CPSC 421/501

Last time: $P := \bigcup_{k \in \mathbb{N}} TIME(n^k)$, = "poly time languages" ("efficient")

$NP := \bigcup_{k \in \mathbb{N}} NTIME(n^k)$. ← { non-deterministic Turing machines, "poly time" }

SAT, 3COLOR, SUBSET-SUM $\in$ NP

Today: Start Cook-Levin Theorem, NP-completeness

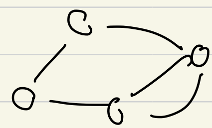
Have 2 weeks of classes

2 weeks of presentations +

some { new material, review }

For us, NP = poly time recognizable languages by a non-deterministic TM

e.g.

3-COLOUR: given graph 

want to know is there a "valid 3-colouring",

i.e. graph = $G = (V, E)$,

"valid" 3-colouring $V \to \{\text{red}, \text{blue}, \text{green}\}$

if each edge has different colours at its endpoints

3-COLOUR $\in$ NP:

given ⟨graph⟩ ← (V, E)

↑

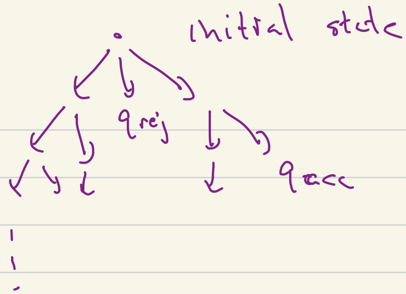
$V = [n] = \{1, 2, \ldots, n\}$

"non-deterministically" { "guess" / "write down" } $V \xrightarrow{c} \{\text{red}, \text{green}, \text{blue}\}$

then check whether or not c is valid.

tree →

children between $0, 1, \ldots, |Q| \cdot |\Gamma| \cdot 2$



non-det "time" = "# of steps" allow $3n^2$ on input length n

input is "accepted" by non-det TM iff one computation end in q_{acc}

$$\delta : Q \times \Gamma \longrightarrow \text{Power}\left(Q \times \Gamma \times \{L, R\}\right)$$

$\#\quad |Q| \cdot |\Gamma| \cdot 2$

So # comp paths

$$\leq \left(|Q| \cdot |\Gamma| \cdot 2\right)^{3n^2}$$

(# comp "children"; $3n^2$ ← time = depth of tree)

time to "simulate" deterministically

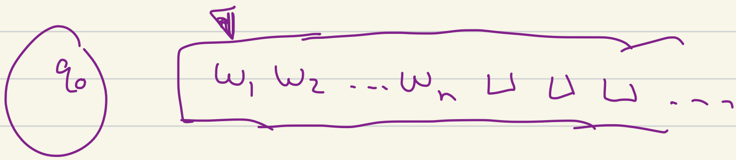
$$\leq c^{3n^2}$$

"exponential time"

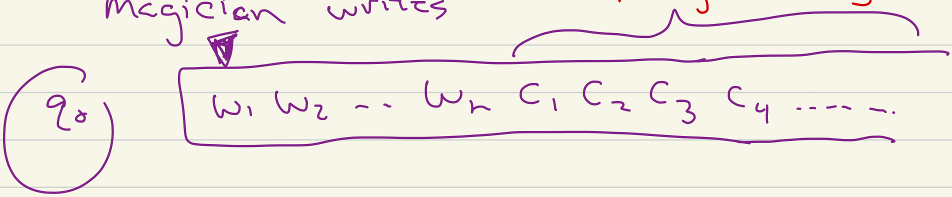
Another idea in [Sip]

NP = { languages that can be {proven / verified} in poly time }

(1) given input $w = (w_1, \ldots, w_n)$ input size n



(2) magician writes magic string



(3) now you "verify" that

$(w_1, \ldots, w_n)$ in language

- poly time in n
- $w_1 \ldots w_n c_1 c_2 \ldots$ gives you q_{acc}

Example $w = \langle G \rangle = \langle \text{Graph} \rangle = w_1 \ldots w_n$

w_1	...	w_n	c_1	...	c_m

magician! describes a map

$$V \to \{\text{red}, \text{green}, \text{blue}\}$$

{check / verify} if this colouring is valid

Formal definition ([Sip] Def 7.18)

A {"prover" / verifier} for $L \subset \Sigma^*$ is a deterministic TM, Ver, s.t.

"magician"

$L = \{ w \in \Sigma^* \mid$ there exists $c_1, c_2, \ldots$ s.t. $\langle w, c \rangle$ is accepted by Ver $\}$

Ver is in "poly-time" if it runs in time $O(n^k)$ for some fixed $k \in \mathbb{N}$, $n = |w|$

Claim: {Verifiable / Provable} in poly time

$\iff$ being in NP

$\iff$ recognized by a non-det poly time algorithm (TM)

---

n size of input $w = (w_1, \ldots, w_n)$

(unfortunately

Boolean formula: $f(x_1, \ldots, x_n)$

Graph: $G(V, E)$, $V = \{1, \ldots, n\}$)

not same

Next topic:

SAT $\in$ NP

↑

Boolean formulas that are satisfiable

Theorem: If SAT $\in$ P, then NP = P.

either {true / false}

I.e. to see whether or not P = NP, it suffices to see whether or not SAT $\in$ P.

—

Cook-Levin theorem.

Idea! If $L \in NP$, i.e. you have a non-det TM, M, for L, then

input w to M —procedure→ "SAT problem" "Boolean formula" based on M, w s.t. formula $\in$ SAT iff M accepts w

---

5-min break, 10:20 - 10:25

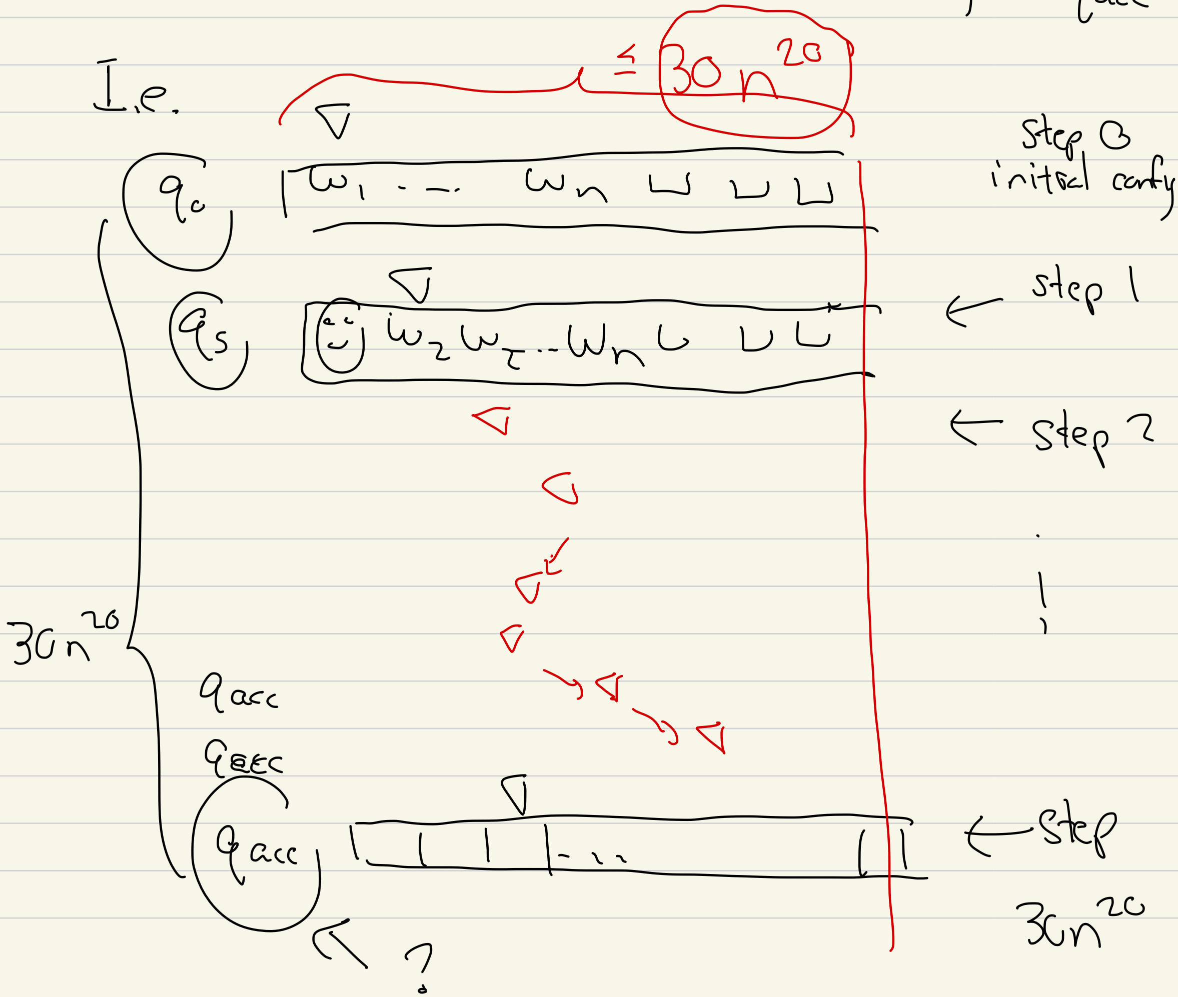
Idea: have non-det M, input w,

say that M runs in time $30n^{20}$.

Given w, w is accepted by M iff

there is a computation path leading to q_{acc}.

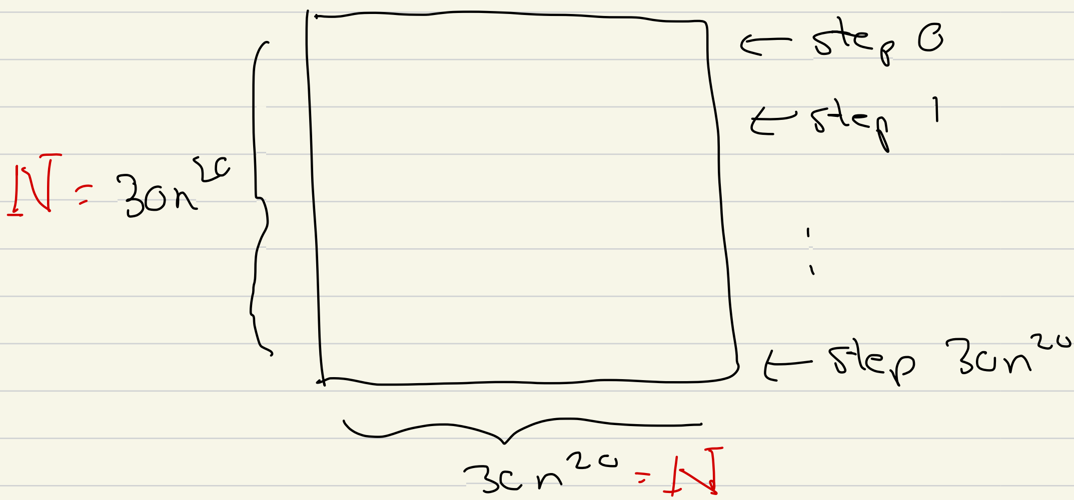
I.e.



$$X_{ijk} = \begin{cases} T & \text{if at time } i\text{, cell } j \text{ has symbol } k \\ F & \text{otherwise} \end{cases}$$

$$Y_{ij} = \begin{cases} T & \text{if the tape head at time } i \text{ is in cell } j \\ F & \end{cases}$$

$$Z_{is} = \begin{cases} T & \text{if at time } i\text{, we are in state } s \end{cases}$$



note: $i = 0, 1, \ldots, N$; $j = 1, 2, \ldots, N+1$,

$k = 1, \ldots, |\Gamma|$, $s = 1, \ldots, |Q|$

X_{ijk}, Y_{ij}, Z_{is} T/F

X_{ijk} ↑ cell contents: time i, cell j, $k \leftrightarrow \Gamma$

Y_{ij} ↑ tape location: time i, cell j

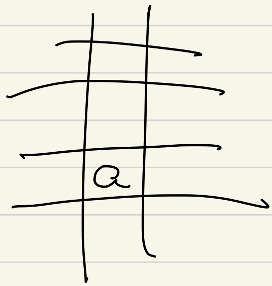
Z_{is} ↑ state: time i, state s

$N = 30n^{20}$ (depends on input)

e.g.

cell 30

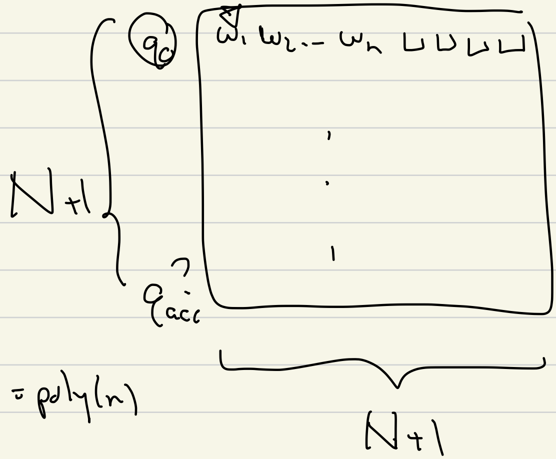
time 23



$X_{23,30,k}$ = T if a symbol number k

F otherwise

Input w,



$N = poly(n)$

The variables

x_{ijk}, y_{ij}, z_{is}

represent a valid computation in M

iff

x_{0jk}, y_{0j}, z_{0s} is the initial config

AND

x_{1jk}, y_{1j}, z_{1s} is a valid 1st config

AND

⋮

AND

x_{Njk}, y_{Nj}, z_{Ns} is a valid config

AND

$z_{N,s} = T$ iff q_{acc} is state s

w_1 is at cell 1 at time 0 → w_1 is symbol

$\Gamma = \{1, \dots, |\Gamma|\}$

$$x_{01k} = \begin{cases} T & \text{if } k = w_1 \\ F & \text{if } k \neq w_1 \end{cases}$$

Want for all i, j: $x_{ij1}, x_{ij2}, \dots, x_{ij|\Gamma|}$ $\begin{cases} \text{one is } T \\ \text{the rest } F \end{cases}$

End of class