7.5
CFGs; Proving a grammar generate a specific language
Inductive proofs for CFGs

**Question:** How do we formally prove that a CFG $L(G) = L$?

**Example:** $S \rightarrow \epsilon | a | b | aSa | bSb$

**Theorem**

$L(G) = \{\text{palindromes}\} = \{w | w = w^R\}$

Two directions:

- $L(G) \subseteq L$, that is, $S \Rightarrow^* w$ then $w = w^R$
- $L \subseteq L(G)$, that is, $w = w^R$ then $S \Rightarrow^* w$
Inductive proofs for CFGs

**Question:** How do we formally prove that a CFG \( L(G) = L \)?

**Example:** \( S \rightarrow \epsilon \mid a \mid b \mid aSa \mid bSb \)

---

**Theorem**

\[ L(G) = \{ \text{palindromes} \} = \{ w \mid w = w^R \} \]

Two directions:

- \( L(G) \subseteq L \), that is, \( S \xrightarrow{*} w \) then \( w = w^R \)
- \( L \subseteq L(G) \), that is, \( w = w^R \) then \( S \xrightarrow{*} w \)
Show that if \( S \rightarrow^{*} w \) then \( w = w^R \)

By induction on length of derivation, meaning

For all \( k \geq 1 \), \( S \rightarrow^{*k} w \) implies \( w = w^R \).

- If \( S \rightarrow^{1} w \) then \( w = \epsilon \) or \( w = a \) or \( w = b \). Each case \( w = w^R \).
- Assume that for all \( k < n \), that if \( S \rightarrow^{k} w \) then \( w = w^R \).
- Let \( S \rightarrow^{n} w \) (with \( n > 1 \)). Wlog \( w \) begin with \( a \).
  - Then \( S \rightarrow aSa \rightarrow^{k-1} au a \) where \( w = au a \).
  - And \( S \rightarrow^{n-1} u \) and hence IH, \( u = u^R \).
  - Therefore \( w^r = (au a)^R = (ua)^Ra = au^Ra = au a = w \).
Show that if $S \Rightarrow^* w$ then $w = w^R$

By induction on length of derivation, meaning

For all $k \geq 1$, $S \Rightarrow^*_k w$ implies $w = w^R$.

- If $S \Rightarrow^1 w$ then $w = \epsilon$ or $w = a$ or $w = b$. Each case $w = w^R$.
- Assume that for all $k < n$, that if $S \Rightarrow^k w$ then $w = w^R$
- Let $S \Rightarrow^n w$ (with $n > 1$). Wlog $w$ begin with $a$.
  - Then $S \Rightarrow aSa \Rightarrow^{k-1} aua$ where $w = aua$.
  - And $S \Rightarrow^{n-1} u$ and hence IH, $u = u^R$.
  - Therefore $w^r = (aua)^R = (ua)^R a = au^Ra = aua = w$. 
Show that if $w = w^R$ then $S \sim^* w$.

By induction on $|w|$
That is, for all $k \geq 0$, $|w| = k$ and $w = w^R$ implies $S \sim^* w$.

Exercise: Fill in proof.
Mutual Induction

Situation is more complicated with grammars that have multiple non-terminals.

See Section 5.3.2 of the notes for an example proof.
THE END

... 

(for now)