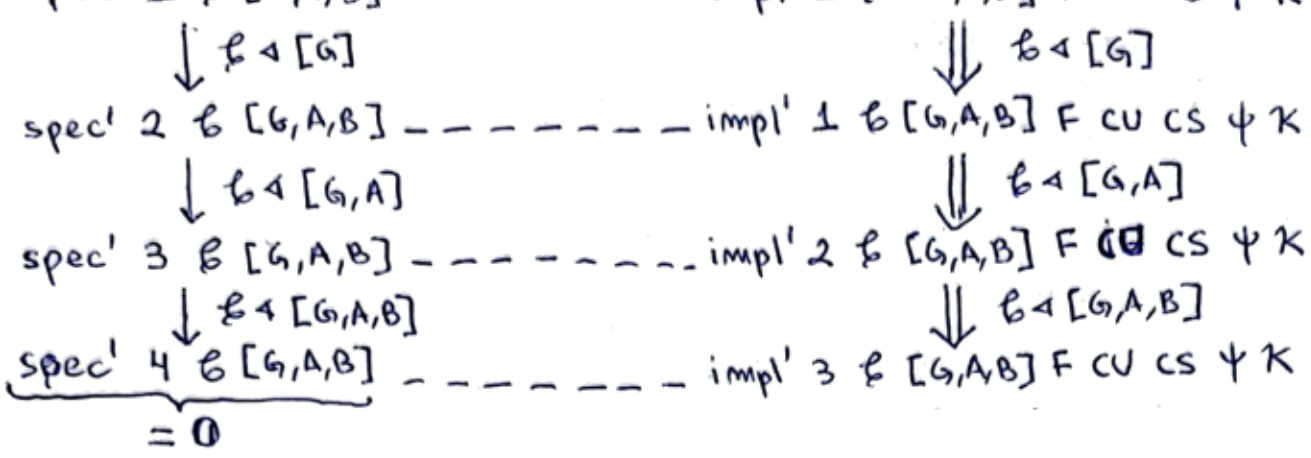
```
spec' K ℬ C = foldr (λC p. ℬ ◁s C; p) [C'. C' ← prefixes C ∧ length C' ≥ K] 0
spec ℬ C    = spec' 1 ℬ C
impl' K ℬ C b φc φs ψ κ = υ ℬ' c s.
  ([[client_main_loop]] ψ κ (take K C) ℬ φc c s ||
   [[server_main_loop]] ψ ℬ' b (take K C) φs c s ||
   ℬ' ◁s^∞ C)
impl ℬ C ψ κ = impl' 1 ℬ C F IF CS ψ κ
```

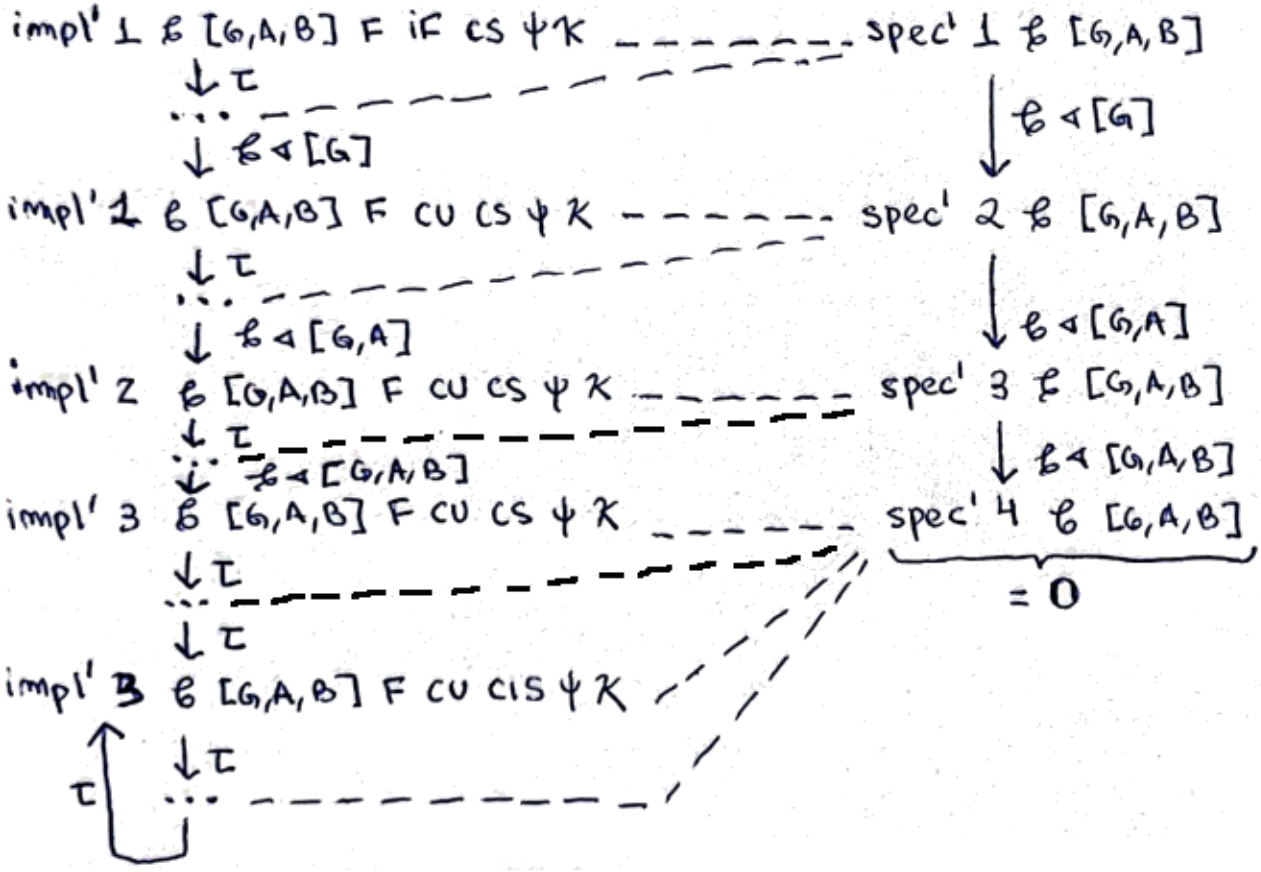
where $[\![\Pi]\!]$ is the translation of program Π to the $\flat$-calculus

$$spec\ \mathcal{B}\ C \approx impl\ \mathcal{B}\ C\ \psi\ \kappa$$

Forward case: (F ≡ False, iF = IntersectionFinding, CS = ClientSyncing, CU = ChainUpdate, CiS = clientInSync)



Backward case:



Theorem: $\text{spec}\ \&\ C \approx \text{impl}\ \&\ C\ \psi\ \kappa$

Proof:

Forward case: $\langle \text{spec}\ \&\ C, \text{impl}\ \&\ C\ \psi\ \kappa \rangle \in \mathcal{R}$.

Assume $\text{spec}\ \&\ C \xrightarrow{\alpha} p$. Then $\alpha = \&\triangleleft \text{hd}\, C$ and $p = \text{spec}'2\ \&\ C$ (since $\text{spec}\ \&\ C = \text{spec}'1$ then $\text{spec}\ \&\ C \xrightarrow{\&\triangleleft[\text{hd}\,C]} \text{spec}'2\ \&\ C$.

Moreover, we will show that $\text{impl}\ \&\ C\ \psi\ \kappa \xrightarrow{\&\triangleleft[\text{hd}\,C]} \text{impl}'1\ \&\ C\ F\ \text{CU}\ CS\ \psi\ \kappa$:

$\text{impl}\ \&\ C\ \psi\ \kappa = \text{impl}'1\ \&\ C\ F\ \text{iF}\ CS\ \psi\ \kappa =$

$\nu\, \&'\, cs.\ (\text{client}\ \psi\ \kappa\ [\text{hd}\,C]\ \&\ \text{iF}\ c\ s \parallel \text{server}\ \psi\ \&'\ F\ [\text{hd}\,C]\ CS\ c\ s \parallel \&'\triangleleft^{\infty} C)$.

Now, by rules SEND and RECV

1. $\text{client}\ \psi\ \kappa\ [\text{hd}\,C]\ \&\ \text{iF}\ c\ s \xrightarrow{s\triangleleft \text{FindIntersect}\,(\kappa\ [\text{hd}\,C])} \downarrow M.\ (\cdots)$
2. $\text{server}\ \psi\ \&'\ F\ [\text{hd}\,C]\ CS\ c\ s \xrightarrow{s\triangleright \text{FindIntersect}\,(\kappa\ [\text{hd}\,C])} \&' \to Cs.\ \cdots$

Then, from 1 and 2 by rules COM and RES and PAR we have

3. $\text{impl}\ \&\ C\ \psi\ \kappa \xrightarrow{\tau} \nu\, \&'\, cs.\ (\downarrow M.\ (\cdots) \parallel \&' \to Cs. \cdots \parallel \&'\triangleleft^{\infty} C)$.

Now, by rules SEND and RECV

4. $\&'\triangleleft^{\infty} C \xrightarrow{\&'\triangleleft C} \&'\triangleleft^{\infty} C$
5. $\&' \to Cs. \cdots \xrightarrow{\&'\triangleright C} \underbrace{\text{case}\ \underbrace{\text{first\_intersection\_point}\ \psi^{*}\,(\kappa\,[\text{hd}\,C])\ C}_{\psi\,(\text{hd}\,C)}\ \text{of}\ \cdots}_{\uparrow \text{Cont}\,(\text{IntersectFound}\,(\psi\,(\text{hd}\,C)));\ \text{server}\ \psi\ \&'\ T\ [\text{hd}\,C]\ CS\ c\ s}$

Then, from 4 and 5 by rules COM and RES and PAR we have ⑧ [see footnote] $\&'\triangleleft^{\infty} C$)

6. $\nu\, \&'\, cs.\ (\downarrow M.\ (\cdots) \parallel \&' \to Cs. \cdots \parallel \&'\triangleleft^{\infty} C) \xrightarrow{\tau}$
   $\nu\, \&'\, cs.\ (\downarrow M.\ (\cdots) \parallel \uparrow \text{Cont}\,(\text{IntersectFound}\,(\psi\,(\text{hd}\,C)));\ \text{server}\ \psi\ \&'\ T\ [\text{hd}\,C]\ CS\ c\ s \parallel$

Now, by rules SEND and RECV

7. $\uparrow \text{Cont}\,(\text{IntersectFound}\,(\psi\,(\text{hd}\,C)));\ \text{server}\ \psi\ \&'\ T\ [\text{hd}\,C]\ CS\ c\ s \xrightarrow{c\triangleleft \text{IntersectFound}\,(\psi\,(\text{hd}\,C))}$
   $\text{server}\ \psi\ \&'\ T\ [\text{hd}\,C]\ CS\ c\ s$
8. $\downarrow M.\ (\cdots) \xrightarrow{c\triangleright \text{IntersectFound}\,(\psi\,(\text{hd}\,C))} \text{client}\ \psi\ \kappa\ [\text{hd}\,C]\ \&\ CU\ c\ s$

Then, from 7 and 8 by rules COM and RES and PAR we have

9. $\underbrace{\nu\, \&'\, cs.\ (\text{client}\ \psi\ \kappa\ [\text{hd}\,C]\ \&\ CU\ c\ s \parallel \text{server}\ \psi\ \&'\ T\ [\text{hd}\,C]\ CS\ c\ s \parallel \&'\triangleleft^{\infty} C)}_{\text{impl}'1\ \&\ C\ T^{CU}_{CS}\ \psi\ \kappa}, \xrightarrow{\tau}$

Now, by rules SEND and RECV

10. $\text{client}\ \psi\ \kappa\ [\text{hd}\,C]\ \&\ CU\ c\ s \xrightarrow{s\triangleleft \text{RequestNext}} \downarrow M.\ (\cdots)$
11. $\text{server}\ \psi\ \&'\ T\ [\text{hd}\,C]\ CS\ c\ s \xrightarrow{s\triangleright \text{RequestNext}} \uparrow \text{Cont}\,(\text{RollBackward}\,(\psi\,(\text{hd}\,C)));$
    $\text{server}\ \psi\ \&'\ F\ [\text{hd}\,C]\ CS\ c\ s$

Then, from 10 and 11 by rules COM and RES and PAR we have 12.

12. $\text{impl}'1\ \&\ C\ T^{CU}_{CS}\ \psi\ \kappa \xrightarrow{\tau} \nu\, \&'\, cs.\ (\downarrow M.\ (\cdots) \parallel \uparrow \text{Cont}\,(\text{RollBackward}\,(\psi\,(\text{hd}\,C)));$
    $\text{server}\ \psi\ \&'\ F\ [\text{hd}\,C]\ CS\ c\ s \parallel \&'\triangleleft^{\infty} C)$

⑧ Actually, the rearranging of processes will be done later by using "up to bisimilarity"

Now, by rules SEND and RECV

13. $\uparrow$Cont(RollBackward(ψ(hd c))); server ψ b' F [hd c] CS c s $\xrightarrow{c \triangleleft \text{RollBackward}(\psi(\text{hd } c))}$ server ψ b' F [hd c] CS c s

14. $\downarrow$M.(···) $\xrightarrow{c \triangleright \text{RollBackward}(\psi(\text{hd } c))}$ b $\leftarrow$ roll_back ψ [hd c] [ψ(hd c)]; client ψ κ [hd c] b CU c s

Then, from 13 and 14 by rules COM, 2nd PAR and RES we have 15.

15. ν b' c s.($\downarrow$M.(···) $\|$ $\uparrow$Cont(RollBackward(ψ(hd c))); server ψ b' F [hd c] CS c s $\|$ b' $\triangleleft^{\infty}$ c) $\xrightarrow{\tau}$ ν b' c s.(b $\leftarrow$ [hd c]; client ψ κ [hd c] b CU c s $\|$ server ψ b' F [hd c] CS c s $\|$ b' $\triangleleft^{\infty}$ c)

Now, by rules SEND

16. b $\leftarrow$ [hd c]; client ψ κ [hd c] b CU c s $\xrightarrow{b \triangleleft [\text{hd } c]}$ client ψ κ [hd c] b CU c s

Then, from 16 by rules PAR and RES we have

17. ν b' c s.(b $\leftarrow$ [hd c]; ··· $\|$ ··· $\|$ b' $\triangleleft^{\infty}$ c) $\xrightarrow{b \triangleleft [\text{hd } c]}$ impl' 1 b C F CU CS ψ κ

Then, from 3, 6, 9, 12, 15 and 17 we have that

impl b C ψ κ $\xRightarrow{b \triangleleft [\text{hd } c]}$ impl' 1 b C F CU CS ψ κ $\in \mathcal{R}$.

And, moreover, $\langle$spec' 2 b C, impl' 1 b C F CU CS ψ $\kappa\rangle \in \mathcal{R}$.

Now, assume $k \in [1, |c|-1]$. Then, $\langle$spec' (k+1) b C, impl' k b C F CU CS ψ $\kappa\rangle \in \mathcal{R}$.

Assume spec' (k+1) b C $\xrightarrow{\alpha}$ p. then, α = b $\triangleleft$ take (k+1) C and p = spec' (k+2) b C.

Then spec' (k+1) b C $\xrightarrow{b \triangleleft \text{take } (k+1)\ c}$ spec' (k+2) b C.

Moreover, we will show that impl' k b C F CU CS ψ κ $\xRightarrow{b \triangleleft \text{take } (k+1)\ c}$ impl' (k+1) b C F CU CS ψ κ.

impl' k b C F CU CS ψ κ = ν b' c s.(client ψ κ (take k c) b CU c s $\|$ server ψ b' F (take k c) CS c s $\|$ b' $\triangleleft^{\infty}$ c).

Now, by rules SEND and RECV

18. client ψ κ (take k C) b CU c s $\xrightarrow{s \triangleleft \text{RequestNext}}$ $\downarrow$M.(···)

19. server ψ b' F (take k C) b CU c s $\xrightarrow{s \triangleleft \text{RequestNext}}$ b' $\rightarrow$ Cs.···

Then, from 18 and 19 by rules COM, PAR and RES 20.

impl' k b C F CU CS ψ κ $\xrightarrow{\tau}$ ν b' c s.($\downarrow$M.(···) $\|$ b' $\rightarrow$ Cs.··· $\|$ b' $\triangleleft^{\infty}$ c)

Now, by rules SEND and RECV

21. b' $\triangleleft^{\infty}$ c $\xrightarrow{b' \triangleleft c}$ b' $\triangleleft^{\infty}$ c

22. b' $\rightarrow$ Cs.··· $\xrightarrow{b' \triangleright c}$ case server_step ψ (take k c) c of ··· Progress (RollForward (c ! k)) (take (k+1) c) $\rightarrow$ $\uparrow$Cont(RollForward(c ! k)); server ψ b' F (take (k+1) c) CS c s

Then, from 21 and 22 by rules COM, PAR and RES

23. ν b' c s.($\downarrow$M.(···) $\|$ b' $\rightarrow$ Cs.··· $\|$ b' $\triangleleft^{\infty}$ c) $\xrightarrow{\tau}$ ν e' c s.($\downarrow$M.(···) $\|$ $\uparrow$Cont(RollForward(c ! k)); ··· $\|$ b' $\triangleleft^{\infty}$ c)

Now, by rules SEND and RECV

24. $\uparrow \mathrm{Cont}(\mathrm{RollForward}(c!k)); \mathrm{server}\ \psi\ b'\ F\ (\mathrm{take}\ (k+1)\ C)\ CS\ c\ s \xrightarrow{c \triangleleft \mathrm{RollForward}(c!k)}$
    $\mathrm{server}\ \psi\ b'\ F\ (\mathrm{take}\ (k+1)\ C)\ CS\ c\ s$

25. $\downarrow M.(\ldots) \xrightarrow{c \triangleright \mathrm{RollForward}(c!k)} b \leftarrow \underbrace{\mathrm{take}\ k\ c\ @\ [c!k]}_{\mathrm{take}\ (k+1)\ c}; \mathrm{client}\ \psi\ k\ (\mathrm{take}\ (k+1)\ C)\ b\ CU\ c\ s$

then, from 24 and 25 by rules COM, PAR and RES

26. $\nu\ b'\ c\ s.(\downarrow M.(\ldots) \parallel \uparrow \mathrm{Cont}(\mathrm{RollForward}(c!k)); \mathrm{server}\ \psi\ b'\ F\ (\mathrm{take}\ (k+1)\ C)\ CS\ c\ s \parallel b' \triangleleft^{\infty} C)$
$\xrightarrow{\tau} \nu\ b'\ c\ s.(b \leftarrow \mathrm{take}\ (k+1)\ c; \mathrm{client}\ \psi\ k\ (\mathrm{take}\ (k+1)\ C)\ b\ CU\ c\ s \parallel$
    $\mathrm{server}\ \psi\ b'\ F\ (\mathrm{take}\ (k+1)\ C)\ CS\ c\ s \parallel b' \triangleleft^{\infty} C)$

Now, by rule SEND

27. $b \leftarrow \mathrm{take}\ (k+1)\ C; \mathrm{client}\ \psi\ k\ (\mathrm{take}\ (k+1)\ C)\ b\ CU\ c\ s \xrightarrow{b \triangleleft \mathrm{take}\ (k+1)\ C}$
    $\mathrm{client}\ \psi\ k\ (\mathrm{take}\ (k+1)\ C)\ b\ CU\ c\ s$

Then, from 27 by rules PAR and RES

28. $\nu\ b'\ c\ s.(b \leftarrow \mathrm{take}\ (k+1)\ c; \mathrm{client}\ \psi\ k\ (\mathrm{take}\ (k+1)\ C)\ b\ CU\ c\ s \parallel$
    $\mathrm{server}\ \psi\ b'\ F\ (\mathrm{take}\ (k+1)\ C)\ CS\ c\ s \parallel b' \triangleleft^{\infty} C) \xrightarrow{b \triangleleft \mathrm{take}\ (k+1)\ C}$

$\mathrm{impl}'\ (k+1)\ b\ C\ F\ CU\ CS\ \psi\ k.$

Then, from 20, 23, 26 and 28 we have that

$\mathrm{impl}'\ k\ b\ C\ F\ CU\ CS\ \psi\ k \xRightarrow{b \triangleleft \mathrm{take}\ (k+1)\ C} \mathrm{impl}'\ (k+1)\ b\ C\ F\ CU\ CS\ \psi\ k.$

And, moreover, $\langle \mathrm{spec}'\ (k+2)\ b\ C, \mathrm{impl}'\ (k+1)\ b\ C\ F\ CU\ CS\ \psi\ k \rangle \in \mathcal{R}.$

Also, when $k = |C| - 1$ it holds that $\mathrm{spec}'\ (k+2)\ b\ C = \mathbf{0}$, therefore there are no further transitions to inspect.

Backward case:

It holds that $\langle impl\ b\ C\ \psi\ K, spec\ b\ C\rangle \in \mathcal{R}$. Now, assume that $impl\ b\ C\ \psi\ K \xrightarrow{\alpha} p$. By [using the same reasoning as the one used in the forward case, but noting that it is the only possible transition] $\circledast$ it holds that $\alpha = \tau$ and $p = \nu b'\, c\, s.(\downarrow M.(\cdots) \parallel b' \rightarrow C s. \cdots \parallel b' \triangleleft^{\infty} C)$.

Then $impl\ b\ C\ \psi\ K \xrightarrow{\tau} \nu b'\, c\, s.(\downarrow M.(\cdots) \parallel b' \rightarrow C s. \cdots \parallel b' \triangleleft^{\infty} C)$.

Moreover, $spec\ b\ C \Rightarrow spec\ b\ C$ (i.e., no step) and

$\langle \nu b'\, c\, s.(\downarrow M.(\cdots) \parallel b' \rightarrow C s. \cdots \parallel b' \triangleleft^{\infty} C), spec\ b\ C\rangle \in \mathcal{R}$.

Now assume $\nu b'\, c\, s.(\downarrow M.(\cdots) \parallel b' \rightarrow C s. \cdots \parallel b' \triangleleft^{\infty} C) \xrightarrow{\alpha} p$. By $\circledast$, it holds that $\alpha = \tau$ and $p = \nu b'\, c\, s.(\downarrow M.(\cdots) \parallel \uparrow Cont(IntersectionFound(\psi(hd\ c)); server\ \psi\ b'\ T\ [hd\ c]\ CS\ c\ s \parallel b' \triangleleft^{\infty} C)$.

Then $\nu b'\, c\, s.(\downarrow M.(\cdots) \parallel b' \rightarrow C s. \cdots \parallel b' \triangleleft^{\infty} C) \xrightarrow{\tau} \nu b'\, c\, s.(\downarrow M.(\cdots) \parallel \uparrow Cont(IntersectionFound(\psi(hd\ c)); server\ \psi\ b'\ T\ [hd\ c]\ CS\ c\ s \parallel b' \triangleleft^{\infty} C)$.

Moreover, $spec\ b\ C \Rightarrow spec\ b\ C$ (i.e., no step) and

$\langle \nu b'\, c\, s.(\downarrow M.(\cdots) \parallel \uparrow Cont(IntersectionFound(\psi(hd\ c)); server\ \psi\ b'\ T\ [hd\ c]\ CS\ c\ s \parallel b' \triangleleft^{\infty} C), spec\ b\ C\rangle \in \mathcal{R}$.

Now assume $\nu b'\, c\, s.(\downarrow M.(\cdots) \parallel \uparrow Cont(IntersectionFound(\psi(hd\ c)); server\ \psi\ b'\ T\ [hd\ c]\ CS\ c\ s \parallel b' \triangleleft^{\infty} C) \xrightarrow{\alpha} p$. By $\circledast$, it holds that $\alpha = \tau$ and $p = impl'\ 1\ b\ C\ T\ CU\ CS\ \psi\ K$. Then

$\nu b'\, c\, s.(\downarrow M.(\cdots) \parallel \uparrow Cont(IntersectionFound(\psi(hd\ c)); \cdots \parallel b' \triangleleft^{\infty} C) \xrightarrow{\tau} impl'\ 1\ b\ C\ T\ CU\ CS\ \psi\ K$.

Moreover, $spec\ b\ C \Rightarrow spec\ b\ C$ (i.e., no step) and

$\langle impl'\ 1\ b\ C\ T\ CU\ CS\ \psi\ K, spec\ b\ C\rangle \in \mathcal{R}$.

Now assume $impl'\ 1\ b\ C\ T\ CU\ CS\ \psi\ K \xrightarrow{\alpha} p$. By $\circledast$, it holds that $\alpha = \tau$ and $p = \nu b'\, c\, s.(\downarrow M.(\cdots) \parallel \uparrow Cont(RollBackward(\psi(hd\ c))); server\ \psi\ b'\ F\ [hd\ c]\ CS\ c\ s \parallel b' \triangleleft^{\infty} C)$

Then $impl'\ 1\ b\ C\ T\ CU\ CS\ \psi\ K \xrightarrow{\tau} \nu b'\, c\, s.(\downarrow M.(\cdots) \parallel \uparrow Cont(RollBackward(\psi(hd\ c))); server\ \psi\ b'\ F\ [hd\ c]\ CS\ c\ s \parallel b' \triangleleft^{\infty} C)$.

Moreover, $spec\ b\ C \Rightarrow spec\ b\ C$ (i.e., no step) and

$\langle \nu b'\, c\, s.(\downarrow N.(\cdots) \parallel \uparrow Cont(RollBackward(\psi(hd\ c))); server\ \psi\ b'\ F\ [hd\ c]\ CS\ c\ s \parallel b' \triangleleft^{\infty} C), spec\ b\ C\rangle \in \mathcal{R}$.

Now, assume $\nu b'\, c\, s.(\downarrow M.(\cdots) \parallel \uparrow Cont(RollBackward(\psi(hd\ c))); \cdots \parallel b' \triangleleft^{\infty} C) \xrightarrow{\alpha} p$.

By $\circledast$, it holds that $\alpha = \tau$ and $p = \nu e'\, c\, s.(b \leftarrow [hd\ c]; client\ \psi\ K\ [hd\ c]\ b\ CU\ c\ s \parallel server\ \psi\ b'\ F\ [hd\ c]\ CS\ c\ s \parallel b' \triangleleft^{\infty} C)$.

Then $\nu b'\, c\, s.(\downarrow M.(\cdots) \parallel \uparrow Cont(RollBackward(\psi(hd\ c))); \cdots \parallel b' \triangleleft^{\infty} C) \xrightarrow{\tau} \nu b'\, c\, s.(b \leftarrow [hd\ c]; client\ \psi\ K\ [hd\ c]\ b\ CU\ c\ s \parallel server\ \psi\ b'\ F\ [hd\ c]\ CS\ c\ s \parallel b' \triangleleft^{\infty} C)$.

Moreover, $spec\ b\ C \Rightarrow spec\ b\ C$ (i.e., no step) and

$\langle \nu b'\, c\, s.(b \leftarrow [hd\ c]; client\ \psi\ K\ [hd\ c]\ b\ CU\ c\ s \parallel server\ \psi\ b'\ F\ [hd\ c]\ CS\ c\ s \parallel b' \triangleleft^{\infty} C), spec\ b\ C\rangle \in \mathcal{R}$.

Now assume $\nu\, b'\, cs.\,(b \leftarrow [\mathrm{hd}\ c];\ \mathrm{client}\ \psi\ k\ [\mathrm{hd}\ c]\ b\ cv\ cs \parallel \mathrm{server}\ \psi\ b'\ F\ [\mathrm{hd}\ c]\ CS\ cs \parallel b' \triangleleft^{\infty} c) \xrightarrow{\alpha} p$. Then, by ⊛ it holds that $\alpha = b \triangleleft [\mathrm{hd}\ c]$ and $p = \mathrm{impl}'\ 1\ b\ C\ F\ cv\ CS\ \psi\ k$. then, $\nu\, b'\, cs.\,(b \leftarrow [\mathrm{hd}\ c];\ \mathrm{client}\ \psi\ k\ [\mathrm{hd}\ c]\ b\ cv\ cs \parallel \mathrm{server}\ \psi\ b'\ F\ [\mathrm{hd}\ c]\ CS\ cs \parallel b' \triangleleft^{\infty} c) \xrightarrow{b \triangleleft [\mathrm{hd}\ c]} \mathrm{impl}'\ 1\ b\ C\ F\ cv\ CS\ \psi\ k$.

Moreover, $\mathrm{spec}\ b\ C \xrightarrow{b \triangleleft [\mathrm{hd}\ c]} \mathrm{spec}'\ 2\ b\ C$, thus $\mathrm{spec}\ b\ C \xrightarrow{b \triangleleft [\mathrm{hd}\ c]} \mathrm{sped}\ 2\ b\ C$, and $\langle \mathrm{impl}'\ 1\ b\ C\ F\ cv\ CS\ \psi\ k, \mathrm{spec}'\ 2\ b\ c \rangle \in \mathcal{R}$.

Now, assume $k \in [1, |c| - 1]$. Then $\langle \mathrm{impl}'\ k\ b\ C\ F\ cv\ CS\ \psi\ k, \mathrm{spec}'\ (k+1)\ b\ C \rangle \in \mathcal{R}$.

Assume $\mathrm{impl}'\ k\ b\ C\ F\ cv\ CS\ \psi\ k \xrightarrow{\alpha} p$. then, by ⊛ it holds that $\alpha = \tau$ and $p = \nu\, b'\, cs.\,(\downarrow M.\,(\cdots) \parallel \uparrow \mathrm{Cont}\,(\mathrm{RollForward}\,(c\,!\,k));\ \mathrm{server}\ \psi\ b'\ F\ (\mathrm{take}\,(k+1)\,c)\ CS\ cs \parallel b' \triangleleft^{\infty} c)$.

Then, $\mathrm{impl}'\ k\ b\ C\ F\ cv\ CS\ \psi\ k \xrightarrow{\tau} \nu\, b'\, cs.\,(\downarrow M.\,(\cdots) \parallel \uparrow \mathrm{Cont}\,(\mathrm{RollForward}\,(c\,!\,k));\ \mathrm{server}\ \psi\ b'\ F\ (\mathrm{take}\,(k+1)\,c)\ CS\ cs \parallel b' \triangleleft^{\infty} c)$.

Moreover, $\mathrm{spec}'\ (k+1)\ b\ C \Longrightarrow \mathrm{spec}'\ (k+1)\ b\ C$ (i.e., no step) and $\langle \nu\, b'\, cs.\,(\downarrow M.\,(\cdots) \parallel \uparrow \mathrm{Cont}\,(\mathrm{RollForward}\,(c\,!\,k));\ \mathrm{server}\ \psi\ b'\ F\ (\mathrm{take}\,(k+1)\,c)\ CS\ cs \parallel b' \triangleleft^{\infty} c,\ \mathrm{spec}'\ (k+1)\ b\ C \rangle \in \mathcal{R}$.

Assume $\nu\, b'\, cs.\,(\downarrow M.\,(\cdots) \parallel \uparrow \mathrm{Cont}\,(\mathrm{RollForward}\,(c\,!\,k));\ \mathrm{server}\ \psi\ b'\ F\ (\mathrm{take}\,(k+1)\,c)\ CS\ cs \parallel b' \triangleleft^{\infty} c) \xrightarrow{\alpha} p$. Then, by ⊛ it holds that $\alpha = \tau$ and

$p = \nu\, b'\, cs.\,(b \leftarrow \mathrm{take}\,(k+1)\,c;\ \mathrm{client}\ \psi\ k\ (\mathrm{take}\,(k+1)\,c)\ b\ cv\ cs \parallel \mathrm{server}\ \psi\ b'\ F\ (\mathrm{take}\,(k+1)\,c)\ CS\ cs \parallel b' \triangleleft^{\infty} c)$.

Then, $\nu\, b'\, cs.\,(\downarrow M.\,(\cdots) \parallel \uparrow \mathrm{Cont}\,(\mathrm{RollForward}\,(c\,!\,k));\ \mathrm{server}\ \psi\ b'\ F\ (\mathrm{take}\,(k+1)\,c)\ CS\ cs \parallel b' \triangleleft^{\infty} c) \xrightarrow{\tau} \nu\, b'\, cs.\,(b \leftarrow \mathrm{take}\,(k+1)\,c;\ \mathrm{client}\ \psi\ k\ (\mathrm{take}\,(k+1)\,c)\ b\ cv\ cs \parallel \mathrm{server}\ \psi\ b'\ F\ (\mathrm{take}\,(k+1)\,c)\ CS\ cs \parallel b' \triangleleft^{\infty} c)$.

Moreover, $\mathrm{spec}'\ (k+1)\ b\ C \Longrightarrow \mathrm{spec}'\ (k+1)\ b\ C$ (i.e., no step) and $\langle \nu\, b'\, cs.\,(b \leftarrow \mathrm{take}\,(k+1)\,c;\ \mathrm{client}\ \psi\ k\ (\mathrm{take}\,(k+1)\,c)\ b\ cv\ cs \parallel \mathrm{server}\ \psi\ b'\ F\ (\mathrm{take}\,(k+1)\,c)\ CS\ cs \parallel b' \triangleleft^{\infty} c),\ \mathrm{spec}'\ (k+1)\ b\ C \rangle \in \mathcal{R}$.

Assume $\nu\, b'\, cs.\,(b \leftarrow \mathrm{take}\,(k+1)\,c;\ \mathrm{client}\ \psi\ k\ (\mathrm{take}\,(k+1)\,c)\ b\ cv\ cs \parallel \mathrm{server}\ \psi\ b'\ F\ (\mathrm{take}\,(k+1)\,c)\ CS\ cs \parallel b' \triangleleft^{\infty} c) \xrightarrow{\alpha} p$. Then, by ⊛ it holds that $\alpha = b \triangleleft \mathrm{take}\,(k+1)\,c$ and $p = \mathrm{impl}'\ (k+1)\ b\ C\ F\ cv\ CS\ \psi\ k$. Then,

$\nu\, b'\, cs.\,(b \leftarrow \mathrm{take}\,(k+1)\,c;\ \cdots \parallel \cdots \parallel b' \triangleleft^{\infty} c) \xrightarrow{b \triangleleft \mathrm{take}\,(k+1)\,c} \mathrm{impl}'\ (k+1)\ b\ C\ F\ cv\ CS\ \psi\ k$.

Moreover, $\mathrm{spec}'\ (k+1)\ b\ C \xrightarrow{b \triangleleft \mathrm{take}\,(k+1)\,c} \mathrm{spec}'\ (k+2)\ b\ C$, thus $\mathrm{spec}'\ (k+1)\ b\ C \xrightarrow{b \triangleleft \mathrm{take}\,(k+1)\,c} \mathrm{spec}'\ (k+2)\ b\ C$, and $\langle \mathrm{impl}'\ (k+1)\ b\ C\ F\ cv\ CS\ \psi\ k, \mathrm{spec}'\ (k+2)\ b\ C \rangle \in \mathcal{R}$.

Now, $\langle \mathrm{impl}'\ |c|\ b\ C\ F\ cv\ CS\ \psi\ k, \underbrace{\mathrm{spec}'\ (|c|+1)\ b\ C}_{\mathbf{0}} \rangle \in \mathcal{R}$.

Assume $\mathrm{impl}'\ |c|\ b\ C\ F\ cv\ CS\ \psi\ k \xrightarrow{\alpha} p$.

(Note that $\mathrm{impl}'\ |c|\ b\ C\ F\ cv\ CS\ \psi\ k = \nu\, b'\, cs.\,(\mathrm{client}\ \psi\ k\ C\ b\ cv\ cs \parallel \mathrm{server}\ \psi\ b'\ F\ C\ CS\ cs \parallel b' \triangleleft^{\infty} c)$.)

By rules SEND and RECV

29. client $\psi\ \kappa\ C\ b\ cv\ cs \xrightarrow{s \lhd RequestNext} \downarrow M.(\cdots)$

30. server $\psi\ b'\ F\ C\ CS\ cs \xrightarrow{s \rhd RequestNext} b' \to C_S.\cdots$

then, from 29 and 30 by rules COM, PAR and RES

31. $impl'\ |C|\ b\ C\ F\ cv\ cs\ \psi\ \kappa \xrightarrow{\tau} \nu b'cs.(\downarrow M.(\cdots) \parallel b' \to C_S.\cdots \parallel b' \lhd^{\infty} C)$

And this is only possible transition, therefore $\alpha = \tau$ and $P = \nu b'cs.(\downarrow M.(\cdots) \parallel b' \to C_S.\cdots \parallel b' \lhd^{\infty} C)$.

Moreover, $spec'(|C|+1)\ b\ C \Longrightarrow spec'(|C|+1)\ b\ C$ (i.e., no step) and $\langle \nu b'cs.(\downarrow M.(\cdots) \parallel b' \to C_S.\cdots \parallel b' \lhd^{\infty} C), spec'(|C|+1)\ b\ C \rangle \in \mathcal{R}$.

Assume that $\nu b'cs.(\downarrow M.(\cdots) \parallel b' \to C_S.\cdots \parallel b' \lhd^{\infty} C) \xrightarrow{\alpha} P$.

By rules SEND and RECV

32. $b' \lhd^{\infty} C \xrightarrow{b \lhd C} b' \lhd^{\infty} C$

33. $b' \to C_S.\cdots \xrightarrow{b \rhd C}$ case server_step $\psi\ C\ C$ of $\cdots$

Wait $\to$ $\uparrow$Cont AwaitReply; server $\psi\ b'\ F\ C\ cis\ cs$

Then, from 32 and 33 by rules COM, PAR and RES

34. $\nu b'cs.(\downarrow M.(\cdots) \parallel b' \to C_S.\cdots \parallel b' \lhd^{\infty} C) \xrightarrow{\tau} \nu b'cs.(\downarrow M.(\cdots) \parallel \uparrow Cont\ AwaitReply;$ server $\psi\ b'\ F\ C\ cis\ cs \parallel b' \lhd^{\infty} C)$. Also, this is the only possible transition, therefore $\alpha = \tau$ and $P = \nu b'cs.(\downarrow M.(\cdots) \parallel \uparrow Cont\ AwaitReply;$ server $\psi\ b'\ F\ C\ cis\ cs \parallel b' \lhd^{\infty} C)$.

Moreover, $spec'(|C|+1)\ b\ C \Longrightarrow spec'(|C|+1)\ b\ C$ (i.e., no step) and $\langle \nu b'cs.(\downarrow M.(\cdots) \parallel \uparrow Cont\ AwaitReply;$ server $\psi\ b'\ F\ C\ cis\ cs \parallel b' \lhd^{\infty} C), spec'(|C|+1)\ b\ C \rangle \in \mathcal{R}$.

Assume that $\nu b'cs.(\downarrow M.(\cdots) \parallel \uparrow Cont\ AwaitReply; \cdots \parallel b' \lhd^{\infty} C) \xrightarrow{\alpha} P$.

By rules SEND and RECV

35. $\uparrow Cont\ AwaitReply; \cdots \xrightarrow{c \lhd AwaitReply}$ server $\psi\ b'\ F\ C\ cis\ cs$, $b' \to C_S.\cdots$

36. $\downarrow M.(\cdots) \xrightarrow{c \rhd AwaitReply} \downarrow M.(\cdots)$

Then, from 35 and 36 by rules COM, PAR and RES

37. $\nu b'cs.(\downarrow M.(\cdots) \parallel \uparrow Cont\ AwaitReply; \cdots \parallel b' \lhd^{\infty} C) \xrightarrow{\tau}$
$\nu b'cs.(\downarrow M.(\cdots) \parallel b' \to C_S.\cdots \parallel b' \lhd^{\infty} C)$. Also, this is the only possible transition, therefore $\alpha = \tau$ and $P = \nu b'cs.(\downarrow M.(\cdots) \parallel b' \to C_S.\cdots \parallel b' \lhd^{\infty} C)$.

Moreover, $spec'(|C|+1)\ b\ C \Longrightarrow spec'(|C|+1)\ b\ C$ (i.e., no step) and $\langle \nu b'cs.(\downarrow M.(\cdots) \parallel b' \to C_S.\cdots \parallel b' \lhd^{\infty} C), spec'(|C|+1)\ b\ C \rangle \in \mathcal{R}$.

Assume $\nu b'cs.(\downarrow M.(\cdots) \parallel b' \to C_S.\cdots \parallel b' \lhd^{\infty} C) \xrightarrow{\alpha} P$.

By rules SEND and RECV

38. $b' \lhd^{\infty} C \xrightarrow{b \lhd C} b' \lhd^{\infty} C$

39. $b' \to C_S.\cdots \xrightarrow{b \rhd C}$ case server_step $\psi\ C\ C$ of $\cdots$

Wait $\to$ server $\psi\ b'\ F\ C\ cis\ cs = b' \to C_S.\cdots$

Then, from 38 and 39 by rules COM, PAR and RES

40. $\nu\, \mathfrak{b}'\, cs.(\downarrow M.(\ldots) \parallel \mathfrak{b}' \rightarrow C_S. \cdots \parallel \mathfrak{b}' \triangleleft^{\infty} C) \xrightarrow{\tau} \nu\, \mathfrak{b}'\, cs.(\downarrow M.(\ldots) \parallel \mathfrak{b} \rightarrow Cs. \cdots \parallel \mathfrak{b}' \triangleleft^{\infty} C)$.

Also, this is the only possible transition, therefore $\alpha = \tau$ and $P = \nu\, \mathfrak{b}'\, cs.(\downarrow M.(\ldots) \parallel \mathfrak{b}' \rightarrow C_S. \cdots \parallel \mathfrak{b}' \triangleleft^{\infty} C)$. Moreover, $spec'(|c|+1)\ \mathfrak{b}\ C \Rightarrow spec'(|c|+1)\ \mathfrak{b}\ C$ (i.e., no step) and (as already stated above)

$\langle \nu\, \mathfrak{b}'\, cs.(\downarrow M.(\ldots) \parallel \mathfrak{b}' \rightarrow C_S. \cdots \parallel \mathfrak{b}' \triangleleft^{\infty} C),\ spec'(|c|+1)\ \mathfrak{b}\ C \rangle \in \mathcal{R}$. ∎

Bisimulation relation:

$\mathcal{R} = \{\langle spec\ \mathfrak{b}\ C,\ impl\ \mathfrak{b}\ C\ \psi\ K \rangle\}$

$\cup\ \{\langle spec'(K+1)\ \mathfrak{b}\ C,\ impl'\ K\ \mathfrak{b}\ C\ F\ CU\ CS\ \psi\ K \rangle : K \in [1, |C|]\}$

$\cup\ \{\langle impl\ \mathfrak{b}\ C\ \psi\ K,\ spec\ \mathfrak{b}\ C \rangle,$

$\langle \nu\, \mathfrak{b}'\, cs.(\downarrow M.(\ldots) \parallel \mathfrak{b}' \rightarrow C_S. \cdots \parallel \mathfrak{b}' \triangleleft^{\infty} C),\ spec\ \mathfrak{b}\ C \rangle,$

$\langle \nu\, \mathfrak{b}'\, cs.(\downarrow M.(\ldots) \parallel \uparrow Cont(IntersectionFound(\psi(hd\ C)));\ldots \parallel \mathfrak{b}' \triangleleft^{\infty} C,\ spec\ \mathfrak{b}\ C \rangle,$

$\langle impl'\ 1\ \mathfrak{b}\ C\ T\ CU\ CS\ \psi\ K,\ spec\ \mathfrak{b}\ C \rangle,$

$\langle \nu\, \mathfrak{b}'\, cs.(\downarrow M.(\ldots) \parallel \uparrow Cont(RollBackward(\psi(hd\ C)));\cdots \parallel \mathfrak{b}' \triangleleft^{\infty} C,\ spec\ \mathfrak{b}\ C \rangle,$

$\langle \nu\, \mathfrak{b}'\, cs.(\mathfrak{b} \leftarrow [hd\ C];\ client\ \psi\ K\ [hd\ C]\ \mathfrak{b}\ CU\ cs \parallel server\ \psi\ \mathfrak{b}'\ F\ [hd\ C]\ CS\ s \parallel \mathfrak{b}' \triangleleft^{\infty} C),$

$spec\ \mathfrak{b}\ C \rangle,$

$\langle impl'\ 1\ \mathfrak{b}\ C\ F\ CU\ CS\ \psi\ K,\ spec'\ 2\ \mathfrak{b}\ C \rangle\}$

$\cup\ \{\langle impl'(K+1)\ \mathfrak{b}\ C\ F\ CU\ CS\ \psi\ K,\ spec'(K+2)\ \mathfrak{b}\ C \rangle : K \in [1, |C|-1]\}$

$\cup\ \{\langle \nu\, \mathfrak{b}'\, cs.(\downarrow M.(\ldots) \parallel \uparrow Cont(RollForward(C!K));\cdots \parallel \mathfrak{b}' \triangleleft^{\infty} C),\ spec'(K+1)\ \mathfrak{b}\ C \rangle :$

$K \in [1, |C|-1]\}$

$\cup\ \{\langle \nu\, \mathfrak{b}'\, cs.(\mathfrak{b} \leftarrow take(K+1)\ \mathfrak{b}\ C;\ldots \parallel \cdots \parallel \mathfrak{b}' \triangleleft^{\infty} C),\ spec'(K+1)\ \mathfrak{b}\ C \rangle : K \in [1, |C|-1]\}$

$\cup\ \{\langle \nu\, \mathfrak{b}'\, cs.(\downarrow M.(\ldots) \parallel \underbrace{\mathfrak{b}' \rightarrow C_S. \cdots}_{\text{the outermost}} \parallel \mathfrak{b}' \triangleleft^{\infty} C),\ spec'(|c|+1)\ \mathfrak{b}\ C \rangle,$

$\langle \nu\, \mathfrak{b}'\, cs.(\downarrow M.(\ldots) \parallel \uparrow Cont\ AwaitReply;\cdots \parallel \mathfrak{b}' \triangleleft^{\infty} C),\ spec'(|c|+1)\ \mathfrak{b}\ C \rangle,$

$\langle \nu\, \mathfrak{b}'\, cs.(\downarrow M.(\ldots) \parallel \underbrace{\mathfrak{b}' \rightarrow C_S. \cdots}_{\text{the innermost}} \parallel \mathfrak{b}' \triangleleft^{\infty} C),\ spec'(|c|+1)\ \mathfrak{b}\ C \rangle\}$