Proving an identity about reversal

September 8, 2017

The reverse x^R of a string x is defined recursively as follows:

1. $\epsilon^R = \epsilon$;
2. If x is a string and a is a single letter, then $(xa)^R = ax^R$.

Using this definition, we can prove the following basic theorem about reverse:

Theorem 1. *For all strings x, y we have $(xy)^R = y^R x^R$.*

Proof. We'll do this by induction. This is, as you know from CS 245 or other courses, the basic technique when dealing with recursive definitions. But induction on what? The usual trick when dealing with words is induction on the length of a string. But we have a choice here – we could do induction on $|x|$, $|y|$, or even $|xy|$. Which should we use?

One correct choice is to do induction on $|y|$. (Exercise: what goes wrong if you try to prove it by induction on $|x|$?)

The base case is $|y| = 0$. In this case $y = \epsilon$. So

$$(xy)^R = (x\epsilon)^R = x^R = \epsilon x^R = \epsilon^R x^R = y^R x^R.$$

Now, the induction step. Assume the claim is true for $|y| < n$. We prove it for $|y| = n$.

If $|y| = n$, then we can write $y = ta$ for t a string of length $n - 1$ and a a single letter. (This, again, is a basic technique for doing induction on strings. You have a choice: you can peel off a single letter from the beginning or end of the string. What goes wrong if you write $y = at$ instead?)

Then we have

$$\begin{aligned}
(xy)^R &= (x(ta))^R && \text{(definition of } y\text{)} \\
&= ((xt)a)^R && \text{(associativity)} \\
&= a(xt)^R && \text{(recursive definition)} \\
&= a(t^R x^R) && \text{(by induction)} \\
&= (at^R)x^R && \text{(associativity)} \\
&= (ta)^R x^R && \text{(recursive definition)} \\
&= y^R x^R && \text{(definition of } y\text{)}
\end{aligned}$$

This completes the proof. □