Lecture 22

Today : NP-completeness of HAMPATH

Cook-Levin Thm proof (3SAT is NP-complete)

* See Review documents (under "Handouts")

for computability

Complexity & NP-completeness

HW4

2. FACTOR problem:

show Factor is in P assuming P=NP.

First give a polytime alg for FIND-PRIME-FACTOR (assuming P=NP)

* ~~Runtime~~ polytime here means poly in $\underbrace{\log x}$ where x is input *

3. (a) ← give your explanation
(but you won't be able to prove your answer)

(b) ← has an answer

4. 3SAT

(a) ϕ is it sat?

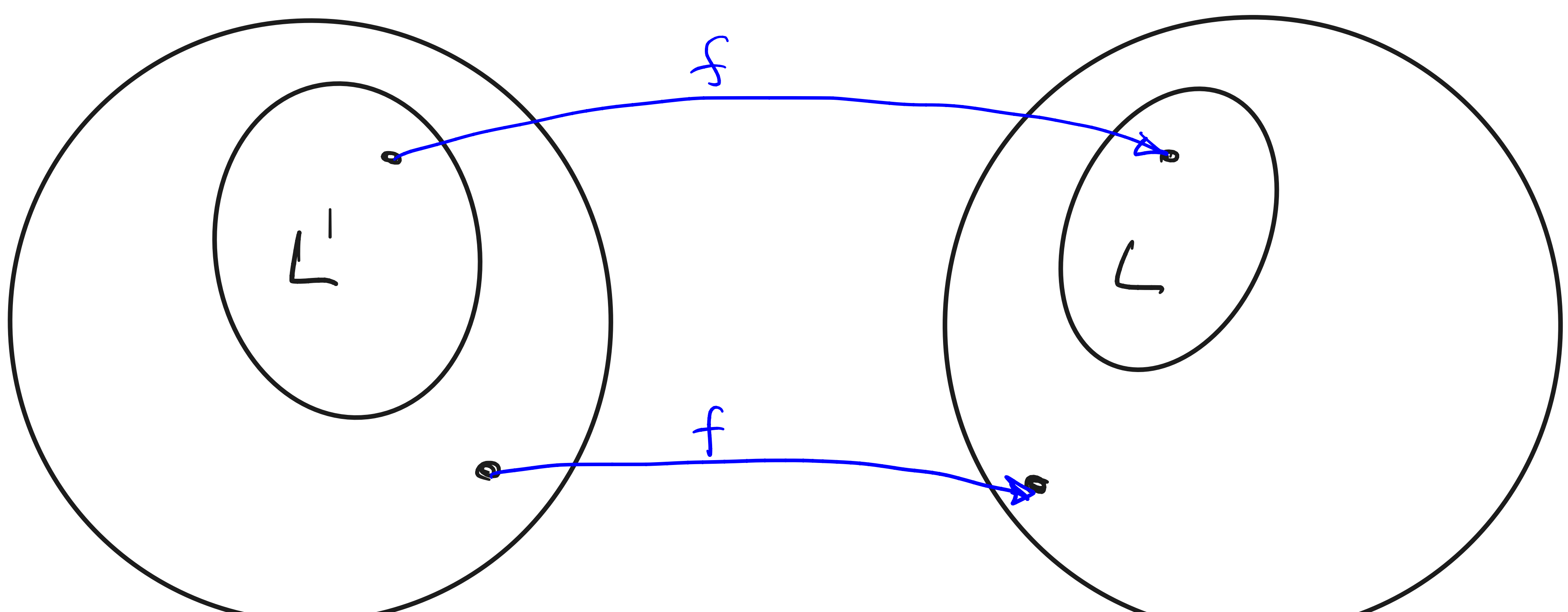
(b) show 3SAT $\xrightarrow[\text{to}]{\text{polytime reduce}}$ exact 3SAT

To prove a language L is NP complete:

(1) Show $L \in NP$

(2) show for some NP-complete language L':

$$L' \leq_p L$$



NP-completeness via Reductions

Theorem HAMPATH is NP-complete

Proof

1. HAMPATH in NP (already did this)
2. We will show $3SAT \leq_p$ HAMPATH (and thus HAMPATH is NP-hard)

Let $\phi = (a_1 \vee b_1 \vee c_1) \wedge (a_2 \vee b_2 \vee c_2) \wedge \dots \wedge (a_m \vee b_m \vee c_m)$ each a_i, b_i, c_i is a literal.

$f : \phi \to (G_\phi, s, t)$

HAMPATH = $\{ (G, s, t) \mid$ G is a directed graph with a hamiltonian path (visits every vertex in G exactly once) from s to t $\}$

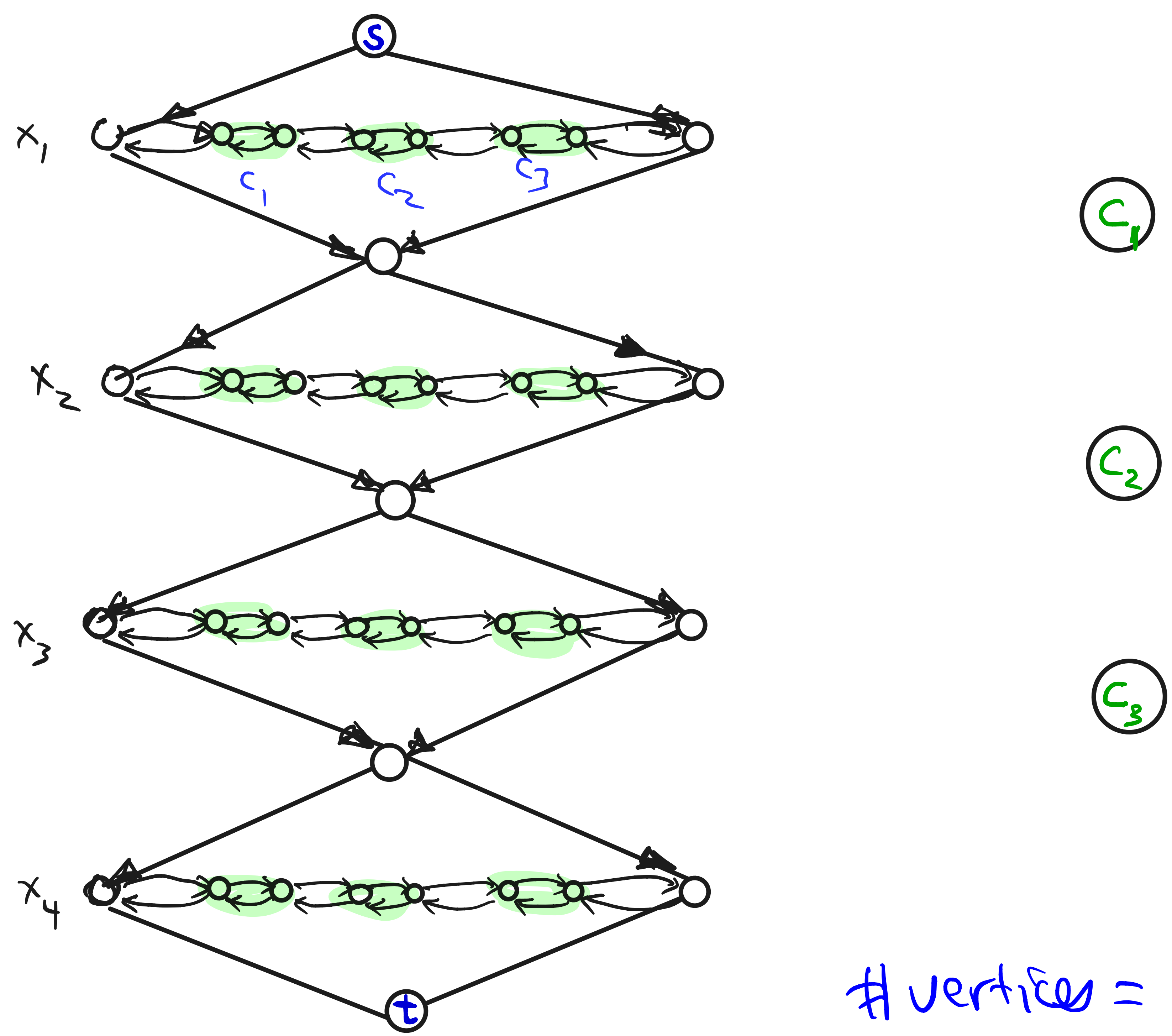
Let $\phi = \underbrace{(x_1 \vee x_3 \vee \bar{x}_4)}_{C_1} \wedge \underbrace{(x_2 \vee \bar{x}_3 \vee x_4)}_{C_2} \wedge \underbrace{(\bar{x}_1 \vee x_2 \vee x_3)}_{C_3}$

$n = \#\text{ vars} = 4$

$m = \#\text{ clauses} = 3$

$f : \phi \rightarrow (g_\phi, s, t)$

g_ϕ :



$\#\text{ vertices} = n + 1 + 2n + 2nm + m$

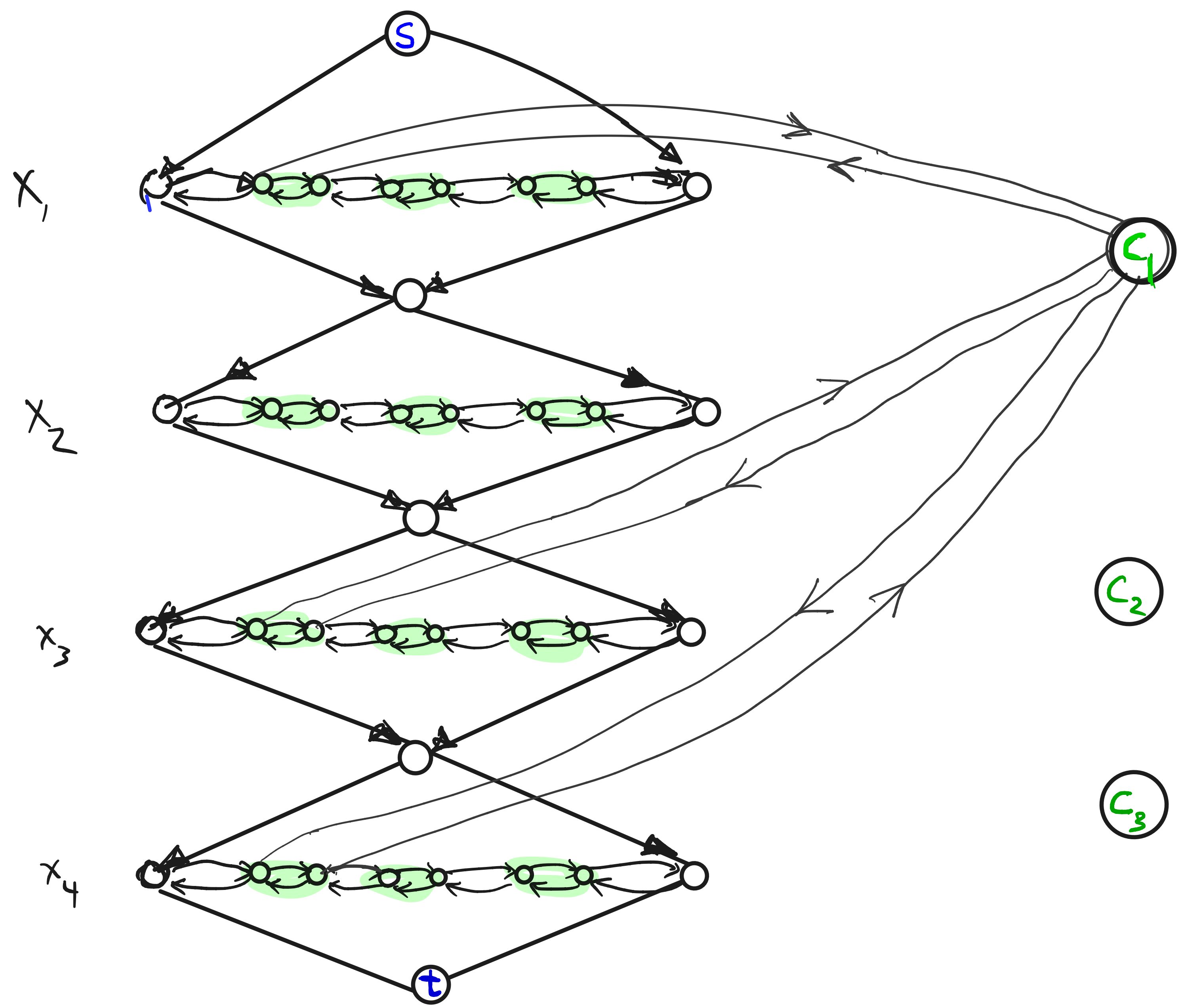
Let $\phi = \underbrace{(x_1 \vee x_3 \vee \bar{x}_4)}_{c_1} \wedge \underbrace{(x_2 \vee \bar{x}_3 \vee x_4)}_{c_2} \wedge \underbrace{(\bar{x}_1 \vee x_2 \vee x_3)}_{c_3}$

$n = \#\text{ vars} = 4$

$m = \#\text{ clauses} = 3$

$f : \phi \rightarrow (g_\phi, s, t)$

g_ϕ :



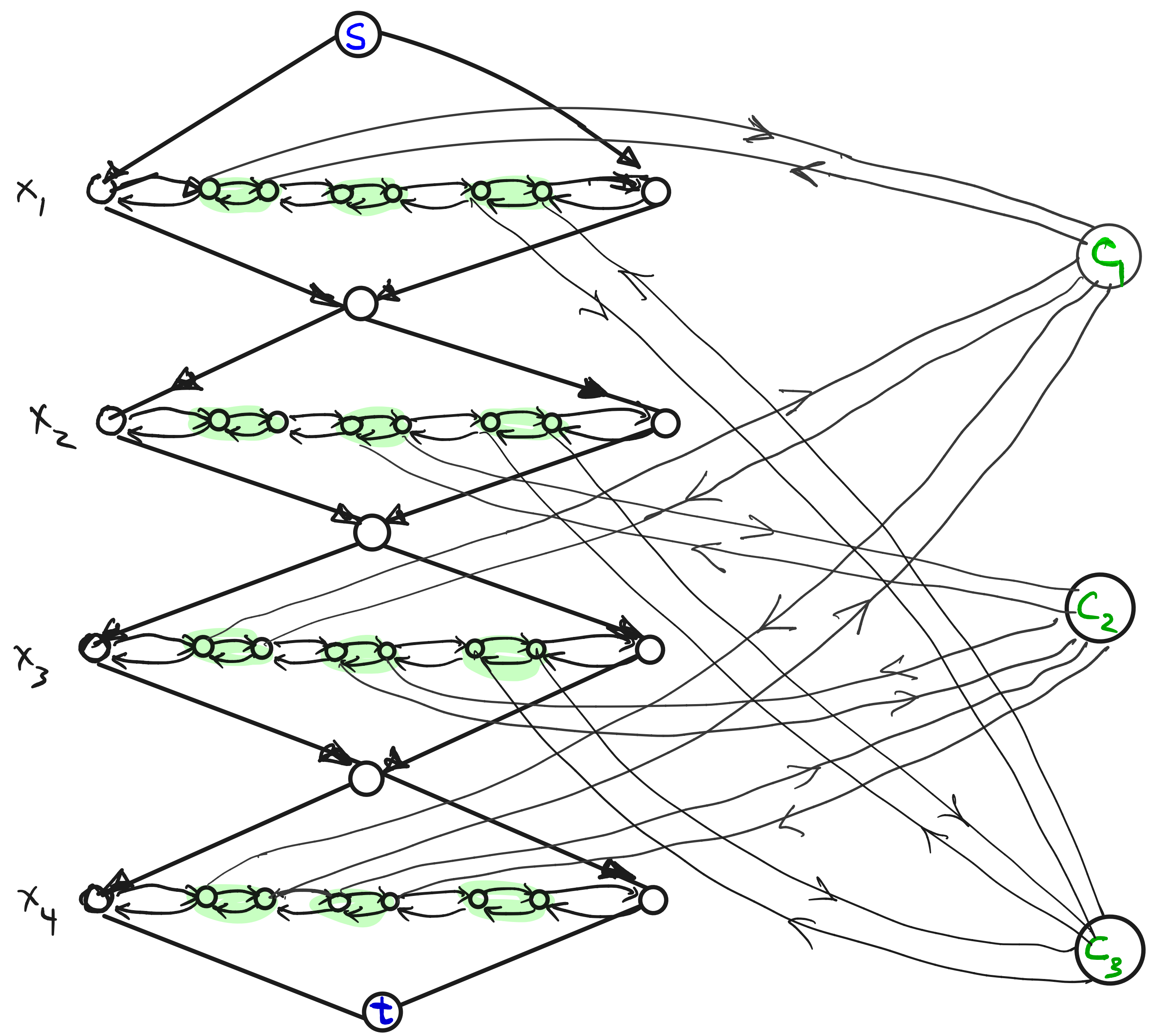
Let $\phi = \underbrace{(x_1 \vee x_3 \vee \bar{x}_4)}_{C_1} \wedge \underbrace{(x_2 \vee \bar{x}_3 \vee x_4)}_{C_2} \wedge \underbrace{(\bar{x}_1 \vee x_2 \vee x_3)}_{C_3}$

$n = \#\text{ vars} = 4$

$m = \#\text{ clauses} = 3$

$f : \phi \rightarrow (g_\phi, s, t)$

g_ϕ:



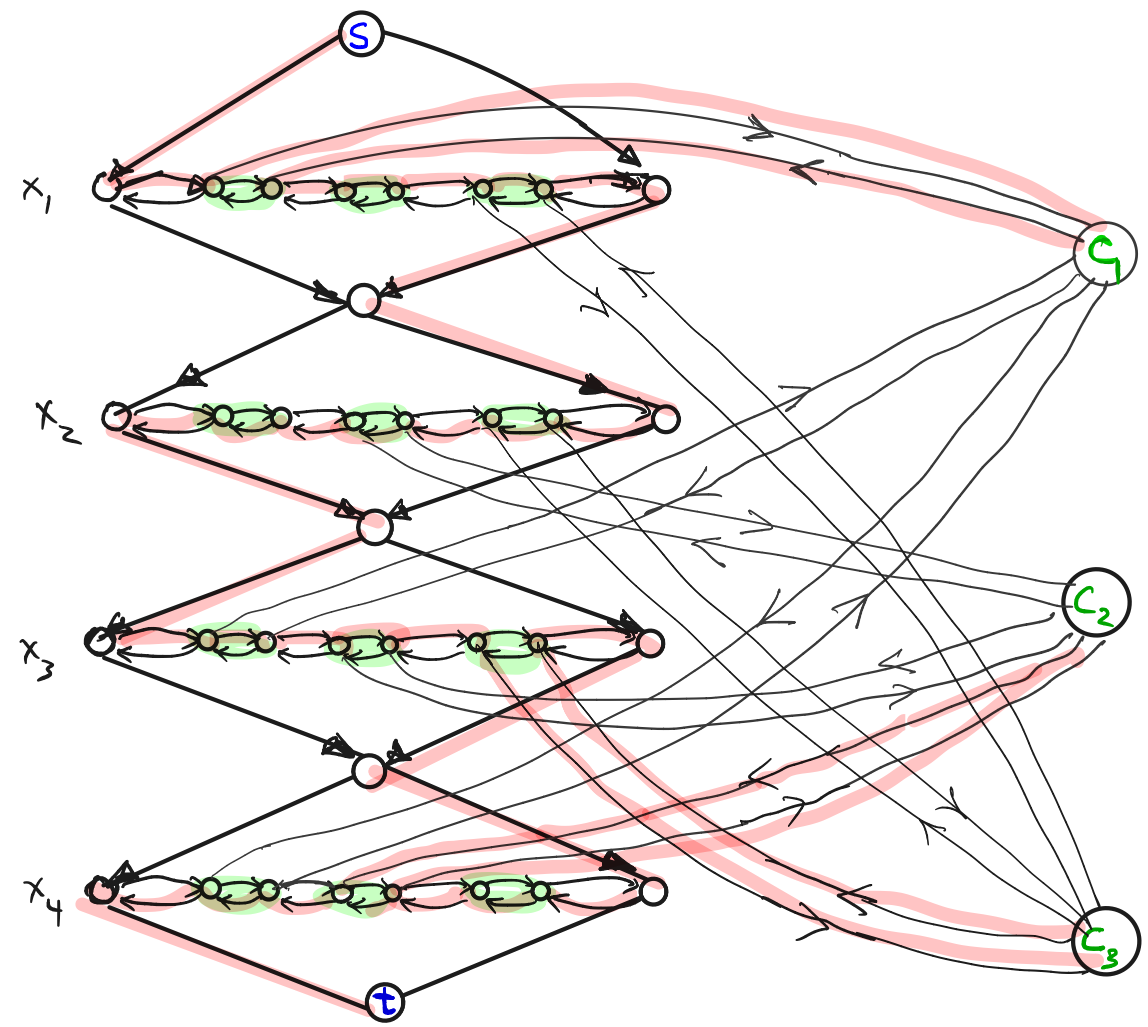
Let $\phi = \underbrace{(\overset{1}{x_1} \vee \overset{1}{x_3} \vee \overset{1}{\bar{x}_4})}_{C_1} \wedge \underbrace{(\overset{0}{x_2} \vee \overset{0}{\bar{x}_3} \vee \overset{1}{\bar{x}_4})}_{C_2} \wedge \underbrace{(\overset{0}{\bar{x}_1} \vee \overset{0}{x_2} \vee \overset{1}{x_3})}_{C_3}$

$n = \#\text{ vars} = 4$

$m = \#\text{ clauses} = 3$

$f : \phi \to (g_\phi, s, t)$

g_ϕ :



Claim ϕ is satisfiable iff g_ϕ has a Hamiltonian path from s to t

$\alpha :\ \underbrace{x_1 = 1}_{C_1}\ \ x_2 = 0\ \ \underbrace{x_3 = 1}_{C_3}\ \ \underbrace{x_4 = 0}_{C_2}$

3SAT IS NP-COMPLETE

- Today we will prove the Cook-Levin Theorem showing that 3SAT is NP-complete
  (actually we will only prove here that CNF-SAT is NP-complete although it can also be shown that 3CNF-SAT (=3SAT) is also NP-complete)

- This is the first language shown to be NP-complete so we need to prove

  (1) 3SAT $\in$ NP (easy, already did)

  * (2) 3SAT is NP hard:

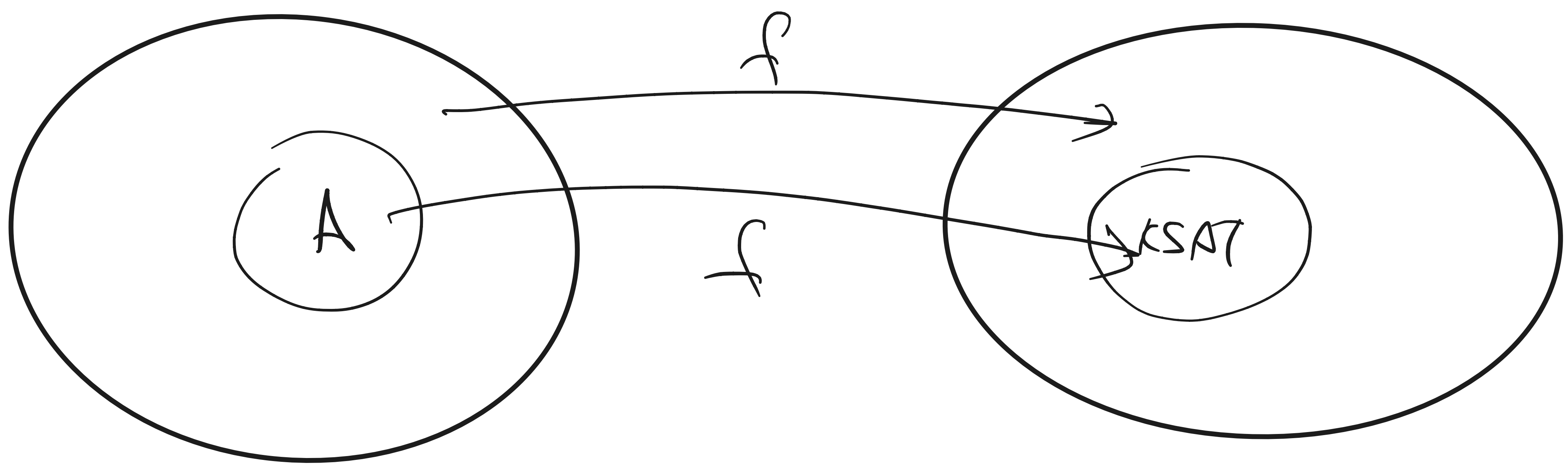
  for every $L \in NP$ $\quad L \leq_p 3SAT$

Cook-Levin Theorem: KSAT is NP-complete

1. KSAT $\in$ NP (already did)
2. To prove KSAT is NP-hard we have to prove:

   For every language $A \in NP$, $A \leq_p$ KSAT

Let $A \in NP$. We want to define a polytime $f : \Sigma^* \to \Sigma^*$ such that:



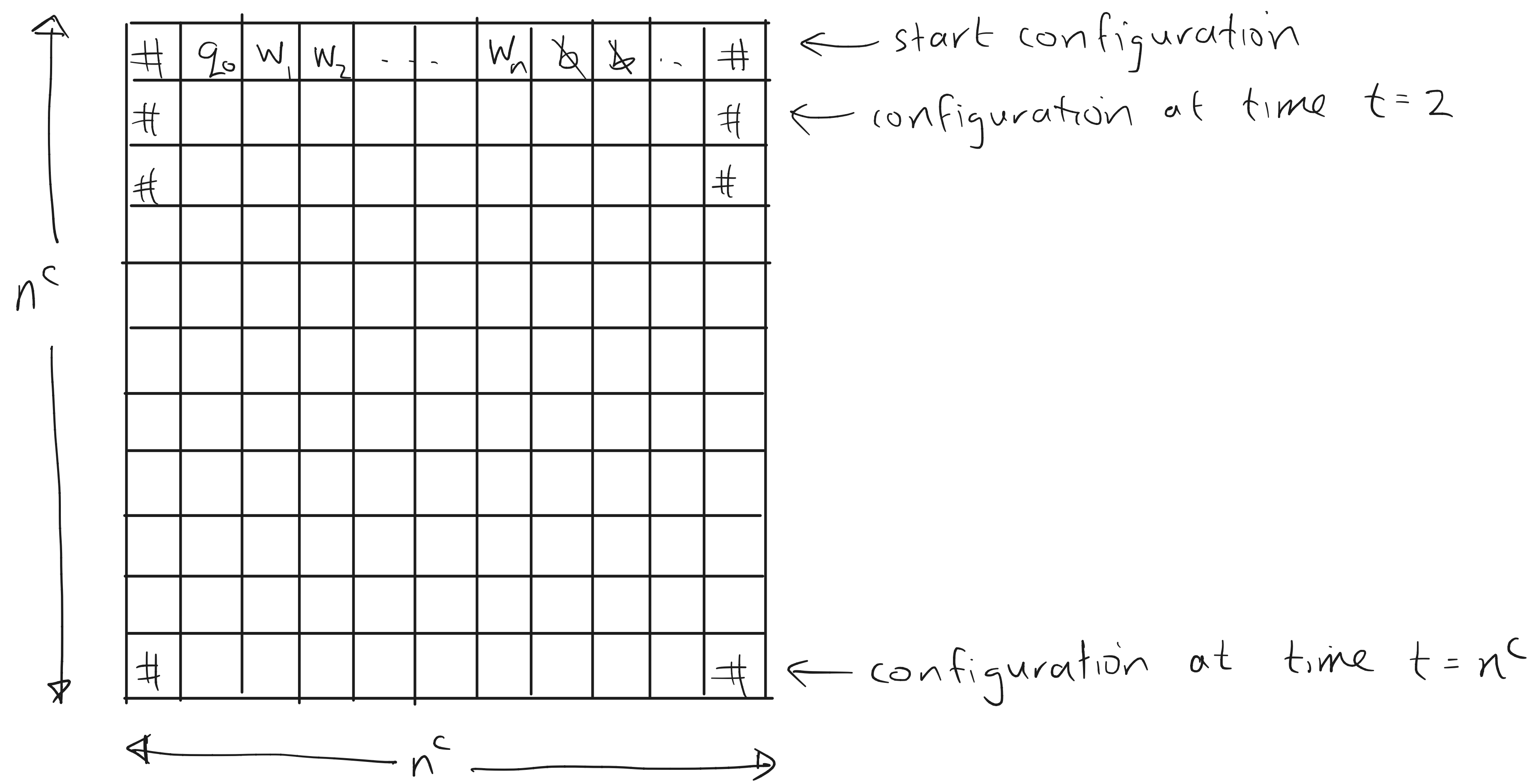
Cook-Levin Theorem: KSAT is NP-complete

1. KSAT $\in$ NP (already did)
2. To prove KSAT is NP-hard we have to prove:

   For every language $A \in NP$, $A \leq_p$ KSAT

Let $A \in NP$ and let N be a Nondet. TM accepting A in polynomial time, n^c, $c \geq 0$.

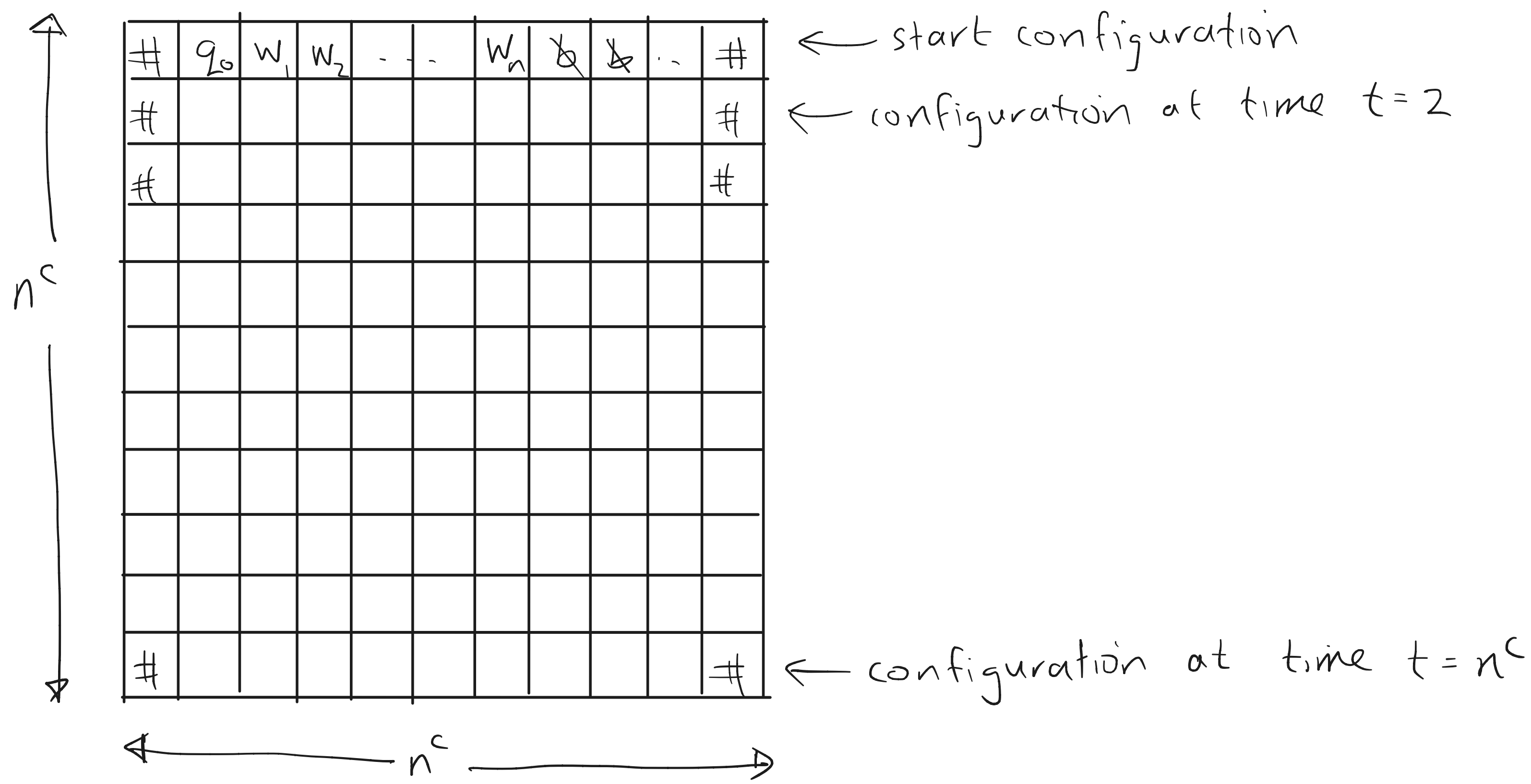
A tableaux for N on input w:



Cook-Levin Theorem: KSAT is NP-complete

Let $A \in NP$ and let N be a Nondet. TM accepting A in polynomial time, n^c, $c \geq 0$.

A tableaux for N on input w:



A tableaux is accepting if for some $t \leq n^c$ configuration at time t is accepting

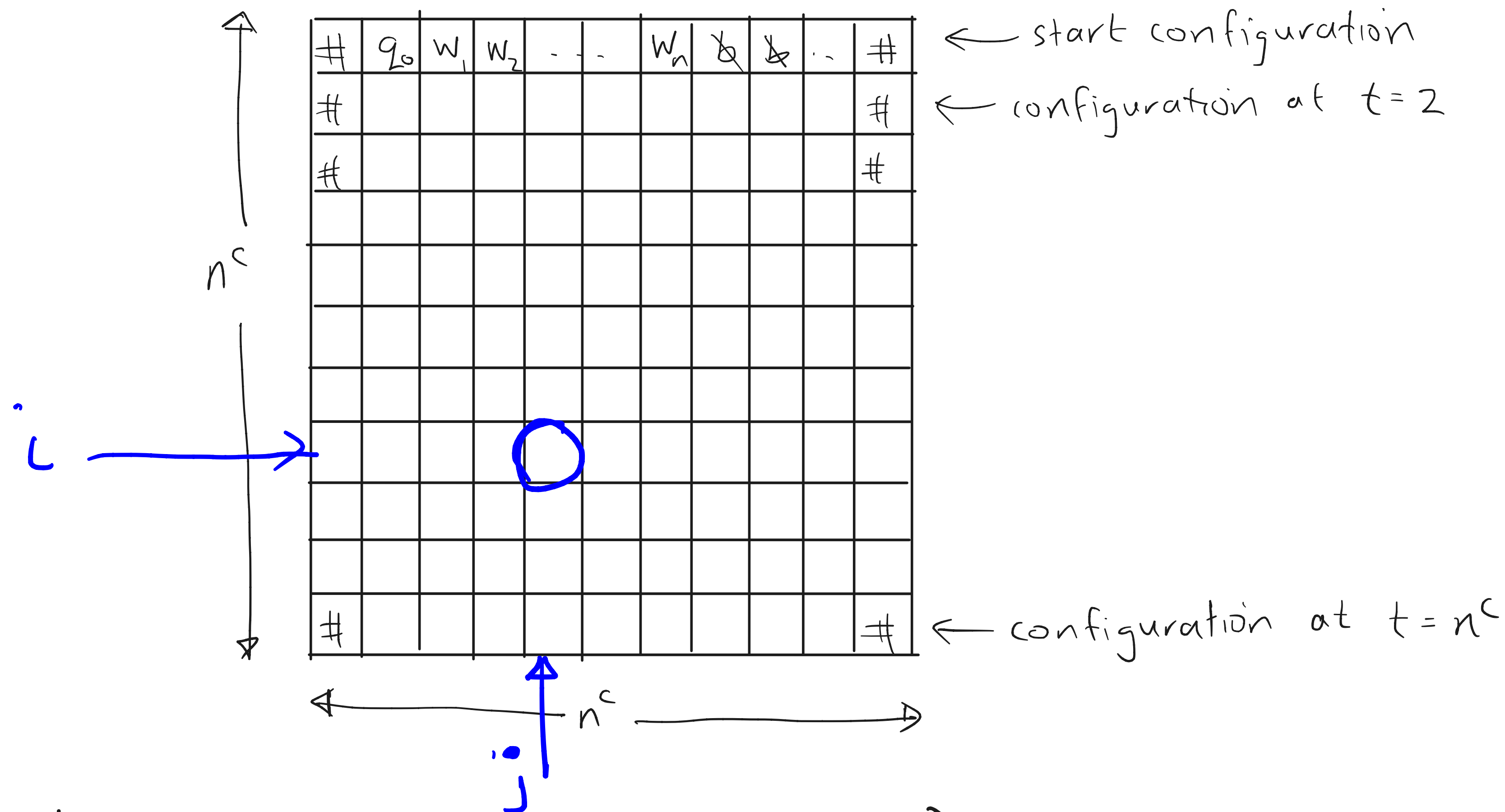
(the state at time t is an accept state

We want $f: \Sigma^* \to \Sigma^*$ such that $\forall w \in \Sigma^*$

w has an accepting tableaux of N iff $f(w) = \phi$ is satisfiable

Cook-Levin Theorem: KSAT is NP-complete

We want $f: w \to \phi$ such that ϕ is satisfiable iff there is an accepting tableaux of N on input w.



Ex: $Q = \{q_0, q_1, q_2\}$ (1, 2, 3)

$\Gamma = \{0, 1, ␣\}$ $\#$ (4, 5, 6, 7)

$\underbrace{x_{i,j,1}, \dots x_{i,j,7}}_{\text{contents of cell } i,j}$

If (i,j) has symbol q_2 in it, then $x_{i,j,3} = 1$

and $\forall k \neq 3$ $x_{i,j,k} = 0$

Variables of ϕ: $x_{i,j,s}$, $i,j \in \{1, \dots, n^c\}$, $s \in Q \cup \Gamma \cup \{\#\}$

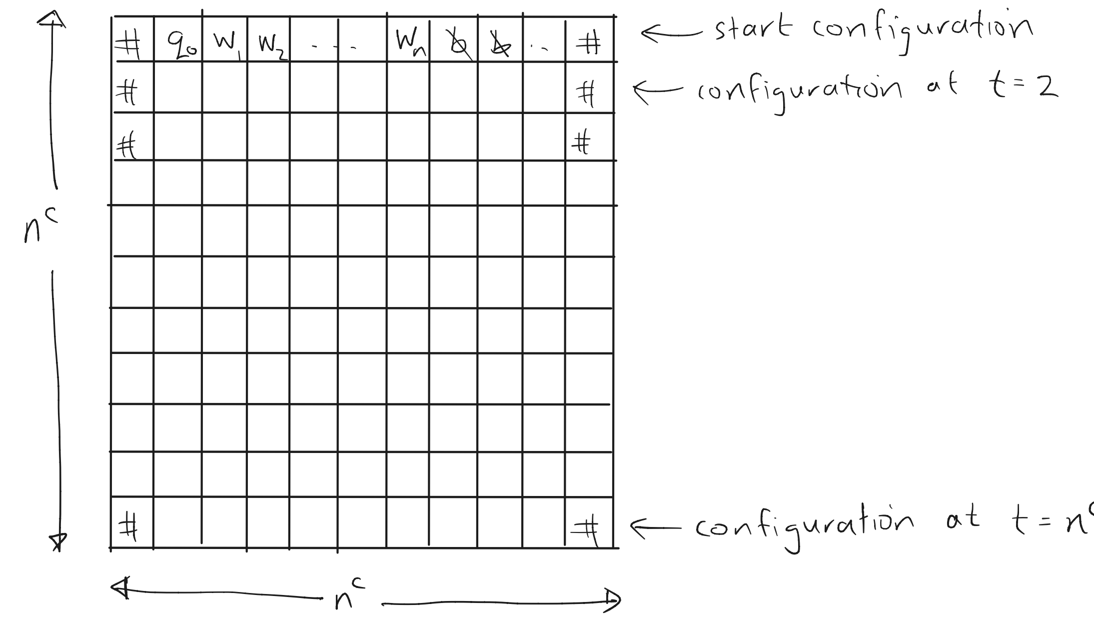
($x_{i,j,s} = 1$ iff cell (i,j) contains symbol s)

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

Q = states of N

Γ = tape alphabet

Cook-Levin Theorem: KSAT is NP-complete



Variables of ϕ: $x_{i,j,s}$, $i,j \in \{1,\dots,n^c\}$, $s \in Q \cup \Gamma \cup \{\#\}$

($x_{i,j,s} = 1$ iff cell (i,j) contains symbol s)

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

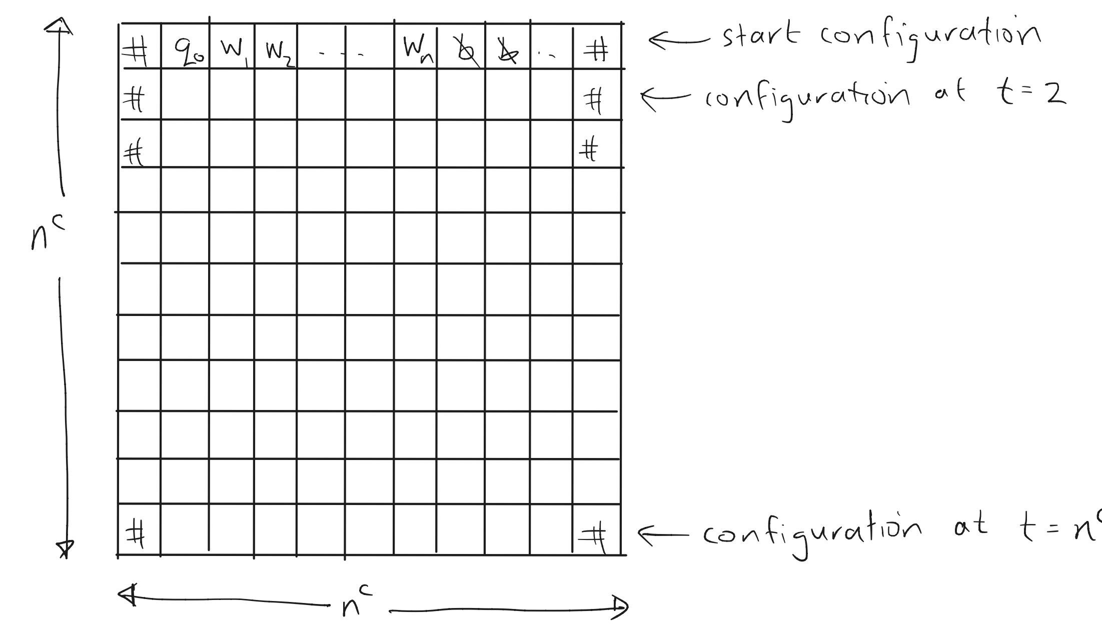
ϕ_{cell}: states that every cell contains exactly one symbol $s \in Q \cup \Gamma \cup \{\#\}$

ϕ_{start}: start config is $\# q_0 w_1 \dots w_n ␣ \dots ␣ \#$

ϕ_{accept}: some cell contains an accept state q_{accept}

ϕ_{move}: each row (configuration at time t) follows from previous row (config at time t-1) by a valid transition according to N's transition function

Cook-Levin Theorem: KSAT is NP-complete



Variables of ϕ: $x_{i,j,s}$, $i,j \in \{1,\dots,n^c\}$, $s \in \underbrace{Q \cup \Gamma \cup \{\#\}}_{C}$

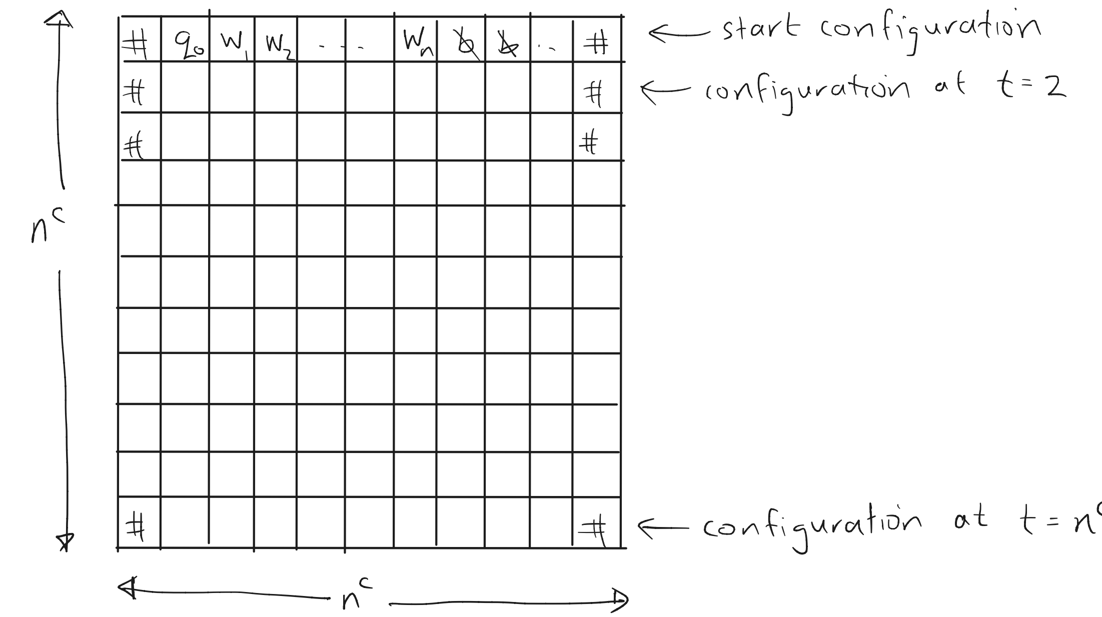
($x_{i,j,s} = 1$ iff cell (i,j) contains symbol s)

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

$\boxed{\phi_{cell}:}$ states that every cell contains exactly one symbol $s \in Q \cup \Gamma \cup \{\#\}$

$$= \bigwedge_{1 \le i,j \le n^c} \left[\left(\bigvee_{s \in C} x_{i,j,s} \right) \wedge \left(\bigwedge_{\substack{s,t \in C \\ s \neq t}} \overline{x_{i,j,s}} \vee \overline{x_{i,j,t}} \right) \right]$$

Cook-Levin Theorem : KSAT is NP-complete



Variables of ϕ : $x_{i,j,s}$, $i,j \in \{1,..,n^c\}$, $s \in Q \cup \Gamma \cup \{\#\}$

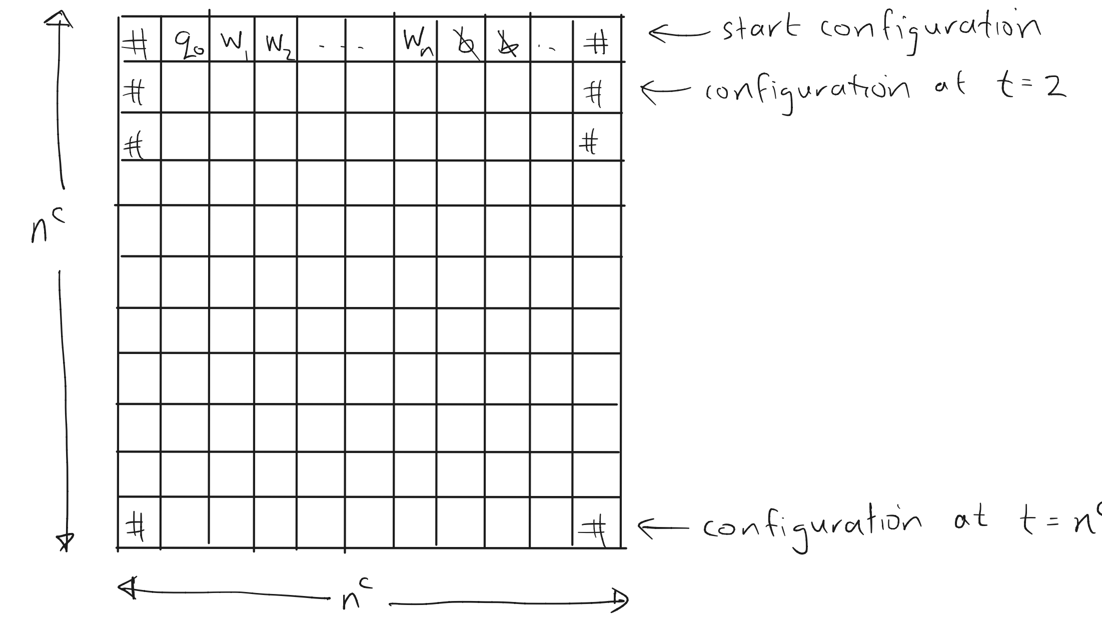
($x_{i,j,s} = 1$ iff cell (i,j) contains symbol s)

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

$\boxed{\phi_{start} :}$ start config is $\# q_0 w_1 \dots w_n \not{b} \dots \not{b} \#$

$$= \underbrace{X_{1,1,\#}}_{\text{starts with }\#} \wedge \underbrace{X_{1,2,q_0}}_{\text{then } q_0} \wedge \underbrace{X_{1,3,w_1} \wedge X_{1,4,w_2} \wedge \dots \wedge X_{1,n+2,w_n}}_{\text{then } w_1 \dots w_n} \wedge \underbrace{X_{1,n+3,\not{b}} \wedge \dots \wedge X_{1,n^c-1,\not{b}}}_{\text{blanks}} \wedge \underbrace{X_{1,n^c,\#}}_{\text{last symbol is }\#}$$

Cook-Levin Theorem : KSAT is NP-complete



Variables of ϕ : $x_{i,j,s}$, $i,j \in \{1,\dots,n^c\}$, $s \in Q \cup \Gamma \cup \{\#\}$

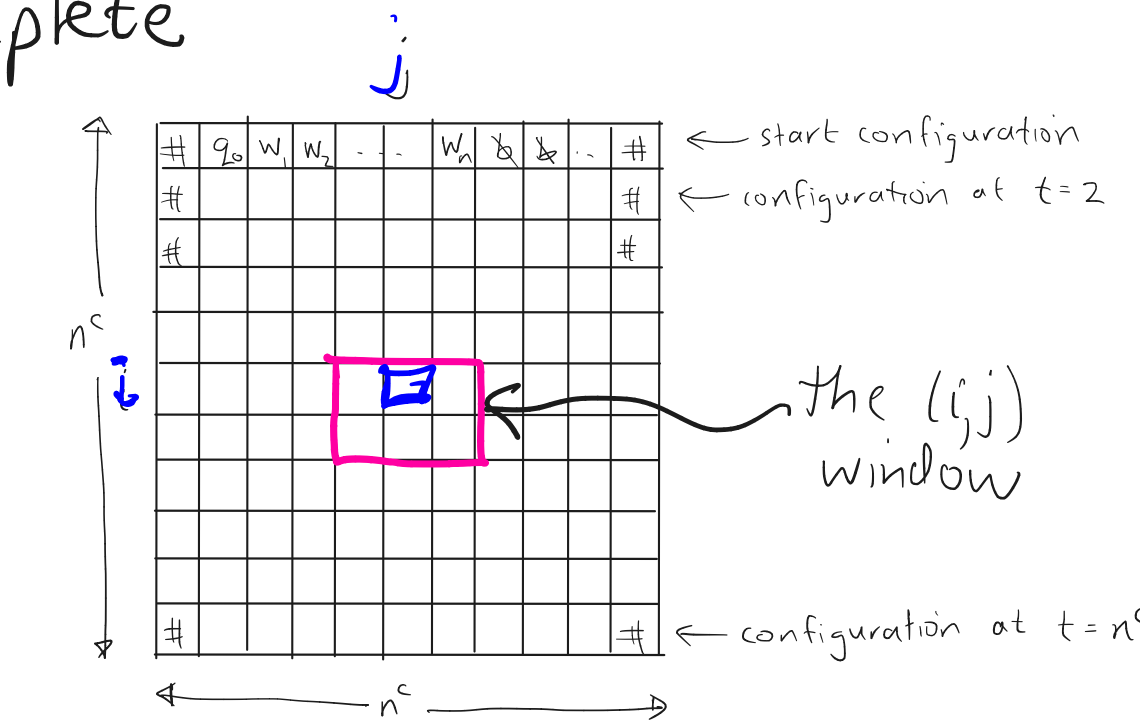
($x_{i,j,s} = 1$ iff cell (i,j) contains symbol s)

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

$\boxed{\phi_{accept}}$: some cell contains an accept state q_{accept}

$$= \bigvee_{1 \le i,j \le n^c} x_{i,j,q_{accept}}$$

Cook-Levin Theorem: KSAT is NP-complete



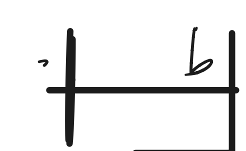
Variables of ϕ: $x_{i,j,s}$, $i,j \in \{1,\dots,n^c\}$, $s \in Q \cup \Gamma \cup \{\#\}$

($x_{i,j,s} = 1$ iff cell (i,j) contains symbol s)

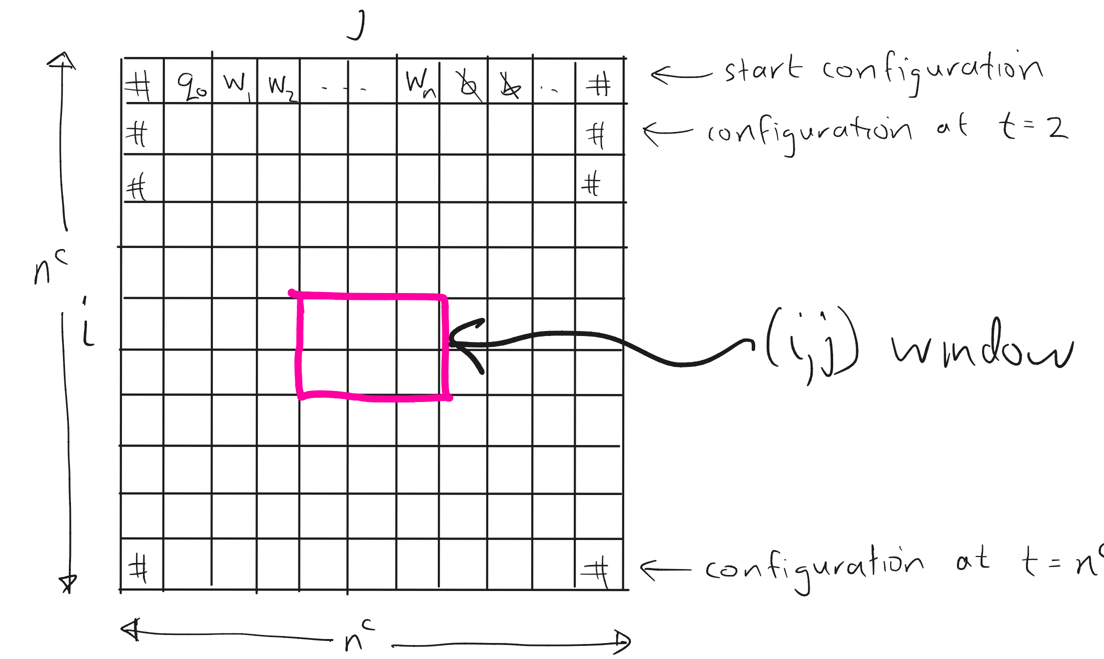
$\phi = \phi_{cell} \wedge \phi_{start} \wedge \boxed{\phi_{move}} \wedge \phi_{accept}$

$\boxed{\phi_{move}:}$ $\bigwedge_{1 \le i,j \le n^c}$ (the (i,j) window is legal)

that is, $\forall (i,j)$ the cell (i,j) is consistent with a legal transition from the configuration at time $i-1$



Cook-Levin Theorem: KSAT is NP-complete



Variables of ϕ : $x_{i,j,s}$, $i,j \in \{1,\dots,n^c\}$, $s \in Q \cup \Gamma \cup \{\#\}$

($x_{i,j,s} = 1$ iff cell (i,j) contains symbol s)

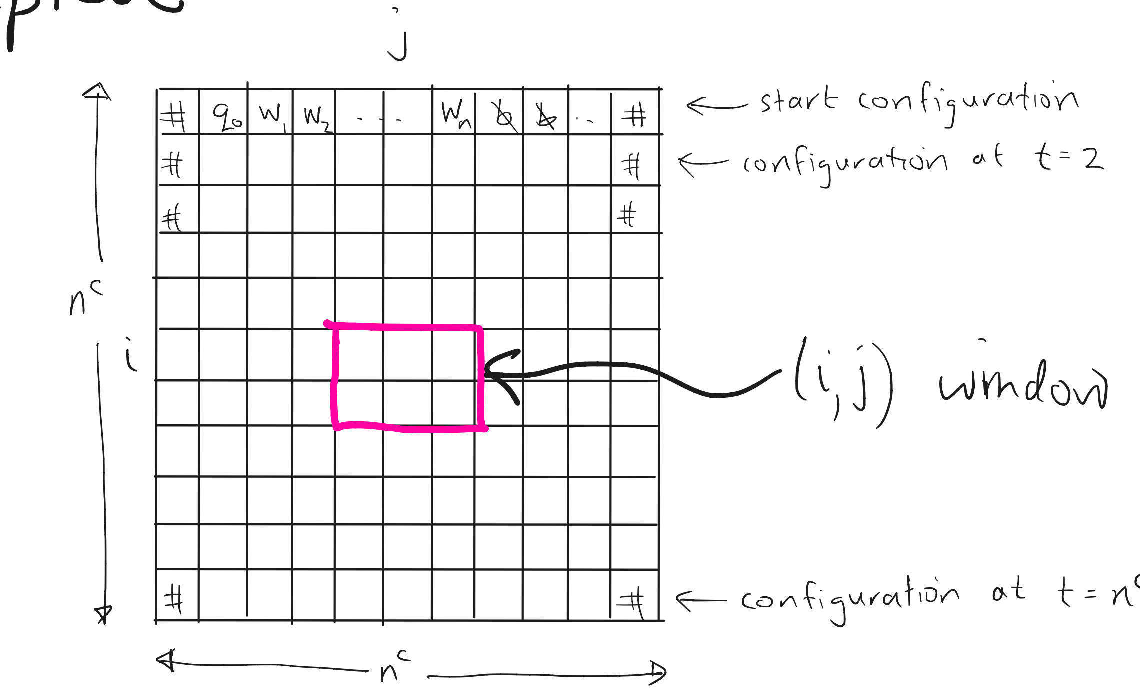
$\phi = \phi_{cell} \wedge \phi_{start} \wedge \boxed{\phi_{move}} \wedge \phi_{accept}$

$\boxed{\phi_{move} :}$ $\quad \bigwedge_{1 \le i,j < n^c}$ (the (i,j) window is legal)

key idea: we can check that entire tableaux is legal by locally checking every 2x3 window

A 2x3 window is legal if it doesn't violate N's transition function.

Cook-Levin Theorem : KSAT is NP-complete



Variables of ϕ : $x_{i,j,s}$, $i,j \in \{1,\dots,n^c\}$, $s \in Q \cup \Gamma \cup \{\#\}$

($x_{i,j,s} = 1$ iff cell (i,j) contains symbol s)

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

$\boxed{\phi_{move} :}$ $\bigwedge_{1 \le i,j \le n^c}$ (the (i,j) window is legal)

Example: $\delta(q_1, a) = \{(q_1, b, R)\}$, $\delta(q_1, b) = \{(q_2, c, L), (q_2, a, R)\}$

Legal windows:

a	q_1	b
q_2	a	c

a	q_1	b
a	a	q_2

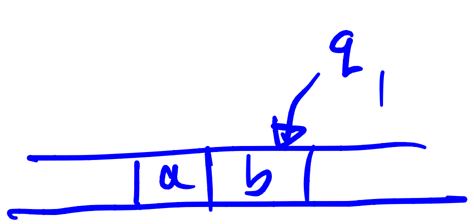
a	a	q_1
a	a	b

#	b	a
#	b	a

a	b	a
a	b	q_2

b	b	b
c	b	b

Corresponds to:



Some Illegal Windows :

a	b	a
a	a	a

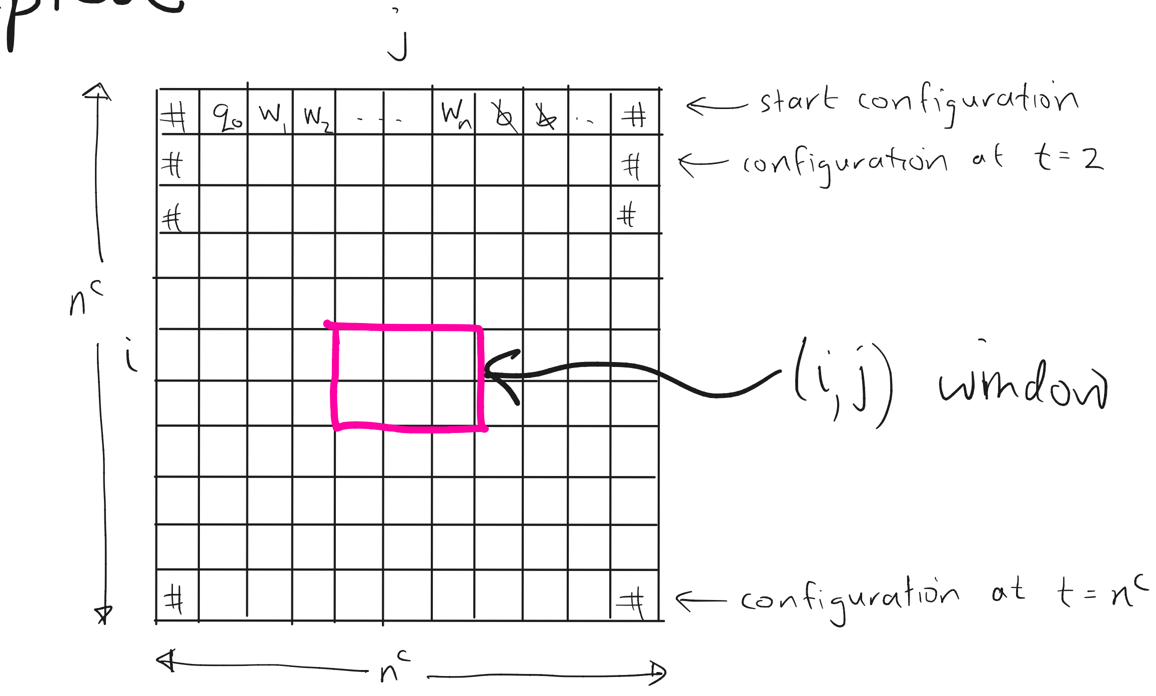
a	q_1	b
q_1	a	a

b	q_1	b
q_2	b	q_2

q_1	q_2	a
a	b	c

also illegal

Cook-Levin Theorem : KSAT is NP-complete

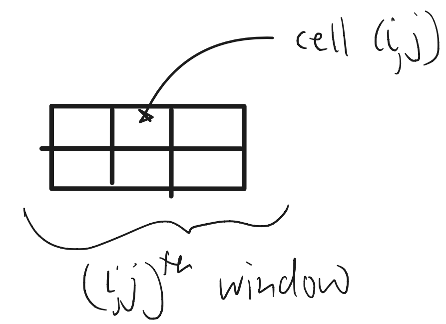


Variables of ϕ : $x_{i,j,s}$, $i,j \in \{1, .., n^c\}$, $s \in Q \cup \Gamma \cup \{\#\}$

($x_{i,j,s} = 1$ iff cell (i,j) contains symbol s)

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

$\boxed{\phi_{move}:}$ $\bigwedge_{1 \leq i,j \leq n^c}$ (the (i,j) window is legal)



$$\phi_{move} = \bigwedge_{1 \leq i,j \leq n^c} \left(\text{the } (i,j)^{th} \text{ window is legal}\right)$$

$$= \bigwedge_{1 \leq i,j \leq n^c} \ \bigvee_{\substack{a_1 a_2 \ldots a_6 \\ \text{is a legal} \\ \text{window}}} \left(x_{i-1,j,a_1} \wedge x_{i,j,a_2} \wedge x_{i+1,j,a_3} \wedge x_{i-1,j+1,a_4} \wedge x_{i,j+1,a_5} \wedge x_{i+1,j+1,a_6} \right)$$

__Claim__ (Claim 7.31 in book)

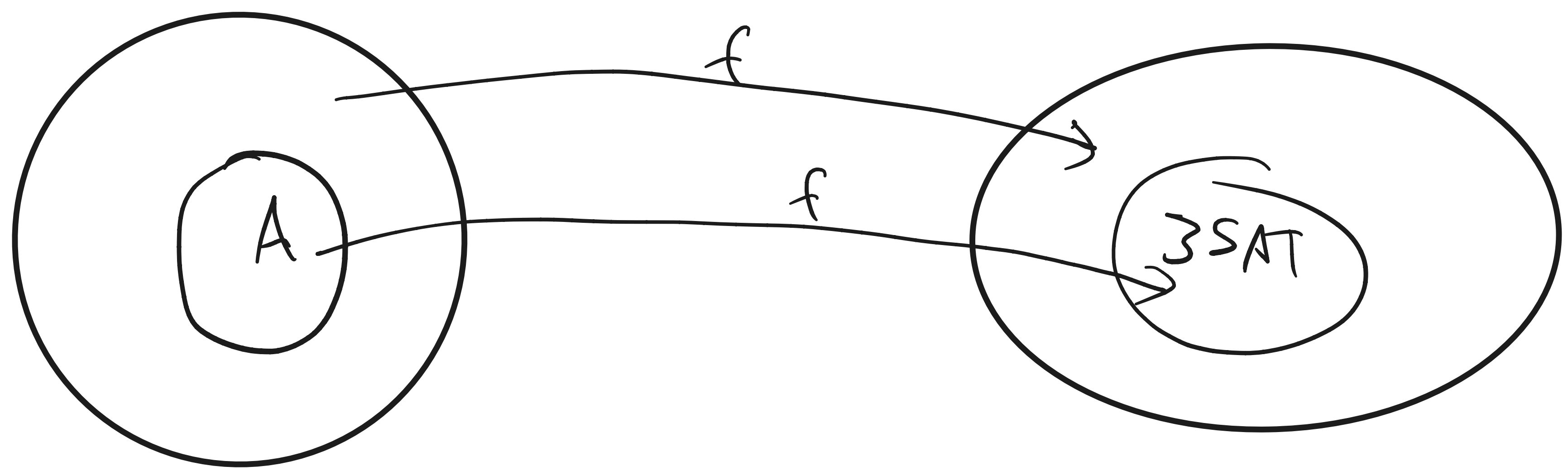
If top row ($i=1$) is the start configuration and every window in the table is legal, then at every time $i \geq 0$, the i^{th} row is a configuration that legally follows from the previous one (at time $i-1$).

Cook-Levin Theorem: KSAT is NP-complete

We want to show: $\forall A \in NP \quad A \leq_p 3SAT$

Let $A \in NP$. We need to define a poly-time function $f: \Sigma^* \to \Sigma^*$

$f(w) \to \phi$



Variables of ϕ: $x_{i,j,s}$, $i,j \in \{1, \ldots, n^c\}$, $s \in Q \cup \Gamma \cup \{\#\}$

($x_{i,j,s} = 1$ iff cell (i,j) contains symbol s)

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