18.404/6.840 Lecture 16

Last time:

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

Today: (Sipser §7.4)

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

Quick Review

Defn: B is NP-complete if

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

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

Importance of NP-completeness

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

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

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?

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

(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.

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

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

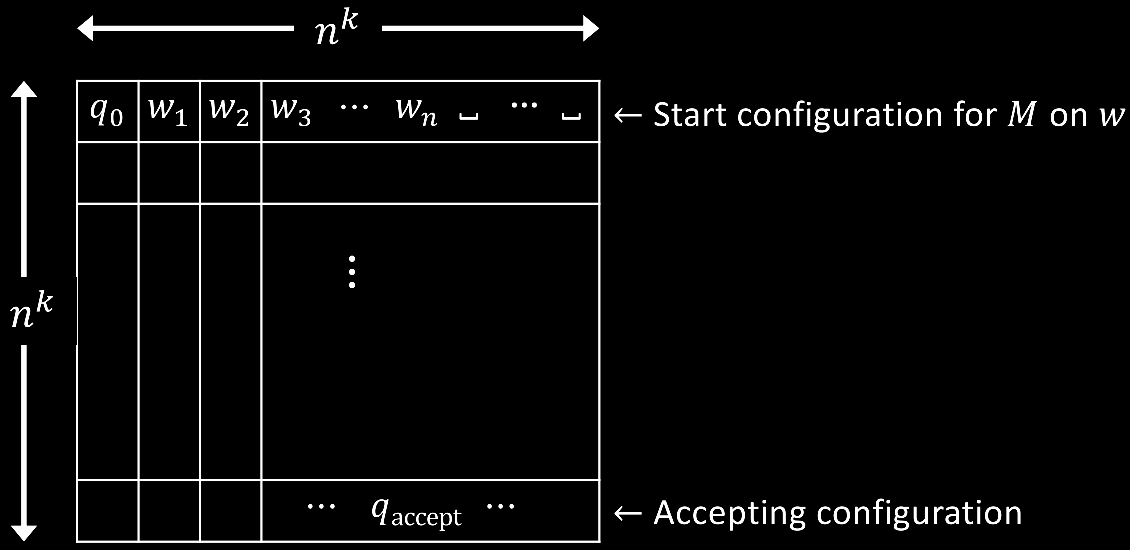
$w \in A$ iff $\phi_{M,w}$ is satisfiable

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.



← Start configuration for M on w

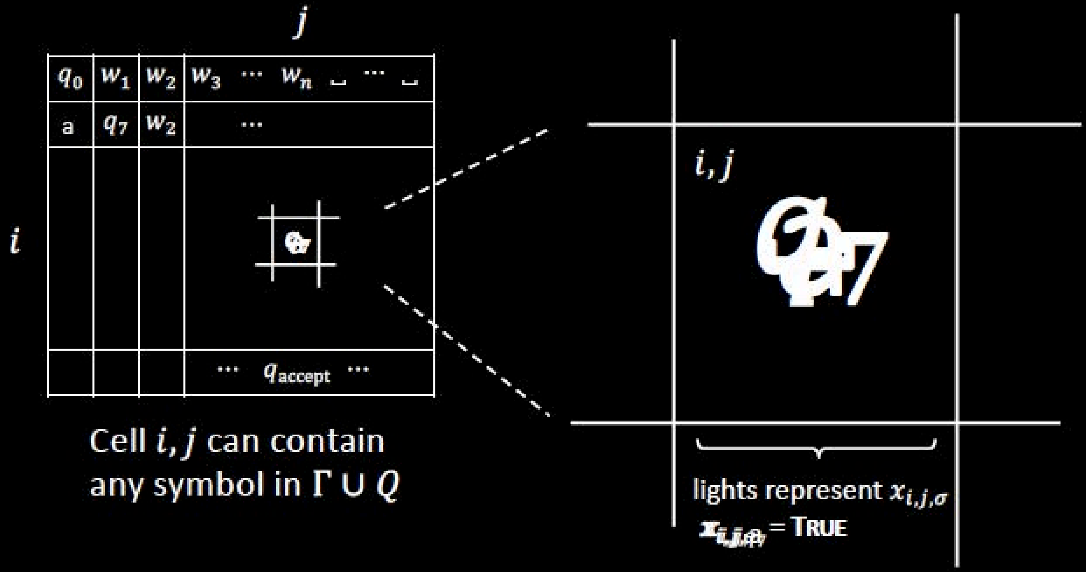
← Accepting configuration

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 $\sigma \in \Gamma \cup Q$.

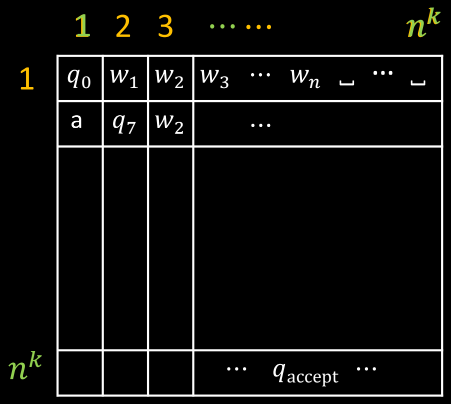
$x_{i,j,\sigma} =$ TRUE means cell i,j contains σ.

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) $O(n^{2k})$

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 ␣ $\cdots$ ␣
	a	q_7	w_2	$\cdots$
n^k				$\cdots$ q_{accept} $\cdots$

← Start configuration

← Accepting configuration

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

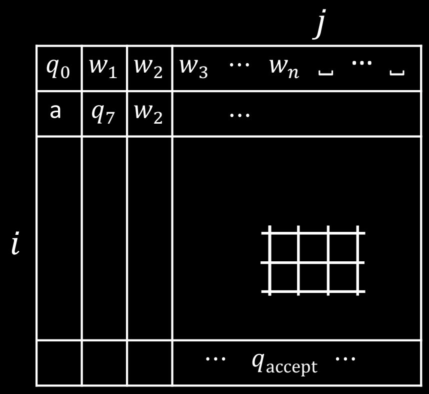
$$\phi_{M,w} = \phi_{\text{cell}} \wedge \phi_{\text{start}} \wedge \phi_{\text{move}} \wedge \phi_{\text{accept}}$$

ϕ_{cell} done ✓

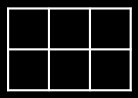
$\phi_{\text{start}} =$

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

Constructing $\phi_{M,w}$: ϕ_{move}



2×3 neighborhood



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

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

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

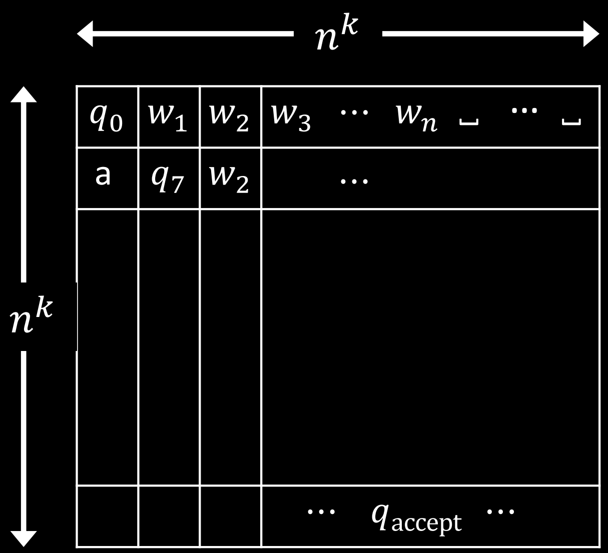
a	q_7	c
q_3	d	q_4

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

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

Says that the neighborhood at i, j is legal

Conclusion: SAT is NP-complete



q_0	w_1	w_2	w_3 $\cdots$ w_n ␣ $\cdots$ ␣
a	q_7	w_2	$\cdots$
			$\cdots$ q_{accept} $\cdots$

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

$$f: \Sigma^* \rightarrow \text{formulas}$$
$$f(w) = \langle \phi_{M,w} \rangle$$

$w \in A$ 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 $O(n^k \times n^k) = O(n^{2k})$.

Therefore f is computable in polynomial time.

$3SAT$ is NP-complete

a	b	a ∨ b = c	
1	1	1	$(a \land b) \to c$
0	1	1	$(\overline{a} \land b) \to c$
1	0	1	$(a \land \overline{b}) \to c$
0	0	0	$(\overline{a} \land \overline{b}) \to \overline{c}$

Theorem: $3SAT$ is NP-complete

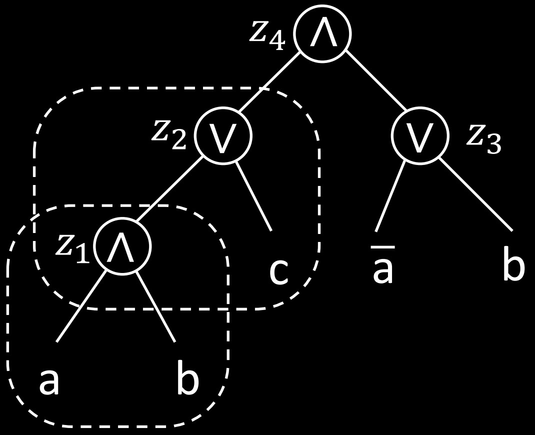
Proof: Show $SAT \leq_P 3SAT$

Give reduction f converting formula ϕ to 3CNF formula ϕ', preserving satisfiability.

(Note: ϕ and ϕ' are not logically equivalent)

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

Tree structure for ϕ:



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

$\phi' = ((a \land b) \to z_1) \land ((\overline{a} \land b) \to \overline{z_1}) \land ((a \land \overline{b}) \to \overline{z_1}) \land ((\overline{a} \land \overline{b}) \to \overline{z_1})$

$\land\ ((z_1 \land c) \to z_2) \land ((\overline{z_1} \land c) \to z_2) \land ((z_1 \land \overline{c}) \to z_2) \land ((\overline{z_1} \land \overline{c}) \to \overline{z_2})$

⋮ 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

18.404J / 18.4041J / 6.840J Theory of Computation
Fall 2020