

## A Telecommunications Protocol

Using Z

Woodcock & Davies

### External view

[M]

*Ext*

*in, out : seq M*

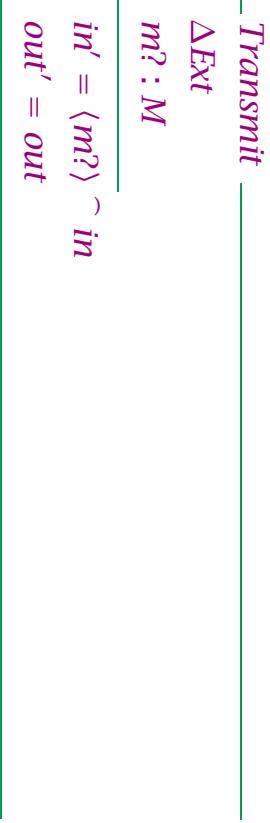
$\exists s : \text{seq } M \bullet in = s \cap out$

Initially

$$\text{ExtInit} \triangleq [\text{Ext}' \mid \text{in}' = \langle \rangle]$$

Ising Z

20-4



**Receive** $\Delta Ext$  $in' = in$  $\#out' = \#out + 1 \vee out' = out$ 

Jsing Z

20-6

**Sectional view**

[SPC]

<i>Section</i>
<i>route</i> : iseq SPC
<i>rec, ins, sent</i> : seq(seq <i>M</i> )
<i>route</i> $\neq \langle \rangle$
# <i>route</i> = # <i>rec</i> = # <i>ins</i> = # <i>sent</i>
<i>rec</i> = <i>ins</i> $\simeq$ <i>sent</i>
<i>front sent</i> = <i>tail rec</i>

$$[X] = \boxed{- \approx - : \text{seq}(\text{seq } X) \times \text{seq}(\text{seq } X) \rightarrow \text{seq}(\text{seq } X)}$$

$$\forall s, t : \text{seq}(\text{seq } X) \mid \#s = \#t \bullet$$

$$\forall i : \text{dom } s \bullet$$

$$(s \approx t)i = (s i) \sim (t i)$$

Ising Z

20-8

$$\text{SectionInit} = \boxed{\text{Section}'}$$

$$\forall i : \text{dom } route \bullet$$

$$rec\ i = ins\ i = sent\ i = \langle \rangle$$

**STransmit**

---

$\Delta \text{Section}$

---

$m? : M$

---

$route' = route$

$head\ rec' = \langle m? \rangle \sim (head\ rec)$

$tail\ rec' = tail\ rec$

$ins' = ins$

$sent' = sent$

Ising Z

20-10

**SReceive**

---

$\Delta \text{Section}$

---

$route' = route$

$rec' = rec$

$front\ ins' = front\ ins$

$last\ ins' = front(last\ ins)$

$front\ sent' = front\ sent$

$last\ sent' = \langle last(last\ ins) \rangle \sim (last\ sent)$

Daemon

ΔSection

$$\exists i : 1 \dots \#route - 1 \mid$$

$$\text{ins } i \neq \langle \rangle \bullet$$

$$\text{ins}' i = \text{front}(\text{ins } i)$$

$$\text{ins}'(i + 1) = \langle \text{last}(\text{ins } i) \rangle \frown \text{ins}(i + 1)$$

$$\forall j : \text{dom route} \mid j \neq i \wedge j \neq i + 1 \bullet$$

$$\text{ins}' j = \text{ins } j$$

Ising Z

20-12

## Consistency

$$\exists s : \text{seq } M \bullet \text{in} = s \frown \text{out}$$

### Section

$$\text{head rec} = (\frown / \text{ins}) \frown (\text{last sent})$$

## Base case

$$(\cap / ins) \cap (last sent)$$

$$= (\cap / \langle ins 1 \rangle) \cap (last \langle sent 1 \rangle)$$

[#route = #ins = #sent = 1]

$$= (ins 1) \cap (sent 1)$$

[by definition of  $\cap /$ ]

$$= rec 1$$

[from Section]

$$= head rec$$

[by definition of *head*]

Jsing Z

20-14

## Inductive step

$$head(front rec) = (\cap / (front ins)) \cap (last(front sent))$$

$$(\cap / ins) \cap (last sent)$$

$$= (\cap / ((front ins) \cap (last ins))) \cap (last sent)$$

[#ins = #route > 1]

$$= (\cap / (front ins)) \cap (last ins) \cap (last sent)$$

[by the definition of  $\cap /$ ]

$$= (\cap / (front ins)) \cap (last rec)$$

[from Section]

$= (\cap / (front \ ins)) \cap (last \ (tail \ rec))$

[#rec = #route > 1]

$= (\cap / (front \ ins)) \cap (last \ (front \ sent))$

[from Section]

$= head(front \ rec)$

[by the inductive hypothesis]

$= head \ rec$

[by a property of *head*]

Ising Z

20-16

## Retrieve relation

<i>RetrieveExtSection</i>
<i>Ext</i>
<i>Section</i>
<i>in = head rec</i>
<i>out = last sent</i>

$\forall Section \bullet \exists_1 Ext \bullet RetrieveExtSection$

## Initialisation

$\forall \text{Ext}'; \text{Section}' \mid$   
 $\text{SectionInit} \wedge \text{RetrieveExtSection}' \bullet$   
 $\text{ExtInit}$

Ising Z

20-18

## Transmission

$\forall \text{Ext}; \text{Section} \mid$   
 $\text{pre } \text{Transmit} \wedge \text{RetrieveExtSection}' \bullet$   
 $\text{pre } \text{STransmit}$

$\forall \text{Ext}; \text{Ext}'; \text{Section}; \text{Section}' \mid$   
 $\text{pre } \text{Transmit} \wedge \text{RetrieveExtSection} \wedge$   
 $\text{STransmit} \wedge \text{RetrieveExtSection}' \bullet$   
 $\text{Transmit}$

Transmit

## The daemon

```
forall Ext; Section |  
  pre ExistExt ∧ RetrieveExtSection' •  
  pre Daemon  
  
forall Ext; Ext'; Section; Section' |  
  pre ExistExt ∧ RetrieveExtSection ∧  
  Daemon ∧ RetrieveExtSection' •  
  Exist
```

Ising Z

20-20

## Inserting a new section

```
<a, b, d, e, f> insert (2, c) = <a, b, c, d, e, f>
```

$$\begin{aligned}
 [X] &= \\
 \_insert\_ : \text{seq } X \times (\mathbb{N} \times X) &\rightarrow \text{seq } X \\
 \forall s : \text{seq } X; i : \mathbb{N}; x : X \bullet \\
 s \text{ insert } (i, x) &= \\
 (1 \dots i) \triangleleft s \frown \langle x \rangle \frown \text{squash}((1 \dots i) \triangleleft s)
 \end{aligned}$$

Ising Z

20-22

$$\begin{aligned}
 \text{InsertSection} &= \\
 \Delta \text{Section} & \\
 s? , new? : SPC & \\
 s? \in \text{ran}(\text{front route}) & \\
 new? \notin \text{ran route} & \\
 \exists i : 1 \dots (\#route - 1) \mid & \\
 i = \text{route}^\sim s? \bullet & \\
 \text{route}' = \text{route insert } (i, new?) & \\
 rec' = rec \text{ insert } (i, sent i) & \\
 ins' = ins \text{ insert } (i, \langle \rangle) & \\
 sent' = sent \text{ insert } (i, rec i + 1) &
 \end{aligned}$$

$\sim / \text{ins}'$

$= \sim /(\text{ins} \text{ insert}(i + 1, \langle \rangle))$

[property of  $\text{ins}'$ ]

$= \sim /((1 .. i \triangleleft \text{ins}) \sim \langle \rangle) \sim (\text{squash}(1 .. i \triangleleft \text{ins}))$

[property of  $\text{insert}$ ]

$= \sim /(1 .. i) \triangleleft \text{s} \sim \langle \rangle \sim \sim / \text{squash}(1 .. i) \triangleleft \text{ins})$

[property of  $\sim /$ ]

Ising Z

20-24

$= \sim /(1 .. i \triangleleft \text{ins}) \sim \sim /(\text{squash}(1 .. i \triangleleft \text{ins}))$

[property of  $\langle \rangle$ ]

$= \sim /((1 .. i \triangleleft \text{ins}) \sim (\text{squash}(1 .. i \triangleleft \text{ins})))$

[property of  $\sim /$ ]

$= \sim / \text{ins}$

[properties of  $\triangleleft$  and  $\triangleleft$ ]