The Cook-Levin theorem

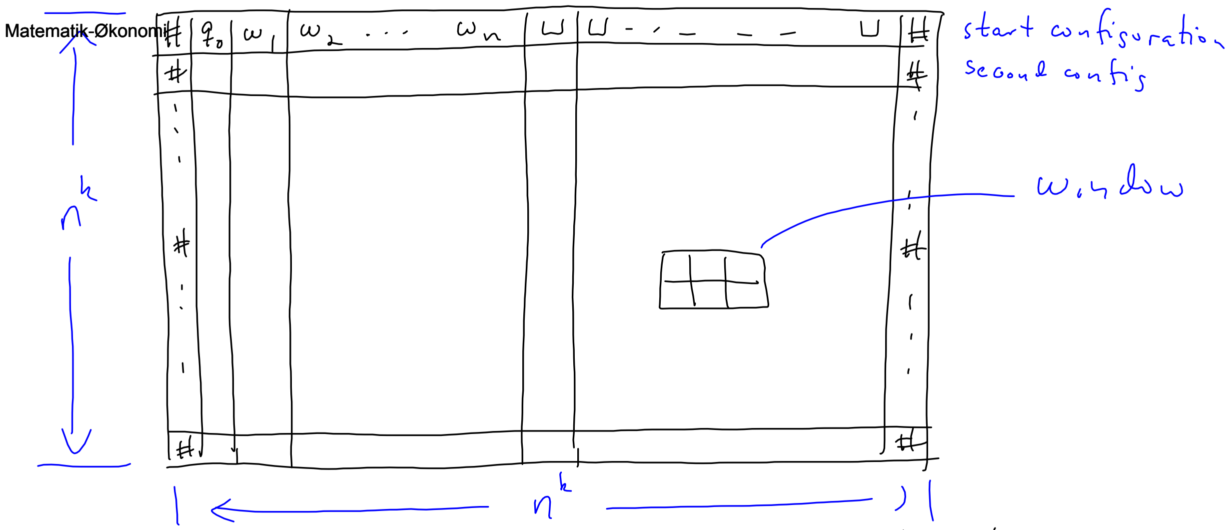
<u>Thm 7.37</u> SAT is NP-complete

<u>proof:</u> Recall that

$NP = \{ L \mid L$ is decided by a NDTM in pol time$\}$

Let $A \in NP$ be arbitrary and let N be a NDTM that decides A in time n^k minus a constant (n = length of input)

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



We have assumed that each configuration starts and ends with #

A tableau is accepting if at least one of its rows corresponds to an accepting configuration of N on w

Every accepting tableau for N on w corresponds to an accepting computation branch for N on w

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

Goal: construct a SAT formula φ from N and w s.t. φ is satisfiable $\iff$ $\exists$ accepting tableau for N on w.

Let N have stateset Q and tapealphabet Γ and set $C = Q \cup \Gamma \cup \{\#\}$

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

each of the n^{2k} entries of a tableau is called a cell and the content of the i,jth cell is denoted $cell[i,j]$ so $cell[i,j] \in C$

We will use $x_{i,j,s}$ variables to indicate content of cells:

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

The formula φ consists of 4 subformulas:

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

φ_{cell} should express that, at any time each cell contains exactly one symbol from C:

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

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

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

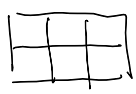
φ_{accept} should express that at least one row in the tableau contains an accepting config for N on w:

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

φ_{move} should express that the rows of the tableau change according to N's transition table.
This is more complicated!!

We must ensure that from one row of the tableau to the next the cells can only change according to what N can do. E.g. if reading head is more than one cell away from a given cell that is is unchanged at the next iteration.

To model this we use 2×3 windows



A 2×3 window (called a window below) is legal if the three bottom cells may result from the three top cells in one step of N

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

Examples: suppose $\underbrace{(q_2,b,R)}_{} \in \overset{(i)}{\delta(q_1,a)}$

and $\underset{(ii)}{(q_2,c,L)}, \underset{(iii)}{(q_1,a,R)} \in \delta(q_2,b)$

Legal:

(ii)

a	q_2	b
q_2	a	c

(iii)

*

a	q_2	b
*	a	a

q_1

(i)

*

q_1	a	c
*	b	q_2

c

not legal

a	b	a
a	a	a

b changed to a but the reading head was not on the middle cell

Claim 7.4.1

If row 1 = start config for N on w and every window of the tableau is legal, then each row in the tableau is a config that legally follows the preceeding one

Proof: Consider two consecutive rows j and j+1 in tableau called upper and lower config

In upper every cell x that contains a tape symbol and is not adjacent to a state symbol has a window

	x	

not a state

so lower also has x

If upper = # ... aqb ... # then the window

a	q	b

mimics what N will do

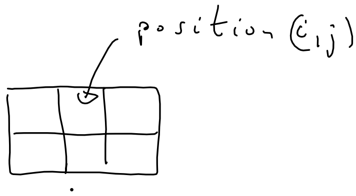
Hence if upper config is legal, then so is the lower config

By induction, and the fact that the first row is the starting config of N on w, all rows of the tableau correspond to consecutive configs of N on w □.

So we can define φ_{move} as

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

when (i,j)-window is



Not a SAT formula yet!
But we can formulate that a window is legal using the variables:

a_1	a_2	a_3
a_4	a_5	a_6

(i,j)-Window is legal

$\Updownarrow$

$$\bigvee_{\substack{a_1 \cdots a_6 \\ \text{is a legal} \\ \text{window}}} \left(X_{i,j-1,a_1} \wedge X_{i,j,a_2} \wedge X_{i,j+1,a_3} \wedge X_{i+1,j-1,a_4} \wedge X_{i+1,j,a_5} \wedge X_{i+1,j+1,a_6} \right)$$

This completes description of $\varphi = \varphi(N,w)$
and we have argued that

φ is satisfiable

$\Updownarrow$

N accepts w

It 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 a constant

- #variables is $n^{2k} * |C| = O(n^{2k})$
- $|\varphi_{start}|$ is $O(n^k)$
- $|\varphi_{accept}|$ is $O(n^{2k})$
- φ_{cell} is $O(n^{2k})$ as formula for each cell only depends on $|C|$ which is constant
- φ_{move} is $O(n^{2k})$ as # of legal cells only depend on N's transition

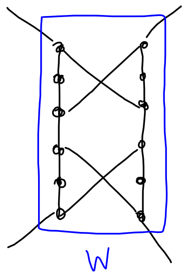
We ignored a factor $O(\log n)$ to handle indices so

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

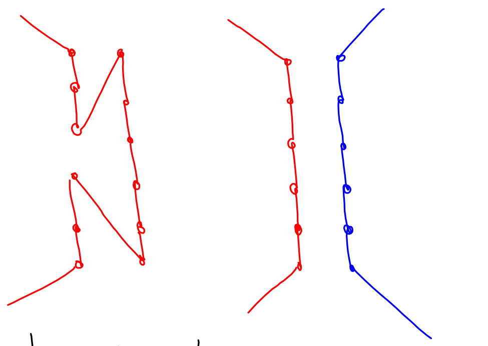
and the proof is complete. $\square$

Hamilton cycle is NPC

Know already that HAMCYCLE $\in$ NP



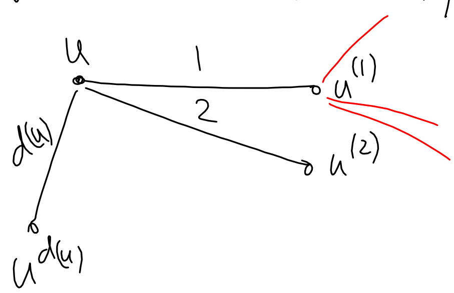
exactly two ways to pick all 12 vertices of W



Given $G=(V,E)$ and k instance of VC

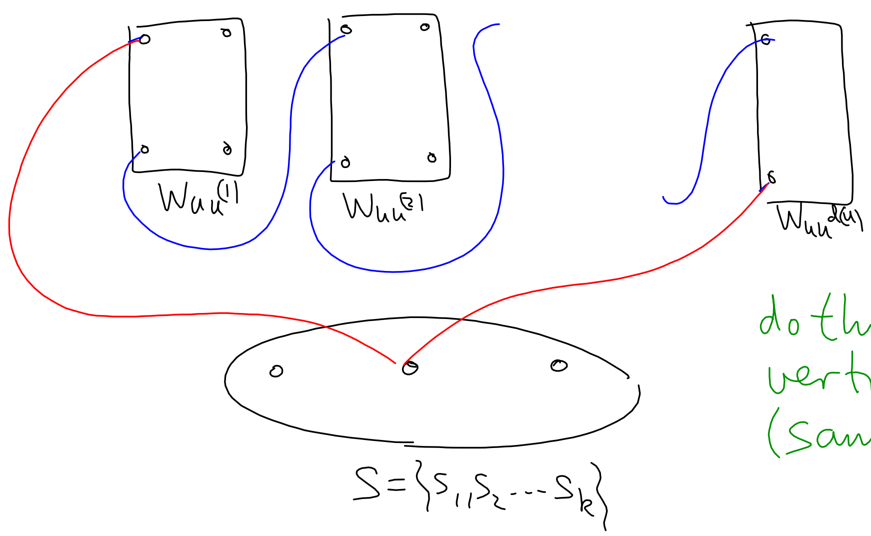
For each edge $uv \in V$ we take a copy W_{uv} of W

For every $u \in V$ order its neighbours arbitrarily



and connect

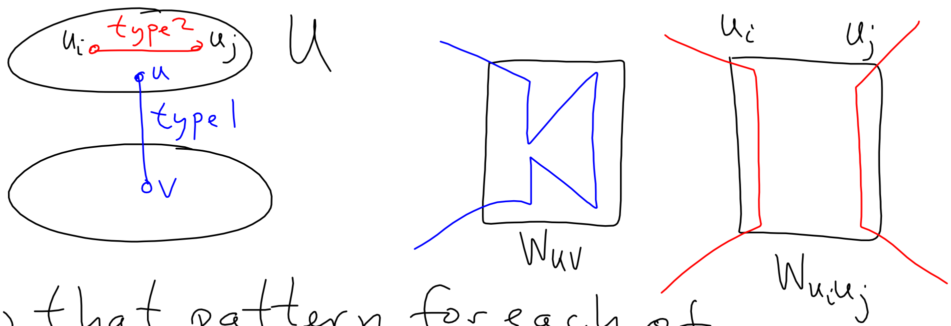
$W_{uu^{(1)}}, W_{uu^{(2)}} \ldots W_{uu^{d(u)}}$ as follows



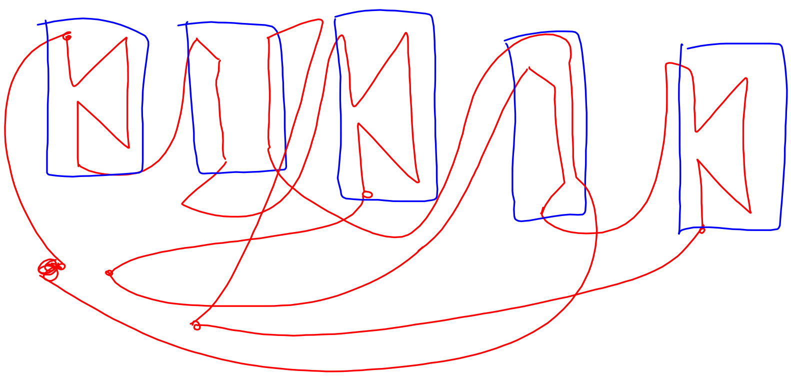
do this for all vertices $u \in V$ (same S)

<u>claim</u>: the resulting graph G' has a hamiltonian cycle iff G has a VC of size k

$\Uparrow$ Let $U=\{u_1,u_2 \dots u_k\}$ be a VC of G

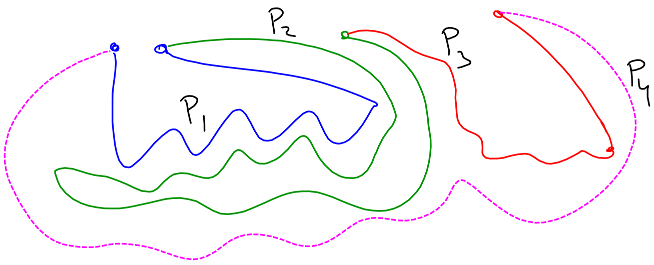


follow that pattern for each of the k ordered collections corresponding to $u_1,u_2 \dots u_k$ and using the k vertices of S



Conversely assume that G' has a hamiltion cycle. C

S is independent so C must be of the kind $s_1 P_1 s_2 P_2 \cdots s_k P_k s_1$



$P_1 \Leftrightarrow$ some vertex u_1'
$\vdots$
$P_k \Leftrightarrow \ldots\ldots\ldots\ u_k'$

s.t $u_1' \cdots u_k'$ is a VC because we may assume that P_i starts at first W of u_i' and ends at the last one.

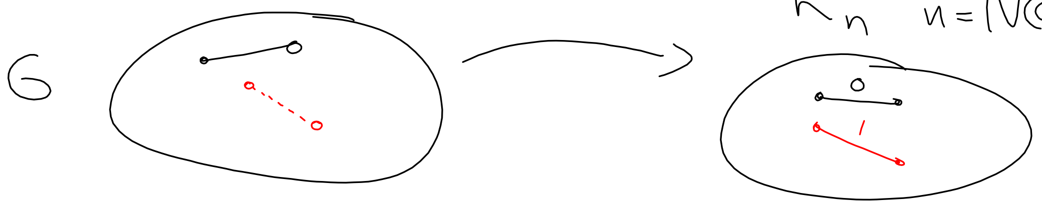
TSP $\underline{\text{input}}$ $K_n, K, \; w: E(K_n) \to \mathbb{Z}_0$

$\underline{\text{Question}}$ does $\exists$ a hamiltonian cycle in K_n of weight $\leq K$?

$TSP \in NP$: we can just show a good permutation of the vertices (if there is one)

$HAMCYCLE \leq_p TSP$

$K_n \quad n = |V(G)|$



1 on nonedges of G

put $K = 0$

h

$\exists$ Hamcycle of cost/weight 0 in K_n

$\Updownarrow$

G has a hamcycle