Sipser section 7.4 Cook-Levin theorem

Theorem 7.37 SAT is NP-complete

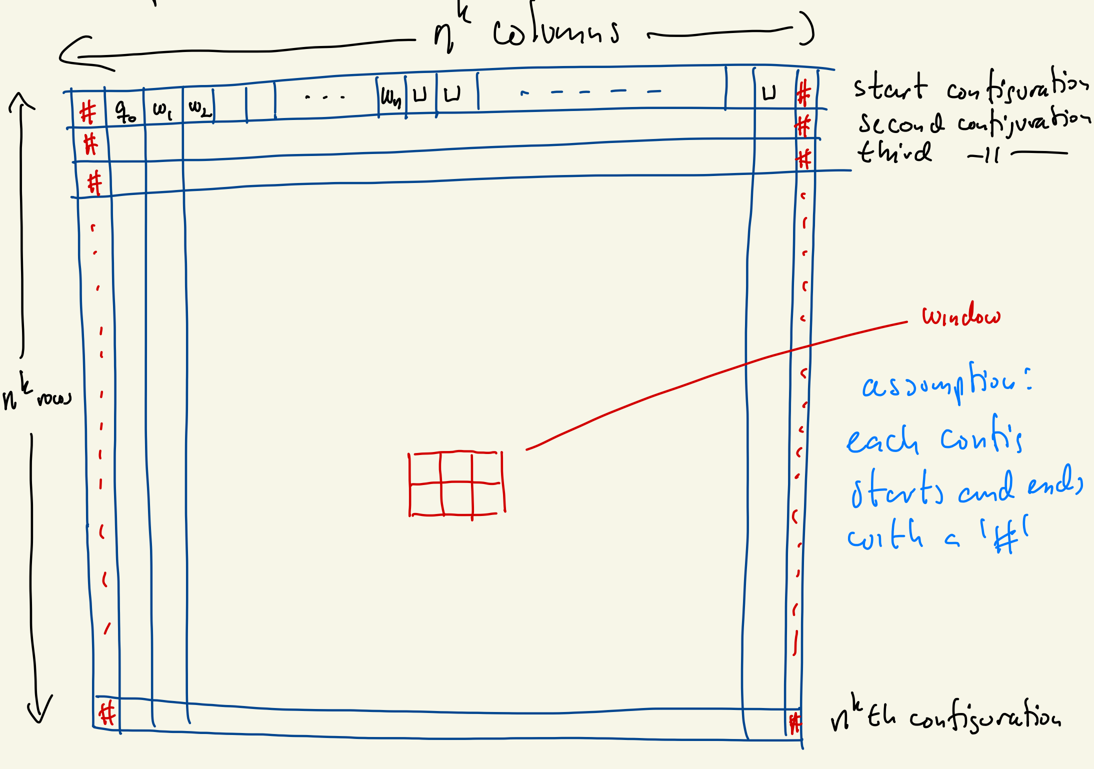
proof: We have argued that SAT $\in$ NP: the certificate is a satisfying truth assignment.

Recall: $NP = \{ L \mid L \text{ is decided by some NDTM in pol time} \}$

We need to show $A \leq_p SAT$ for every $A \in NP$

Let $A \in NP$ and let N be a NDTM that decides A in time n^k minus a constant, when n is the size of the input

A tableau for N on the string w is an $n^k \times n^k$ table showing N's tape in steps $1, 2, \ldots n^k$ for one particular branch of N's computation on w



$\boxed{\text{We call a tableau accepting if at least one of its rows corresponds to an accepting configuration of } N \text{ on } w}$

Note that if row i corresponds to an accepting configuration, then row j = row i for all $j \geq i$ in the tableau.

$\boxed{\text{Every accepting configuration of } N \text{ on } w \text{ corresponds to an accepting computation branch for } N \text{ on } w}$

Hence: N accepts w $\iff$ $\exists$ an accepting tableau for N on w

Our goal: construct a SAT formula φ from N and w such that φ is satisfiable $\iff$ $\exists$ an accepting tableau for N on w

- Let N have state set Q, tape alphabet Γ

  Set $C = Q \cup \Gamma \cup \{\#\}$

- φ will have variables $x_{i,j,s}$, where $i,j \in [n^k] = \{1, 2 \ldots n^k\}$ and $s \in C$

- Each of the $n^k \cdot n^k = n^{2k}$ entries of a tableau is called a cell and $cell[i,j]$ denotes the content of the (i,j)th cell

  so $cell[i,j] \in C$

- The variables $x_{i,j,s}$ will indicate the content of cells:

  $cell[i,j] = s \iff x_{i,j,s} = 1$ and $x_{i,j,t} = 0 \;\; \forall t \in C \text{ s.t. } t \neq s$

The formula φ consists of 4 subformulas

$$\varphi = \varphi_{cell} \wedge \varphi_{start} \wedge \varphi_{move} \wedge \varphi_{accept}$$

φ_{cell} : Expresses that at any time, each cell has precisely one symbol from C

$$\varphi_{cell} = \bigwedge_{i,j \in [n^k]} \left[\bigvee_{s \in C} x_{i,j,s} \wedge \left(\bigwedge_{\substack{s,t \in C \\ s \neq t}} \left(\overline{x_{i,j,s}} \vee \overline{x_{i,j,t}} \right) \right) \right]$$

φ_{start} : Expresses that N starts in the configuration $q_0 w$

$$\varphi_{start} = x_{1,1,\#} \wedge x_{1,2,q_0} \wedge x_{1,3,w_1} \wedge \cdots \wedge x_{1,n+2,w_n} \wedge$$
$$x_{1,n+3,\sqcup} \wedge \cdots \wedge x_{1,n^k-1,\sqcup} \wedge x_{1,n^k,\#}$$

φ_{accept} : Expresses that at least one row of the tableau contains an accepting configuration for N on w

$$\varphi_{accept} = \bigvee_{i,j \in [n^k]} x_{i,j,q_{accept}}$$

φ_{move}: should express that the rows of the tableau change according to N's transition table

More complicated!!

We must ensure that from one row in the tableau to the next the cells can only change according to what N can do in one step.

E.g. if reading head is more than one cell away from a given cell, then this cell is unchanged in the next iteration.

Solution: use 2x3 windows

just called a **window** below

> A window is **legal** if the 3 bottom cells may result from the 3 top cells in one step of N

NB: we do not give a complete description of legal windows, but you should be able to argue whether a given window is legal, based on N's transition table.

Example suppose $\delta(q_1, a) = \{\overset{(i)}{(q_2, b, R)}\}$ and $\overset{(ii)}{(q_2, c, L)}, \overset{(iii)}{(q_1, a, R)} \in \delta(q_2, b)$

Legal

(i)

q_1	a	c
b	q_2	c

(ii)

a	q_2	b
q_2	a	c

(iii)

a	q_2	b
a	a	q_1

a	b	c
a	b	c

b	a	b
c	a	b

(ii)

a	b	q_1
a	b	b

a

not legal

a	b	a
a	a	a

q_1	a	c
b	c	q_2

Claim 7.4.1

If row 1 ~ start configuration of N on w and every window of the tableau is legal, then each row of the tableau ~ config that legally follows the predecessor of that row.

Proof: Consider two consecutive rows j and j+1 called upper and lower configurations

- In upper every cell i,j containing a tape symbol x and which is not adjacent to a state symbol has a window

		j	
i	y	x	z
		x	

$y, z \in \Gamma \cup \{\#\}$

← also x here

So cell i,j also contains x in row j+1

- if upper = # - - - . a q s . . . . . # then the window

a	q	s

mimics what N will do so if upper config is legal then so is the lower configuration

- By induction and the fact that the first row is the starting configuration of N on w, the rows in the tableau corresponds to consecutive configurations of N on w

□.

Construction of φ_{move}:

The formula needs to correspond to all windows of the tableau are legal

Informally:

$$\varphi_{move} = \bigwedge_{\substack{i \in [n^k] \\ 1 < j < n^k}} \left(\text{the } (i,j)\text{-window is legal}\right)$$

when (i,j)-window =

	$j-1$	j	$j+1$
i			
$i+1$			

Not a SAT formula

But we can formulate that a window is legal using

6 variables

a_1	a_2	a_3
a_4	a_5	a_6

(i,j)-window is legal

$\Updownarrow$

$$\bigvee_{\substack{a_1,a_2,a_3 \\ a_4,a_5,a_6}} \left(x_{i,j-1,a_1} \wedge x_{i,j,a_2} \wedge x_{i,j+1,a_3} \wedge x_{i+1,j-1,a_4} \wedge x_{i+1,j,a_5} \wedge x_{i+1,j+1,a_6} \right)$$

a_1,a_2,a_3
a_4,a_5,a_6 legal window

For a legal window $a_1 \ldots a_6 \in C$ so at most

$|C|^6$ legal windows (far less)

We have shown

$\varphi = \varphi_{cell} \wedge \varphi_{start} \wedge \varphi_{move} \wedge \varphi_{accept}$ is satisfiable

$\Updownarrow$

N accepts w $\iff$ $w \in A$

Remains to prove that given N, w we can construct φ in polynomial time in $|N| + |w|$

Note that for fixed $A \in NP$, N is also fixed so $|N|$ is a constant

- # variables in φ is $n^{2k} * |C| \in O(n^{2k})$
- $|\varphi_{start}| \in O(n^k)$
- $|\varphi_{accept}| \in O(n^{2k})$
- $|\varphi_{cell}| \in O(n^{2k})$ as $|C|$ is a constant
- $|\varphi_{move}|$ is $O(n^{2k})$ as # legal windows only depends on N's transition table

We ignored a factor $O(\log n)$ to handle indices

So $|\varphi| \in O(n^{2k} \log n)$ which is polynomial in $|w|$

We have show that $A \leq_p SAT$ and $A \in NP$ was arbitrary so $SAT \in NPC$

$\square$.