GSep

John Wickerson

1 Preliminaries

1.1 Spatial closure operators

Suppose R and S are of type $\mathit{expr} \to \mathit{expr} \to \mathit{assertion}$. Define:

$$\begin{aligned} R;S &\stackrel{\text{def}}{=} \lambda x\,z.\,\exists y.\,R\,x\,y \wedge S\,y\,z \\ R \vee S &\stackrel{\text{def}}{=} \lambda x\,y.\,R\,x\,y \vee S\,x\,y \\ \mathit{id} &\stackrel{\text{def}}{=} \lambda x\,y.\,x = y \wedge \mathit{emp} \end{aligned}$$

Then let R^* be the least function satisfying $R^* = \mathit{id} \vee (R;R^*)$ and let $R^+ = R;R^*$.

2 A singly-indexed list (no carrier set)

Our first datastructure is a singly-indexed list. Every node has a value and a pointer to the next node. The final node's next pointer is set to 0. The first node is a sentinel, at a fixed location r. Our datastructure can be described by the following formulae:

$$\begin{aligned} \mathit{list}\,r &\stackrel{\text{def}}{\iff} \mathit{el}^+\,r\,0 \\ x \in \mathit{list}\,r &\stackrel{\text{def}}{\iff} \mathit{el}^+\,r\,x \;*\; \mathit{el}^+\,x\,0 \end{aligned}$$

where:

$$\mathit{el}\,x\,y \;=\; x^1 \overset{.5}{\mapsto} \_ \;*\; x^2 \mapsto y$$

Our datastructure provides two methods: insertion and deletion. These are implemented as follows.

```
insert(x){
  int* p = r;
  while ([p+1]!=0 && ...) do p:=[p+1];
  [x+1]:=[p+1];
  [p+1]:=x;
}
```

```
remove(x){
  int* p = r;
  while ([p+1]!=x) do p:=[p+1];
  [p+1]:=[x+1];
}
```

We can specify these methods like so:

$$c{:}C \vdash \left\{\boxed{\mathit{list}\,\mathtt{r}}_c \;*\; \mathtt{x}^1 \mapsto v \;*\; \mathtt{x}^2 \mapsto \_\right\} \mathtt{insert(x)} \left\{\boxed{\mathtt{x} \in \mathit{list}\,\mathtt{r}}_c \;*\; \mathtt{x}^1 \overset{.5}{\mapsto} v\right\}$$
$$c{:}C \vdash \left\{\boxed{\mathtt{x} \in \mathit{list}\,\mathtt{r}}_c \;*\; \mathtt{x}^1 \overset{.5}{\mapsto} v\right\} \mathtt{remove(x)} \left\{\boxed{\mathit{list}\,\mathtt{r}}_c \;*\; \mathtt{x}^1 \mapsto v \;*\; \mathtt{x}^2 \mapsto \_\right\}$$

The region c denotes the module's internal state. Its interference, C, is as follows:

$$C \stackrel{\text{def}}{=} \bigcup_{x \in \mathbb{N}} \{\textsc{Add}\, x, \textsc{Rm}\, x\}$$

where:

action $\textsc{Add}\, x$

pre	$p^2 \mapsto p'$
post	$p^2 \mapsto x \;*\; x^1 \overset{.5}{\mapsto} v \;*\; x^2 \mapsto p'$
context	$el^*\, r\, p$

action $\textsc{Rm}\, x$

pre	$p^2 \mapsto x \;*\; x^1 \overset{.5}{\mapsto} v \;*\; x^2 \mapsto p'$
post	$p^2 \mapsto p'$
context	$el^*\, r\, p$
guard	$x^1 \overset{.5}{\mapsto} \_$

It is important to note that the pre- and post-conditions of `insert` and `remove` are stable under C.

2.1 Verification of the `insert` method

```
insert(x){
  {[list r]_c * x^1 ↦ v * x^2 ↦ _}
  // begin frame
    {[list r]_c}
    {[el^+ r 0]_c}
    {[el^* r r * el^+ r 0]_c}
    int* p = r; // using Hoare's assignment axiom
```

$\left\{\boxed{\mathit{list}\,\mathtt{r}}_c \;*\; \mathtt{x}^1 \mapsto v \;*\; \mathtt{x}^2 \mapsto \_\right\}$

$\left\{\boxed{\mathit{list}\,\mathtt{r}}_c\right\}$

$\left\{\boxed{el^+\,\mathtt{r}\,0}_c\right\}$

$\left\{\boxed{el^*\,\mathtt{r}\,\mathtt{r} \;*\; el^+\,\mathtt{r}\,0}_c\right\}$

```
  $\left\{\boxed{el^*\,\mathtt{r}\,\mathtt{p} * el^+\,\mathtt{p}\,0}_c\right\}$
  $\left\{\exists p'.\,\boxed{el^*\,\mathtt{r}\,\mathtt{p} * el\,\mathtt{p}\,p' * el^*\,p'\,0}_c\right\}$
  $\left\{\exists p'.\,\boxed{el^*\,\mathtt{r}\,\mathtt{p} * \mathtt{p}^1 \overset{.5}{\mapsto} \_ * \mathtt{p}^2 \mapsto p' * el^*\,p'\,0}_c\right\}$
  // begin existential
    $\left\{\boxed{el^*\,\mathtt{r}\,\mathtt{p} * \mathtt{p}^1 \overset{.5}{\mapsto} \_ * \mathtt{p}^2 \mapsto p' * el^*\,p'\,0}_c\right\}$
    int* t = [p+1]; // using RegRead axiom
    $\left\{\boxed{el^*\,\mathtt{r}\,\mathtt{p} * \mathtt{p}^1 \overset{.5}{\mapsto} \_ * \mathtt{p}^2 \mapsto \mathtt{t} * el^*\,\mathtt{t}\,0}_c\right\}$
  // end existential
  $\left\{\exists p'.\,\boxed{el^*\,\mathtt{r}\,\mathtt{p} * \mathtt{p}^1 \overset{.5}{\mapsto} \_ * \mathtt{p}^2 \mapsto \mathtt{t} * el^*\,\mathtt{t}\,0}_c\right\}$
  $\left\{\boxed{el^*\,\mathtt{r}\,\mathtt{p} * \mathtt{p}^1 \overset{.5}{\mapsto} \_ * \mathtt{p}^2 \mapsto \mathtt{t} * el^*\,\mathtt{t}\,0}_c\right\}$
  $\left\{\boxed{el^*\,\mathtt{r}\,\mathtt{p} * el\,\mathtt{p}\,\mathtt{t} * el^*\,\mathtt{t}\,0}_c\right\}$
  while (t!=0 && ...) do {
    $\left\{\boxed{el^*\,\mathtt{r}\,\mathtt{p} * el\,\mathtt{p}\,\mathtt{t} * el^*\,\mathtt{t}\,0}_c * \mathtt{t} \dot{\neq} 0\right\}$
    $\left\{\boxed{el^*\,\mathtt{r}\,\mathtt{t} * el^*\,\mathtt{t}\,0}_c * \mathtt{t} \dot{\neq} 0\right\}$
    $\left\{\exists t'.\,\boxed{el^*\,\mathtt{r}\,\mathtt{t} * \mathtt{t}^1 \overset{.5}{\mapsto} \_ * \mathtt{t}^2 \mapsto t' * el^*\,t'\,0}_c\right\}$
    p:=t; // using Hoare's assignment axiom
    $\left\{\exists t'.\,\boxed{el^*\,\mathtt{r}\,\mathtt{p} * \mathtt{p}^1 \overset{.5}{\mapsto} \_ * \mathtt{p}^2 \mapsto t' * el^*\,t'\,0}_c\right\}$
    // begin existential
      $\left\{\boxed{el^*\,\mathtt{r}\,\mathtt{p} * \mathtt{p}^1 \overset{.5}{\mapsto} \_ * \mathtt{p}^2 \mapsto t' * el^*\,t'\,0}_c\right\}$
      t:=[p+1]; // using RegRead axiom
      $\left\{\boxed{el^*\,\mathtt{r}\,\mathtt{p} * \mathtt{p}^1 \overset{.5}{\mapsto} \_ * \mathtt{p}^2 \mapsto \mathtt{t} * el^*\,\mathtt{t}\,0}_c\right\}$
    // end existential
    $\left\{\exists t'.\,\boxed{el^*\,\mathtt{r}\,\mathtt{p} * \mathtt{p}^1 \overset{.5}{\mapsto} \_ * \mathtt{p}^2 \mapsto \mathtt{t} * el^*\,\mathtt{t}\,0}_c\right\}$
    $\left\{\boxed{el^*\,\mathtt{r}\,\mathtt{p} * \mathtt{p}^1 \overset{.5}{\mapsto} \_ * \mathtt{p}^2 \mapsto \mathtt{t} * el^*\,\mathtt{t}\,0}_c\right\}$
  }
// end frame
$\left\{\boxed{el^*\,\mathtt{r}\,\mathtt{p} * \mathtt{p}^1 \overset{.5}{\mapsto} \_ * \mathtt{p}^2 \mapsto \mathtt{t} * el^*\,\mathtt{t}\,0}_c * \mathtt{x}^1 \mapsto v * \mathtt{x}^2 \mapsto \_\right\}$
// begin null action on region $c$
  $\left\{\mathtt{x}^1 \mapsto v * \mathtt{x}^2 \mapsto \_\right\}$
  [x+1]:=t;
  $\left\{\mathtt{x}^1 \mapsto v * \mathtt{x}^2 \mapsto \mathtt{t}\right\}$
  // end null action
  $\left\{\boxed{el^*\,r\,p * p^1 \overset{.5}{\mapsto} \_ * p^2 \mapsto t * el^*\,t\,0}_c * x^1 \mapsto v * x^2 \mapsto t\right\}$
  // begin action $\textsc{Add}\,x$ on region $c$
    $\left\{p^2 \mapsto t * x^1 \mapsto v * x^2 \mapsto t\right\}$
    [p+1]:=x;
    $\left\{p^2 \mapsto x * x^1 \overset{.5}{\mapsto} v * x^2 \mapsto t * x^1 \overset{.5}{\mapsto} v\right\}$
  // end action
  $\left\{\boxed{el^*\,r\,p * p^1 \overset{.5}{\mapsto} \_ * p^2 \mapsto x * x^1 \overset{.5}{\mapsto} v * x^2 \mapsto t * el^*\,t\,0}_c * x^1 \overset{.5}{\mapsto} v\right\}$
  $\left\{\boxed{el^+\,r\,x * el^+\,x\,0}_c * x^1 \overset{.5}{\mapsto} v\right\}$
  $\left\{\boxed{x \in list\,r}_c * x^1 \overset{.5}{\mapsto} v\right\}$
}
```

3 A singly-indexed list (with carrier set)

$$\begin{aligned}
list\,\emptyset\,x &\overset{\text{def}}{\iff} x = 0 \wedge emp \\
list\,X\,x &\overset{\text{def}}{\iff} x \in X \wedge \exists y.\, x^1 \overset{.5}{\mapsto} \_ * x^2 \mapsto y * list\,(X - \{x\})\,y
\end{aligned}$$

Our datastructure provides two methods: insertion and deletion. These are implemented as follows.

```
insert(x){
  int* p = r;
  while ([p+1]!=0 && ...) do p:=[p+1];
  [x+1]:=[p+1];
  [p+1]:=x;
}

remove(x){
  int* p = r;
  while ([p+1]!=x) do p:=[p+1];
  [p+1]:=[x+1];
}
```

We can specify these methods like so:

$$\begin{aligned}
&\vdash \left\{list\,(\{r\} \uplus X)\,r * x \mapsto \_\,\_\right\}\ \mathtt{insert(x)}\ \left\{list\,(\{r\} \uplus \{x\} \uplus X)\,r * x^1 \overset{.5}{\mapsto} v\right\} \\
&\vdash \left\{list\,(\{r\} \uplus \{x\} \uplus X)\,r * x^1 \overset{.5}{\mapsto} v\right\}\ \mathtt{remove(x)}\ \left\{list\,(\{r\} \uplus X)\,r * x \mapsto \_\,\_\right\}
\end{aligned}$$

We can reason using this specification like so:

```
$\left\{ \mathit{list}\,\{\mathtt{r}\}\,\mathtt{r} * \mathtt{x} \mapsto \_\,\_ * \mathtt{y} \mapsto \_\,\_ \right\}$
insert(r,x) // framing on $\mathtt{y} \mapsto \_\,\_$
$\left\{ \mathit{list}\,(\{\mathtt{r}\} \uplus \{\mathtt{x}\})\,\mathtt{r} * \mathtt{y} \mapsto \_\,\_ \right\}$
insert(r,y)
$\left\{ \mathit{list}\,(\{\mathtt{r}\} \uplus \{\mathtt{x}\} \uplus \{\mathtt{y}\})\,\mathtt{r} \right\}$
remove(r,x)
$\left\{ \mathit{list}\,(\{\mathtt{r}\} \uplus \{\mathtt{y}\})\,\mathtt{r} * \mathtt{x} \mapsto \_\,\_ \right\}$
```

3.1 Verification of the insert method

```
insert(x){
  $\left\{ \boxed{\mathit{list}\,(\{\mathtt{r}\} \uplus X)\,\mathtt{r}}_c * \mathtt{x}^1 \mapsto v * \mathtt{x}^2 \mapsto \_ \right\}$
  // begin action $\textsc{Add}_{\mathtt{r}}\,\mathtt{x}$ on region $c$
    $\left\{ \boxed{\mathit{list}\,\mathtt{r}}_c \right\}$
    $\left\{ \boxed{\mathit{el}^+\,\mathtt{r}\,0}_c \right\}$
    $\left\{ \boxed{\mathit{el}^*\,\mathtt{r}\,\mathtt{r} * \mathit{el}^+\,\mathtt{r}\,0}_c \right\}$
    int* p = r; // using Hoare's assignment axiom
    $\left\{ \boxed{\mathit{el}^*\,\mathtt{r}\,\mathtt{p} * \mathit{el}^+\,\mathtt{p}\,0}_c \right\}$
    $\left\{ \exists p'.\, \boxed{\mathit{el}^*\,\mathtt{r}\,\mathtt{p} * \mathit{el}\,\mathtt{p}\,p' * \mathit{el}^*\,p'\,0}_c \right\}$
    $\left\{ \exists p'.\, \boxed{\mathit{el}^*\,\mathtt{r}\,\mathtt{p} * \mathtt{p}^1 \overset{.5}{\mapsto} \_ * \mathtt{p}^2 \mapsto p' * \mathit{el}^*\,p'\,0}_c \right\}$
    // begin existential
      $\left\{ \boxed{\mathit{el}^*\,\mathtt{r}\,\mathtt{p} * \mathtt{p}^1 \overset{.5}{\mapsto} \_ * \mathtt{p}^2 \mapsto p' * \mathit{el}^*\,p'\,0}_c \right\}$
      int* t = [p+1]; // using RegRead axiom
      $\left\{ \boxed{\mathit{el}^*\,\mathtt{r}\,\mathtt{p} * \mathtt{p}^1 \overset{.5}{\mapsto} \_ * \mathtt{p}^2 \mapsto \mathtt{t} * \mathit{el}^*\,\mathtt{t}\,0}_c \right\}$
    // end existential
    $\left\{ \exists p'.\, \boxed{\mathit{el}^*\,\mathtt{r}\,\mathtt{p} * \mathtt{p}^1 \overset{.5}{\mapsto} \_ * \mathtt{p}^2 \mapsto \mathtt{t} * \mathit{el}^*\,\mathtt{t}\,0}_c \right\}$
    $\left\{ \boxed{\mathit{el}^*\,\mathtt{r}\,\mathtt{p} * \mathtt{p}^1 \overset{.5}{\mapsto} \_ * \mathtt{p}^2 \mapsto \mathtt{t} * \mathit{el}^*\,\mathtt{t}\,0}_c \right\}$
    $\left\{ \boxed{\mathit{el}^*\,\mathtt{r}\,\mathtt{p} * \mathit{el}\,\mathtt{p}\,\mathtt{t} * \mathit{el}^*\,\mathtt{t}\,0}_c \right\}$
    while (t!=0 && ...) do {
      $\left\{ \boxed{\mathit{el}^*\,\mathtt{r}\,\mathtt{p} * \mathit{el}\,\mathtt{p}\,\mathtt{t} * \mathit{el}^*\,\mathtt{t}\,0}_c * \mathtt{t} \dot{\neq} 0 \right\}$
      $\left\{ \boxed{\mathit{el}^*\,\mathtt{r}\,\mathtt{t} * \mathit{el}^*\,\mathtt{t}\,0}_c * \mathtt{t} \dot{\neq} 0 \right\}$
      $\left\{\exists t'.\,\boxed{el^*\,\mathtt{r}\,\mathtt{t} \ast \mathtt{t}^1 \overset{.5}{\mapsto} \_ \ast \mathtt{t}^2 \mapsto t' \ast el^*\,t'\,0}_c\right\}$
      p:=t; // using Hoare's assignment axiom
      $\left\{\exists t'.\,\boxed{el^*\,\mathtt{r}\,\mathtt{p} \ast \mathtt{p}^1 \overset{.5}{\mapsto} \_ \ast \mathtt{p}^2 \mapsto t' \ast el^*\,t'\,0}_c\right\}$
      // begin existential
        $\left\{\boxed{el^*\,\mathtt{r}\,\mathtt{p} \ast \mathtt{p}^1 \overset{.5}{\mapsto} \_ \ast \mathtt{p}^2 \mapsto t' \ast el^*\,t'\,0}_c\right\}$
        t:=[p+1]; // using RegRead axiom
        $\left\{\boxed{el^*\,\mathtt{r}\,\mathtt{p} \ast \mathtt{p}^1 \overset{.5}{\mapsto} \_ \ast \mathtt{p}^2 \mapsto \mathtt{t} \ast el^*\,\mathtt{t}\,0}_c\right\}$
      // end existential
      $\left\{\exists t'.\,\boxed{el^*\,\mathtt{r}\,\mathtt{p} \ast \mathtt{p}^1 \overset{.5}{\mapsto} \_ \ast \mathtt{p}^2 \mapsto \mathtt{t} \ast el^*\,\mathtt{t}\,0}_c\right\}$
      $\left\{\boxed{el^*\,\mathtt{r}\,\mathtt{p} \ast \mathtt{p}^1 \overset{.5}{\mapsto} \_ \ast \mathtt{p}^2 \mapsto \mathtt{t} \ast el^*\,\mathtt{t}\,0}_c\right\}$
    }
  // end frame
  $\left\{\boxed{el^*\,\mathtt{r}\,\mathtt{p} \ast \mathtt{p}^1 \overset{.5}{\mapsto} \_ \ast \mathtt{p}^2 \mapsto \mathtt{t} \ast el^*\,\mathtt{t}\,0}_c \ast \mathtt{x}^1 \mapsto v \ast \mathtt{x}^2 \mapsto \_\right\}$
  // begin null action on region $c$
    $\left\{\mathtt{x}^1 \mapsto v \ast \mathtt{x}^2 \mapsto \_\right\}$
    [x+1]:=t;
    $\left\{\mathtt{x}^1 \mapsto v \ast \mathtt{x}^2 \mapsto \mathtt{t}\right\}$
  // end null action
  $\left\{\boxed{el^*\,\mathtt{r}\,\mathtt{p} \ast \mathtt{p}^1 \overset{.5}{\mapsto} \_ \ast \mathtt{p}^2 \mapsto \mathtt{t} \ast el^*\,\mathtt{t}\,0}_c \ast \mathtt{x}^1 \mapsto v \ast \mathtt{x}^2 \mapsto \mathtt{t}\right\}$
  // begin action ADD x on region $c$
    $\left\{\mathtt{p}^2 \mapsto \mathtt{t} \ast \mathtt{x}^1 \mapsto v \ast \mathtt{x}^2 \mapsto \mathtt{t}\right\}$
    [p+1]:=x;
    $\left\{\mathtt{p}^2 \mapsto \mathtt{x} \ast \mathtt{x}^1 \overset{.5}{\mapsto} v \ast \mathtt{x}^2 \mapsto \mathtt{t} \ast \mathtt{x}^1 \overset{.5}{\mapsto} v\right\}$
  // end action
  $\left\{\boxed{el^*\,\mathtt{r}\,\mathtt{p} \ast \mathtt{p}^1 \overset{.5}{\mapsto} \_ \ast \mathtt{p}^2 \mapsto \mathtt{x} \ast \mathtt{x}^1 \overset{.5}{\mapsto} v \ast \mathtt{x}^2 \mapsto \mathtt{t} \ast el^*\,\mathtt{t}\,0}_c \ast \mathtt{x}^1 \overset{.5}{\mapsto} v\right\}$
  $\left\{\boxed{el^+\,\mathtt{r}\,\mathtt{x} \ast el^+\,\mathtt{x}\,0}_c \ast \mathtt{x}^1 \overset{.5}{\mapsto} v\right\}$
  $\left\{\boxed{\mathtt{x} \in list\,\mathtt{r}}_c \ast \mathtt{x}^1 \overset{.5}{\mapsto} v\right\}$
}
```

4 Doubly-linked list

We propose to describe the datastructure in a very different way. We shall see it as two *separate* lists (that is, we will use separating conjunction where previously we had ordinary conjunction). But in order to preserve the close relationship between the two lists (namely, that every node appearing in one list also appears in the other) we shall use ‘ghost pointers’, which map each element of one list to its counterpart in the other list. Here is our first attempt:

$$\begin{aligned} \mathit{2list}\, r &\overset{\text{def}}{\Longleftrightarrow} \text{И}a.\,\text{И}b.\, \boxed{\widehat{el}^{+}_{b,r}\, r\, 0}_{a} \ast \boxed{\widehat{el}^{+}_{a,r}\, r\, 0}_{b} \\ x \in \mathit{2list}\, r &\overset{\text{def}}{\Longleftrightarrow} \text{И}a.\,\text{И}b.\, \boxed{\widehat{el}^{+}_{b,r}\, r\, x \ast \widehat{el}^{+}_{b,r}\, x\, 0}_{a} \ast \boxed{\widehat{el}^{+}_{a,r}\, r\, x \ast \widehat{el}^{+}_{a,r}\, x\, 0}_{b} \end{aligned}$$

where:

$$\begin{aligned} el_0\, x\, y &\overset{\text{def}}{\Longleftrightarrow} x^1 \overset{.25}{\mapsto} \_ \ast x^2 \mapsto y \\ el_1\, x\, y &\overset{\text{def}}{\Longleftrightarrow} x^1 \overset{.25}{\mapsto} \_ \ast x^3 \mapsto y \end{aligned}$$

and:

$$\begin{aligned} in_{a,r}\, x &\overset{\text{def}}{\Longleftrightarrow} \boxed{el_0^{*}\, r\, x \ast \mathsf{tt}}_{a} \\ in_{b,r}\, x &\overset{\text{def}}{\Longleftrightarrow} \boxed{el_1^{*}\, r\, x \ast \mathsf{tt}}_{b} \end{aligned}$$

and:

$$\begin{aligned} \widehat{el}_{b,r}\, x\, y &\overset{\text{def}}{\Longleftrightarrow} el_0\, x\, y \ast in_{b,r}\, x \\ \widehat{el}_{a,r}\, x\, y &\overset{\text{def}}{\Longleftrightarrow} el_1\, x\, y \ast in_{a,r}\, x \end{aligned}$$

The predicate $\widehat{el}_{b,r}$ describes an element that appears in the first list. It uses the $in_{b,r}$ predicate to specify that the element appears in the second list too. From this and the symmetric fact about $\widehat{el}_{a,r}$, we can deduce that the two lists pass through exactly the same set of elements.

We specify the insert and remove methods in the same way as before (but now with the new implementation of the *2list* predicate):

$$\begin{aligned} c{:}C_{\mathtt{r}} &\vdash \left\{ \boxed{\mathit{2list}\, \mathtt{r}}_{c} \ast \mathtt{x}^1 \mapsto v \ast \mathtt{x}^2 \mapsto \_ \ast \mathtt{x}^3 \mapsto \_ \right\} \mathtt{insert(x)} \left\{ \boxed{\mathtt{x} \in \mathit{2list}\, \mathtt{r}}_{c} \ast \mathtt{x}^1 \overset{.5}{\mapsto} v \right\} \\ c{:}C_{\mathtt{r}} &\vdash \left\{ \boxed{\mathtt{x} \in \mathit{2list}\, \mathtt{r}}_{c} \ast \mathtt{x}^1 \overset{.5}{\mapsto} v \right\} \mathtt{remove(x)} \left\{ \boxed{\mathit{2list}\, \mathtt{r}}_{c} \ast \mathtt{x}^1 \mapsto v \ast \mathtt{x}^2 \mapsto \_ \ast \mathtt{x}^3 \mapsto \_ \right\} \end{aligned}$$

where

$$C_r \overset{\text{def}}{=} \bigcup_{x \in \mathbb{N}} \{\textsc{Add}_r\, x, \textsc{Rm}_r\, x\}$$

and

$$\begin{array}{l} \textsf{action } \textsc{Add}_r\, x \\ \left\lfloor \begin{array}{ll} \textsf{pre} & p^2 \mapsto p' \ast q^3 \mapsto q' \\ \textsf{post} & p^2 \mapsto x \ast q^3 \mapsto x \ast x^1 \overset{.5}{\mapsto} v \ast x^2 \mapsto p' \ast x^3 \mapsto q' \\ \textsf{context} & el_0^{*}\, r\, p \ast el_1^{*}\, r\, q \end{array} \right. \end{array}$$

$$\begin{array}{l} \textsf{action } \textsc{Rm}_r\, x \\ \left\lfloor \begin{array}{ll} \textsf{pre} & p^2 \mapsto x \ast q^3 \mapsto x \ast x^1 \overset{.5}{\mapsto} v \ast x^2 \mapsto p' \ast x^3 \mapsto q' \\ \textsf{post} & p^2 \mapsto p' \ast q^3 \mapsto q' \\ \textsf{context} & el_0^{*}\, r\, p \ast el_1^{*}\, r\, q \\ \textsf{guard} & x^1 \overset{.5}{\mapsto} v \end{array} \right. \end{array}$$

4.1 Verifying the `insert` method

$$\left\{ \boxed{\mathit{2list}\,\mathtt{r}}_c \;*\; \mathtt{x}^1 \mapsto v \;*\; \mathtt{x}^2 \mapsto \_ \;*\; \mathtt{x}^3 \mapsto \_ \right\}$$

```
insert(x){
  // begin frame
```

$$\left\{ \boxed{\mathit{2list}\,\mathtt{r}}_c \;*\; \mathtt{x}^1 \overset{.5}{\mapsto} v \;*\; \mathtt{x}^2 \mapsto \_ \;*\; \mathtt{x}^3 \mapsto \_ \right\}$$

```
    // begin frame
```

$$\left\{ \boxed{\mathit{2list}\,\mathtt{r}}_c \right\}$$

$$\left\{ \boxed{Иa.\,Иb.\, \boxed{\widehat{el}^{+}_{b,\mathtt{r}}\,\mathtt{r}\,0}_a \;*\; \boxed{\widehat{el}^{+}_{a,\mathtt{r}}\,\mathtt{r}\,0}_b}_c \right\}$$

$$\left\{ \boxed{Иa.\,Иb.\, \boxed{\widehat{el}^{*}_{b,\mathtt{r}}\,\mathtt{r}\,\mathtt{r} \;*\; \widehat{el}^{+}_{b,\mathtt{r}}\,\mathtt{r}\,0}_a \;*\; \boxed{\widehat{el}^{*}_{a,\mathtt{r}}\,\mathtt{r}\,\mathtt{r} \;*\; \widehat{el}^{+}_{a,\mathtt{r}}\,\mathtt{r}\,0}_b}_c \right\}$$

```
    int* p = r;
    int* q = r;
```

$$\left\{ \boxed{Иa.\,Иb.\, \boxed{\widehat{el}^{*}_{b,\mathtt{r}}\,\mathtt{r}\,\mathtt{p} \;*\; \widehat{el}^{+}_{b,\mathtt{r}}\,\mathtt{p}\,0}_a \;*\; \boxed{\widehat{el}^{*}_{a,\mathtt{r}}\,\mathtt{r}\,\mathtt{q} \;*\; \widehat{el}^{+}_{a,\mathtt{r}}\,\mathtt{q}\,0}_b}_c \right\}$$

$$\left\{ \exists p'\, q'.\, \boxed{\begin{array}{l} Иa.\,Иb.\, \boxed{\widehat{el}^{*}_{b,\mathtt{r}}\,\mathtt{r}\,\mathtt{p} \;*\; \widehat{el}_{b,\mathtt{r}}\,\mathtt{p}\,p' \;*\; \widehat{el}^{+}_{b,\mathtt{r}}\,p'\,0}_a \\ \quad *\; \boxed{\widehat{el}^{*}_{a,\mathtt{r}}\,\mathtt{r}\,\mathtt{q} \;*\; \widehat{el}_{a,\mathtt{r}}\,\mathtt{q}\,q' \;*\; \widehat{el}^{+}_{a,\mathtt{r}}\,q'\,0}_b \end{array}}_c \right\}$$

```
    int* t = [p+1];
    int* u = [q+2];
```

$$\left\{ \boxed{\begin{array}{l} Иa.\,Иb.\, \boxed{\widehat{el}^{*}_{b,\mathtt{r}}\,\mathtt{r}\,\mathtt{p} \;*\; \widehat{el}_{b,\mathtt{r}}\,\mathtt{p}\,\mathtt{t} \;*\; \widehat{el}^{+}_{b,\mathtt{r}}\,\mathtt{t}\,0}_a \\ \quad *\; \boxed{\widehat{el}^{*}_{a,\mathtt{r}}\,\mathtt{r}\,\mathtt{q} \;*\; \widehat{el}_{a,\mathtt{r}}\,\mathtt{q}\,\mathtt{u} \;*\; \widehat{el}^{+}_{a,\mathtt{r}}\,\mathtt{u}\,0}_b \end{array}}_c \right\}$$

```
    while (t!=0 && ...) do { p:=t; t:=[p+1]; }
    while (u!=0 && ...) do { q:=u; u:=[q+2]; }
```

$$\left\{ \boxed{\begin{array}{l} Иa.\,Иb.\, \boxed{\widehat{el}^{*}_{b,\mathtt{r}}\,\mathtt{r}\,\mathtt{p} \;*\; \widehat{el}_{b,\mathtt{r}}\,\mathtt{p}\,\mathtt{t} \;*\; \widehat{el}^{+}_{b,\mathtt{r}}\,\mathtt{t}\,0}_a \\ \quad *\; \boxed{\widehat{el}^{*}_{a,\mathtt{r}}\,\mathtt{r}\,\mathtt{q} \;*\; \widehat{el}_{a,\mathtt{r}}\,\mathtt{q}\,\mathtt{u} \;*\; \widehat{el}^{+}_{a,\mathtt{r}}\,\mathtt{u}\,0}_b \end{array}}_c \right\}$$

```
  // end frame
```

$$\left\{ \begin{array}{l} \boxed{\begin{array}{l} Иa.\,Иb.\, \boxed{\widehat{el}^{*}_{b,\mathtt{r}}\,\mathtt{r}\,\mathtt{p} \;*\; \widehat{el}_{b,\mathtt{r}}\,\mathtt{p}\,\mathtt{t} \;*\; \widehat{el}^{+}_{b,\mathtt{r}}\,\mathtt{t}\,0}_a \\ \quad *\; \boxed{\widehat{el}^{*}_{a,\mathtt{r}}\,\mathtt{r}\,\mathtt{q} \;*\; \widehat{el}_{a,\mathtt{r}}\,\mathtt{q}\,\mathtt{u} \;*\; \widehat{el}^{+}_{a,\mathtt{r}}\,\mathtt{u}\,0}_b \end{array}}_c \\ *\; \mathtt{x}^1 \overset{.5}{\mapsto} v \;*\; \mathtt{x}^2 \mapsto \_ \;*\; \mathtt{x}^3 \mapsto \_ \end{array} \right\}$$

```
  [x+1]:=t;
  [x+2]:=u;
```

$$\left\{ \begin{array}{l} \boxed{\begin{array}{l} Иa.\,Иb.\, \boxed{\widehat{el}^{*}_{b,\mathtt{r}}\,\mathtt{r}\,\mathtt{p} \;*\; \widehat{el}_{b,\mathtt{r}}\,\mathtt{p}\,\mathtt{t} \;*\; \widehat{el}^{+}_{b,\mathtt{r}}\,\mathtt{t}\,0}_a \\ \quad *\; \boxed{\widehat{el}^{*}_{a,\mathtt{r}}\,\mathtt{r}\,\mathtt{q} \;*\; \widehat{el}_{a,\mathtt{r}}\,\mathtt{q}\,\mathtt{u} \;*\; \widehat{el}^{+}_{a,\mathtt{r}}\,\mathtt{u}\,0}_b \end{array}}_c \\ *\; \mathtt{x}^1 \overset{.5}{\mapsto} v \;*\; \mathtt{x}^2 \mapsto \mathtt{t} \;*\; \mathtt{x}^3 \mapsto \mathtt{u} \end{array} \right\}$$

$$\left\{\begin{array}{l}\boxed{\begin{array}{l}\text{И}a.\,\text{И}b.\,\boxed{\widehat{el}^{*}_{b,\mathtt{r}}\,\mathtt{r}\,\mathtt{p} * \widehat{el}_{b,\mathtt{r}}\,\mathtt{p}\,\mathtt{t} * \widehat{el}^{+}_{b,\mathtt{r}}\,\mathtt{t}\,0}_{a}\\ * \boxed{\widehat{el}^{*}_{a,\mathtt{r}}\,\mathtt{r}\,\mathtt{q} * \widehat{el}_{a,\mathtt{r}}\,\mathtt{q}\,\mathtt{u} * \widehat{el}^{+}_{a,\mathtt{r}}\,\mathtt{u}\,0}_{b}\end{array}}_{c}\\ * \mathtt{x}^1 \overset{.5}{\mapsto} v * \mathtt{x}^2 \mapsto \mathtt{t} * \mathtt{x}^3 \mapsto \mathtt{u}\end{array}\right\}$$

$$\left\{\begin{array}{l}\boxed{\begin{array}{l}el_0\,\mathtt{p}\,\mathtt{t} * el_1\,\mathtt{q}\,\mathtt{u} *\\ \left(\begin{array}{l}el_0\,\mathtt{p}\,\mathtt{t} * el_1\,\mathtt{q}\,\mathtt{u} \mathrel{-\!\!\circledast}\\ \text{И}a.\,\text{И}b.\,\boxed{\widehat{el}^{*}_{b,\mathtt{r}}\,\mathtt{r}\,\mathtt{p} * \widehat{el}_{b,\mathtt{r}}\,\mathtt{p}\,\mathtt{t} * \widehat{el}^{+}_{b,\mathtt{r}}\,\mathtt{t}\,0}_{a}\\ * \boxed{\widehat{el}^{*}_{a,\mathtt{r}}\,\mathtt{r}\,\mathtt{q} * \widehat{el}_{a,\mathtt{r}}\,\mathtt{q}\,\mathtt{u} * \widehat{el}^{+}_{a,\mathtt{r}}\,\mathtt{u}\,0}_{b}\end{array}\right)\end{array}}_{c}\\ * \mathtt{x}^1 \overset{.5}{\mapsto} v * \mathtt{x}^2 \mapsto \mathtt{t} * \mathtt{x}^3 \mapsto \mathtt{u}\end{array}\right\}$$

`// tricky step (see below)`

$$\left\{\begin{array}{l}\boxed{\begin{array}{l}el_0\,\mathtt{p}\,\mathtt{t} * el_1\,\mathtt{q}\,\mathtt{u} *\\ \left(\begin{array}{l}el_0\,\mathtt{p}\,\mathtt{x} * el_0\,\mathtt{x}\,\mathtt{t} * el_1\,\mathtt{q}\,\mathtt{x} * el_1\,\mathtt{x}\,\mathtt{u} \mathrel{-\!\!\circledast}\\ \text{И}a.\,\text{И}b.\,\boxed{\widehat{el}^{*}_{b,\mathtt{r}}\,\mathtt{r}\,\mathtt{p} * \widehat{el}_{b,\mathtt{r}}\,\mathtt{p}\,\mathtt{x} * \widehat{el}_{b,\mathtt{r}}\,\mathtt{x}\,\mathtt{t} * \widehat{el}^{+}_{b,\mathtt{r}}\,\mathtt{t}\,0}_{a}\\ * \boxed{\widehat{el}^{*}_{a,\mathtt{r}}\,\mathtt{r}\,\mathtt{q} * \widehat{el}_{a,\mathtt{r}}\,\mathtt{q}\,\mathtt{x} * \widehat{el}_{a,\mathtt{r}}\,\mathtt{x}\,\mathtt{u} * \widehat{el}^{+}_{a,\mathtt{r}}\,\mathtt{u}\,0}_{b}\end{array}\right)\end{array}}_{c}\\ * \mathtt{x}^1 \overset{.5}{\mapsto} v * \mathtt{x}^2 \mapsto \mathtt{t} * \mathtt{x}^3 \mapsto \mathtt{u}\end{array}\right\}$$

`// begin action` $\textsc{Add}_{\mathtt{r}}\,\mathtt{x}$ `on region` c

$$\left\{el_0\,\mathtt{p}\,\mathtt{t} * el_1\,\mathtt{q}\,\mathtt{u} * \mathtt{x}^1 \overset{.5}{\mapsto} v * \mathtt{x}^2 \mapsto \mathtt{t} * \mathtt{x}^3 \mapsto \mathtt{u}\right\}$$

```
[p+1]:=x;
[q+2]:=x;
```

$$\left\{el_0\,\mathtt{p}\,\mathtt{x} * el_1\,\mathtt{q}\,\mathtt{x} * \mathtt{x}^1 \overset{.5}{\mapsto} v * \mathtt{x}^2 \mapsto \mathtt{t} * \mathtt{x}^3 \mapsto \mathtt{u}\right\}$$

$$\left\{el_0\,\mathtt{p}\,\mathtt{x} * el_0\,\mathtt{x}\,\mathtt{t} * el_1\,\mathtt{q}\,\mathtt{x} * el_1\,\mathtt{x}\,\mathtt{u}\right\}$$

`// end action`

$$\left\{\begin{array}{l}\boxed{\begin{array}{l}el_0\,\mathtt{p}\,\mathtt{x} * el_0\,\mathtt{x}\,\mathtt{t} * el_1\,\mathtt{q}\,\mathtt{x} * el_1\,\mathtt{x}\,\mathtt{u} *\\ \left(\begin{array}{l}el_0\,\mathtt{p}\,\mathtt{x} * el_0\,\mathtt{x}\,\mathtt{t} * el_1\,\mathtt{q}\,\mathtt{x} * el_1\,\mathtt{x}\,\mathtt{u} \mathrel{-\!\!\circledast}\\ \text{И}a.\,\text{И}b.\,\boxed{\widehat{el}^{*}_{b,\mathtt{r}}\,\mathtt{r}\,\mathtt{p} * \widehat{el}_{b,\mathtt{r}}\,\mathtt{p}\,\mathtt{x} * \widehat{el}^{n}_{b,\mathtt{r}}\,\mathtt{x}\,\mathtt{t} * \widehat{el}^{+}_{b,\mathtt{r}}\,\mathtt{t}\,0}_{a}\\ * \boxed{\widehat{el}^{*}_{a,\mathtt{r}}\,\mathtt{r}\,\mathtt{q} * \widehat{el}_{a,\mathtt{r}}\,\mathtt{q}\,\mathtt{x} * \widehat{el}^{n}_{a,\mathtt{r}}\,\mathtt{x}\,\mathtt{u} * \widehat{el}^{+}_{a,\mathtt{r}}\,\mathtt{u}\,0}_{b}\end{array}\right)\end{array}}_{c}\\ * \mathtt{x}^1 \overset{.5}{\mapsto} v * \mathtt{x}^2 \mapsto \mathtt{t} * \mathtt{x}^3 \mapsto \mathtt{u}\end{array}\right\}$$

$$\left\{\boxed{\begin{array}{l}\text{И}a.\,\text{И}b.\,\boxed{\widehat{el}^{*}_{b,\mathtt{r}}\,\mathtt{r}\,\mathtt{p} * \widehat{el}_{b,\mathtt{r}}\,\mathtt{p}\,\mathtt{x} * \widehat{el}_{b,\mathtt{r}}\,\mathtt{x}\,\mathtt{t} * \widehat{el}^{+}_{b,\mathtt{r}}\,\mathtt{t}\,0}_{a}\\ * \boxed{\widehat{el}^{*}_{a,\mathtt{r}}\,\mathtt{r}\,\mathtt{q} * \widehat{el}_{a,\mathtt{r}}\,\mathtt{q}\,\mathtt{x} * \widehat{el}^{n}_{a,\mathtt{r}}\,\mathtt{x}\,\mathtt{u} * \widehat{el}^{+}_{a,\mathtt{r}}\,\mathtt{u}\,0}_{b}\end{array}}_{c}\right\}$$

$$\left\{\boxed{\mathtt{x} \in \mathit{2list}\,\mathtt{r}}_{c}\right\}$$

`// end frame`

}

$$\left\{\boxed{\mathtt{x} \in \mathit{2list}\,\mathtt{r}}_{c} * \mathtt{x}^1 \overset{.5}{\mapsto} v\right\}$$

The tricky step requires us to show that:

$$\begin{array}{l} el_0\,\mathtt{p}\,\mathtt{t} \;*\; el_1\,\mathtt{q}\,\mathtt{u} \;-\!\!*\\ \text{И}a.\,\text{И}b.\,\boxed{\widehat{el}^{*}_{b,\mathrm{r}}\,\mathtt{r}\,\mathtt{p} \;*\; \widehat{el}_{b,\mathrm{r}}\,\mathtt{p}\,\mathtt{t} \;*\; \widehat{el}^{+}_{b,\mathrm{r}}\,\mathtt{t}\,0}_a\\ *\;\boxed{\widehat{el}^{*}_{a,\mathrm{r}}\,\mathtt{r}\,\mathtt{q} \;*\; \widehat{el}_{a,\mathrm{r}}\,\mathtt{q}\,\mathtt{u} \;*\; \widehat{el}^{+}_{a,\mathrm{r}}\,\mathtt{u}\,0}_b \end{array}$$

implies

$$\begin{array}{l} el_0\,\mathtt{p}\,\mathtt{x} \;*\; el_0\,\mathtt{x}\,\mathtt{t} \;*\; el_1\,\mathtt{q}\,\mathtt{x} \;*\; el_1\,\mathtt{x}\,\mathtt{u} \;-\!\!*\\ \text{И}a.\,\text{И}b.\,\boxed{\widehat{el}^{*}_{b,\mathrm{r}}\,\mathtt{r}\,\mathtt{p} \;*\; \widehat{el}_{b,\mathrm{r}}\,\mathtt{p}\,\mathtt{x} \;*\; \widehat{el}_{b,\mathrm{r}}\,\mathtt{x}\,\mathtt{t} \;*\; \widehat{el}^{+}_{b,\mathrm{r}}\,\mathtt{t}\,0}_a\\ *\;\boxed{\widehat{el}^{*}_{a,\mathrm{r}}\,\mathtt{r}\,\mathtt{q} \;*\; \widehat{el}_{a,\mathrm{r}}\,\mathtt{q}\,\mathtt{x} \;*\; \widehat{el}_{a,\mathrm{r}}\,\mathtt{x}\,\mathtt{u} \;*\; \widehat{el}^{+}_{a,\mathrm{r}}\,\mathtt{u}\,0}_b \end{array}$$

That is, if we are obliged to provide length-1 chains from `p` to `t` and from `q` to `u`, then it suffices for us to provide length-2 chains from `p` to `x` to `t` and from `q` to `x` to `u`, and the resultant list will be duly extended by 1.