

A Telecommunications Protocol

Using Z
Woodcock & Davies

External view

$[M]$

Ext

$in, out : \text{seq } M$

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

Initially

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

Transmit

ΔExt

$m? : M$

$in' = \langle m? \rangle \cap in$

$out' = out$

Receive

ΔExt

$in' = in$

$\#out' = \#out + 1 \vee out' = out$

Sectional view

[*SPC*]

Section

route : iseq *SPC*

rec, ins, sent : seq(seq *M*)

route $\neq \langle \rangle$

#*route* = #*rec* = #*ins* = #*sent*

rec = *ins* $\hat{=}$ *sent*

front sent = *tail rec*

$[X]$

$$_ \doteq _ : \text{seq}(\text{seq } X) \times \text{seq}(\text{seq } X) \rightarrow \text{seq}(\text{seq } X)$$

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

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

$$(s \doteq t)i = (s i) \cap (t i)$$

SectionInit

Section'

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

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

S_{Transmit}

$\Delta S_{Section}$

$m? : M$

$route' = route$

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

$tail\ rec' = tail\ rec$

$ins' = ins$

$sent' = sent$

SReceive

$\Delta \text{Section}$

$\text{route}' = \text{route}$

$\text{rec}' = \text{rec}$

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

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

$\text{front sent}' = \text{front sent}$

$\text{last sent}' = \langle \text{last}(\text{last ins}) \rangle \cap (\text{last sent})$

Daemon

ΔSection

$$\begin{aligned} \exists i : 1 .. \#route - 1 \mid \\ & ins\ i \neq \langle \rangle \bullet \\ & ins'\ i = front(ins\ i) \\ & ins'(i + 1) = \langle last(ins\ i) \rangle \cap ins(i + 1) \\ \forall j : \text{dom } route \mid j \neq i \wedge j \neq i + 1 \bullet \\ & ins'\ j = ins\ j \end{aligned}$$

Consistency

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

Section
 $\overline{\text{head } rec = (\wedge / ins) \wedge (\text{last sent})}$

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*]

Inductive step

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

$$(\cap / \text{ins}) \cap (\text{last } \text{sent})$$

$$= (\cap / ((\text{front } \text{ins}) \cap \langle \text{last } \text{ins} \rangle)) \cap (\text{last } \text{sent})$$

[#ins = #route > 1]

$$= (\cap / (\text{front } \text{ins})) \cap (\text{last } \text{ins}) \cap (\text{last } \text{sent})$$

[by the definition of $\cap /$]

$$= (\cap / (\text{front } \text{ins})) \cap (\text{last } \text{rec})$$

[from *Section*]

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

[$\#rec = \#\text{route} > 1$]

$$= (\cap / (\text{front ins})) \cap (\text{last}(\text{front sent}))$$

[from *Section*]

$$= \text{head}(\text{front rec})$$

[by the inductive hypothesis]

$$= \text{head } rec$$

[by a property of *head*]

Retrieve relation

RetrieveExtSection

Ext

Section

in = head rec

out = last sent

$\forall \text{Section} \bullet \exists_1 \text{Ext} \bullet \text{RetrieveExtSection}$

Initialisation

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

Transmission

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

The daemon

$\forall Ext; Section \mid$
 pre $\exists Ext \wedge RetrieveExtSection' \bullet$

 pre *Daemon*

$\forall Ext; Ext'; Section; Section' \mid$
 pre $\exists Ext \wedge RetrieveExtSection \wedge$
 Daemon $\wedge RetrieveExtSection' \bullet$
 $\exists Ext$

Inserting a new section

$$\langle a, b, d, e, f \rangle \text{ insert } (2, c) = \langle a, b, c, d, e, f \rangle$$

$[X]$ $_insert_ : \text{seq } X \times (\mathbb{N} \times X) \rightarrow \text{seq } X$ $\forall s : \text{seq } X; i : \mathbb{N}; x : X \bullet$ $s \text{ insert } (i, x)$ $=$ $(1 .. i) \triangleleft s \cap \langle x \rangle \cap \text{squash}((1 .. i) \triangleleft s)$

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

\cap / ins' $= \cap / (ins insert (i + 1, \langle \rangle))$

[property of *ins'*]

 $= \cap / ((1 .. i \triangleleft ins) \cap \langle \rangle \cap (squash(1 .. i \triangleleft ins)))$

[property of *insert*]

 $= \cap / (1 .. i) \triangleleft s \cap \langle \rangle \cap \cap / squash((1 .. i) \triangleleft ins)$

[property of $\cap /$]

$$= \cap / (1 .. i \triangleleft ins) \cap \cap / (squash(1 .. i \triangleleft ins))$$

[property of $\langle \rangle$]

$$= \cap / ((1 .. i \triangleleft ins) \cap (squash(1 .. i \triangleleft ins)))$$

[property of $\cap /$]

$$= \cap / ins$$

[properties of \triangleleft and \triangleleft]