Cook-Levin Theorem

- $SAT \in$ P iff P $=$ NP. I.e., SAT is at least as hard as any problem in NP and $SAT \in$ NP.
- SAT is in NP. Why?
- There is a *polynomial time reduction* from any other problem in NP to SAT.
- These two conditions imply that SAT is NP-complete.
- A language L is *NP-complete* if
  - L is in NP
  - There is a *polynomial time reduction* from any other language in NP to L.

Polynomial-time reductions

- We want a definition of reduction so that if (1) L is polynomial time reducible to L' and (2) L' is in P, then L is in P.

- A function $f : \Sigma^* \to \Sigma^*$ is a *polynomial time computable function* if some polynomial time deterministic TM exists which when any input w is input, the TM halts with just $f(w)$ on its tape.

- A language A is *polynomial time reducible* to language B, $A \leq_P B$ if there is a polynomial time computable function $f : \Sigma^* \to \Sigma^*$ such that:

$$w \in A \Longleftrightarrow f(w) \in B$$

The function f is a *polynomial time reduction* from A to B.

Poly-time reductions

Theorem: If $A \leq_P B$ and $B \in \mathsf{P}$ then $A \in \mathsf{P}$.

Proof: Suppose M is a polytime alg. for deciding B and f is a polytime reduction from A to B. Here is a polytime TM to decide A:

1. Compute $f(w)$

2. Run M on $f(w)$ and output whatever M outputs

Why won't the old definition of reduction work?

NP-completeness

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

Proof: Suppose that B is NP-complete and $B \in \mathsf{P}$. Let L be any language in NP. Since B NP-complete, $L \leq_P B$. Since, $B \in \mathsf{P}$ we use the previous theorem to conclude that $L \in \mathsf{P}$.

So the assumptions imply $\mathsf{NP} \subseteq \mathsf{P}$. Since it is clear that $\mathsf{P} \subseteq \mathsf{NP}$, we conclude that $\mathsf{P} = \mathsf{NP}$.

Proving a language L is NP-complete

We first show the following

Lemma: If $A \leq_P B$ and $B \leq_P C$, then $A \leq_P C$.

Proof: Let f be a poly-time reduction from A to B and g be a poly-time reduction from B to C. We claim that $f \circ g$ is a poly-time reduction from A to C.

Proof of claim: (Exercise)

Proving a language L is NP-complete

Theorem: A language L is NP-complete if

1. L is in NP and
2. there is an NP-complete language B and $B \leq_P L$.

Proof: Let L_A be any language in NP. Since B is NP-complete, $L_A \leq_P B$. By assumption (2), $L_A \leq_P L$. Combining this with assumption (1), we can conclude that L is NP-complete.

Restatement of the Cook Levin Theorem

SAT is NP complete.

We will go over the proof in a later lecture.