CPSC 421/501 Nov 30, 2021

Schedule:

Today: Jerry: CFG's

Compare [Sip], Ch 2

=

Thursday: Mia & Sophie: QC

(not covered at all in [Sip])

Tuesday (Dec 7):

Zack: TRS (term rewriting systems)

Grigorii: Kolmogorv Complexity

(compare Section 6.4 [Sip])

Today! Jerry starts after break

Dec 2 & 7 talks:

- Start at beginning of class
- Time leftover! "office hours":
  questions on homework + exam practice

Dec 22: Final Exam

Today! Proof of Cook-Levin theorem. [Sip] Ch 7 &

how "to solve P vs NP"

=

There will be a HW 10

[A] ~~Could~~ will be handed in, OR

[B] ~~Could~~ will not be handed in,
if you are reasonably
certain that do it
sometime before final exam
(regardless of midterm score)

B carries (not unanimously)

Cook-Levin Theorem:

Last time:

$$SAT := \{ \langle f \rangle \mid f \text{ is satisfiable} \}$$

e.g.

$X_1 \text{ AND } \neg X_1$ not satisfiable,

$X_1 \text{ OR } \neg X_1$ is satisfiable,

i.e.

f is satisfiable iff there is a truth assignment to f,

$f = f(x_1, \ldots, x_n)$, n Boolean variables, s.t.

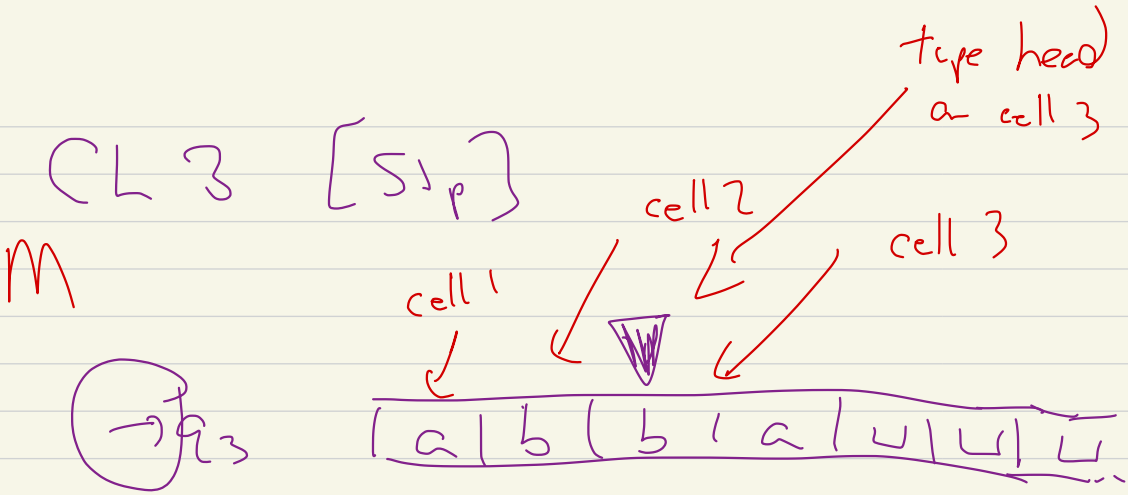
for some values $x_1^*, \ldots, x_n^*$

either T/F, $f(x_1^*, \ldots, x_n^*) = T$

=

$\langle f \rangle$ over some alphabet

$\Sigma = \{ \text{AND}, \text{OR}, \text{NOT}, (,), x, 0, \ldots, 9 \}$



[S, p] config notation

a b q_3 b a

cell 1 cell 2 cell 3 cell 4

indicates type head is on cell 3

anything not in $\Sigma_{config} = Q_m \cup \Gamma_m$

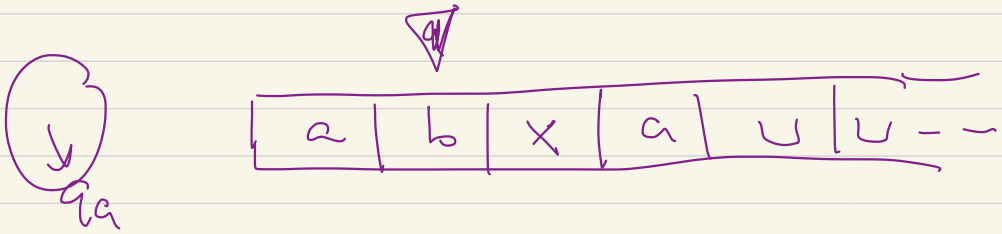
$Q_m \sqcup \Gamma_m$ is think of

$Q_m \cup \Gamma_m$ where Q_m, Γ_m are

regarded as disjoint

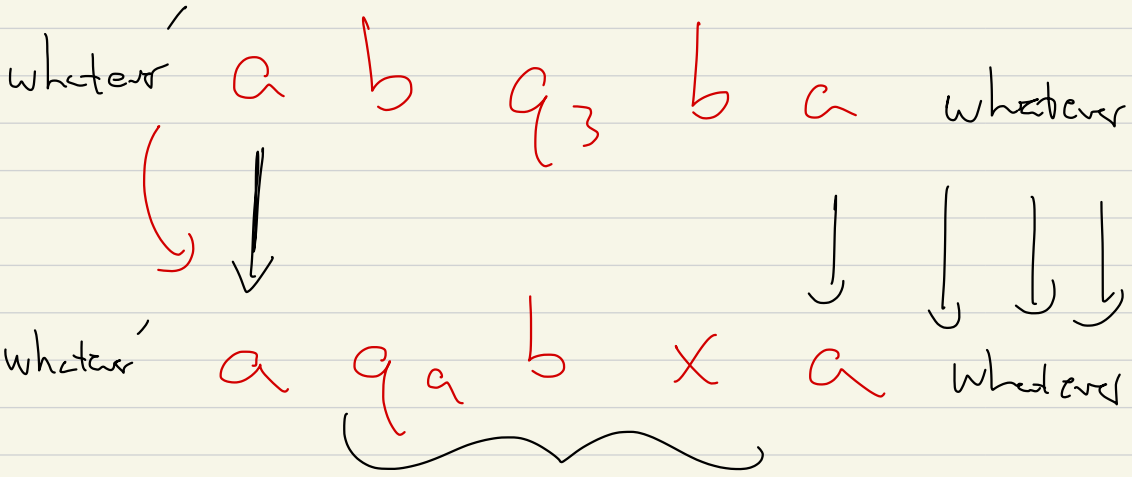
$(a, b, q_3, b, c) \in \Sigma^*_{config}$

next step, say

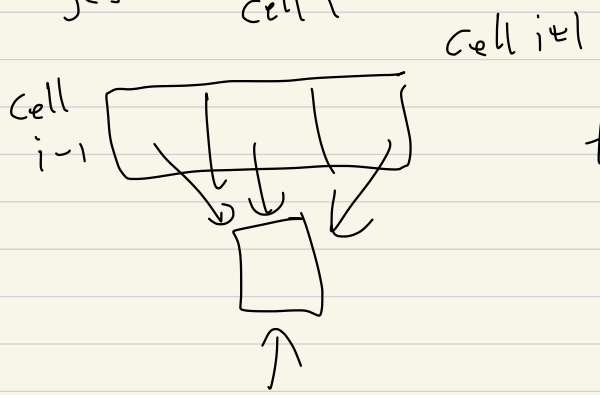


$a\ q_q\ b\ x\ a$

In one step:



What changes



cell i, time t+1

Entire TM amounts to

cell$_i$
time
$t+1$

$\Leftarrow$

$$trans\left(\begin{matrix} cell_{i-1} \\ time\ t \end{matrix}, \begin{matrix} cell_i \\ time\ t \end{matrix}, \begin{matrix} cell_{i+1} \\ time\ t \end{matrix}\right)$$

$\uparrow$

$$trans_M : \Sigma_{config,M}^{3} \longrightarrow \Sigma_{config,M}$$

and Σ_{config} depends on M, but is finite

Thm [Cook-Levin]: If $SAT \in P$ then $P = NP$, i.e.

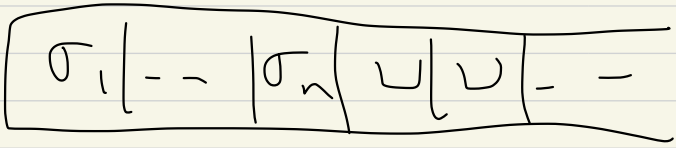
if $L \in NP$ = {verify in poly time}

then $L \in P$, i.e. there is a poly time (rather than $\begin{cases} \text{non-det poly time} \\ NP \end{cases}$).

Proof:

What is NP:

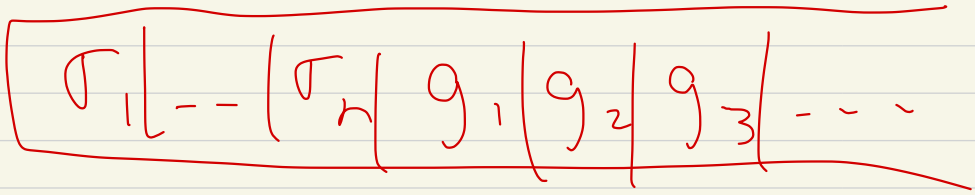
$L \in NP$ means:

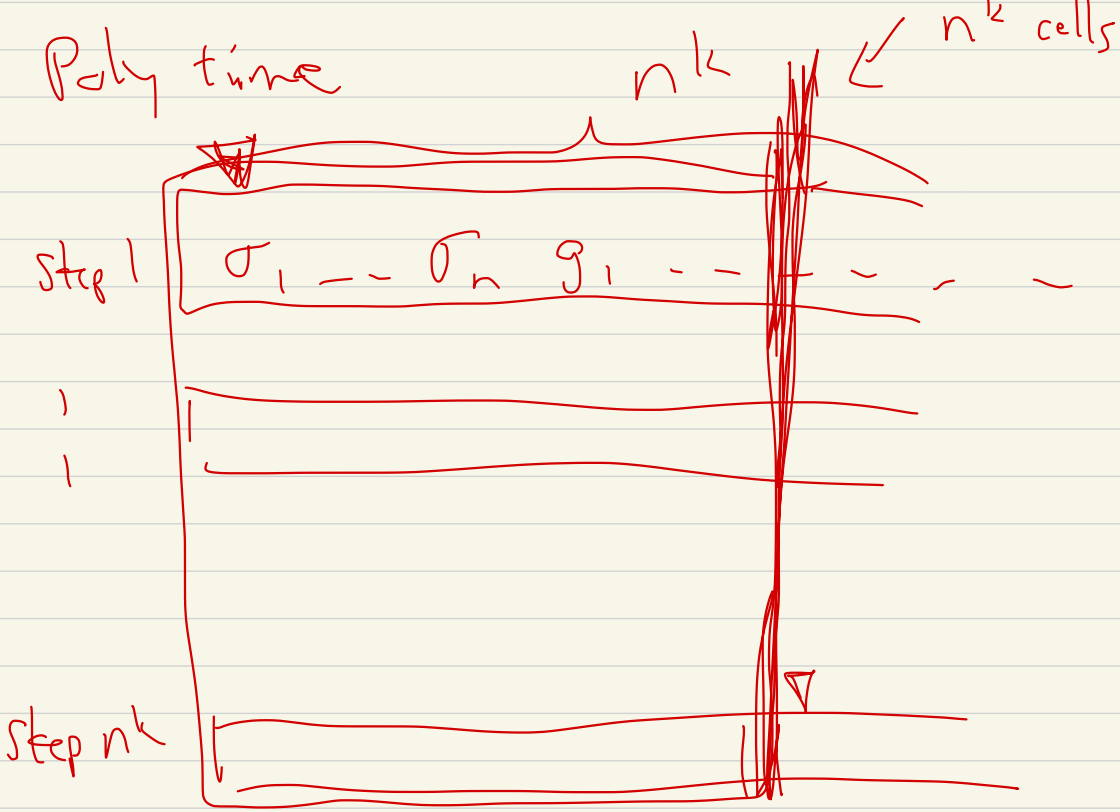
Step-1: 

$w = \sigma_1 \cdots \sigma_n$ input, $\sigma_i \in \Sigma$

oracle calls, guess, non-det, ...

step 0:





after n^k steps, tape head can only see

So -- $\exists$ TM, M', s.t.

(1) $w \in L \iff$ some { oracle, guess, non-det } will accept w + $\top_{guess}$

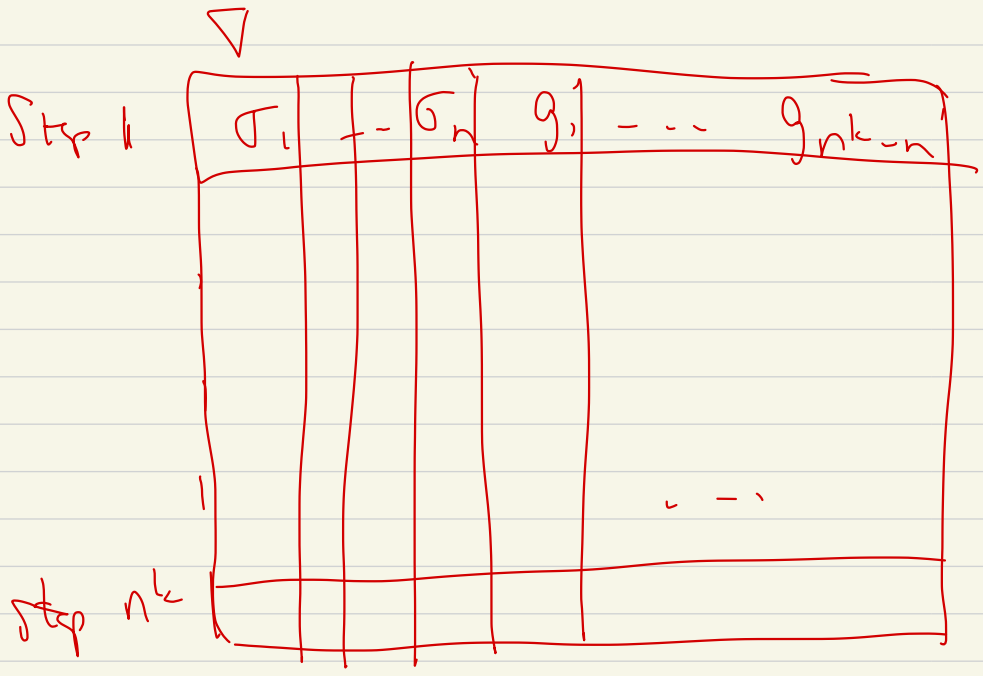
(2) $w \notin L$ there's no guess that has M' accepting

$\sigma_1 -- \sigma_n \, g_1 --- g_{n^k - n}$

in time n^k

Poly Time $:= \bigcup_{k=1,2,--} TIME(n^k)$

So in time n^k



you involve $\leq (n^k)(n^k)$

cells taped location

cells in time

So computation is correct if ...

initially set up right step 1

AND

step 2 ⇝ step 1 correctly

AND

⋮

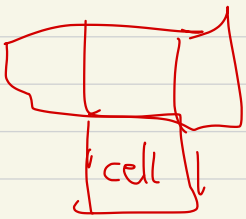
AND

step n^k — step n^{k-1}

AND

we finish in q_{acc}

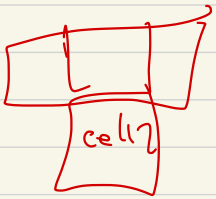
step 2 from 1 is correct



← step 1

← step 2

AND



5- mm break

10:15 – 10:20

better $n^k \rightarrow$ poly(n)