Mock Answer for PLSV, 2011

April 23, 2011

Question 6

Invariants:

$$I(\mathtt{r1}) \overset{\mathsf{def}}{=} \mathit{lseg}(\mathtt{h}, \mathtt{x}) * \mathit{lseg}(\mathtt{x}, \mathit{null})$$

$$I(\mathtt{r2}) \overset{\mathsf{def}}{=} \mathtt{x}.\mathit{val} \mapsto \_$$

Proof:

```
{$lseg(\mathtt{h}, nil)$}
 zerolist(h) {
   cont := 1;
   x := h;
  {$lseg(\mathtt{h}, null) \wedge \mathtt{x} = \mathtt{h}$}
   // definition of the lseg predicate
  {$lseg(\mathtt{h}, \mathtt{x}) * lseg(\mathtt{x}, null)$}
   resource r1 in {
    {emp}
     // definition of emp
    {emp * emp}
     // parallel rule
    (
     {emp}
     while(cont == 1 ) {
      {emp}
       with r1 when true in {
        {$lseg(\mathtt{h}, \mathtt{x}) * lseg(\mathtt{x}, null)$}
         if(x != null) {
          {$lseg(\mathtt{h}, \mathtt{x}) * lseg(\mathtt{x}, null) \wedge \mathtt{x} \neq null$}
           // definition of lseg predicate
          {$lseg(\mathtt{h}, \mathtt{x}) * \exists y.\, \mathtt{x}.val \mapsto \_ * \mathtt{x}.nxt \mapsto y * lseg(y, null)$}
           resource r2 in {
            {$lseg(\mathtt{h}, \mathtt{x}) * \exists y.\, \mathtt{x}.nxt \mapsto y * lseg(y, null)$}
             // frame rule, then parallel rule.
            (
            {emp}
             with r2 when true {
```

```
          $\{\mathrm{x}.\mathit{val} \mapsto \_\}$
           [x.val] := 0
          $\{\mathrm{x}.\mathit{val} \mapsto \_\}$
         }
        $\{\mathsf{emp}\}$
        ||
        $\{\mathsf{emp}\}$
         with r2 when true {
          $\{\mathrm{x}.\mathit{val} \mapsto \_\}$
           [x.val] := 0
          $\{\mathrm{x}.\mathit{val} \mapsto \_\}$
         }
        $\{\mathsf{emp}\}$
        )
        $\{\mathit{lseg}(\mathrm{h},\mathrm{x}) * \exists y.\, \mathrm{x}.\mathit{nxt} \mapsto y * \mathit{lseg}(y, \mathit{null})\}$
       }
      $\{\mathit{lseg}(\mathrm{h},\mathrm{x}) * \exists y.\, \mathrm{x}.\mathit{val} \mapsto \_ * \mathrm{x}.\mathit{nxt} \mapsto y * \mathit{lseg}(y, \mathit{null})\}$
       x := [x.nxt];
      $\{\exists z.\, \mathit{lseg}(\mathrm{h},z) * z.\mathit{val} \mapsto \_ * z.\mathit{nxt} \mapsto \mathrm{x} * \mathit{lseg}(\mathrm{x}, \mathit{null})\}$
       // lseg join lemma
      $\{\mathit{lseg}(\mathrm{h},\mathrm{x}) * \mathit{lseg}(\mathrm{x}, \mathit{null})\}$
     } else {
      $\{\mathit{lseg}(\mathrm{h},\mathrm{x}) * \mathit{lseg}(\mathrm{x}, \mathit{null}) \wedge \mathrm{x} = \mathit{null}\}$
       cont := 0
      $\{\mathit{lseg}(\mathrm{h},\mathrm{x}) * \mathit{lseg}(\mathrm{x}, \mathit{null})\}$
     }
   }
  $\{\mathit{lseg}(\mathrm{h},\mathrm{x}) * \mathit{lseg}(\mathrm{x}, \mathit{null})\}$
 }
$\{\mathsf{emp}\}$
||
$\{\mathsf{emp}\}$
 with r1 when true in {
  $\{\mathit{lseg}(\mathrm{h},\mathrm{x}) * \mathit{lseg}(\mathrm{x}, \mathit{null})\}$
   if (x != null) {
    $\{\mathit{lseg}(\mathrm{h},\mathrm{x}) * \mathit{lseg}(\mathrm{x}, \mathit{null}) \wedge \mathrm{x} \neq \mathit{null}\}$
     // definition of lseg predicate
    $\{\mathit{lseg}(\mathrm{h},\mathrm{x}) * \exists y.\, \mathrm{x}.\mathit{val} \mapsto \_ * \mathrm{x}.\mathit{nxt} \mapsto y * \mathit{lseg}(y, \mathit{null})\}$
     [x.val] := 0;
    $\{\mathit{lseg}(\mathrm{h},\mathrm{x}) * \exists y.\, \mathrm{x}.\mathit{val} \mapsto \_ * \mathrm{x}.\mathit{nxt} \mapsto y * \mathit{lseg}(y, \mathit{null})\}$
     x := [x.nxt];
    $\{\exists z.\, \mathit{lseg}(\mathrm{h},z) * z.\mathit{val} \mapsto \_ * z.\mathit{nxt} \mapsto \mathrm{x} * \mathit{lseg}(\mathrm{x}, \mathit{null})\}$
     // lseg join lemma
    $\{\mathit{lseg}(\mathrm{h},\mathrm{x}) * \mathit{lseg}(\mathrm{x}, \mathit{null})\}$
   }
 }
$\{\mathsf{emp}\}$
```

```
        )
        $\{\mathsf{emp} * \mathsf{emp}\}$
         // definition of emp
        $\{\mathsf{emp}\}$
      }
  }
 $\{\,lseg(\mathtt{h},\mathtt{x}) * lseg(\mathtt{x}, null)\,\}$
  // lseg join lemma
 $\{\,lseg(\mathtt{h}, null)\,\}$
```

Hint for bonus question. The invariant associated with `r1` can be defined as follows:

$$\begin{aligned} I(\mathtt{r1}) \quad \overset{\mathsf{def}}{=} \quad & (\mathtt{cont} = 1 \wedge \mathit{zerolist}(\mathtt{head}, \mathtt{x}) * \mathit{onelist}(\mathtt{x}, \mathit{null})) \\ & \qquad\qquad\qquad\qquad \vee \mathit{zerolist}(\mathtt{head}, \mathit{null}) \end{aligned}$$