{x_{i,j,s}} \vee \overline{x_{i,j,t}}\big)\Big)$$

2) Need to start in initial configuration

$c_1 c_2 c_3 \dots$

$$(x_{1,1,c_1} \wedge x_{1,2,c_2} \wedge x_{1,3,c_3} \dots\dots)$$

3) Need to reach q_{accept} somewhere

$$\Big(\bigvee_{i,j} x_{i,j,q_{accept}}\Big)$$

4) Every transition must be valid.

a	q	b
q	a	b

a	q	b
q	a	c

a	q	b
a	c	q_1

......

$$\bigwedge_{i,j} \Big((x_{i,j,a} \wedge x_{i,j+1,q} \wedge x_{i,j+2,b} \Rightarrow x_{i,j+1,q_1} \wedge x_{i+1,j+1,a} \wedge x_{i+1,j+2,b})$$

$\vee\ (\dots\dots)$ ..all allowed transitions.

Thus $x \in L$ iff

$F = (1) \wedge (2) \wedge (3) \wedge (4)$

has a solution s.t. F is SATisfiable.

Size of formula $\leq n^k \cdot n^k \cdot (|Q| + |\Gamma|) \cdot C$

$= O(n^{2k})$.

$L \leq_p SAT$.

By our early observations,

if $SAT \to L$ and $L \in NP$,

then L is also NP-complete.

<u>Thm</u> Clique is NP-complete.

<u>Pf.</u> $SAT \to$ Clique.