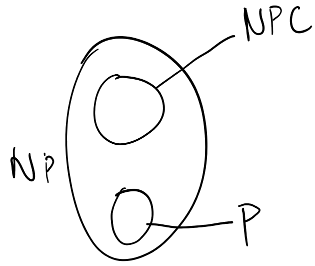
Cook Levin Theorem

11 April 2021 23:28

<u>Theorem</u>: SAT is NP-Complete

We use a "computation histories" - kind of idea here.

We have to show



(1) SAT $\in$ NP

(2) $\forall A \in NP$, $A \leq_p SAT$.

<u>SAT $\in$ NP</u>: Guess TRUE / FALSE for $x_1, x_2 \ldots x_n$.

Verify if ϕ is satisfied for the guessed assignment.

The main part is (2). We must show that any language $A \in NP$ must reduce to SAT.

That is, we need f such that

$$w \in A \iff f(w) \in SAT.$$

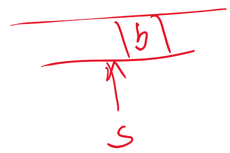
All that we know about A is that $A \in NP$.

We cannot assume any other structure of a any specific language / problem.

<u>$A \in NP$</u>: A is decided by an NTM N in time n^k.

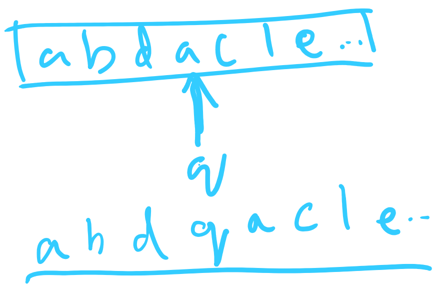
When $w \in A$, there is a sequence of computations that leads N to accept w. This sequence has that leads N to accept w. This sequence has $\leq n^k$ steps. When $w \notin A$, no sequence of computations accept.

$\delta(q,a) = \{(r,b,R),(s,b,L),(s',c,R),\dots\}$



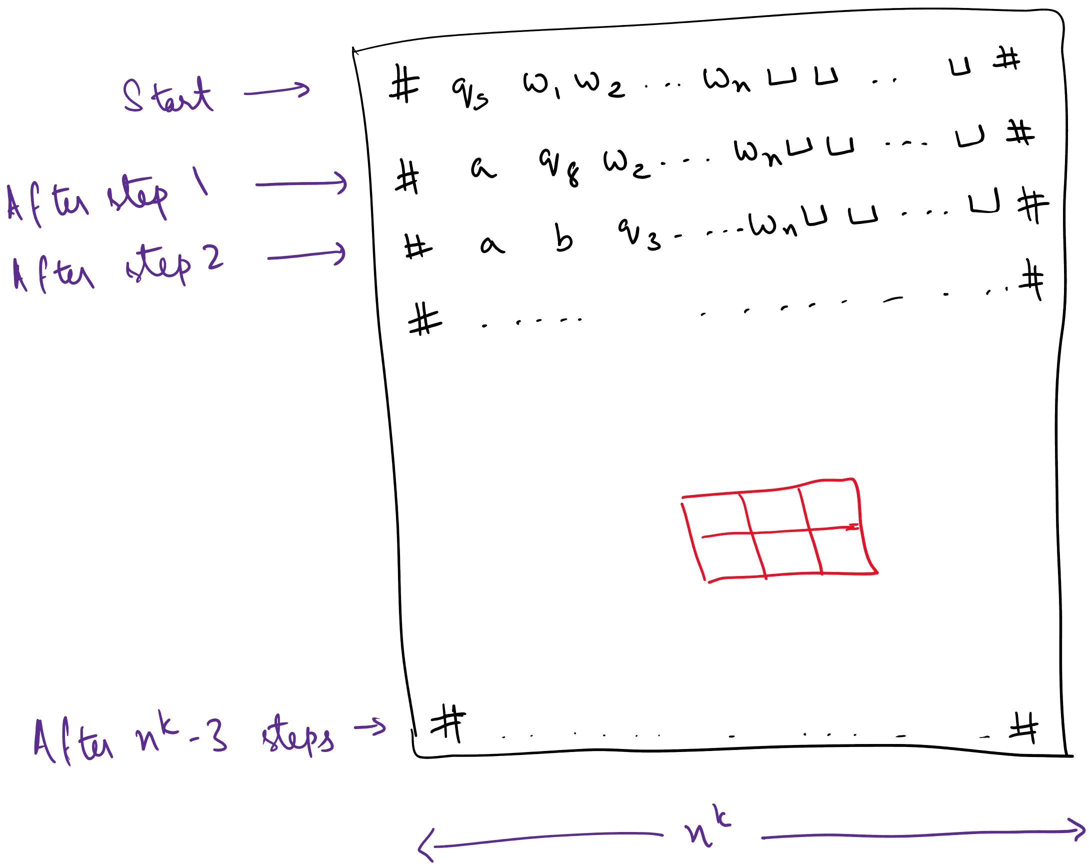
Let $N = (Q, \Sigma, \Gamma, \delta, q_s, q_a, q_r)$.

Let N be a 1-tape NTM, runs in time $\leq n^k$ (actually $n^k - 3$). Let us define $\Delta = Q \cup \Gamma \cup \{\#\}$.



Gadget for reduction: Table or Tableau

Successive configurations. Each row is a configuration.



If the TM N accepts/rejects before n^k steps, the configuration remains unchanged after that.

We will create a formula ϕ which uses Boolean logic to check whether the tableau represents an accepting computation for N on w.

If there exists a path for N to accept w, then ϕ will have a satisfying assignment. Else ϕ won't have a sat. assignment.

ϕ checks the following:

(1) Does N start correctly?

(2) Does N move correctly?

(3) Does N end correctly?

And (4) we also need to check if the variables form a "proper encoding" of the table.

$$\phi = \phi_{cell} \wedge \phi_{start} \wedge \phi_{move} \wedge \phi_{accept}.$$

We have an $n^k \times n^k$ table. We have $|\Delta|$

We have an $n^k \times n^k$ table. We have $|\Delta|$ variables that can occupy each cell.

$$\underbrace{x_{i,j,l}}_{1 \le i,j \le n^k,\ l \in \Delta} = \begin{cases} \text{TRUE} & \text{if } (i,j)^{th} \text{ cell has entry } l \\ \text{FALSE} & \text{if } (i,j)^{th} \text{ cell has entry} \neq l \end{cases}$$

ϕ_{cell} : Is the table properly encoded.

$$\phi_{cell} = \bigwedge_{1 \le i,j \le n^k} \left[\underbrace{\left(\bigvee_{l \in \Delta} x_{i,j,l} \right)}_{\text{Cell } (i,j) \text{ contains at least one entry}} \wedge \underbrace{\left(\bigwedge_{\substack{l,l' \in \Delta \\ l \neq l'}} \left[\overline{x_{i,j,l}} \vee \overline{x_{i,j,l'}} \right] \right)}_{\text{Cell } (i,j) \text{ does not contain} > 1 \text{ entry}} \right]$$

Cell (i,j) contains at least one entry

Cell (i,j) does not contain >1 entry.

So ϕ_{cell} ensures that each cell (i,j) contains exactly one member of Δ.

ϕ_{start} : First row is a legal starting config for N on w.

$$\phi_{start} = x_{1,1,\#} \wedge x_{1,2,q_{start}} \wedge x_{1,3,w_1} \wedge x_{1,4,w_2} \wedge$$

$$\ldots \wedge x \ldots \wedge \ldots$$

$\varphi_{start} = \ldots$

$\ldots \wedge x_{1,n+2,w_n} \wedge x_{1,n+3,\sqcup} \wedge \ldots$

$\ldots \wedge x_{1,n^k-1,\sqcup} \wedge x_{1,n^k,\#}$

$\underline{\phi_{accept}}$: The table represents an accepting computation.

$$\phi_{accept} = \bigvee_{1 \le i,j \le n^k} \left(x_{i,j,q_{accept}} \right)$$

$\underline{\phi_{move}}$: This is the hardest. We have to check that each configuration legally follows from the previous one.

The $\underline{\text{main idea}}$ here is that it is enough to check all the 2×3 windows. We say a window is valid if it is part of a valid transition.

$$\frac{b \quad q \quad a}{b \quad d \quad r} \quad \text{when} \quad (r, d, R) \in \delta(q, a)$$

$$\forall\, b \in \Gamma \cup \{\#\}$$

$$\frac{b \quad q \quad a}{r \quad b \quad d} \quad \text{when } (r, d, L) \in \delta(q, a)$$

$\forall\, b \in \Gamma$

$$\frac{\# \quad q \quad a}{\# \quad r \quad d} \quad \text{when } (r, d, L) \in \delta(q, a)$$

$$\frac{b \quad c \quad q}{b \quad c \quad d} \quad \text{if } (r, d, R) \in \delta(q, a)$$

for some $a \in \Gamma$.

where $b \in \Gamma \cup \{\#\}$, $c \in \Gamma$.

$$\frac{q \quad a \quad b}{d \quad r \quad b} \quad \text{if } (r, d, R) \in \delta(q, a)$$

where $b \in \Gamma \cup \{\#\}$

$$\frac{a \quad b \quad c}{a \quad b \quad c}$$

where $a \in \Gamma \cup \{\#\}$, $b, c \in \Gamma$

OR $a, b \in \Gamma$, $c \in \Gamma \cup \{\#\}$

Like this, one can list all the valid windows.

No. of valid windows is finite, and depends only on N. It is independent of $|w|$.