We must construct a reduction that works as follows:

> On input w, we build ϕ_w such that $w \in A \iff \phi_w$ is satisfiable; i.e., $f(\langle w \rangle) = \langle \phi_w \rangle$.

We construct ϕ_w based on the accepting table insight: the variables are x_{ijs}, where x_{ijs} is true if position (i, j) in the table contains symbol $s \in Q \cup \Gamma \cup \{\#\}$.

Then,

$$\phi_w = \phi_{\text{cell}} \wedge \phi_{\text{start}} \wedge \phi_{\text{move}} \wedge \phi_{\text{accept}}$$

where the first ensures that only one symbol is assigned to each cell, the second ensures that the first row of the table is the initial configuration, i.e.,

$$\# q_0 w_1 w_2 \ldots w_n \sqcup \sqcup \ldots \sqcup \#$$

B is **NP**-complete if it is in **NP**, and for every $A \in \mathbf{NP}$, $A \leq_{\mathrm{L}} B$.

Theorem: If B is **NP**-complete, and $B \in \mathbf{P}$, then **P**=**NP**.

Theorem: If B is **NP**-complete, and $B \leq_{\mathrm{L}} C$, for $C \in \mathbf{NP}$, then C is **NP**-complete.

Theorem [Cook-Levin]: SAT is **NP**-complete.

Proof: If $A \in \mathbf{NP}$, then $A = L(N)$, where N is a nondet TM that runs in time n^k.

$\therefore$ each config of N can be described with a string of length n^k.

Any branch of computation has length at most n^k. So any branch can be described with an $n^k \times n^k$ table.

To determine whether N accepts w, we must determine if an accepting table exists.

Corollary: 3SAT is **NP**-complete.

Proof: ϕ_w can be given in 3CNF, using tricks such as $(a_1 \vee a_2 \vee \ldots \vee a_n)$ is "equivalent" to:

$$(a_1 \vee a_2 \vee z_1) \wedge (\overline{z}_1 \vee a_3 \vee z_2) \wedge (\overline{z}_2 \vee a_4 \vee z_3) \wedge \ldots \wedge (\overline{z}_{n-3} \vee a_{n-1} \vee a_n)$$

Now we can show that many others are **NP**-complete:

CLIQUE
VERTEX-COVER
HAMPATH
SUBSET-SUM
TRAVELLING-SALESMAN

ϕ_{accept} ensures that the last row is an accepting row (need a trick: once we get an accepting row, we repeat it until we reach the n^k-th row). It is easy to give it:

$$\bigvee_{1 \leq i,j \leq n^k} x_{ijq_{\text{accept}}}$$

ϕ_{move} ensures that each row follows from the previous by a legal move (or, in the case that the previous row was accepting, the next one is its copy).

This is easy to implement, because each row is exactly like the previous one, except in the four squares surrounding the state.

Claim: ϕ_w can be constructed in log-space in $|w|$. QED.

A QBF is fully quantified if it has no free variables.

TQBF $= \{\langle\phi\rangle \mid \phi$ is a true QBF $\}$

Theorem: TQBF is **PSPACE**-complete

Proof: TQBF $\in$ **PSPACE**: try all the assignments recursively.

Let A be any language decided by TM M in space n^k. We show $A \leq_{\mathrm{L}}$ TQBF.

Let $\phi_{\mathbf{c}_1,\mathbf{c}_2,t}$ be a QBF, where:

$\mathbf{c}_1, \mathbf{c}_2$ are two groups of variables representing configurations of M on a particular w ($|w| = n$),

and t is a parameter denoting the number of steps of M, so $t \leq 2^{O(n^k)}$.

We show how to construct $\phi_{\mathbf{c}_1,\mathbf{c}_2,t}$.

A **Quantified Boolean Formula**:

1. p
2. $\alpha \vee \beta, \alpha \wedge \beta, \neg\alpha$
3. $\forall x\alpha, \exists x\alpha$

Semantically, $\exists x\alpha(x) \equiv (\alpha(0/x) \vee \alpha(1/x))$, and $\forall x\alpha(x) \equiv (\alpha(0/x) \wedge \alpha(1/x)$.

The advantage of these boolean quantifiers is succinctness, not increased power of expressability. For example, $\exists x_1 \exists x_2 \ldots \exists x_n \alpha(x_1, x_2, \ldots, x_n)$ is equivalent to

$$\bigvee_{a_1 a_2 \ldots a_n \in \{0,1\}^n} \alpha(a_1/x_1, a_2/x_2, \ldots, a_n/x_n)$$

Games

Formula game: $\phi = \exists x_1 \forall x_2 \exists x_3 \ldots Q x_k [\psi]$.

FORMULA-GAME $= \{\langle\phi\rangle |$ Player E has winning strategy $\}$

A winning strategy (for player E) is a choice of x_1 such that no matter what player A chooses for x_2, E can choose a value for x_3, such that no mater what A chooses for x_4, etc., ϕ is made true by the resulting assignment.
FORMULA-GAME is **PSPACE**-complete.

Geography: Peoria $\rightarrow$ Amherst $\rightarrow$ Tucson $\rightarrow$ Nashua ...

GG (Generalized Geography) is a directed graph, with a designated starting node, and Player I selects an edge out of the start node, and then Player II selects an edge out of that node, etc. The looser has nowhere to go (cannot repeat nodes).
GG is **PSPACE**-complete.

$\phi_{\mathbf{c}_1,\mathbf{c}_2,1}$ is quantifier-free, and formalizes the notion that $\mathbf{c}_1, \mathbf{c}_2$ are either the same config, or $\mathbf{c}_1 \rightarrow \mathbf{c}_2$. (Recall ϕ_{move}.)

For $t > 1$, we build our formula recursively as follows: $\phi_{\mathbf{c}_1,\mathbf{c}_2,t}$ is

$$\exists \mathbf{m}_1 [\phi_{\mathbf{c}_1,\mathbf{m}_1,\lceil \frac{t}{2} \rceil} \wedge \phi_{\mathbf{m}_1,\mathbf{c}_2,\lceil \frac{t}{2} \rceil}]$$

$$\equiv \exists \mathbf{m}_1 \forall \mathbf{x} \forall \mathbf{y} [\left\{ \begin{array}{c} \mathbf{x} \Leftrightarrow \mathbf{c}_1 \wedge \mathbf{y} \Leftrightarrow \mathbf{m}_1 \\ \vee \\ \mathbf{x} \Leftrightarrow \mathbf{m}_1 \wedge \mathbf{y} \Leftrightarrow \mathbf{c}_2 \end{array} \right\} \supset \phi_{\mathbf{x},\mathbf{y},\lceil \frac{t}{2} \rceil}]$$

$\therefore w \in A \iff \langle \phi_{\mathbf{c}_{\text{start}},\mathbf{c}_{\text{accept}},2^{O(n^k)}} \rangle \in \text{TQBF}$

Corollary: TQBF $\notin$ **NL**

Proof: By the hierarchy theorem, **NL** $\subsetneq$ **PSPACE**.

Relativization

An **oracle** is a language A. An **oracle TM** M^A is an ordinary TM with an extra tape called the **oracle tape**.

M writes a string on the oracle tape, queries the oracle, and gets the answer in one step.

Let $\mathbf{P}^A$ and $\mathbf{NP}^A$ be the set of languages decidable with polytime det (respectively, nondet) TMs with an oracle for A.

Ex. $\mathbf{NP}, \textbf{co-NP} \subseteq \mathbf{P}^{\mathrm{SAT}}$.

Ex. NON-MIN-FORMULA =
$\{\langle\phi\rangle |\ \phi$ is not a minimal Boolean formula $\}$ is in $\mathbf{NP}^{\mathrm{SAT}}$.
(Non-equiv of Boolean formulas is in **NP**, so equiv is in **co-NP**, so a nondet TM can guess a smaller ϕ' and test using the oracle that $\phi' \equiv \phi$.)

So, $\mathbf{NP}^{\mathrm{SAT}}$ is believed to be bigger than **NP**.

Recall that regular expressions are built up from $\emptyset, \varepsilon, a \in \Sigma$, by using the regular operations $\cup, \circ, *$.

The language $\mathrm{EQ}_{\mathrm{REX}}$ given by
$\{\langle R, S\rangle |\ R, S$ are reg. exp. and $L(R) = L(S)\}$ is in **PSPACE**.

Introduce an exponentiation operator, $R^k = R \uparrow k = R \circ R \circ \cdots \circ R$.

Let $\mathrm{EQ}_{\mathrm{REX}\uparrow}$ be like the set above except we allow regular expressions with exponentiation.

Theorem: $\mathrm{EQ}_{\mathrm{REX}\uparrow}$ is EXPSPACE-complete.

Corollary: $\mathrm{EQ}_{\mathrm{REX}\uparrow}$ is *intractable*.

Proof of Cor: If it were in **P**, then it would certainly be in **PSPACE**, but by completeness it would follow that **EXPSPACE** $\subseteq$ **PSPACE**, contradicting the separation we obtained from the (Space) Hierarchy Theorems.

Let $M_1^{\sqcup}, M_2^{\sqcup}, M_3^{\sqcup}, \ldots$, be a list of polytime oracle TMs.
Arrange it so that $M_i^{\sqcup}$ runs in time n^i (how?)
We build A in stages to ensure that $L(M_i^A) \neq L_A$.

At **stage i** A is finite, so we pick n such that $n > |w|$ for all $w \in A$, and $2^n > n^i$ (running time of $M_i^{\sqcup}$).

We now extend A in such a way so that $L(M_i^A) \neq L_A$

Run $M_i(1^n)$: each time M_i queries the oracle with a string y, if $y \overset{?}{\in} A$ has been determined, we do nothing to A. (Note that all the strings whose status has been determined are shorter than n.)

If y's status is undetermined, we answer NO (i.e., declare $y \notin A$).

If $M_i(1^n) =$ yes, declare all remaining y, $|y| = n$, not in A. If $M_i(1^n) =$ no, find a y_0 such that $|y_0| = n$, and y_0 has not been queried (it must exist, because in n^i time M_i cannot query all $2^n > n^i$ y's of length n), and put y_0 in A. $\underline{M_i(1^n) = \text{yes iff } 1^n \notin L_A}$.

Theorem: There exist oracles A, B such that:
(i) $\mathbf{P}^A \neq \mathbf{NP}^A$ and (ii) $\mathbf{P}^B = \mathbf{NP}^B$

Proof: For (ii) let $B = \text{TQBF}$. Then:

$$\mathbf{NP}^{\text{TQBF}} \overset{(1)}{\subseteq} \mathbf{NPSPACE} \overset{(2)}{\subseteq} \mathbf{PSPACE} \overset{(3)}{\subseteq} \mathbf{P}^{\text{TQBF}}$$

For (i), given any oracle A, define L_A as follows:

$$\{w | \exists x \in A \text{ such that } |x| = |w|\}$$

Clearly, $L_A \in \mathbf{NP}^A$.

We now present an A which ensures that $L_A \notin \mathbf{P}$.