We will show that CIRCUIT-SAT is NP-complete.

**Input**: Boolean circuit
- directed acyclic graph, vertices \( \oplus \) are gates,
- AND-gates and OR-gates have indegree 2,
- NOT-gates have indegree 1,
- **known** input gates have indegree 0 and are labeled TRUE or FALSE,
- **unknown** input gates have indegree 0 and are labeled "?",
- there is one output gate (whose outdegree is 0)

**Question**: Is it possible to assign a truth-value to each unknown input gate, such that the output of the circuit is TRUE?
\[
\begin{align*}
\text{CIRCUIT-SAT} &= \{ B : B \text{ is a Boolean circuit such that } \\
& \quad \exists \text{ truth-values for the unknown input gates such that the output of } \\
& \quad B \text{ is TRUE} \}\nonumber
\end{align*}
\]
To show that CIRCUIT-SAT is NP-complete, we have to do the following:

* Show that CIRCUIT-SAT is in NP:
  - certificate = sequence for truth-values for the unknown input gates
  - verification = evaluate the circuit (use topological sort)

* Show that for all L \in NP: L \leq_p CIRCUIT-SAT.

Let L \in NP. We need a function f such that

1. f: input x for L \rightarrow Boolean circuit B = f(x),
2. x \in L \iff B \in CIRCUIT-SAT,
3. time to compute B is polynomial in the length of x.
We know that $L \in NP$:

- verification algorithm $V$
  - input to $V$ is $(x, y)$ where $x$ is an input for $L$ and $y$ is a certificate.
  - $x \in L \iff$
    - $\exists$ certificate $y$ such that
      - $|y| \leq |x|^c$,
      - $V(x, y)$ returns YES,
      - running time of $V(x, y)$ is $\leq |x|^c$.  

We now define the function $f$:

Let $x$ be an input for $L$.

Define a new algorithm $V_x$:

- Input is a string $y$ of length $\leq |x|c$.
- $V_x(y)$ runs $V(x,y)$.
- If $V(x,y)$ terminates in $\leq |x|c'$ steps, then $V_x(y)$ terminates and returns the output of $V(x,y)$.
- If $V(x,y)$ has not terminated after $|x|c'$ steps, then $V_x(y)$ terminates and returns NO.

Observe: * running time of algorithm $V_x$ is $\leq |x|c'$.

* $x \in L \iff \exists$ input $y$ for algorithm $V_x$ such that $V_x(y)$ returns YES.
Algorithm $V_x$ is a program that can be run on a computer.

$V_x$ can be represented by a Boolean circuit $B$:

$$\text{size of } B : \quad O\left(1|x| + 1|y| + 1|x|^c \right) \quad \leq |x|^c$$

polynomial in $|x|$. 

[Diagram of a Boolean circuit with inputs $x$ and $y$, and output $B$.]
The function $f$ maps $x$ to $B$.

$x \in L \iff \exists y : V_x (y) \text{ returns YES} \iff \exists y : \text{output of } B \text{ is TRUE} \iff B \in \text{CIRCUIT-SAT}.$

Conclusion: CIRCUIT-SAT is NP-complete.

Now we can start using the theorem on page 206 to show that other problems are NP-complete.