18.404/6.840 Lecture 16

Last time:

- NP-completeness
- $3SAT \leq_{\mathrm{P}} CLIQUE$
- $3SAT \leq_{\mathrm{P}} HAMPATH$

Today:

- Cook-Levin Theorem: SAT is NP-complete
- $3SAT$ is NP-complete

Quick Review

Defn: B is NP-complete if

1) $B \in \mathrm{NP}$
2) For all $A \in \mathrm{NP}$, $A \leq_{\mathrm{P}} B$

If B is NP-complete and $B \in \mathrm{P}$ then $\mathrm{P} = \mathrm{NP}$.

Importance of NP-completeness

1) Evidence of computational intractability.
2) Gives a good candidate for proving $\mathrm{P} \neq \mathrm{NP}$.

To show some language C is NP-complete, show $3SAT \leq_{\mathrm{P}} C$.

or some other previously shown NP-complete language

Check-in 16.1

The big sigma notation means summing over some set.

$$\sum_{1 \leq i \leq n} i = 1 + 2 + \cdots + n$$

The big AND (or OR) notation has a similar meaning.

For example, if $x = x_1 \cdots x_n$ and $y = y_1 \cdots y_n$ are two strings of length n, when does the following hold?

$$\left(\bigwedge_{1 \leq i \leq n} x_i = y_i \right) = \textsc{True}$$

(a) Whenever x and y agree on some symbol.

(b) Whenever $x = y$.

Check-in 16.1

Cook-Levin Theorem (idea)

Theorem: SAT is NP-complete

Proof: 1) $SAT \in NP$ (done)

2) Show that for each $A \in NP$ we have $A \leq_P SAT$:

Let $A \in NP$ be decided by NTM M in time n^k.

Give a polynomial-time reduction f mapping A to SAT.

$f\colon \Sigma^* \to$ formulas

$f(w) = \langle \phi_{M,w} \rangle$

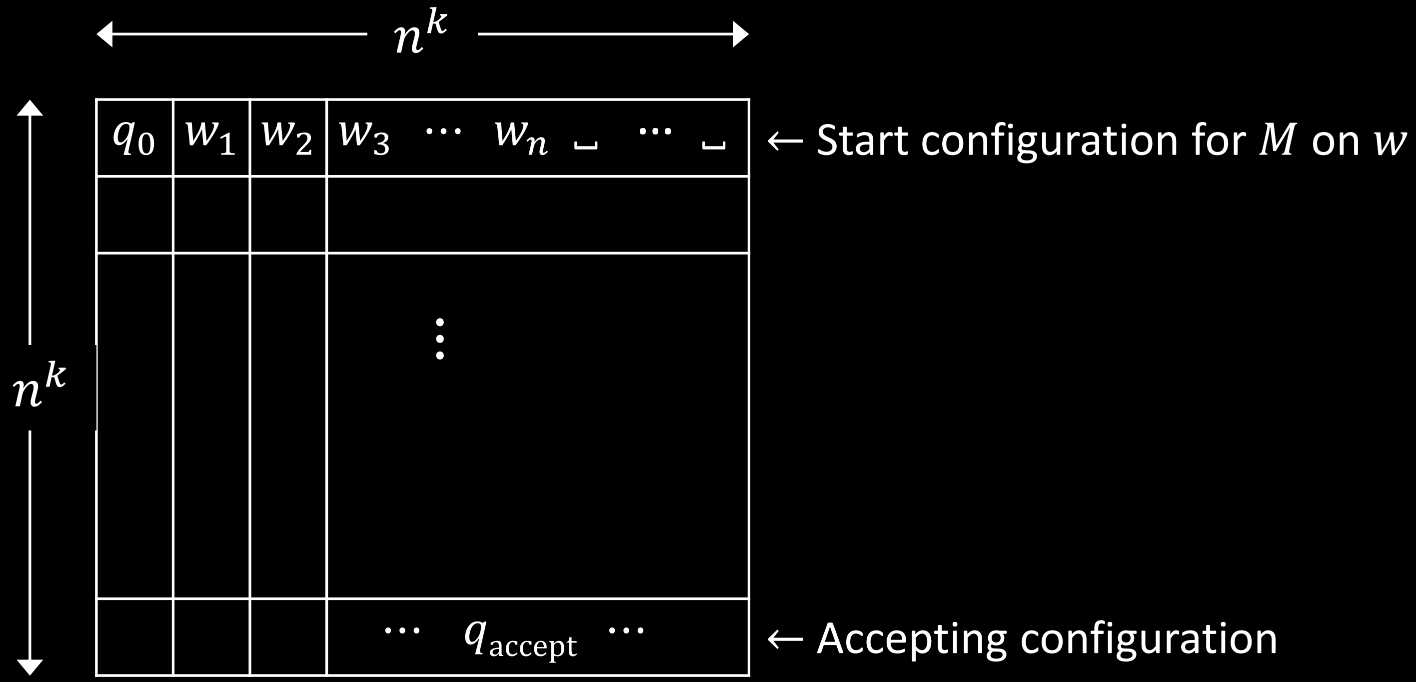
$w \in A$ iff $\phi_{M,w}$ is satisfiable

Idea: $\phi_{M,w}$ simulates M on w. Design $\phi_{M,w}$ to "say" M accepts w.

Satisfying assignment to $\phi_{M,w}$ is a computation history for M on w.

Tableau for M on w

Defn: An (accepting) tableau for NTM M on w is an $n^k \times n^k$ table representing an computation history for M on w on an accepting branch of the nondeterministic computation.

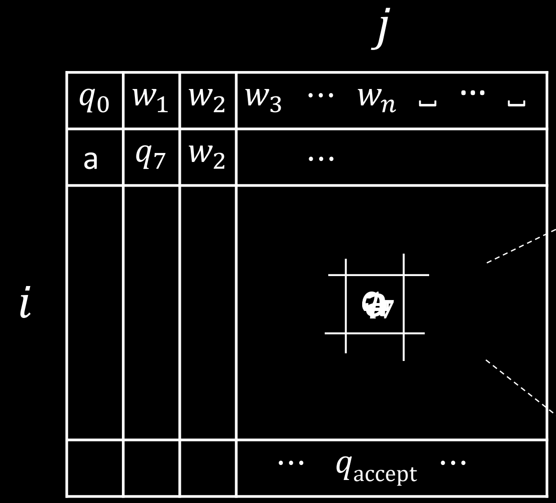


Construct $\phi_{M,w}$ to “say” M accepts w.

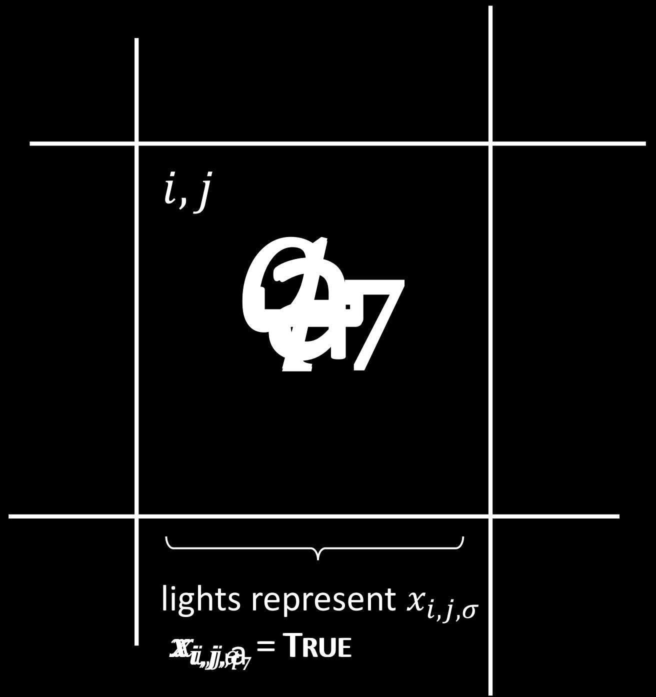
$\phi_{M,w}$ “says” a tableau for M on w exists.

$\phi_{M,w} = \phi_{\text{cell}} \wedge \phi_{\text{start}} \wedge \phi_{\text{move}} \wedge \phi_{\text{accept}}$

Constructing $\phi_{M,w}$: ϕ_{cell}



Cell i, j can contain any symbol in $\Gamma \cup Q$



The variables of $\phi_{M,w}$ are $x_{i,j,\sigma}$ for $1 \leq i, j \leq n^k$ and $\sigma \in \Gamma \cup Q$.

$x_{i,j,\sigma}$ = TRUE means cell i, j contains σ.

Check-in 16.2

How many variables does $\phi_{M,w}$ have?
Recall that $n = |w|$.

(a) $O(n)$
(b) $O(n^2)$
(c) $O(n^k)$
(d) $O(n^{2k})$

Check-in 16.2

Constructing $\phi_{M,w}$: ϕ_{start} and ϕ_{accept}

	1	2	3	$\cdots\cdots$ n^k	
1	q_0	w_1	w_2	w_3 $\cdots$ w_n ␣ $\cdots$ ␣	← Start configuration
	a	q_7	w_2	$\cdots$	
n^k				$\cdots$ q_{accept} $\cdots$	← Accepting configuration

$\phi_{M,w}$ "says" a tableau for M on w exists.

$$\phi_{M,w} = \phi_{\text{cell}} \wedge \phi_{\text{start}} \wedge \phi_{\text{move}} \wedge \phi_{\text{accept}}$$

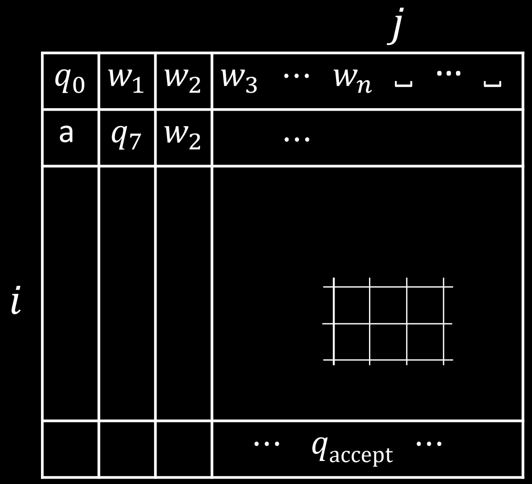
ϕ_{cell} done ✓

$\phi_{\text{start}} =$

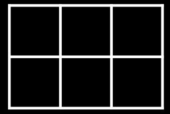
$$\phi_{\text{accept}} = \bigvee_{1 \le j \le n^k} x_{n^k, j, q_{\text{accept}}}$$


Coffee Break

Constructing $\phi_{M,w}$: ϕ_{move}



2×3 neighborhood



$\phi_{M,w}$ "says" a tableau for M on w exists.

$\phi_{M,w} = \phi_{\text{cell}} \wedge \phi_{\text{start}} \wedge \phi_{\text{move}} \wedge \phi_{\text{accept}}$

✓ ✓ ✓

Legal neighborhoods: consistent with M's transition function

potential examples:

a	q_7	b
q_3	a	c

a	b	c
a	b	c

a	b	c
a	b	q_5

a	b	c
d	b	c

Illegal neighborhoods: not consistent with M's transition function

examples:

a	b	c
a	d	c

a	b	c
a	q_2	c

a	q_7	c
a	b	c

a	q_7	c
q_3	d	q_4

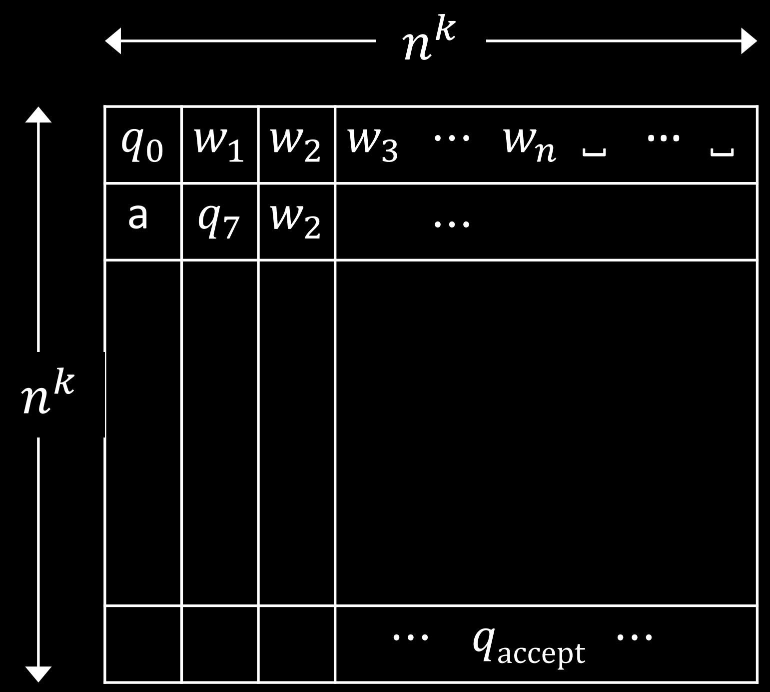
Claim: If every 2×3 neighborhood is legal then tableau corresponds to a computation history.

$$\phi_{\text{move}} = \bigwedge_{1<i,j<n^k} \left(\bigvee_{\text{Legal}} \left(x_{i,j-1,r} \wedge x_{i,j,s} \wedge x_{i,j+1,t} \wedge x_{i+1,j-1,v} \wedge x_{i+1,j,y} \wedge x_{i+1,j+1,z} \right) \right)$$

Says that the neighborhood at i, j is legal

r	s	t
v	y	z

Conclusion: SAT is NP-complete



Summary:

For $A \in$ NP, decided by NTM M,
we gave a reduction f from A to SAT:

$f\colon \Sigma^* \rightarrow$ formulas

$f(w) = \langle \phi_{M,w} \rangle$

$w \in A$ iff $\phi_{M,w}$ is satisfiable.

$$\phi_{M,w} = \phi_{\text{cell}} \wedge \phi_{\text{start}} \wedge \phi_{\text{move}} \wedge \phi_{\text{accept}}$$

The size of $\phi_{M,w}$ is roughly the size of the tableau for M on w, so size is $O\left(n^k \times n^k\right) = O\left(n^{2k}\right)$.

Therefore f is computable in polynomial time.

$3SAT$ is NP-complete

a	b	a ∨ b = c	
1	1	1	$(a \land b) \rightarrow c$
0	1	1	$(\bar{a} \land b) \rightarrow c$
1	0	1	$(a \land \bar{b}) \rightarrow c$
0	0	0	$(\bar{a} \land \bar{b}) \rightarrow \bar{c}$

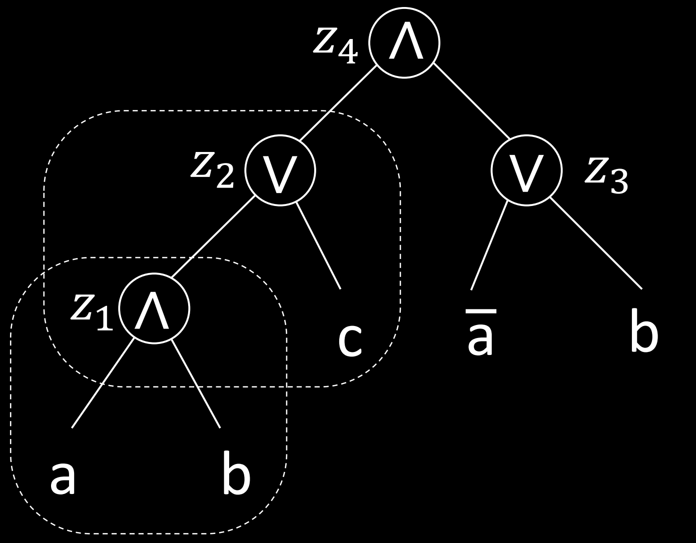
Theorem: $3SAT$ is NP-complete

Proof: Show $SAT \leq_P 3SAT$

Give reduction f converting formula ϕ to 3CNF formula ϕ', <u>preserving satisfiability</u>.
(Note: ϕ and ϕ' are not logically equivalent)

Example: Say $\phi = \big((a \land b) \lor c\big) \land (\bar{a} \lor b)$

Tree structure for ϕ:



Logical equivalence: $(A \rightarrow B)$ and $(\bar{A} \lor B)$ $\overline{(A \land B)}$ and $(\bar{A} \lor \bar{B})$

$$\phi' = \big((a \land b) \rightarrow z_1\big) \land \big((\bar{a} \land b) \rightarrow \bar{z_1}\big) \land \big((a \land \bar{b}) \rightarrow \bar{z_1}\big) \land \big((\bar{a} \land \bar{b}) \rightarrow \bar{z_1}\big)$$

$$\land \big((z_1 \land c) \rightarrow z_2\big) \land \big((\bar{z_1} \land c) \rightarrow z_2\big) \land \big((z_1 \land \bar{c}) \rightarrow z_2\big) \land \big((\bar{z_1} \land \bar{c}) \rightarrow \bar{z_2}\big)$$

⋮ repeat for each z_i

$\land \ (z_4)$

Check-in 16.3

If ϕ has k operations (∧ and ∨), how many clauses has ϕ'?

(a) $k + 1$

(b) $4k + 1$

(c) k^2

(d) $2k^2$

Check-in 16.3

Quick review of today

1. SAT is NP-complete
2. $3SAT$ is NP-complete