CPSC 421/501 Nov 10, 2023

Today:

1. Formally define NP
   (non-deterministic polynomial time decidable)

2. 3COLOR, SAT, 3SAT, ... $\in NP$

3. Start:

$$P = NP \iff SAT \in P$$

$$\iff 3SAT \in P$$

$$\iff 3COLOR \in P$$

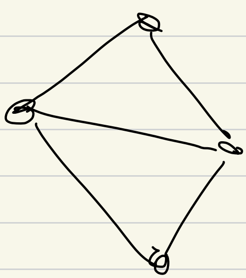
$$\iff \ldots$$

"NP-complete"

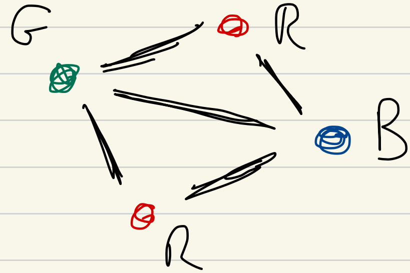
3COLOR =

$$\{\langle G\rangle \mid G \text{ has a 3-colouring}\}$$

is decidable by a non-det. T.m as follows:



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



$G = (V, E)$

Non-determinism: you "non-deterministically choose a map

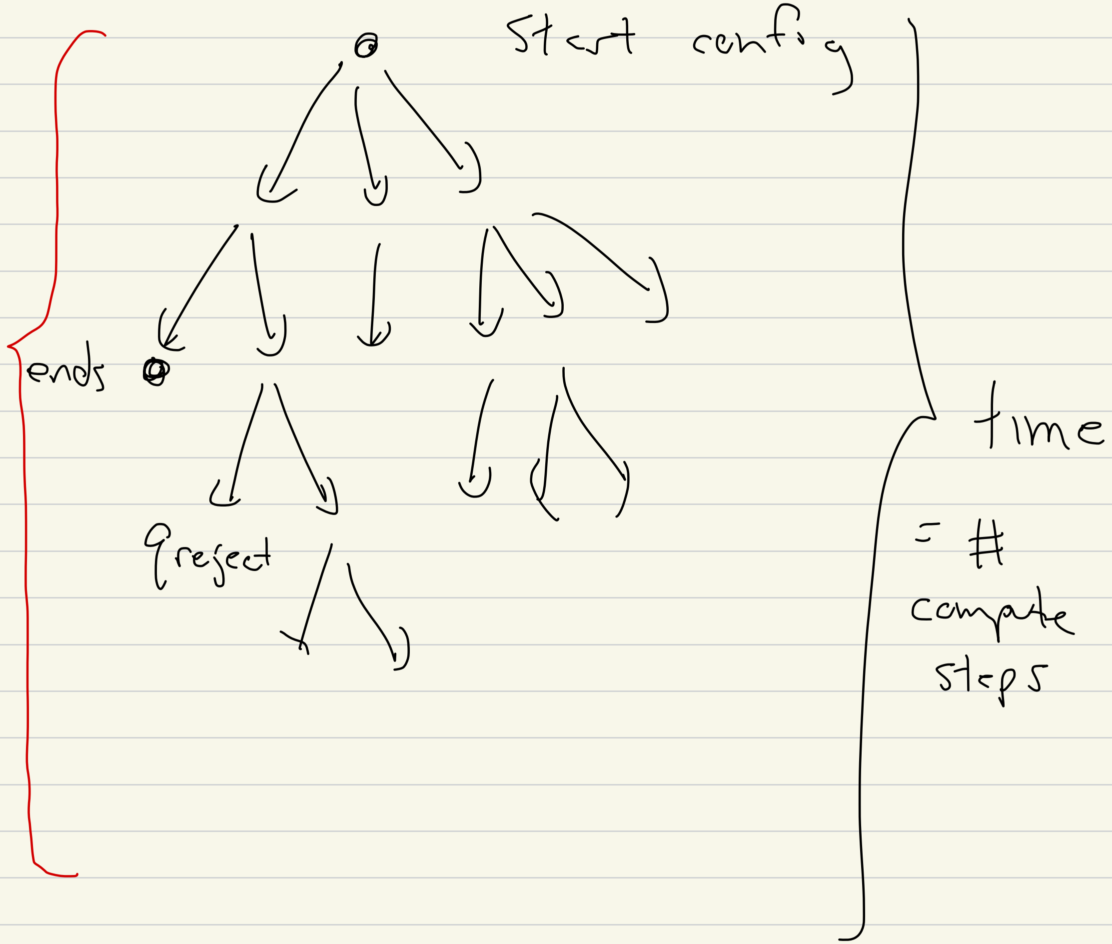
$V \to \{R, G, B\}$,

Then verify that this map gives a (valid) 3-colouring.

$\#$ 3-colourings $= 3^{|V|}$

but verifying that the colouring is valid 3-colouring takes poly time in $|\langle G \rangle|$, i.e. length of $\langle G \rangle$.

non-deterministic computation



We say non-det TM <u>decides</u>

a language, L, in time $f(n)$

all computation paths end in time $\leq f(n)$

on all inputs of length n.

$=$

$\text{NTIME}(g(n)) = \{ L$ decidable

by a non-deterministic T.M.

in time $\leq f(n)$, where

$f(n) = O(g(n)) \}$

$$NP = \bigcup_{k=1,2,\ldots} \text{NTIME}(n^k)$$

$$\left[\; P = \bigcup_{k=1,\ldots} \text{TIME}(n^k) \right.$$

3COLOR $\in$ NP

SAT $\in$ NP !

Boolean formula on $x_1, \ldots x_n$

any formula :

$$\neg \left(\left(x_1 \text{ AND } \neg x_2 \right) \text{ or } x_3 \right) \text{ AND }$$

$$\left(x_2 \text{ OR } \neg x_4 \right) \ldots$$

Problem :

$$\left(\neg (\alpha \wedge \beta) \vee \quad \right) \vee \left(a \text{ or } \sqrt{2} \right)$$

Insist on formulas with

$X_1, \ldots, X_N$ for some $N \in \mathbb{N}$

use symbols

$$\{ X, (,), \wedge, \vee, \neg, 0, \ldots, 9 \}$$

and or

$$\left(X_{37} \text{ AND } (\neg X_3) \right)$$

$$X\,3\,7 \wedge (\neg\; X\,3)$$

$f(x_1, \ldots, x_N)$ is <u>satisfiable</u>

if there are $y_1, \ldots, y_N \in \{T, F\}$

s.t.

$$f(y_1, \ldots, y_N) = T$$

e.g.

$(\neg X_1)$ AND X_1 is not satifiable

$$(\neg X_1) \text{ AND } X_2 = f(x_1, x_2)$$

$$f(F, T) = (\neg F) \text{ AND } T = T$$

$$\left\{ \langle f \rangle \;\middle|\; \begin{array}{l} f \text{ is a satifiable} \\ \text{Boolean formula} \end{array} \right\}$$

$= SAT$

$SAT \in NP$: given $\langle f \rangle$, you "non-determistically guess" T/F of $x_1, \ldots, x_N$ and see if these values make f true.

$\Rightarrow$ 3COLOR, SAT, ... $\in NP$

but we don't if they are in P...

Theorem: If SAT $\in P$,

then $NP = P$. (Cook-Levin Thm)

Proof: Say $L \in NP$, i.e. you

have a non-det Turing machine,

M, that decides L in time

$\leq C n^k$, some const C, k

$(k = 1, 2, \ldots)$

M = non-det Turing machine

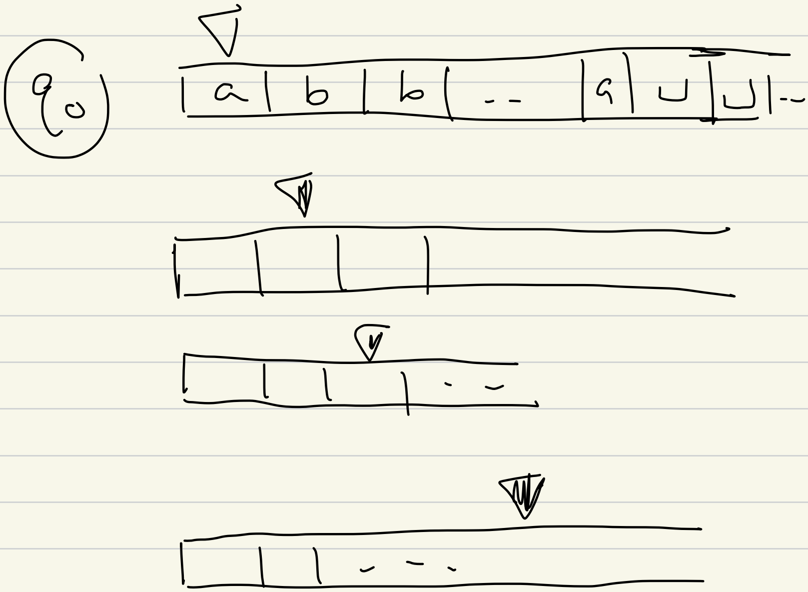
step 1

step 2

step 3

⋮

step Cn^k



$\left(\{s, p\}\ n^k \right.$
$\left. \quad \text{not } Cn^k \right)$

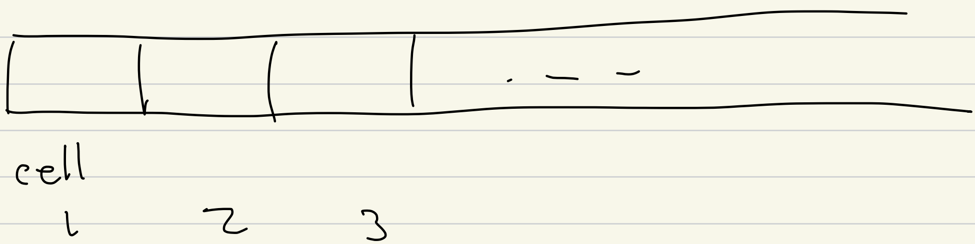
at step Cn^k,

the tape head is in

position $\leq Cn^k$ cells

to the right of 1^{st} cell

Cell$[i,j]$ = the cell at step i, position j



For $i, j \in \{1, \ldots, Cn^k\}$, $\gamma \in \Gamma$ tape symbol

$$X_{ij\gamma} = \begin{cases} \text{True} & \text{if cell}[i,j] \text{ has } \gamma \\ \text{False} & \text{otherwise} \end{cases}$$

$$Y_{ij} = \begin{cases} \text{True} & \text{if } \quad \text{is over position } j \text{ at step } i \\ \text{False} & \text{otherwise} \end{cases}$$

$$z_{i,q} = \begin{cases} T & \text{if at step } i \text{ we are in state } q \\ F & \text{otherwise} \end{cases}$$

$i \in 1, \ldots, Cn^k$, $q \in Q$ set of states

Rem: We build horrifically large Boolean formula to express that on input $\sigma_1 \ldots \sigma_n \in \Sigma^n$ the is at least one computation path that accepts $i = \sigma_1 \ldots \sigma_n$

In cell$[i,j]$ we need to see exactly one symbol in $\Gamma = \{\gamma_1, \dots, \gamma_7\}$

At least one symboll

$$(X_{111} \text{ OR } X_{112} \text{ OR } \dots \text{ OR } X_{117})$$

AND

$$\left.\begin{array}{l} (\neg(X_{111} \text{ AND } X_{112})) \text{ AND} \\ (\neg(X_{111} \text{ AND } X_{113})) \text{ AND} \\ \neg \\ \vdots \end{array}\right\} \#\text{variables} \quad 2\binom{|\Gamma|}{2}$$

constant

m is fixed, c, k fixed

Doing this for not only Cell[1,1]

but all cells:

$$(Cn^k)(Cn^k) \quad 2\binom{|\Gamma|}{2}$$

poss values of i

— —
‥ j

$$= \text{constant} \quad n^{2k}$$