15-312 Foundations of Programming Languages  
Recitation 2: Rule Induction  

Daniel Spoonhower  
spoons+@cs  
September 3, 2003  

1 Matching Parentheses

Recall from lecture our original definition (through inference rules) of the language of matching parentheses.

\[
\begin{align*}
\varepsilon & \vdash M_1 \\
M_1 & \vdash s_1 M \\
M_2 & \vdash s_2 M \\
(\ell s) & \vdash M_3
\end{align*}
\]

Recall also our “parser” for this language, given in terms in the following judgment and inference rules.

\[
\begin{align*}
\varepsilon & \vdash \varepsilon \\
\ell k & \vdash \varepsilon \\
k & \vdash (\ell s) \\
k & \vdash s
\end{align*}
\]

We would like to show that the languages defined by \( M \) and \( \vdash \) are one and the same, and we began in lecture with a proof of the following: if \( s \vdash \varepsilon \) then \( \varepsilon \vdash s \).

We will continue today be showing inclusion in the opposite direction. In particular, that

**Theorem 1.** If \( \varepsilon \vdash s \) then \( s \vdash M \).

**Proof.** By rule induction on the derivation of \( \varepsilon \vdash s \). We consider each case in turn.

(Rule \( \vdash_1 \)) Then \( s = \varepsilon \).

\[
\begin{align*}
\varepsilon & \vdash M_1 \\
& \vdash s_1 M \\
& \vdash s_2 M \\
& \vdash \ell s \\
& \vdash M_3
\end{align*}
\]

By \( M_1 \)

(Rule \( \vdash_2 \)) Then \( s = (s') \).

\[
\begin{align*}
(\ell s') & \vdash M_2 \\
& \vdash (\ell s') \\
& \vdash ?
\end{align*}
\]

Subderivation
What’s gone wrong? Normally, this is the point of the proof where we’d cleverly apply the induction hypothesis – why can we not do so in this case? What, according to a recent lecture, are our alternatives if we find ourselves stuck in such a situation?

The first answer here is to generalize the induction hypothesis. To claim the equivalence of the languages $M$ and $\triangleleft$, our theorem is strong enough, but it is not strong enough for us to carry out our proof. Let’s try it again.

**Theorem 1 (Revised).** If $k \triangleright s$ then $k s M$.

*Proof.* By rule induction on the derivation of $k \triangleright s$. We consider each case in turn.

(Rule $\triangleright_1$) (as above)

(Rule $\triangleright_2$) Then $s = (s')$.

\[
\begin{align*}
  k (\triangleright s') & \quad \text{Subderivation} \\
  k (s' M) & \quad \text{By i.h.} \\
  k s M & \quad \text{Since $s = (s')$.}
\end{align*}
\]

(Rule $\triangleright_3$) Then $s = )s'$ and $k = k'(\)$. 

\[
\begin{align*}
  k' \triangleright s' & \quad \text{Subderivation} \\
  k' s' M & \quad \text{By i.h.} \\
  (\) M & \quad \text{By $M_1$, $M_3$} \\
  ?
\end{align*}
\]

We’re so close this time! We’d like to conclude $k'(\) s' M$, but we’re not quite there yet. Intuitively, this should work out: we should be able to add a pair of (balanced) parentheses anywhere within a string of whose parentheses are already matched. (Are you convinced? Try some examples.) We’ll use another strategy from lecture: we’ll prove a lemma! To keep the syntax under control, I’ll use $l$, $r$, and $c$ instead of just $s$ to stand for strings of parentheses.

**Lemma 2.** If $lr M$ and $c M$ then $lcr M$.

(Before you read on, think about how we will go about proving this? By induction? Over what?)

*Proof.* By rule induction on the derivation of $lr M$. We consider each case in turn.

(Rule $M_1$) Then $lr = \varepsilon$.

\[
\begin{align*}
  c M & \quad \text{By assumption} \\
  lcr M & \quad \text{Since $l = r = \varepsilon$}
\end{align*}
\]
(Rule $M_2$)

One might think that the derivation of $lr M$ looks something like this:

\[
\begin{array}{c}
\vdots \\
l M \quad r M \\
\hline
lr M
\end{array}
\]

Why is this not the case? Just because we have chosen to break our string into two parts $l$ and $r$ doesn’t mean that they each have matching parentheses. (Think about where we’d like to use this lemma and about a statement of the form $l \triangleright r$. Must $l$ (in particular) and $r$ have matching parentheses?)

To complete this case, we must consider a number of subcases, one for each way that $lr$ might be broken down into two strings of matching parentheses. First we take the case where $l$ is split.

(Rule $M_2$, Subcase 1) Let $l = l_1 l_2$.

\[
\begin{array}{c}
\vdots \\
l_1 M \quad l_2 r M \\
\hline
l_1 l_2 r M
\end{array}
\]

$l_2 r M$  
$l_1 l_2 r M$  
$l r M$  

(by i.h.)  
(by $M_2$)  
(since $l = l_1 l_2$)

(Rule $M_2$, Subcase 2) Let $r = r_1 r_2$.

\[
\begin{array}{c}
\vdots \\
l r_1 M \quad r_2 M \\
\hline
l r_1 r_2 M
\end{array}
\]

(as above)

(What if the split really was between $l$ and $r$? Do we need a separate case for this?)

(Rule $M_3$)

Again, we must consider each of the ways that $lr$ might be split in a derivation that ends with

\[
\begin{array}{c}
\vdots \\
s M \\
\hline
(s) M
\end{array}
\]

3
(Rule $M_3$, Subcase 1) Let $l = \langle l' \text{ and } r = r' \rangle$.

\[
\begin{array}{c}
\vdots \\
l' r' M \\
\hline
(l' r') M
\end{array}
\]

Subderivation

$\vdash l' r' M$ By i.h.

$\vdash l' r M$ By $M_3$

$\vdash l_1 M \quad l_2 r M$ Since $l = \langle l' \text{ and } r = r' \rangle$

(Rule $M_3$, Subcase 2) Let $l = \varepsilon$ and $r = \langle r' \rangle$.

\[
\begin{array}{c}
l r M \\
r M \\
\hline
c r M
\end{array}
\]

By assumption

Since $l = \varepsilon$

By $M_2$

Since $l = \varepsilon$

(Rule $M_3$, Subcase 3) Let $l = \langle l' \rangle$ and $r = \varepsilon$. (as above)

Given this lemma, we can now return to our main theorem. In fact, we now have all the right tools to complete the proof: the last case goes through easily using our new lemma.

1.1 Alternatives to Rule Induction?

We have focused this time on rule induction, but there are other properties of strings that we might reason about. In many cases, we might want to carry out some proof by reasoning inductively over the lengths of strings. (Quick: think of a handful from 212!) Reconsider the case from our lemma where we split $l$ into two pieces $l_1$ and $l_2$. The end of the derivation looked something like this:

\[
\begin{array}{c}
\vdots \\
l_1 M \\
\hline
l_1 l_2 r M
\end{array}
\]

What if $l_1 = l_2 = \varepsilon$? Then $l_2 r$ is not any shorter than $l_1 l_2 r$! If we were to reason about the lengths of the strings in this case, we could not apply the induction hypothesis. Here (and in many proofs in this class) rule induction will prove to be the better choice.