W13 L1 NP-completeness and Cook-Levin Theorem

Monday, April 27, 2020 9:06

Announcements:
- no quiz this week
- homework 10 available this afternoon

We want to combine diagrams with $P$ & $NP$.

$A \leq_P B$

How do you prove a new problem $B$ is $NP$-complete?
Need to show that $A \leq_P B$ for every $A \in NP$.

This seems challenging BUT

Thm: If $C \leq_P D$ and $D \leq_P E$ then $C \leq_P E$.
(\leq_P \text{ are transitive})

Alternatively, need to show: $A \leq_P B$ for some $NP$-complete $A$.
(Of course, need $B \in NP$ as well.)
Definitions:
- a variable is something like $x, y, z$ (these are logical variables, so they can take on the values true/false)
- a literal is a variable or its negation, for example $x, \overline{x}$
- a disjunction is an "or" and we write it $\lor$, for example "x or y" is written $x \lor y$
- a conjunction is an "and" and we write it $\land$, for example "x and y" is written $x \land y$
- a clause is a disjunction of several literals, for example ($x \lor y \lor z$), and ($x \lor \overline{x} \lor y \lor w$) and ($y$)
- a formula is in conjunctive normal form if it is the conjunction of some clauses for example ($x \lor y) \land (z \lor \overline{x}) \land (w \lor y \lor \overline{z}) \land (y)$
- a satisfying assignment is a way to give each variable a Boolean value to make the overall expression evaluate to TRUE

Define $SAT = \{ \langle \varphi \rangle | \varphi \text{ is a conjunctive normal form formula and also } \varphi \text{ has a satisfying assignment} \}$. For example $(x) \land (\overline{x})$ is not in SAT, but $(x \lor y) \land (z)$ is in SAT.

Theorem: (Cook and Levin) $SAT$ is NP-complete.
Proof: Need to show that $SAT \in NP$ and also that for any $A \in NP$, $A \leq_P SAT$.

$SAT \in NP$: The certificate is the truth assignment, and we just check that the input is a properly-formatted formulae $\varphi$ in conjunctive normal form and that the given truth assignment evaluates to TRUE.

Take any language $A \in NP$. We need to come up with a polynomial-time reduction $A \leq_P SAT$.

From the assumption that $A \in NP$, we know there is some nondeterministic polynomial-time TM $N$ which decides $A$. Let's say that $N$ runs in time $n^k$ for some $k \in \mathbb{N}$. We know that on input string $w$, some branch of $N$'s computation will accept string $w$.

On that branch, we will go through configurations of $N$:
first one is the starting configuration: $q_0w$
next one will be some configuration we get to by following a transition of $N$ based on the last configuration
next one will be some configuration we get to by following a transition of $N$ based on the last configuration
next one will be some configuration we get to by following a transition of $N$ based on the last configuration
next one will be some configuration we get to by following a transition of $N$ based on the last configuration
...next one is an accepting configuration where $N$ is in state $q_{accept}$.

Let's think about this accepting computation as a table of $n^k \times n^k$ many squares:
Now we know that \( w \in A \) if and only if there is some table like the above, which has the following properties:
- it is \( n^k \times n^k \)
- the first row is \( \#q_0w \) (blanks) \( \# \)
- the \( i^{th} \) row is one step of computation after the \( i - 1^{th} \) row
- there is a row where we reached \( q_{\text{accept}} \)

Our goal is now to write a formula \( \varphi \) which is satisfiable if and only if this table can exist.
(Want that \( w \in A \) if and only if \( \varphi \in SAT \).)