1. **(20 points)** The September 5 lecture defined a function called f (slide 22):

$$\begin{aligned} f(\epsilon) &= 0 \\ f(s \cdot 0) &= f(s) - 1 \\ f(s \cdot 1) &= f(s) + 1 \end{aligned}$$

and made four observations about f. Prove the two properties from that slide that are stated below:

(a) **(10 points)** $f(xy) = f(x) + f(y)$.
Hint: use induction on the construction (i.e. length) of y.
Solution: Proof by induction on the length of y. Let $|y| = k$.
If $y = \epsilon$, then

$$f(xy) = f(x \cdot \epsilon) = f(x) + 0 = f(x) + f(\epsilon) = f(x) + f(y)$$

so the claim holds.
If $y = w \cdot c$, we split into two cases according to the value of c.
Case $c = 0$:

$$f(xy) = f(xwc) = f(xw0) = f(xw) - 1$$

Applying the induction hypothesis to w, we get $f(xw) = f(x) + f(w)$ and thus

$$f(xy) = f(xw) - 1 = f(x) + f(w) - 1 = f(x) + f(w0) = f(x) + f(y)$$

so the claim holds.
Case $c = 1$: analogous to the $c = 0$ case.

(b) If $f(s) > 0$ then for all $k \in [0 \ldots f(s)]$, s can be divided into two strings, x, and y, such that $s = xy$ and $f(x) = k$.
Hint: my solution uses induction on k and the result from part (a).
Solution: We first establish a lemma: If $f(y) > 0$, then there exists w such that $y = wy'$ and $f(w) = 1$.
Proof: When $|w| = 0$, $f(w) = 0$ and when $w = y$, $f(w) = f(y) > 0$ (assume that $f(w) > 1$, otherwise we choose w to be y). If there were no choice of w such that $f(w) = 1$, then there would exist two prefixes of y: w and $w \cdot c$ such that $f(w) <= 0$ and $f(w \cdot c) > 1$. This contradicts the definition of f.
Now we prove by induction on k.
Basis: When $k = 0$, then $x = \epsilon$ and $y = s$. Clearly, $s = x \cdot y$ and $f(x) = f(\epsilon) = 0$.
Induction Step: Assume $s = xy$ such that $f(x) = k$, for some k in the range $[0...f(s) - 1]$. Since $f(s) = f(x) + f(y)$, it follows that $f(y) > 0$; by the above lemma, there exists w such that $y = wy'$ and $f(w) = 1$. Therefore, $s = xwy'$ and taking $x' = xw$, $f(x') = f(x) + f(w) = k + 1$. We have now found strings x' and y' such that $s = x'y'$ and $f(x') = k + 1$.

2. **(20 points)** Define the set Q inductively as shown below:

$$\begin{aligned} (0, 1) &\in Q \\ \text{if } (x, y) &\in Q \text{ then } (x + y, y + 2) \in Q \end{aligned}$$

(a) **(5 points)** Write down the first four tuples in Q (i.e. the four with the smallest values for x or y).
Solution: $Q = \{(0, 1), (1, 3), (4, 5), (9, 7), ...\}$.

(b) **(5 points)** Describe the set Q using one English sentence. This should be something along the linese of:

(x, y) is in Q iff *some property of x and y holds*.

Your job is to figure out what that property is and state it.
Solution: (x, y) is in Q iff $x = z^2$ and $y = 2z + 1$ for some $z \in \mathbb{N}$.

(c) **(10 points)** Use induction to prove that Q is the set that you described in part (b). Remember to include both directions of the proof.
Solution: ($\Rightarrow$)
Take $(x, y) \in Q$
Base case: If $(x, y) = (0, 1)$, then $z = 0$ satisfies the claim.
Induction Step: If $(x, y) \neq (0, 1)$, there exists $(u, v) \in Q$ such that $(x, y) = (u + v, v + 2)$. Assume there exists $k \in \mathbb{N}$ such that $(u, v) = (k^2, 2k + 1)$. Then

$$(x, y) = (k^2 + (2k + 1), (2k + 1) + 2) = ((k + 1)^2, 2(k + 1) + 1$$

and the claim holds (let $z = k + 1$).
($\Leftarrow$)
Base case: if $z = 0$, then $(z^2, 2z + 1) = (0, 1) \in Q$.
Induction Step: Assume $(k^2, kz + 1) \in Q$ for some $k \in \mathbb{N}$. By the induction hypothesis, $(k^2, 2k + 1) \in Q$ and the second rule in the definition of Q implies that $(k^2+2k+1, 2k+1+2) = ((k+1)^2, 2(k+1)+1) \in Q$.

3. **(25 points)** Let Σ be an alphabet. For $s \in \Sigma^*$ define $s^{\mathcal{R}}$ to be the *reverse* of s as given below:

$$\epsilon^{\mathcal{R}} = \epsilon$$
$$(w \cdot c)^{\mathcal{R}} = c \cdot w^{\mathcal{R}}$$

a. **(5 points)** Show that $(\texttt{know})^{\mathcal{R}} = \texttt{wonk}$ by repeatedly applying the definition of $\mathcal{R}$.

Solution: $(\texttt{know})^{\mathcal{R}} = \texttt{w(kno)}^{\mathcal{R}} = \texttt{wo(kn)}^{\mathcal{R}} = \texttt{won(k} \cdot \epsilon)^{\mathcal{R}} = \texttt{wonk} \cdot \epsilon^{\mathcal{R}} = \texttt{wonk}$

A string $s \in \Sigma^*$ is a *palindrome* iff $s = s^{\mathcal{R}}$. Let P be the set of all palindromes.

b. **(5 points)** Give an inductive definition of P.
Solution: $\epsilon \in P$
$c \in P$ for all $c \in \Sigma$
If $s \in P$ and $c \in \Sigma$ then $c \cdot s \cdot c \in P$

c. **(5 points)** Give a short explanation in English of why your definition is correct.
(This is preparation for the proof requested in part (d).
Solution: Even length palindromes begin with ϵ as the base case. Odd length palindromes begin with c as the base case. Palindromes are constructed be appending the same symbol to the start and end of another palindrome.

d. **(10 points)** Use induction to prove that the set P that you described in part (b) is indeed the set of all palindromes.

4. **Solution:**

$(s \in P) \Rightarrow (s = s^{\mathcal{R}})$:
By induction on the definition of P (note how the proof has one case for each case in the defintion of P):
$s = \epsilon$: Then $s^{\mathcal{R}} = \epsilon$ by the defintion of $\mathcal{R}$. Thus $s = s^{\mathcal{R}}$ as required.
$s = c$, for some $c \in \Sigma$: then

$$\begin{aligned} s^{\mathcal{R}} &= (\epsilon \cdot c)^{\mathcal{R}} \\ &= (c \cdot \epsilon^{\mathcal{R}}), \text{def. } \mathcal{R} \\ &= c \cdot \epsilon, \text{def. } \mathcal{R} \\ &= c \\ &= s \end{aligned}$$

Thus $s = s^{\mathcal{R}}$ as required.

$s = c \cdot x \cdot c$, for some $c \in \Sigma$ and $x \in P$: then

$$\begin{aligned} s^{\mathcal{R}} &= ((c \cdot x) \cdot c)^{\mathcal{R}}, \text{case hyp.} \\ &= c \cdot (c \cdot x)^{\mathcal{R}}, \text{def. } \mathcal{R} \\ &= c \cdot (x^{\mathcal{R}} \cdot c), \text{lemma 3.1 (below)} \\ &= c \cdot (x \cdot c), x \in P, \text{thus } x = x^{\mathcal{R}} \\ &= s, \text{case hyp.} \end{aligned}$$

$(s \in P) \Leftarrow (s = s^{\mathcal{R}})$:

By induction on the definition of strings (note how the proof hase one case for each case in the definition of *strings*):

$s = \epsilon$: Then $s \in P$ by the first case in the defintion of P.

$s = x \cdot c$, for string $x \in \Sigma^*$ and some symbol $c \in \Sigma$: Then, $s^{\mathcal{R}} = c \cdot x^{\mathcal{R}}$. Note that $x^{\mathcal{R}}$ is a string. I'll consider two cases according whether or not $x^{\mathcal{R}}$ is empty.

case $x^{\mathcal{R}} = \epsilon$: Then $x = \epsilon$ and $s = c$ for some $c \in \Sigma$. Thus, $s \in P$ by the second case in the definition of P.

case $x^{\mathcal{R}} = u \cdot d$, for string $u \in \Sigma^*$ and some symbol $d \in \Sigma$: Then $s^{\mathcal{R}} = c \cdot u \cdot d$. By lemma 3.2, $s^{\mathcal{R}^{\mathcal{R}}} = s$, which means that $s = d \cdot u^{\mathcal{R}} \cdot c$. Because $s = s^{\mathcal{R}}$ we have

$$d \cdot u^{\mathcal{R}} \cdot c \quad = \quad c \cdot u \cdot d$$

and we conclude that $c = d$ and $u = u^{\mathcal{R}}$. by the definition of string equality. This means that $s = c \cdot u \cdot c$.

Now, we just need to show that $u \in P$ and we can use the third case in the defintion of P to conclude that $s \in P$. The induction hypothesis gives us that $u \in P$ because we've already shown that $u = u^{\mathcal{R}}$. So, we use the third case in the definition of P to conclude that $s \in P$ as required.

□

We still owe you two lemmas. Here they are.

Remark 1:

Lemma 3.1: For any strings x and y, $(xy)^{\mathcal{R}} = y^{\mathcal{R}} \cdot y^{\mathcal{R}}$.

Proof – by induction (of course) on y:

case $y = \epsilon$:

$$\begin{aligned} (xy)^{\mathcal{R}} &= (x\epsilon)^{\mathcal{R}}, && \text{case hyp: } y = \epsilon \\ &= x^{\mathcal{R}}, && \text{def. concatenation} \\ &= \epsilon \cdot x^{\mathcal{R}}, && \text{def. concatenation} \\ &= \epsilon^{\mathcal{R}} \cdot x^{\mathcal{R}}, && \text{def. } \mathcal{R} \\ &= y^{\mathcal{R}} \cdot x^{\mathcal{R}}, \text{case hyp.} \end{aligned}$$

✓

Technically, I should show that $\epsilon \cdot s = s$ as the definition of concatenation only shows that $s \cdot \epsilon = s$. I will have no objection if you assumed this without even thinking about it. But, for those that want every last detail proven (and to see that this chain of lemmas has an end), I'll do that in lemma 3.3 below.

case $y = u \cdot c$:

$$\begin{aligned} (xy)^{\mathcal{R}} &= (x(uc))^{\mathcal{R}}, && \text{case hyp: } y = uc \\ &= ((xu)c)^{\mathcal{R}}, && \text{concatenation is associative} \\ &= c(xu)^{\mathcal{R}}, \text{def. } \mathcal{R} \\ &= c \cdot (u^{\mathcal{R}} \cdot x^{\mathcal{R}}), \text{ind. hyp.} \\ &= (c \cdot u^{\mathcal{R}}) \cdot x^{\mathcal{R}}, \text{concatenation is associative} \\ &= y^{\mathcal{R}} \cdot x^{\mathcal{R}}, \text{case hyp: } y = uc, \text{def. } \mathcal{R} \end{aligned}$$

✓

□ OK, we've never actually proven that string concatenation is associative. See lemma 3.4 below.

Lemma 3.2: For any string s, $s = s^{\mathcal{R}\mathcal{R}}$.

The proof, of course, is by induction on s.

case $s = \epsilon$:

$$\begin{aligned} s^{\mathcal{R}\mathcal{R}} &= \epsilon^{\mathcal{R}\mathcal{R}}, \text{case hyp: } s = \epsilon \\ &= \epsilon^{\mathcal{R}}, \text{def. } \mathcal{R}\text{: } \epsilon^{\mathcal{R}} = \epsilon \\ &= \epsilon \text{def. } \mathcal{R}\text{: } \epsilon^{\mathcal{R}} = \epsilon \\ &= s, \text{case hyp: } s = \epsilon \end{aligned}$$

✓

case $s = x \cdot c$:

$$\begin{aligned} s^{\mathcal{R}\mathcal{R}} &= (x \cdot c)^{\mathcal{R}\mathcal{R}}, && \text{case hyp: } s = x \cdot c \\ &= (c \cdot x^{\mathcal{R}})^{\mathcal{R}}, && \text{def. } \mathcal{R} \end{aligned}$$

Now, we consider the two cases for $x^{\mathcal{R}}$:

case $x^{\mathcal{R}} = \epsilon$: Then, $x = \epsilon$ because we established in the previous case. It is straightforward to show that

$$s \;=\; s^{\mathcal{R}} \;=\; s^{\mathcal{R}\mathcal{R}} \;=\; c$$

which establishes this case.

case $x^{\mathcal{R}} = u \cdot d$: Then,

$$\begin{aligned} s^{\mathcal{R}\mathcal{R}} &= (c \cdot (u \cdot d))^{\mathcal{R}}, && \text{case hyp.} \\ &= (u \cdot d)^{\mathcal{R}} \cdot c, && \text{def. } \mathcal{R} \\ &= x^{\mathcal{R}\mathcal{R}} \cdot c, && \text{case hyp: } x = u \cdot d \\ &= x \cdot c, && \text{ind. hyp: } x = x^{\mathcal{R}\mathcal{R}} \\ &= s, && \text{case hyp: } s = x \cdot c \end{aligned}$$

✓

□

Lemma 3.3: $\epsilon \cdot s = s$.

The proof is by induction on s:

$s = \epsilon$:

$$\begin{aligned} \epsilon \cdot s &= \epsilon \cdot \epsilon \\ &= \epsilon \\ &= s \end{aligned}$$

✓

$s = x\dot{c}$:

$$\begin{aligned} \epsilon \cdot s &= \epsilon \cdot (x \cdot c), && \text{case hyp: } s = x \cdot c \\ &= (\epsilon \cdot x) \cdot c, && \text{lemma 3.4} \\ &= x \cdot c, && \text{ind. hyp.} \\ &= s, && \text{case hyp: } s = x \cdot c \end{aligned}$$

✓

□

Lemma 3.4: For any strings $x, y, z \in \Sigma^*$, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.

The proof is by induction on z.

case $z = \epsilon$:

$$\begin{aligned} x \cdot (y \cdot z) &= x \cdot (y \cdot \epsilon) \\ &= x \cdot y \\ &= (x \cdot y) \cdot \epsilon \\ &= (x \cdot y) \cdot z \end{aligned}$$

✓

case $z = u \cdot c$:

$$
\begin{array}{rcll}
x \cdot (y \cdot z) & = & x \cdot (y \cdot (u \cdot c)), & \text{case hyp: } z = u \cdot c \\
 & = & x \cdot ((y \cdot u) \cdot c), & \text{ind. hyp.} \\
 & = & (x \cdot (y \cdot u)) \cdot c), & \text{ind. hyp.} \\
 & = & ((x \cdot y) \cdot u) \cdot c), & \text{ind. hyp.} \\
 & = & (x \cdot y) \cdot (u \cdot c), & \text{ind. hyp.} \\
 & = & (x \cdot y) \cdot z, & \text{case hyp: } z = u \cdot c \\
 & \checkmark & &
\end{array}
$$

□