Assignment # 7.1a Key

1. Write a CFG to show the language is a CFL or use the Pumping Lemma for CFLs to prove that it is not for each of the following.
   a) \( L = \{ a^i b^j | j = i^2, i, j > 0 \} \)
   Assume this language is a CFL
   PL: Provides \( N>0 \)
   Me: \( a^N b^{N^2} \)
   PL: \( a^N b^{N^2} = uvwxy, |vwx| \leq N, |vx|>0, \) and \( \forall i uv^iwx^iy \in L \)
   ME: \( i=2 \).
   Case 1) \( vwx \) contains some a’s. Then \( uv^2wx^2y \) has at least \( N+1 \) a’s and at most \( N^2 + N - 1 \) b’s. But \( (N+1)^2 \) is \( N^2 + 2N + 1 \) and \( N^2 + 2N + 1 > N^2 + N - 1 \) since \( 2N+1 > N-1 \) for \( N>0 \) (even for \( N = 0 \)), Thus, \( uv^2wx^2y \notin L \)
   Case 2) \( vwx \) contains only b’s. Then \( uv^2wx^2y \) has exactly \( N \) a’s and at least \( N^2 + 1 \) b’s. But then it has too many b’s. Thus, \( uv^2wx^2y \notin L \)
   These cases cover all possibilities, so \( L \) is not a CFL.
Assignment # 7.1b Key

1. Write a CFG to show the language is a CFL or use the Pumping Lemma for CFLs to prove that it is not for each of the following.

   b) \( L = \{ a^i b^j c^k d^m \mid m + k = i + j \} \)

   The language is a CFL as can be seen by \( G = (\{S, \}, \{a,b,c,d\}, R, S) \)
   
   \[
   \begin{align*}
   S & \rightarrow a \ S \ d \mid T \mid U \\
   T & \rightarrow a \ T \ c \mid V \\
   U & \rightarrow b \ U \ d \mid V \\
   V & \rightarrow b \ V \ c \mid \lambda
   \end{align*}
   \]
2. Consider the context-free grammar $G = \{ \{S\}, \{a,b\}, R, S \}$

- $R$
  - $S \rightarrow a \mid b \mid a a \mid b b \mid a S a \mid b S b$

Provide a proof that shows

$$ L = \{ w \mid w \in \{a,b\}^* \text{ and } w \text{ is a palindrome} \} $$

You will need to provide an inductive proof in both directions. Actually, though, the best approach is to prove a Lemma first that is used in the proofs going in each direction of containment.

**Lemma 1:** $S \Rightarrow^* \beta$, where $\beta$ contains a nonterminal, iff $\beta$ is of the form $xSx_R$, where $x \in \{a,b\}^*$. We provide this inductively on the length of the derivation, i.e., we show, for all $k \geq 0$ that $S \Rightarrow^k xSx_R$ for all strings $x \in \{a,b\}^*$, $|x|=k$, and that these are the only non-terminal strings that can be derived in $G$ by derivations of length $k$.

**Base ($k=0$):** $S \Rightarrow^0 S$ is the only length zero derivation. The form of this is $xSx$ for $|x| = 0$, and that is the only string that can be derived in zero steps, so our base case is shown.

**IH($k$):** $S \Rightarrow^k \beta$, $k \geq 0$, where $\beta$ contains a nonterminal, iff $\beta$ is of the form $xSx_R$, where $x \in \{a,b\}^*$ and $|x|=k$.

**IS($k+1$):** Each derivation of length $k+1$ containing a non-terminal string in $L(G)$ must start with application of one of the following two rules $S \rightarrow a S a \mid b S b$. This means that any derivation of length $k+1$ starts $S \Rightarrow aS \rightarrow^{k} aSxR_{a}$ or $S \Rightarrow bS \rightarrow^{k} bSxR_{b}$ and these are the only possibilities. But then, $S \Rightarrow^{k+1} \beta$, $k \geq 0$, where $\beta$ contains a nonterminal, iff $\beta$ is of the form $xSx_R$, where $x \in \{a,b\}^*$ and $|x|=k+1$.

This proves our Lemma.
2. Consider the context-free grammar $G = \{ \{S\}, \{a,b\}, R, S \}$

$R:\$

$S \rightarrow a \mid b \mid a\ a \mid b\ b \mid a\ S\ a \mid b\ S\ b$

Provide a proof that shows

$L = \{ w \mid w \in \{a,b\}^+ \text{ and } w \text{ is a palindrome} \}$

We wish to prove that $L(G) = L$. Specifically, we show $S \Rightarrow^* \beta$ where $\beta$ is over terminals, iff $\beta$ is of the form $xx^R$, where $x \in \{a,b\}^*$. By Lemma 1, $S \Rightarrow^* \beta$, where $\beta$ contains a nonterminal, iff $\beta$ is of the form $xSx^R$, where $x \in \{a,b\}^*$. $R$ has four roles that can replace the one non-terminal $S$ with terminals only; these are $S \rightarrow a \mid b \mid a\ a \mid b\ b$. All strings in $L$ are of one of the forms $xax^R$, $xbx^R$, $xaax^R$ or $xbbx^R$, where $x \in \{a,b\}^*$. Using the Lemma and our observation about the only terminating rules in $R$, we have that $S \Rightarrow^* \beta$ where $\beta$ is over terminals, iff $\beta$ is of one of the forms $xax^R$, $xbx^R$, $xaax^R$ or $xbbx^R$, where $x \in \{a,b\}^*$. But this shows that the words in $L$ are exactly those that can be generated in $L(G)$. Thus, we have shown that $L(G) = L$ as was desired.