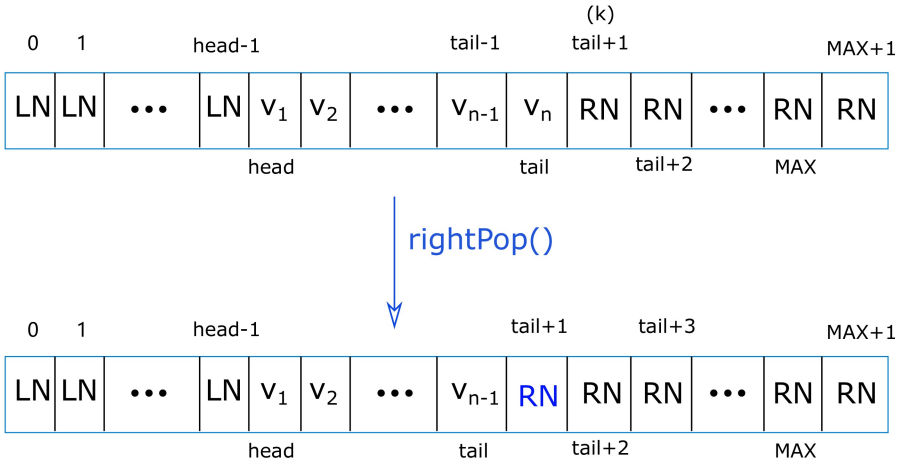

Fig.24 Transition caused by rightPop.

A Full Explanations of the Example

We will first show what a deque is by defining the abstract specification, which is a straightforward atomic implementation. Then we will show the practical obstruction-free implementation of deque from [15]. Finally, we will show how to verify the linearizability (*w.r.t* the abstract specification) and obstruction-freedom of the practical implementation.

A.1 Abstract Specification

There are four operations of the deque: rightPush(v), rightPop(), leftPush(v) and leftPop(). The operations are explained in the following.

- As shown in Fig. 13, rightPush(v) pushes the value v to the right ending of the deque (*i.e.*, storing v to s[tail + 1] and incrementing tail), under the assumption that tail < MAX.
- As shown in Fig. 24, rightPop() pops the value at the right ending of the deque (*i.e.*, poping s[tail] and decrementing tail), under the assumption that tail > head.
- leftPush(v) and leftPop() are similar to rightPush(v) and rightPop(), except that they operate at the left ending of the deque.

The abstract specification (a straightforward atomic implementation) is shown in Fig. 25 and 26.

A.2 A Practical Obstruction-free Implementation of Deque

This subsection shows the obstruction-free implementation of deque from [15].

The code for rightPush and rightPop is shown Fig. 27. The code for leftPush and leftPop is shown Fig. 28.

A.3 Verifying the Implementation

R and G^{rPush} The definition of G^{rPush} is shown in Fig. 19, which describes the actions updating the shared resources during the execution of rightPush.

The definition of G^{rPush} has the following two connotations:

```
int s[MAX+2], Head, Tail;
int LN, RN, EMPTY:=RN, MAX;

int rightPush(int v) {
  local B:=0;
  C_rpush;
  return B
}

C_rpush def=
  <if (Tail = MAX || v = LN || v = RN) B := -1
  else {
    s[Tail+1] := V;
    Tail := Tail + 1;
    B := 1
  }>

int rightPop(){
  local B:=0, V;
  C_rpop;
  if (B = -1) return EMPTY
  else return V
}

C_rpop def=
  <if (Head = Tail + 1) B := -1
  else {
    V := s[Tail];
    s[Tail] := RN;
    B := 1
  }>
```

Fig.25 Abstract spec for deque(right)

```
int leftPush(int v) {
  local B:=0;
  C_lpush;
  return B
}
```

$C_{\mathsf{lpush}} \stackrel{\mathsf{def}}{=}$

```
  <if (Head = 1 || v = LN || v = RN) B := -1
  else {
    s[Head-1] := V;
    Head := Head - 1;
    B := 1
  }>
```

```
int leftPop(){
  local B:=0, V;
  C_lpop;
  if (B = -1) return EMPTY
  else return V
}
```

$C_{\mathsf{rpop}} \stackrel{\mathsf{def}}{=}$

```
  <if (Head = Tail + 1) B := -1
  else {
    V := s[Head];
    s[Head] := LN;
    B := 1
  }>
```

Fig.26 Abstract spec for deque(left)

```
int rightPush(int v) {
1   local b:=0, k, prev, cur;
2   if (v = Rn || v = Ln) return −1;
3   while (b=0){
4     k := findRn();
5     prev := a[k−1];
6     cur := a[k];
7     if (prev.val != Rn && cur.val=Rn) {
8       if (k = Max + 1) b := −1
9       else {
10        if CAS(&a[k−1], prev, (prev.val, prev.ctr+1))
11          b := CAS(&a[k], cur, (v, cur.ctr+1))
        }
      }
    }
12  return b // b = −1 "error"; b = 1 "succeed"
}

int rightPop() {
13    local b:=0, cur, next;
14    while (b=0){
15      k := findRn();
16      cur := a[k−1];
17      next := a[k];
18      if (cur.val != Rn && next.val = Rn) {
19        if (cur.val = Ln && a[k−1] = cur) b := −1
          else {
20          if CAS(&a[k], next, (next.val, next.ctr+1))
21            b := CAS(&a[k−1], cur, (Rn, cur.ctr+1))
          }
        }
      }
22    if (b=−1) return Empty
23    else return cur.val
}
```

Fig.27 Implementation of rightPush and rightPop.

```
int leftPush(int v) {
  local b:=0, k, next, cur;
  if (v = Rn || v = Ln) return −1;
  while (b=0){
    k := findLn();
    next := a[k+1];
    cur := a[k];
    if (next.val != Ln && cur.val=Ln) {
      if (k = 0) b := −1
      else {
        if CAS(&a[k+1], next, (next.val, next.ctr+1))
          b := CAS(&a[k], cur, (v, cur.ctr+1))
      }
    }
  }
  return b // b = −1 "error"; b = 1 "succeed"
}

int leftPop() {
  local b:=0, cur, prev;
  while (b=0){
    k := findLn();
    cur := a[k+1];
    prev := a[k];
    if (cur.val != Ln && prev.val = Ln) {
      if (cur.val = Rn && A[k+1] = cur) b := −1
      else {
        if CAS(&a[k], prev, (prev.val, prev.ctr+1))
          b := CAS(&a[k+1], cur, (Ln, cur.ctr+1))
      }
    }
  }
  if (b=−1) return Empty
  else return cur.val
}
```

Fig.28 Implementation for leftPush and leftPop.

- It consists four transitions: rPush_1, rPush_2, rPush_3 and identical transition Id.
- All those transitions (together with possible identical parts denoted by Id) affects only shared resources (denoted by $I \ltimes I$).

With the definition, we know G_t^{rPush} satisfies the requirement $I \rhd G_t^{\mathsf{rPush}}$ in the OBJ rule.

The following are the explainations of rPush_1, rPush_2 and rPush_3.

- $\mathsf{rPush}_1^{\mathsf{t}}$ specifies the behavior of the first CAS in $\mathsf{rightPush}$. The action increments the version number of the item at the tail of the deque and sets $\mathsf{absq}[\mathsf{t}]$ from nil to $(\mathsf{rPush} :: v :: \mathsf{tail}+1 :: A(\mathsf{tail}+1) :: \mathsf{nil})$, which are preparations for the following actions.
- $\mathsf{rPush}_2^{\mathsf{t}}$ specifies the action that successfully pushes the value into the deque. This action requires that the first CAS be successful (*i.e.*, $\mathsf{absq}[t]$ is not nil) and that the value of $A[k]$ be equal to the fourth items of $\mathsf{absq}[t]$ (*i.e.*, if the value of $\mathsf{absq}[t]$ is $(\_ :: \_ :: k :: (\mathsf{val}, \mathsf{ctr}) :: \mathsf{nil})$, then $A[k]$ should be equal to $(\mathsf{val}, \mathsf{ctr})$). If all requirements are met, $\mathsf{rPush}_2^{\mathsf{t}}$ pushes v into the $\mathsf{tail}+1$ slot of the deque and resets $\mathsf{absq}[t]$ to nil.
- $\mathsf{rPush}_3^{\mathsf{t}}$ specifies the action when the second CAS fails. This action only resets $\mathsf{absq}[t]$ to nil.

Definitions of G^{rPop}, G^{lPush} and G^{lPop} are shown in Fig. 29, 30, 31.

Finally, we define R at the bottom of Fig. 19, which contains all actions that other threads may perform. It is worth noting that our definitions of R and G meet the requirements in the OBJ rule.

$$
\begin{array}{l}
\mathsf{rPop}_1^{\mathsf{t}} \stackrel{\mathsf{def}}{=} \exists \mathsf{head}, \mathsf{tail}, \mathsf{ctr}, A, a, s, \mathsf{rn}, \mathsf{ln}, \mathsf{max}. \\
\quad (\mathsf{absq}[t] \mapsto \mathsf{nil}) * (\mathsf{head} \le \mathsf{tail}+1) * \\
\quad \mathsf{queue}(A, \mathsf{head}, \mathsf{tail}, (a, s, \mathsf{rn}, \mathsf{ln}, \mathsf{max})) \\
\quad \ltimes \\
\quad (\mathsf{absq}[t] \mapsto \mathsf{rPop} :: \mathsf{tail} :: A(\mathsf{tail}) :: \mathsf{nil}) * \\
\quad A(\mathsf{tail}+1) = (\mathsf{rn}, \mathsf{ctr}) * A' = A\{\mathsf{tail}+1 \rightsquigarrow (\mathsf{rn}, \mathsf{ctr}+1)\} * \\
\quad \mathsf{queue}(A', \mathsf{head}, \mathsf{tail}, (a, s, \mathsf{rn}, \mathsf{ln}, \mathsf{max}))
\end{array}
$$

$$
\begin{array}{l}
\mathsf{rPop}_2^{\mathsf{t}} \stackrel{\mathsf{def}}{=} \exists \mathsf{head}, \mathsf{tail}, \mathsf{val}, \mathsf{ctr}, A, a, s, \mathsf{rn}, \mathsf{ln}, \mathsf{max}. \\
\quad (\mathsf{absq}[t] \mapsto \mathsf{rPop} :: k :: (\mathsf{val}, \mathsf{ctr}) :: \mathsf{nil}) * \\
\quad (A(k) = (\mathsf{val}, \mathsf{ctr})) * (k = \mathsf{tail}) \\
\quad \mathsf{queue}(A, \mathsf{head}, \mathsf{tail}, (a, s, \mathsf{rn}, \mathsf{ln}, \mathsf{max})) \\
\quad \ltimes \\
\quad (\mathsf{absq}[t] \mapsto \mathsf{nil}) * A' = A\{\mathsf{tail} \rightsquigarrow (\mathsf{rn}, \mathsf{ctr}+1)\} * \\
\quad \mathsf{queue}(A', \mathsf{head}, \mathsf{tail}-1, (a, s, \mathsf{rn}, \mathsf{ln}, \mathsf{max}))
\end{array}
$$

$$
\begin{array}{l}
\mathsf{rPop}_3^{\mathsf{t}} \stackrel{\mathsf{def}}{=} \exists \mathsf{head}, \mathsf{tail}, \mathsf{val}, \mathsf{ctr}, A, a, s, \mathsf{rn}, \mathsf{ln}, \mathsf{max}. \\
\quad (\mathsf{absq}[t] \mapsto \mathsf{rPop} :: k :: (\mathsf{val}, \mathsf{ctr}) :: \mathsf{nil}) * \\
\quad (A(k) \neq (\mathsf{val}, \mathsf{ctr})) * \\
\quad \mathsf{queue}(A, \mathsf{head}, \mathsf{tail}, (a, s, \mathsf{rn}, \mathsf{ln}, \mathsf{max})) \\
\quad \ltimes \\
\quad (\mathsf{absq}[t] \mapsto \mathsf{nil}) * \mathsf{queue}(A, \mathsf{head}, \mathsf{tail}, (a, s, \mathsf{rn}, \mathsf{ln}, \mathsf{max}))
\end{array}
$$

$$
G_{\mathsf{t}}^{\mathsf{rPop}} \stackrel{\mathsf{def}}{=} (\mathsf{rPop}_1^{\mathsf{t}} \vee \mathsf{rPop}_2^{\mathsf{t}} \vee \mathsf{rPop}_3^{\mathsf{t}} \vee \mathsf{Id}) * \mathsf{Id} \wedge (I \ltimes I)
$$

Fig.29 Definition of G^{rPop}.

$$
\begin{array}{l}
\mathsf{lPush}_1^{\mathsf{t}} \stackrel{\mathsf{def}}{=} \exists \mathsf{head}, \mathsf{tail}, v, \mathsf{val}, \mathsf{ctr}, A, a, s, \mathsf{rn}, \mathsf{ln}, \mathsf{max}. \\
\quad (\mathsf{absq}[t] \mapsto \mathsf{nil}) * (\mathsf{head} > 1) * (v \notin \{\mathsf{ln}, \mathsf{rn}\}) * \\
\quad \mathsf{queue}(A, \mathsf{head}, \mathsf{tail}, (a, s, \mathsf{rn}, \mathsf{ln}, \mathsf{max})) \\
\quad \ltimes \\
\quad (\mathsf{absq}[t] \mapsto \mathsf{lPush} :: v :: (\mathsf{head} - 1) :: A(\mathsf{head} - 1) :: \mathsf{nil}) * \\
\quad A(\mathsf{head}) = (\mathsf{val}, \mathsf{ctr}) * A' = A\{\mathsf{head} \rightsquigarrow (\mathsf{val}, \mathsf{ctr} + 1)\} * \\
\quad \mathsf{queue}(A', \mathsf{head}, \mathsf{tail}, (a, s, \mathsf{rn}, \mathsf{ln}, \mathsf{max}))
\end{array}
$$

$$
\begin{array}{l}
\mathsf{lPush}_2^{\mathsf{t}} \stackrel{\mathsf{def}}{=} \exists k, \mathsf{head}, \mathsf{tail}, v, \mathsf{ctr}, A, a, s, \mathsf{rn}, \mathsf{ln}, \mathsf{max}. \\
\quad (\mathsf{absq}[t] \mapsto \mathsf{lPush} :: v :: k :: (\mathsf{ln}, \mathsf{ctr}) :: \mathsf{nil}) * \\
\quad (A(k) = (\mathsf{ln}, \mathsf{ctr})) * (k = \mathsf{head} - 1) * \\
\quad \mathsf{queue}(A, \mathsf{head}, \mathsf{tail}, (a, s, \mathsf{rn}, \mathsf{ln}, \mathsf{max})) \\
\quad \ltimes \\
\quad (\mathsf{absq}[t] \mapsto \mathsf{nil}) * A' = A\{k \rightsquigarrow (v, \mathsf{ctr} + 1)\} * \\
\quad \mathsf{queue}(A', \mathsf{head} - 1, \mathsf{tail}, (a, s, \mathsf{rn}, \mathsf{ln}, \mathsf{max}))
\end{array}
$$

$$
\begin{array}{l}
\mathsf{lPush}_3^{\mathsf{t}} \stackrel{\mathsf{def}}{=} \exists k, \mathsf{head}, \mathsf{tail}, v, \mathsf{ctr}, A, a, s, \mathsf{rn}, \mathsf{ln}, \mathsf{max}. \\
\quad (\mathsf{absq}[t] \mapsto \mathsf{lPush} :: v :: k :: (\mathsf{ln}, \mathsf{ctr}) :: \mathsf{nil}) * \\
\quad (A(k) \neq (\mathsf{ln}, \mathsf{ctr})) * \\
\quad \mathsf{queue}(A, \mathsf{head}, \mathsf{tail}, (a, s, \mathsf{rn}, \mathsf{ln}, \mathsf{max})) \\
\quad \ltimes \\
\quad (\mathsf{absq}[t] \mapsto \mathsf{nil}) * \\
\quad \mathsf{queue}(A, \mathsf{head}, \mathsf{tail}, (a, s, \mathsf{rn}, \mathsf{ln}, \mathsf{max}))
\end{array}
$$

$$
G_{\mathsf{t}}^{\mathsf{lPush}} \stackrel{\mathsf{def}}{=} (\mathsf{lPush}_1^{\mathsf{t}} \vee \mathsf{lPush}_2^{\mathsf{t}} \vee \mathsf{lPush}_3^{\mathsf{t}} \vee \mathsf{Id}) * \mathsf{Id} \wedge (I \ltimes I)
$$

Fig.30 Definition of G^{lPush}.

A.3.1 Verifying the Judgment

For the proof sketch in Fig. 32, 33 and 34, we will focus on the reasoning for the two CAS statements. The first CAS is at line 9. If this CAS is successfully executed (*i.e.*, b_0 is 1), we know that the value of a[k − 1] is the same as prev. It can be inferred that the environment has not finished any rPush_1 or rPop_2 after the current thread finished executing line 3, as rPush_1 and rPop_2 will increment the version number of a[k − 1]. Therefore, the tail of the deque remains $(k-1)$ since line 3. The auxiliary code below line 9 updates the value of absq[t].

The second CAS is at line 11. If this CAS succeeds, we know that the value of a[k] is equal to cur, which records the value of a[k] at the point when the current thread executes line 5. Thus it can be inferred that the environment has not finished any rPush_2 or rPop_1 since line 5, as these actions will increase the version number of a[k − 1]. Therefore, the tail of the deque is equal to $k-1$ since line 5. Line 11 is also the linearizable point of rightPush, which means the abstract code C_{rpush} should be performed if this CAS succeeds. The auxiliary code below line 11 resets absq[t] to nil. As the rest of the proof sketch is straightforward, the explanations are omitted here.

Finally, the last part of the proof is shown in Fig. 35, which is the proof for the newly added side-condition in the while rule. Because there is only one while in the implementation, we only need to construct the sequential total-correctness judgment for the while statement at line 2 (as shown in Fig. 35). The proof is trivial because the while statement will obviously terminate in the sequential setting.

According to proof in Fig. 32, 33, 34 and 35, it can be concluded that the implementation of rightPush is

$$
\begin{array}{l}
\mathsf{lPop}_1^{\mathsf{t}} \stackrel{\mathsf{def}}{=} \exists \mathsf{head}, \mathsf{tail}, \mathsf{ctr}, A, a, s, \mathsf{rn}, \mathsf{ln}, \mathsf{max}. \\
\quad (\mathsf{absq}[t] \mapsto \mathsf{nil}) * (\mathsf{head} \leq \mathsf{tail} + 1) * \\
\quad \mathsf{queue}(A, \mathsf{head}, \mathsf{tail}, (a, s, \mathsf{rn}, \mathsf{ln}, \mathsf{max})) \\
\quad \ltimes \\
\quad (\mathsf{absq}[t] \mapsto \mathsf{lPop} :: \mathsf{head} :: A(\mathsf{head}) :: \mathsf{nil}) * \\
\quad A(\mathsf{head} - 1) = (\mathsf{ln}, \mathsf{ctr}) * A' = A\{\mathsf{head} - 1 \rightsquigarrow (\mathsf{ln}, \mathsf{ctr} + 1)\} * \\
\quad \mathsf{queue}(A', \mathsf{head}, \mathsf{tail}, (a, s, \mathsf{rn}, \mathsf{ln}, \mathsf{max}))
\end{array}
$$

$$
\begin{array}{l}
\mathsf{lPop}_2^{\mathsf{t}} \stackrel{\mathsf{def}}{=} \exists \mathsf{head}, \mathsf{tail}, \mathsf{val}, \mathsf{ctr}, A, a, s, \mathsf{rn}, \mathsf{ln}, \mathsf{max}. \\
\quad (\mathsf{absq}[t] \mapsto \mathsf{lPop} :: k :: (\mathsf{val}, \mathsf{ctr}) :: \mathsf{nil}) * \\
\quad (A(k) = (\mathsf{val}, \mathsf{ctr})) * (k = \mathsf{head}) \\
\quad \mathsf{queue}(A, \mathsf{head}, \mathsf{tail}, (a, s, \mathsf{rn}, \mathsf{ln}, \mathsf{max})) \\
\quad \ltimes \\
\quad (\mathsf{absq}[t] \mapsto \mathsf{nil}) * A' = A\{\mathsf{head} \rightsquigarrow (\mathsf{ln}, \mathsf{ctr} + 1)\} * \\
\quad \mathsf{queue}(A', \mathsf{head} + 1, \mathsf{tail}, (a, s, \mathsf{rn}, \mathsf{ln}, \mathsf{max}))
\end{array}
$$

$$
\begin{array}{l}
\mathsf{lPop}_3^{\mathsf{t}} \stackrel{\mathsf{def}}{=} \exists \mathsf{head}, \mathsf{tail}, \mathsf{val}, \mathsf{ctr}, A, a, s, \mathsf{rn}, \mathsf{ln}, \mathsf{max}. \\
\quad (\mathsf{absq}[t] \mapsto \mathsf{lPop} :: k :: (\mathsf{val}, \mathsf{ctr}) :: \mathsf{nil}) * \\
\quad (A(k) \neq (\mathsf{val}, \mathsf{ctr})) * \\
\quad \mathsf{queue}(A, \mathsf{head}, \mathsf{tail}, (a, s, \mathsf{rn}, \mathsf{ln}, \mathsf{max})) \\
\quad \ltimes \\
\quad (\mathsf{absq}[t] \mapsto \mathsf{nil}) * \\
\quad \mathsf{queue}(A, \mathsf{head}, \mathsf{tail}, (a, s, \mathsf{rn}, \mathsf{ln}, \mathsf{max}))
\end{array}
$$

$$
G_{\mathsf{t}}^{\mathsf{lPop}} \stackrel{\mathsf{def}}{=} (\mathsf{lPop}_1^{\mathsf{t}} \vee \mathsf{lPop}_2^{\mathsf{t}} \vee \mathsf{lPop}_3^{\mathsf{t}} \vee \mathsf{Id}) * \mathsf{Id} \wedge (I \ltimes I)
$$

Fig.31 Definition of G^{lPop}.

linearizable and obstruction-free.

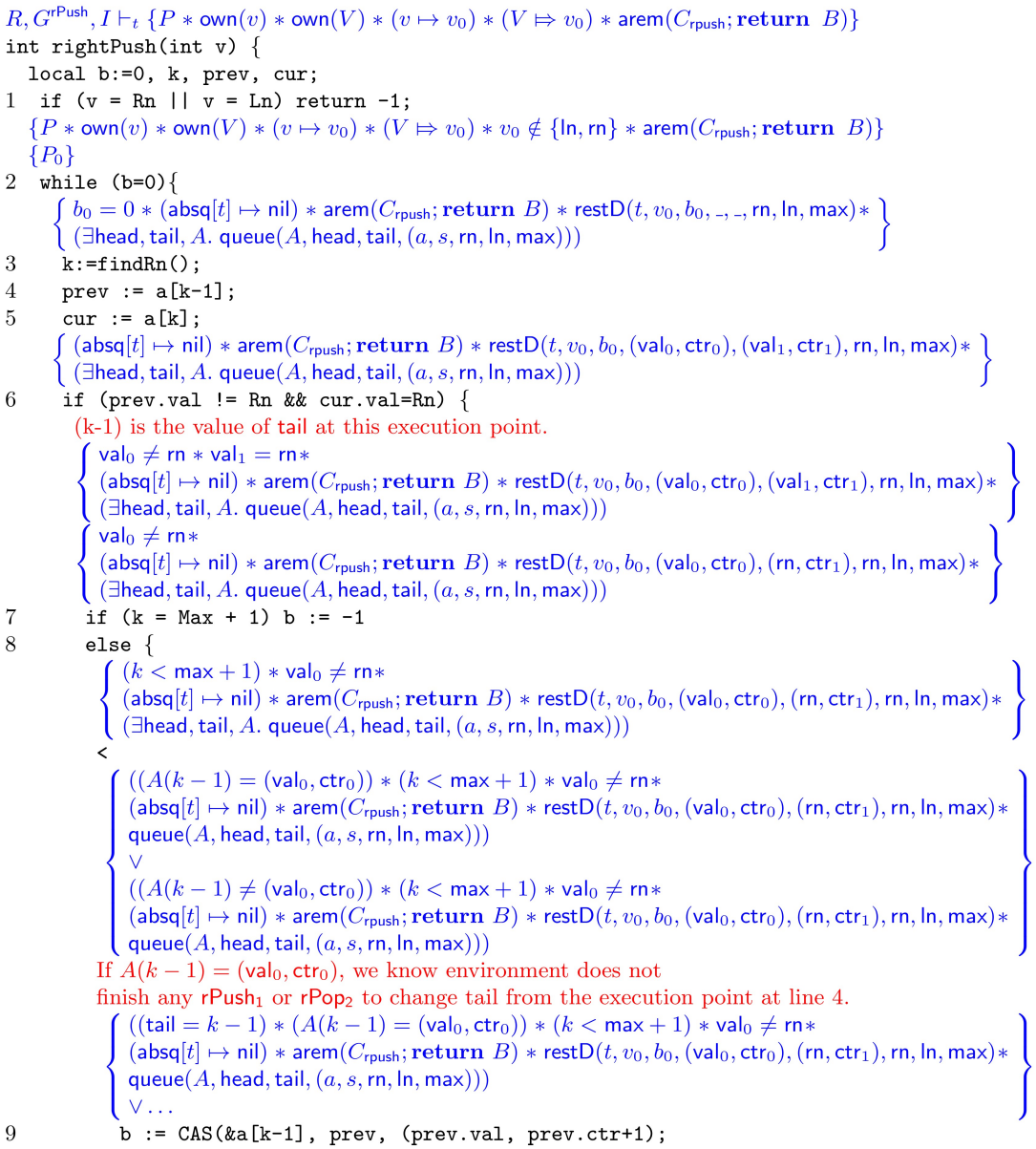

Fig.32 Proof sketch(part 1)

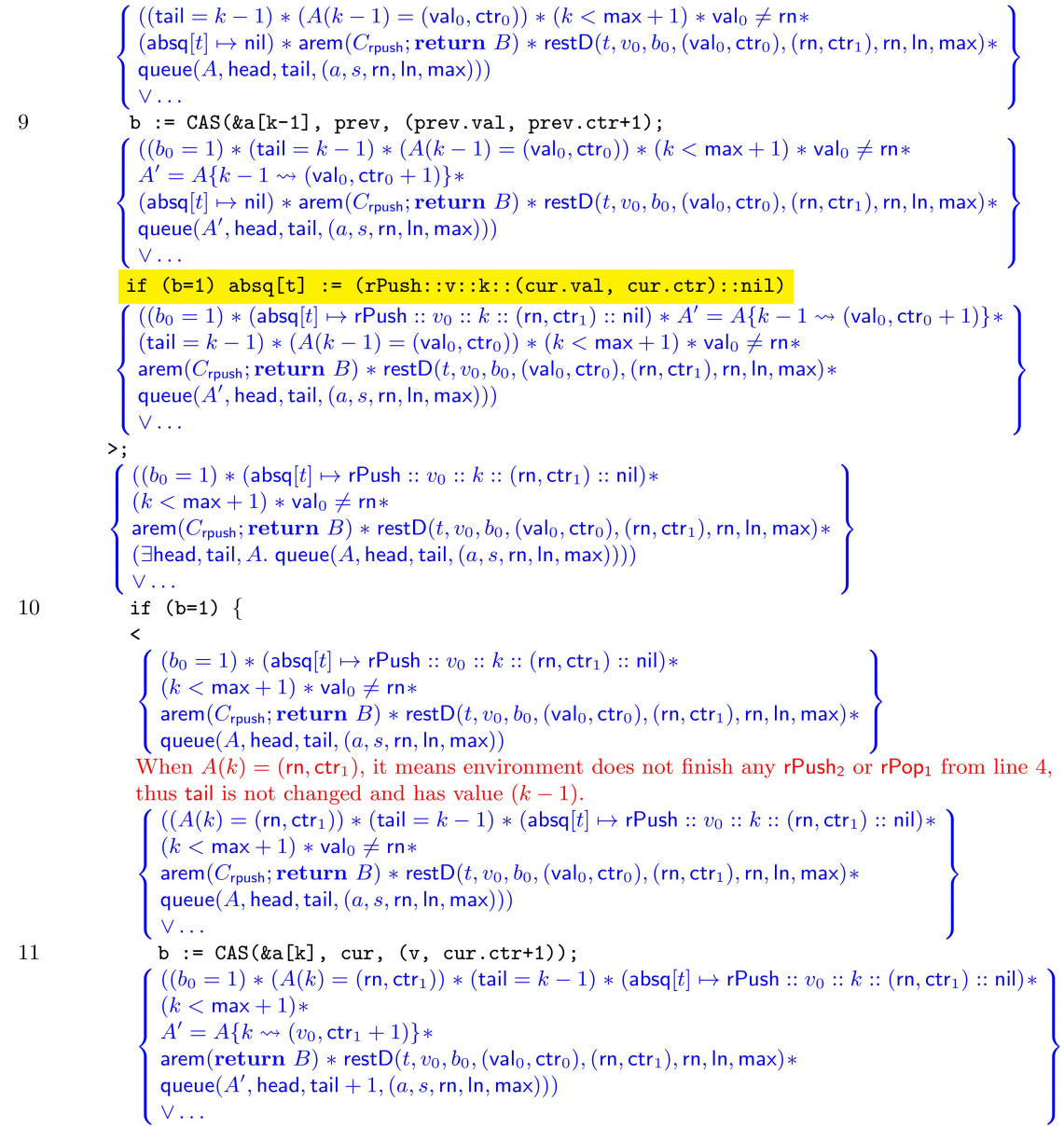

Fig.33 Proof sketch(part 2).

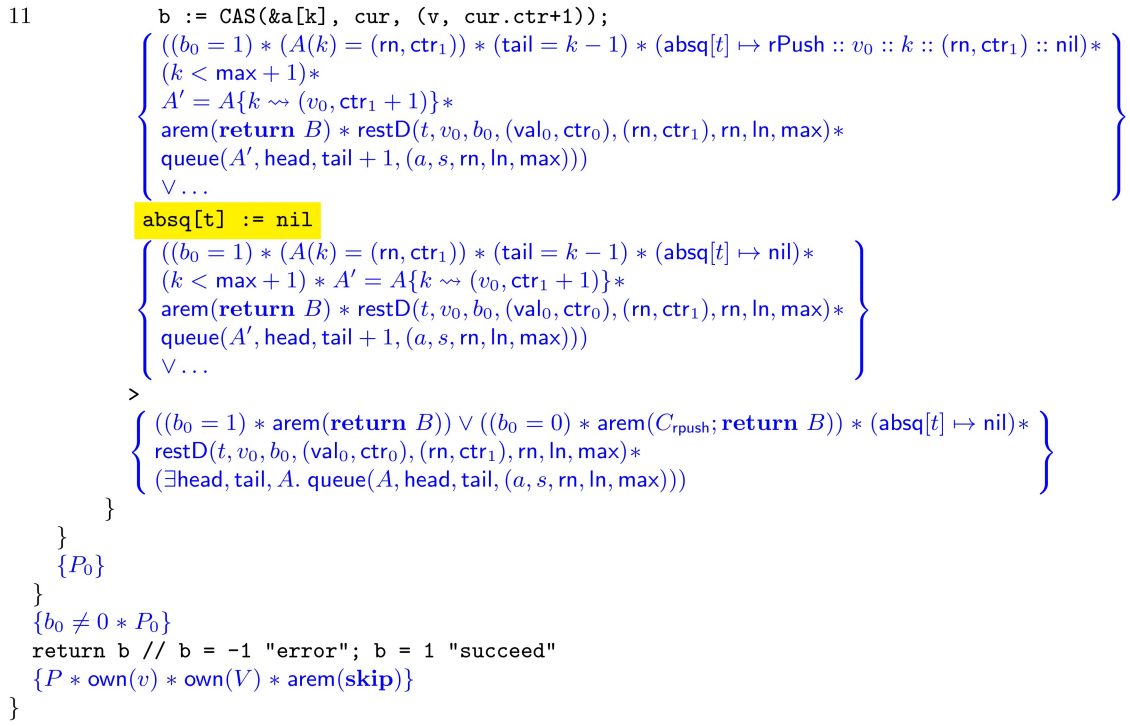

Fig.34 Proof sketch(part 3)

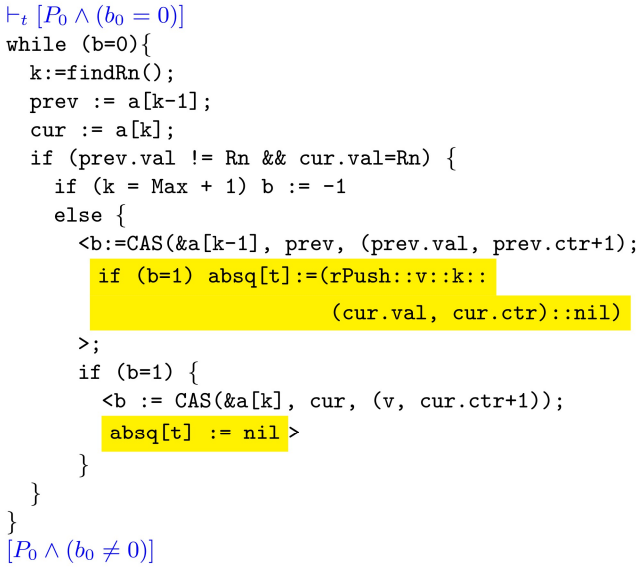

Fig.35 Proof sketch(sequential total correctness).

B Definitions for Linearizability and Obstruction-Freedom

$$\mathcal{T}[\![W,(\sigma_c,\sigma_o)]\!] \stackrel{\text{def}}{=} \{\lfloor \mathsf{T} \rfloor_W \mid \exists W', S'.(\lfloor \mathsf{W} \rfloor, (\sigma_c,\sigma_o,\circledcirc)) \overset{T}{\longmapsto}{}^{*} (W',S') \vee (\lfloor \mathsf{W} \rfloor, (\sigma_c,\sigma_o,\circledcirc)) \overset{T}{\longmapsto}{}^{*} \mathbf{abort}\}$$

$$\mathcal{T}_\omega[\![W,(\sigma_c,\sigma_o)]\!] \stackrel{\text{def}}{=} \{\lfloor \mathsf{T} \rfloor_W \mid (\lfloor \mathsf{W} \rfloor, (\sigma_c,\sigma_o,\circledcirc)) \overset{T}{\longmapsto}{}^{\omega} \cdot \vee (\lfloor \mathsf{W} \rfloor, (\sigma_c,\sigma_o,\circledcirc)) \overset{T}{\longmapsto}{}^{*} (\mathbf{skip}, \_) \vee (\lfloor \mathsf{W} \rfloor, (\sigma_c,\sigma_o,\circledcirc)) \overset{T}{\longmapsto}{}^{*} \mathbf{abort}\}$$

$$\begin{aligned}
\lfloor \mathbf{let}\ \Pi\ \mathbf{in}\ \mathsf{C}_1 \parallel \ldots \parallel \mathsf{C}_n \rfloor &\stackrel{\text{def}}{=} \mathbf{let}\ \Pi\ \mathbf{in}\ (C_1;\mathbf{end}) \parallel \ldots \parallel (C_n;\mathbf{end}) \\
\lfloor \mathsf{T} \rfloor_{(\mathbf{let}\ \Pi\ \mathbf{in}\ C_1 \parallel \ldots \parallel C_n)} &\stackrel{\text{def}}{=} (\mathbf{spawn}, n) :: T \\
\circledcirc &\stackrel{\text{def}}{=} \{t_1 \rightsquigarrow \circ, \ldots, t_n \rightsquigarrow \circ\} \\
\mathsf{iso}(T)\ \ \mathsf{iff}\ \ |T| = \omega &\implies \exists \mathsf{t}, i.\ (\forall j.\ j \geq i \implies \mathsf{tid}(T(j)) = \mathsf{t})
\end{aligned}$$

$$\begin{aligned}
\mathcal{H}[\![W,(\sigma_c,\sigma_o)]\!] &\stackrel{\text{def}}{=} \{\mathsf{get_hist}(T) \mid T \in \mathcal{T}[\![W,(\sigma_c,\sigma_o)]\!]\} \\
\mathcal{O}[\![W,(\sigma_c,\sigma_o)]\!] &\stackrel{\text{def}}{=} \{\mathsf{get_obsv}(T) \mid T \in \mathcal{T}[\![W,(\sigma_c,\sigma_o)]\!]\} \\
\mathcal{O}_\omega[\![W,(\sigma_c,\sigma_o)]\!] &\stackrel{\text{def}}{=} \{\mathsf{get_obsv}(T) \mid T \in \mathcal{T}_\omega[\![W,(\sigma_c,\sigma_o)]\!]\} \\
\mathcal{O}_{i\omega}[\![W,(\sigma_c,\sigma_o)]\!] &\stackrel{\text{def}}{=} \{\mathsf{get_obsv}(T) \mid T \in \mathcal{T}_\omega[\![W,(\sigma_c,\sigma_o)]\!] \wedge \mathsf{iso}(T)\}
\end{aligned}$$

Fig.36 Auxiliary definitions for traces.

$$\begin{aligned}
\mathsf{is_inv}(e)\ \ \mathsf{iff}\ \ &\exists \mathsf{t}, f, n.\ e = (\mathsf{t}, f, n) \\
\mathsf{is_ret}(e)\ \ \mathsf{iff}\ \ &\exists \mathsf{t}, n'.\ e = (\mathsf{t}, \mathbf{ret}, n') \\
\mathsf{is_obj_abt}(e)\ \ \mathsf{iff}\ \ &\exists \mathsf{t}.\ e = (t, \mathbf{obj}, \mathbf{abort}) \\
\mathsf{is_res}(e)\ \ \mathsf{iff}\ \ &\mathsf{is_ret}(e) \vee \mathsf{is_obj_abt}(e) \\
\mathsf{is_obj}(e)\ \ \mathsf{iff}\ \ &e = (_, \mathbf{obj}) \vee \mathsf{is_inv}(e) \vee \mathsf{is_res}(e) \\
\mathsf{is_clt_abt}(e)\ \ \mathsf{iff}\ \ &\exists \mathsf{t}.\ e = (\mathsf{t}, \mathbf{clt}, \mathbf{abort}) \\
\mathsf{is_abt}(e)\ \ \mathsf{iff}\ \ &\mathsf{is_obj_abt}(e) \vee \mathsf{is_clt_abt}(e) \\
\mathsf{is_clt}(e)\ \ \mathsf{iff}\ \ &\exists \mathsf{t}, n.\ e = (\mathsf{t}, \mathbf{clt}) \vee e = (\mathsf{t}, \mathbf{out}, n) \vee e = (\mathsf{t}, \mathbf{clt}, \mathbf{abort})
\end{aligned}$$

Fig.37 Predicates for events.

B.1 Linearizability

Definition 1 (Extensions of a History)**.**

$$\frac{\mathsf{well\_formed}(T)}{T \in \mathsf{extensions}(T)} \qquad \frac{T' \in \mathsf{extensions}(T) \quad \mathsf{is\_ret}(e) \quad \mathsf{well\_formed}(T' :: e)}{T' :: e \in \mathsf{extensions}(T)}$$

Definition 2 (Completions of a History)**.**

$$\begin{aligned}
\mathsf{truncate}(\epsilon) &\stackrel{\text{def}}{=} \epsilon \\
\mathsf{truncate}(e :: T) &\stackrel{\text{def}}{=} \begin{cases} e :: \mathsf{truncate}(T) & \text{if } \mathsf{is_ret}(e) \text{ or } \exists i.\mathsf{match}(e, T(i)) \\ \mathsf{truncate}(T) & \text{otherwise} \end{cases} \\
\mathsf{completions}(T) &\stackrel{\text{def}}{=} \{\mathsf{truncate}(T') | T' \in \mathsf{extensions}(T)\}.
\end{aligned}$$

$$\mathsf{match}(e_1, e_2) \stackrel{\mathsf{def}}{=} \mathsf{is\_inv}(e_1) \wedge \mathsf{is\_res}(e_2) \wedge (\mathsf{tid}(e_1) = \mathsf{tid}(e_2))$$

$$\frac{}{\mathsf{seq}(\epsilon)} \quad \frac{\mathsf{is\_inv}(e)}{\mathsf{seq}(e :: \epsilon)} \quad \frac{\mathsf{match}(e_1, e_2) \quad \mathsf{seq}(T)}{\mathsf{seq}(e_1 :: e_2 :: T)}$$

$$\mathsf{well\_formed}(T) \stackrel{\mathsf{def}}{=} \forall t. \mathsf{seq}(T|_t)$$
$$\mathsf{pend\_inv}(T) \stackrel{\mathsf{def}}{=} \{e \mid \exists i. e = T(i) \wedge \mathsf{is\_inv}(e) \wedge (\forall j. i < j \leq |T| \implies \neg \mathsf{match}(e, T(j)))\}$$

Fig.38 Auxiliary definitions

Definition 3 (Linearizable Histories)**.** $T \preceq^{\mathsf{lin}} \mathbb{T}$ iff

1. $\forall t. T|_t = \mathbb{T}|_t$;
2. there exists a bijection $\pi : \{1, \ldots, |T|\} \to \{1, \ldots, |\mathbb{T}|\}$ such that $\forall i. T(i) = \mathbb{T}(\pi(i))$ and $\forall i, j. i < j \wedge \mathsf{is\_ret}(T(i)) \wedge \mathsf{is\_inv}(T(j)) \implies \pi(j) < \pi(j)$.

Definition 4 (Linearizability of Objects)**.** $\Pi \preceq_P^{\mathsf{lin}} \Gamma$ iff

$$\forall n, C_1, \ldots, C_n, \sigma_c, \sigma_o, \Sigma, T.$$
$$T \in \mathcal{H}[\![(\mathbf{let}\ \Pi\ \mathbf{in}\ C_1 \parallel \ldots \parallel C_n), (\sigma_c, \sigma_o)]\!] \wedge (\sigma_o, \Sigma) \models P$$
$$\implies \exists T_c, \mathbb{T}.\ T_c \in \mathsf{completions}(T) \wedge \Gamma \rhd (\Sigma, \mathbb{T}) \wedge T_c \preceq^{\mathsf{lin}} \mathbb{T},$$

where $(\Gamma \rhd (\Sigma, \mathbb{T}))$ is defined as:

$$\exists n, C_1, \ldots, C_n, \sigma_c. \mathbb{T} \in \mathcal{H}[\![(\mathbf{let}\ \Gamma\ \mathbf{in}\ C_1 \parallel \ldots \parallel C_n), (\sigma_c, \Sigma)]\!] \wedge \mathsf{seq}(\mathbb{T}).$$

B.2 Obstruction-Free Object

Definition 5 (Obstruction-Free Event Trace)**.** $\mathsf{obstruction\text{-}free}(T)$ iff one of the following holds:

1. for any i and e, if $e \in \mathsf{pend\_inv}(T(1..i))$, then one of the following holds:
   (a) there exists $j > i$ such that $\mathsf{match}(e, T(j))$; or
   (b) $\forall j > i.\ \exists k.\ k \geq j \wedge \mathsf{tid}(T(k)) \neq \mathsf{tid}(e)$;
2. there exists i such that $\mathsf{is\_abt}(T(i))$ holds.

Definition 6 (Obstruction-Free Object)**.** $\mathsf{obstruction\text{-}free}_P(\Pi)$ iff

$$\forall n, C_1, \ldots, C_n, \sigma_c, \sigma_o, T.\ T \in \mathcal{T}_\omega[\![(\mathbf{let}\ \Pi\ \mathbf{in}\ C_1 \parallel \ldots \parallel C_n), (\sigma_c, \sigma_o)]\!] \wedge (\exists \Sigma.\ (\sigma_o, \Sigma) \models P)$$
$$\implies \mathsf{obstruction\text{-}free}(T).$$

C Full Proof of Soundness

C.1 Proof for ①

Definition 7 (Contextual Refinement for Obstruction-Freedom)**.** $\Pi \sqsubseteq_P^{i\omega} \Gamma$ iff

$$\forall n, C_1, \ldots, C_n, \sigma_c, \sigma_o, \Sigma.\ (\sigma_o, \Sigma) \models P \implies$$
$$\mathcal{O}_{i\omega}[\![(\textbf{let } \Pi \textbf{ in } C_1 \parallel \ldots \parallel C_n), (\sigma_c, \sigma_o)]\!] \subseteq \mathcal{O}_{\omega}[\![(\textbf{let } \Gamma \textbf{ in } C_1 \parallel \ldots \parallel C_n), (\sigma_c, \Sigma)]\!].$$

Lemma 1 (① in Fig. 11)**.**

$$\Pi \preceq_P^{\mathsf{lin}} \Gamma \wedge \mathsf{obstruction\text{-}free}_P(\Pi) \iff \Pi \sqsubseteq_P^{i\omega} \Gamma$$

This lemma is the same as the Theorem 18 in [**?**]. And the proof is at Section B.5 in [**?**].

C.2 Proof for ②

Definition 8. $\Pi \precsim_P^{i\omega} \Gamma$ iff there exist R, G, I such that $R, G, I \models \{P\}\Pi \precsim^{i\omega} \Gamma$ holds.

$R, G, I \models \{P\}\Pi \precsim^{i\omega} \Gamma$ iff, for any $f \in dom(\Pi)$, for any σ and Σ, for any t, if $\Pi(f) = (x, C), \Gamma(f) = (y, \mathbb{C})$, and $((\sigma, \Sigma), \textbf{skip}) \models P_t * \mathsf{own}(x) * \mathsf{own}(y) \wedge (x = y) * \mathsf{arem}(\textbf{skip})$, then there exists a natural number m such that

$$R, G, I \models_t (C, \sigma) \precsim (\mathbb{C}, \Sigma)\Diamond m \Downarrow (P * \mathsf{own}(x) * \mathsf{own}(y) * \mathsf{arem}(\textbf{skip}))$$

Here $R, G, I \models_t (C, \sigma) \precsim (\mathbb{C}, \Sigma)\Diamond m \Downarrow Q$ is co-inductively defined as follows. Whenvever $R, G, I \models_t (C, \sigma) \precsim (\mathbb{C}, \Sigma)\Diamond m \Downarrow Q$ holds, then the following hold:

(1) If $C = \mathbf{E}[\textbf{return } E]$, then for any Σ_F such that $\Sigma \perp \Sigma_F$, there exists $\mathbb{E}$ and Σ' such that
   a. $(\mathbb{C}, \Sigma \uplus \Sigma_F) \rightarrowtriangle_{\mathsf{t}}^* (\textbf{return } \mathbb{E}, \Sigma' \uplus \Sigma_F)$, and
   b. $((\sigma, \Sigma'), \textbf{skip}) \models Q_t$ and $[\![E]\!]_{\sigma.s} = [\![\mathbb{E}]\!]_{\Sigma'.s}$, and
   c. $((\sigma, \Sigma), (\sigma, \Sigma')) \models G_t * \mathsf{True}$.

(2) For any σ_F, $\neg((C, \sigma \uplus \sigma_F) \rightarrowtriangle_{\mathsf{t}} \textbf{abort})$.

(3) For any C', σ'', σ_F and Σ_F, if $(C, \sigma \uplus \sigma_F) \rightarrowtriangle_{\mathsf{t}} (C', \Sigma'')$ and $\Sigma \perp \Sigma_F$, then there exist $\sigma', \mathbb{C}', \Sigma'$ and m' such that
   a. $\sigma'' = \sigma' \uplus \sigma_F$, and
   b. $(\mathbb{C}, \Sigma \uplus \Sigma_F) \rightarrowtriangle_{\mathsf{t}}^n (\mathbb{C}', \Sigma' \uplus \Sigma_F)$, and
   c. $R, G, I \models_t (C', \sigma') \precsim (\mathbb{C}', \Sigma')\Diamond m' \Downarrow Q$, and
   d. $((\sigma, \Sigma), (\sigma', \Sigma')) \models G_t * \mathsf{True}$, and
   e. either $n > 0$, or $m' < m$.

(4) For any σ' and Σ', if $((\sigma, \Sigma), (\sigma', \Sigma')) \models R_t * \mathsf{Id}$, then there exists m' such that $R, G, I \models_t (C, \sigma') \precsim (\mathbb{C}, \Sigma')\Diamond m' \Downarrow Q$.

Lemma 2 (② in Fig. 11)**.** For any Π, Γ, P, R, G and I, if

1. $\Pi \precsim_P^{i\omega} \Gamma$,
2. $\forall t, t'.t \neq t' \implies (G_t \Rightarrow R_{t'})$,
3. $\forall t.I \rhd \{R_t, G_t\}$ and $P \Rightarrow I$,

$$(C,\sigma)\Downarrow \ \text{iff}\ \neg((C,\sigma)\rightarrowtriangle_{\mathsf{t}}^{*}\ \mathbf{abort})\wedge \neg((C,\sigma)\rightarrowtriangle_{\mathsf{t}}^{\omega}\cdot)$$

$$M'\leq M\ \ \text{iff}\ \ (dom(M')=dom(M))\wedge(\forall t\in dom(M).M'(t)\leq M(t))$$

$$M'<M\ \ \text{iff}\ \ (M'\leq M)\wedge(\exists t.M'(t)<M(t))$$

$$|M| \quad \stackrel{\mathsf{def}}{=} \sum_{t\in dom(M)}^{M(t)}$$

Fig.39 Auxiliary defintions.

then $\Pi \sqsubseteq_P^{i\omega} \Gamma$.

Proof. By Lemma 16 and premise 1, we have: for any t and C,

$$R,G,I \models_t \{P\}(\Pi,C) \precsim (\Gamma,C)\{P\} \tag{*2.1}$$

By Lemma 3, we only need to prove: for any $C_1,\ldots,C_n$,

$$\{P\}(\mathbf{let}\ \Pi\ \mathbf{in}\ C_1 \parallel \ldots \parallel C_n) \precsim (\mathbf{let}\ \Gamma\ \mathbf{in}\ C_1 \parallel \ldots \parallel C_n)$$

By Lemma 14, (*2.1) and the premise 2, we prove it. □

Definition 9 (Simulation for Program)**.** $\{P\}W \precsim \mathbb{W}$ iff, for any σ_c,σ and Σ, if $(\sigma,\Sigma)\models P$, there exist $M\in \mathsf{ThrdID}\rightharpoonup N$, such that

$$(\lfloor \mathsf{W} \rfloor,(\sigma_c,\sigma,\circledcirc)) \precsim (\lfloor \mathbb{W} \rfloor,(\sigma_c,\Sigma,\circledcirc))\diamond M$$

Here $(W,S)\precsim(\mathbb{W},\mathbb{S})\diamond M$ is co-inductively defined as follows.

Whenever $(W,S)\precsim(\mathbb{W},\mathbb{S})\diamond M$ holds, then the following holds.

(1) $dom(M)=\mathsf{activeThrds}(W)=\mathsf{activeThrds}(\mathbb{W})$.

(2) If $(W,S)\longmapsto(\mathbf{skip},S')$, then there exist $\mathbb{T}$ and $\mathbb{S}'$ such that $\mathsf{get\_obsv}(\mathbb{T})=\epsilon$ and $(\mathbb{W},\mathbb{S})\stackrel{\mathbb{T}}{\longmapsto}{}^{+}(\mathbf{skip},\mathbb{S}')$.

(3) If $(W,S)\stackrel{e}{\longmapsto}\mathbf{abort}$, then there exist t and $\mathbb{T}$ such that $e=(t,\mathbf{clt},\mathbf{abort})$, $e=\mathsf{get\_obsv}(\mathbb{T})$ and $(\mathbb{W},\mathbb{S})\stackrel{\mathbb{T}}{\longmapsto}{}^{+}\mathbf{abort}$.

(4) If $(W,S)\stackrel{e}{\longmapsto}(W',S')$, then there exist $t,\mathbb{T},\mathbb{W}',\mathbb{S}',M'$ and n such that all the following hold.

(a) $(\mathbb{W},\mathbb{S})\stackrel{\mathbb{T}}{\longmapsto}{}^{n}(\mathbb{W}',\mathbb{S}')$.

(b) $t=\mathsf{tid}(e)$, $\mathsf{get\_obsv}(e)=\mathsf{get\_obsv}(\mathbb{T})$, and $(e=(t,\mathbf{term}))\implies(e=\mathsf{last}(\mathbb{T}))$.

(c) $(W',S')\precsim(\mathbb{W}',\mathbb{S}')\diamond M'$.

(d) If $n=0$, then $M'(t)<M(t)$ and $M'\leq M$.

Definition 10. Whenever $T\models(W,S)\precsim(\mathbb{W},\mathbb{S})\diamond M$ holds, then the following holds. (Here $M\in\mathsf{ThrdID}\rightharpoonup N$).

(1) $dom(M) = \mathsf{activeThrds}(W) = \mathsf{activeThrds}(\mathbb{W})$.

(2) If $(W, S) \longmapsto (\mathbf{skip}, S')$ and $T = \epsilon$, then there exist $\mathbb{T}$ and $\mathbb{S}'$ such that $\mathsf{get\_obsv}(\mathbb{T}) = \epsilon$ and $(\mathbb{W}, \mathbb{S}) \overset{\mathbb{T}}{\longmapsto}{}^{+} (\mathbf{skip}, \mathbb{S}')$.

(3) If $(W, S) \overset{e}{\longmapsto} \mathbf{abort}$ and $T = e :: \epsilon$, then there exist t and $\mathbb{T}$ such that $e = (t, \mathbf{clt}, \mathbf{abort})$, $e = \mathsf{get\_obsv}(\mathbb{T})$ and $(\mathbb{W}, \mathbb{S}) \overset{\mathbb{T}}{\longmapsto}{}^{+} \mathbf{abort}$.

(4) If $(W, S) \overset{e}{\longmapsto} (W', S')$ and $T = e :: T'$, then there exist $t, \mathbb{T}, \mathbb{W}', \mathbb{S}', M'$ and n such that all the following hold.

(a) $(\mathbb{W}, \mathbb{S}) \overset{\mathbb{T}}{\longmapsto}{}^{n} (\mathbb{W}', \mathbb{S}')$.

(b) $t = \mathsf{tid}(e)$, $\mathsf{get\_obsv}(e) = \mathsf{get\_obsv}(\mathbb{T})$, and $(e = (t, \mathbf{term})) \implies (e = \mathsf{last}(\mathbb{T}))$.

(c) $T' \models (W', S') \precsim (\mathbb{W}', \mathbb{S}') \diamond M'$.

(d) If $n = 0$, then $M'(t) < M(t)$ and $M' \leq M$.

$$\frac{(W, S) \overset{T}{\longmapsto}{}^{+} \mathbf{abort} \quad \mathsf{get\_obsv}(T) = T_0}{T \models \mathcal{O}^{\mathsf{co}}_{i\omega}(W, S, T_0)}$$

$$\frac{(W, S) \overset{T}{\longmapsto}{}^{+} (\mathbf{skip}, \_) \quad \mathsf{get\_obsv}(T) = T_0}{T \models \mathcal{O}^{\mathsf{co}}_{i\omega}(W, S, T_0)}$$

$$\frac{|T :: T'| = \omega \quad (W, S) \overset{T}{\longmapsto}{}^{+} (W', S') \quad \mathsf{get\_obsv}(T) = \epsilon \quad T' \models \mathcal{O}^{\mathsf{co}}_{i\omega}(W', S', \epsilon) \quad \mathsf{iso}(T')}{T :: T' \models \mathcal{O}^{\mathsf{co}}_{i\omega}(W, S, \epsilon)}$$

$$\frac{\begin{array}{c}|T :: e :: T'| = \omega \quad (W, S) \overset{T}{\longmapsto}{}^{*} (W', S') \quad \mathsf{get\_obsv}(T) = \epsilon \\ (W', S') \overset{e}{\longmapsto} (W'', S'') \quad T' \models \mathcal{O}^{\mathsf{co}}_{i\omega}(W'', S'', T'_0) \quad \mathsf{iso}(T')\end{array}}{T :: e :: T' \models \mathcal{O}^{\mathsf{co}}_{i\omega}(W, S, e :: T'_0)}$$

Fig.40

$$\frac{(W, S) \overset{T}{\longmapsto}{}^{+} \mathbf{abort} \quad \mathsf{get\_obsv}(T) = T_0}{\mathcal{O}^{\mathsf{co}}_{\omega}(W, S, T_0)}$$

$$\frac{(W, S) \overset{T}{\longmapsto}{}^{+} (\mathbf{skip}, \_) \quad \mathsf{get\_obsv}(T) = T_0}{\mathcal{O}^{\mathsf{co}}_{\omega}(W, S, T_0)}$$

$$\frac{(W, S) \overset{T}{\longmapsto}{}^{+} (W', S') \quad \mathsf{get\_obsv}(T) = \epsilon \quad \mathcal{O}^{\mathsf{co}}_{\omega}(W', S', \epsilon)}{\mathcal{O}^{\mathsf{co}}_{\omega}(W, S, \epsilon)}$$

$$\frac{(W, S) \overset{T}{\longmapsto}{}^{+} (W', S') \quad \mathsf{get\_obsv}(T) = e :: T_0 \quad \mathcal{O}^{\mathsf{co}}_{\omega}(W', S', T'_0)}{\mathcal{O}^{\mathsf{co}}_{\omega}(W, S, e :: T_0 :: T'_0)}$$

Fig.41

Lemma 3. For any $C_1, \ldots, C_n$,

$$
\begin{array}{l}
(T_0, T) \in \mathcal{O}_{i\omega}[\![W, S]\!] \quad \mathsf{iff} \\
(((W, S) \overset{T}{\longmapsto}{}^{+} \mathbf{abort} \wedge T_0 = \mathsf{get\_obsv}(T)) \vee \\
\ ((W, S) \overset{T}{\longmapsto}{}^{+} (\mathbf{skip}, \_) \wedge T_0 = \mathsf{get\_obsv}(T)) \vee \\
\ ((W, S) \overset{T}{\longmapsto}{}^{\omega} \cdot \wedge T_0 = \mathsf{get\_obsv}(T)) \wedge \\
(|T| = \omega \implies \mathsf{iso}(T)))
\end{array}
$$

Fig.42

if $\{P\}(\mathbf{let}\ \Pi\ \mathbf{in}\ C_1 \parallel \ldots \parallel C_n) \precsim (\mathbf{let}\ \Gamma\ \mathbf{in}\ \mathbb{C}_1 \parallel \ldots \parallel \mathbb{C}_n)$,
then $\Pi \sqsubseteq_P^{i\omega} \Gamma$.

Proof. Let

$$W = \mathbf{let}\ \Pi\ \mathbf{in}\ C_1 \parallel \ldots \parallel C_n$$

$$\mathbb{W} = \mathbf{let}\ \Gamma\ \mathbf{in}\ \mathbb{C}_1 \parallel \ldots \parallel \mathbb{C}_n$$

By definition, we know there exist $\sigma_c, \sigma_o, \Sigma$ such that

$$(\sigma_o, \Sigma) \models P,$$

$$\{P\}W \precsim \mathbb{W},$$

and need to prove:

$$\mathcal{O}_{i\omega}[\![W, (\sigma_c, \sigma_o, \circledcirc)]\!] \subseteq \mathcal{O}_{\omega}[\![\mathbb{W}, (\sigma_c, \Sigma, \circledcirc)]\!].$$

Unfold $\{P\}W \precsim \mathbb{W}$, we have

$$(W, (\sigma_c, \sigma_o, \circledcirc)) \precsim (\mathbb{W}, (\sigma_c, \Sigma, \circledcirc)) \diamond M \tag{*2.0-1}$$

Thus we have: for any T_0,

$$T_0 \in \mathcal{O}_{i\omega}[\![W, (\sigma_c, \sigma_o, \circledcirc)]\!]$$

and we need to prove:

$$T_0 \in \mathcal{O}_{\omega}[\![\mathbb{W}, (\sigma_c, \Sigma, \circledcirc)]\!]$$

Let $S = (\sigma_c, \sigma_o, \circledcirc)$ and $\mathbb{S} = (\sigma_c, \Sigma, \circledcirc)$.
By Lemma 4 and $T_0 \in \mathcal{O}_{i\omega}[\![W, S]\!]$, we have there exists T,

$$T \models \mathcal{O}_{i\omega}^{\mathsf{co}}(W, S, T_0) \tag{*2.0-2}$$

By Lemma 12, (*2.0-2) and (*2.0-1), we have:

$$T \models (W, S) \precsim (\mathbb{W}, \mathbb{S}) \diamond M \tag{*2.0-3}$$

By Lemma 7, (*2.0-2) and (*2.0-3), we have:

$$\mathcal{O}^{\mathsf{co}}_{\omega}(\mathbb{W}, \mathbb{S}, T_0) \tag{*2.0-4}$$

By Lemma 6 and (*2.0-4), we have

$$T_0 \in \mathcal{O}_{\omega}[\![\mathbb{W}, \mathbb{S}]\!]$$

Thus we finish this proof. □

Lemma 4. $(T_0 \in \mathcal{O}_{i\omega}[\![W, S]\!]) \iff (\exists T.(T \models \mathcal{O}^{\mathsf{co}}_{i\omega}(W, S, T_0)))$.

Proof. By definition, we know:

$$(T_0 \in \mathcal{O}_{i\omega}[\![W, S]\!]) \iff (\exists T.(T_0, T) \in \mathcal{O}_{i\omega}[\![W, S]\!]).$$

By Lemma 5, prove it directly. □

Lemma 5. $((T_0, T) \in \mathcal{O}_{i\omega}[\![W, S]\!]) \iff (T \models \mathcal{O}^{\mathsf{co}}_{i\omega}(W, S, T_0))$.

Proof. We prove it by the following cases (1)(2).

(1) If $T \models \mathcal{O}^{\mathsf{co}}_{i\omega}(W, S, T_0)$, then $(T, T_0) \in \mathcal{O}_{i\omega}[\![W, S]\!]$.

Proof:

By destruction whether T is diverge, we have the following two cases.

(a) If $|T| \neq \omega$, then $(T_0, T) \in \mathcal{O}_{i\omega}[\![W, S]\!]$.

Proof:

By inversion over $T \models \mathcal{O}^{\mathsf{co}}_{i\omega}(W, S, T_0)$, we have the following two cases:

- If $(W, S) \overset{T}{\longmapsto}{}^{*}$ **abort** and $\mathsf{get\_obsv}(T) = T_0$:

  We directly have $(T_0, T) \in \mathcal{O}_{i\omega}[\![W, S]\!]$.
- If $(W, S) \overset{T}{\longmapsto}{}^{*}$ **skip** and $\mathsf{get\_obsv}(T) = T_0$:

  We directly have $(T_0, T) \in \mathcal{O}_{i\omega}[\![W, S]\!]$.

(b) If $|T| = \omega$, then by definition, we need to prove
$(W, S) \overset{T}{\longmapsto}{}^{\omega} \cdot$, $\mathsf{get\_obsv}(T) = T_0$ and $\mathsf{iso}(T)$.

- $(W, S) \overset{T}{\longmapsto}{}^{\omega} \cdot$.

  Proof:

  By co-induction, we have the following cases.

  (I) we need to prove: if there exist T_1 and T_2, such that

  $T = T_1 :: T_2$, $T_0 = \epsilon$,
  $(W, S) \overset{T_1}{\longmapsto}{}^{+} (W', S')$, $\mathsf{get\_obsv}(T_1) = \epsilon$,
  $T_2 \models \mathcal{O}^{\mathsf{co}}_{i\omega}(W', S', \epsilon)$ and $\mathsf{iso}(T_2)$,
  then $(W, S) \overset{T_1 :: T_2}{\longmapsto}{}^{\omega} \cdot$.

Thus we only need to prove:

$$(W', S') \overset{T_2}{\longmapsto}{}^{\omega} \cdot$$

By co-inductive hypothesis, $T_2 \models \mathcal{O}^{\mathsf{co}}_{i\omega}(W', S', \epsilon)$ and $|T_2| = \omega$, we prove it.

(II) We can prove it in a similar way.

- $\mathsf{get\_obsv}(T) = T_0$.

  Proof: By co-induction, we can prove it directly.

- $\mathsf{iso}(T)$.

  Proof:

  By there exist T_1 and T_2, such that $T = T_1 :: T_2$ and $\mathsf{iso}(T_2)$, we prove it directly.

(2) We want to prove:

If $(T, T_0) \in \mathcal{O}_{i\omega}[\![W, S]\!]$, then $T \models \mathcal{O}^{\mathsf{co}}_{i\omega}(W, S, T_0)$.

Proof:

By destructing whether T is diverge, we have following two cases.

- If $|T| \neq \omega$, then $T \models \mathcal{O}^{\mathsf{co}}_{i\omega}(W, S, T_0)$.

  Proof: It is trivially hold.

- If $|T| = \omega$, then $T \models \mathcal{O}^{\mathsf{co}}_{i\omega}(W, S, T_0)$.

  Proof:

  By co-induction, we have following cases.

  (a) If there exists T_1, such that $(W, S) \overset{T_1}{\longmapsto}{}^{+} (W', S')$, $\mathsf{get\_obsv}(T_1) = \epsilon$, and $T_0 = \epsilon$, then there exists T_2, such that $T = T_1 :: T_2$, $T_2 \models \mathcal{O}^{\mathsf{co}}_{i\omega}(W', S', \epsilon)$ and $\mathsf{iso}(T)$.

  Proof:

  By $(T_0, T) \in \mathcal{O}_{i\omega}[\![W, S]\!]$, we have

  $$(W, S) \overset{T}{\longmapsto}{}^{\omega} \cdot, \text{ and}$$
  $$T_0 = \mathsf{get\_obsv}(T), \text{ and}$$
  $$\mathsf{iso}(T)$$

  By $(W, S) \overset{T_1}{\longmapsto}{}^{+} (W', S')$, we know there exists T_2, such that

  $$(W', S') \overset{T_2}{\longmapsto}{}^{\omega} \cdot, \text{ and}$$
  $$T_1 :: T_2 = T$$

  Thus we know

  $$(\epsilon, T_2) \in \mathcal{O}_{i\omega}[\![W', S']\!]$$

  By co-induction hypothesis, we prove it.

- We can prove this case in a similar way.

Thus we have done.

□

Lemma 6. If $\mathcal{O}^{\mathsf{co}}_{\omega}(W, S, T_0)$, then $T_0 \in \mathcal{O}_{\omega}[\![W, S]\!]$.

Proof. We can prove it in a similar way with Lemma 4. □

Lemma 7. For any $W, S, T_0, \mathbb{W}, \mathbb{S}$ and M,

if

1. $T \models \mathcal{O}^{\mathsf{co}}_{i\omega}(W, S, T_0)$,
2. $T \models T \precsim (W, S) \diamond (\mathbb{W}, \mathbb{S})M$,

then $\mathcal{O}^{\mathsf{co}}_{\omega}(\mathbb{W}, \mathbb{S}, T_0)$.

Proof. By destruction whether $|T|$ is ω and T_0 is ϵ, we have three cases.

Then by Lemma 8, 9 and 11, we finish this proof. □

Lemma 8. For any $T, W, S, T_0, \mathbb{W}, \mathbb{S}$ and M,

if

1. $|T| \neq \omega$,
2. $T \models \mathcal{O}^{\mathsf{co}}_{i\omega}(w, S, T_0)$,
3. $T \models (W, S) \precsim (\mathbb{W}, \mathbb{S}) \diamond M$,

then $\mathcal{O}^{\mathsf{co}}_{\omega}(\mathbb{W}, \mathbb{S}, T_0)$.

Proof. This can be proved easily by definition of simulation for program. □

Lemma 9. For any $n, M, T, W, S, \mathbb{W}$ and $\mathbb{S}$,

if

1. $|M| = n$,
2. $|T| = \omega$,
3. $T \models \mathcal{O}^{\mathsf{co}}_{i\omega}(W, S, \epsilon)$,
4. $T \models (W, S) \precsim (\mathbb{W}, \mathbb{S}) \diamond M$,

then $\mathcal{O}^{\mathsf{co}}_{\omega}(\mathbb{W}, \mathbb{S}, \epsilon)$.

Proof. By co-induction, we only need to prove: there exist $\mathbb{W}', \mathbb{S}', \mathbb{T}$ such that

$$(\mathbb{W}, \mathbb{S}) \overset{\mathbb{T}}{\longmapsto}{}^{+} (\mathbb{W}', \mathbb{S}'), \text{ and}$$

$$\mathsf{get\_obsv}(\mathbb{T}) = \epsilon, \text{ and}$$

$$\mathcal{O}^{\mathsf{co}}_{\omega}(\mathbb{W}', \mathbb{S}', \epsilon)$$

We do induction over n.

- **Base case:** $n = 0$.

  Thus we have:

$$|M| = 0 \tag{*2.3.2-1}$$

  By Lemma 10, premise 2 and premise 2, we have:

  there exist W', S', e and T' such that

$$(W, S) \overset{e}{\longmapsto} (W', S') \tag{*2.3.2-2}$$

$$\mathsf{get\_obsv}(e) = \epsilon$$

$$T = e :: T'$$

$$T' \models \mathcal{O}^{\mathsf{co}}_{i\omega}(W', S', \epsilon) \tag{*2.3.2-3}$$

$$\mathsf{iso}(T')$$

  By premise 4, (*2.3.2-2), we know there exist $\mathbb{T}, \mathbb{W}', \mathbb{S}', m, t$ and M'.

$$(\mathbb{W}, \mathbb{S}) \overset{\mathbb{T}}{\longmapsto}^{m} (\mathbb{W}', \mathbb{S}')$$

$$\mathsf{get\_obsv}(\mathbb{T}) = \epsilon \tag{*2.3.2-4}$$

$$t = \mathsf{tid}(e)$$

$$T' \models (W', S') \precsim (\mathbb{W}', \mathbb{S}') \diamond M' \tag{*2.3.2-5}$$

$$m = 0 \implies M'(t) < M(t) \wedge M' \leq M$$

  By destruct whether m is 0, we have the following cases.

  (1) If $m = 0$.

  Then we know:

$$M'(t) < M(t)$$

  By (*2.3.2-1), we know

$$M'(t) < 0$$

  which is impossible.

  (2) If $m > 0$.

  Then we have:

$$(\mathbb{W}, \mathbb{S}) \overset{\mathbb{T}}{\longmapsto}^{+} (\mathbb{W}', \mathbb{S}') \tag{*2.3.2-6}$$

  By (*2.3.2-4), (*2.3.2-6), we only need to prove:

$$\mathcal{O}^{\mathsf{co}}_{\omega}(\mathbb{W}', \mathbb{S}', \epsilon)$$

By co-induction hypothesis, we only need to prove:

$$T' \models \mathcal{O}^{\mathsf{co}}_{i\omega}(W', S', \epsilon)$$
$$T' \models (W', S') \precsim (\mathbb{W}', \mathbb{S}') \diamond M'$$

By (*2.3.2-3) and (*2.3.2-5), we prove it.

- **Inductive case:** $n = k + 1$.

  By Lemma 10, premise 3 and premise 2, we have:

  there exist W', S', e and T' such that

$$(W, S) \overset{e}{\longmapsto} (W', S') \tag{*2.3.2-7}$$
$$\mathsf{get\_obsv}(e) = \epsilon$$
$$T = e :: T'$$
$$T' \models \mathcal{O}^{\mathsf{co}}_{i\omega}(W', S', \epsilon) \tag{*2.3.2-8}$$
$$\mathsf{iso}(T')$$

  By premise 4, we know there exist $m, \mathbb{T}, \mathbb{W}', \mathbb{S}', t$ and M' such that

$$(\mathbb{W}, \mathbb{S}) \overset{\mathbb{T}}{\longmapsto}^{m} (\mathbb{W}', \mathbb{S}'),$$
$$t = \mathsf{tid}(e),$$
$$\mathsf{get\_obsv}(\mathbb{T}) = \epsilon, \tag{*2.3.2-9}$$
$$T' \models (W', S') \precsim (\mathbb{W}', \mathbb{S}') \diamond M', \tag{*2.3.2-10}$$
$$n = 0 \implies M'(t) < M(t) \wedge M' \leq M$$

  By destructing whether m is 0, we have following two cases.

  (1) If $m > 0$.

  Then this case is trivially holds.

  (2) If $m = 0$.

  Then we know

$$M' < M.$$

  Thus we have

$$|M'| < k + 1$$

  Therefore

$$|M'| \leq k$$

By inductive hypothesis, (*2.3.2-8) and (*2.3.2-10), we have:

$$\mathcal{O}^{\mathsf{co}}_{\omega}(\mathbb{W}, \mathbb{S}, \epsilon).$$

Thus we finish this case.

Thus we have done. □

Lemma 10. For any T, W, and S,

if

1. $|T| = \omega$,
2. $T \models \mathcal{O}^{\mathsf{co}}_{i\omega}(W, S, \epsilon)$,

then there exist W', S', T' and e, such that

$$T = e :: T', \text{ and}$$
$$(W, S) \overset{e}{\longmapsto} (W', S'), \text{ and}$$
$$\mathsf{get\_obsv}(e) = \epsilon, \text{ and}$$
$$\mathsf{iso}(T'), \text{ and}$$
$$T' \models \mathcal{O}^{\mathsf{co}}_{i\omega}(W', S', \epsilon).$$

Proof. By premise 2, we have there exist T_x, T_y, W_y, S_y and m such that

$$T = T_x :: T_y,$$
$$(W, S) \overset{T_x}{\longmapsto}{}^{m} (W_y, S_y) \quad (m > 0), \tag{*2.3.2.1-1}$$
$$\mathsf{get\_obsv}(T_x) = \epsilon,$$
$$T_y \models \mathcal{O}^{\mathsf{co}}_{i\omega}(W_y, S_y, \epsilon), \tag{*2.3.2.1-2}$$
$$\mathsf{iso}(T_y) \tag{*2.3.2.1-3}$$

If $m = 1$, then we finish this proof directly.

If $m > 1$, by (*2.3.2.1-1), we have there exist W_x, S_x, e and T'_x, such that

$$(W, S) \overset{e}{\longmapsto} (W_x, S_x),$$
$$(W_x, S_x) \overset{T'_x}{\longmapsto}{}^{+} (W_y, S_y), \tag{*2.3.2.1-4}$$
$$\mathsf{get\_obsv}(e) = \epsilon,$$
$$T_x = e :: T'_x,$$
$$\mathsf{get\_obsv}(T'_x) = \epsilon.$$

By (*2.3.2.1-4), (*2.3.2.1-2) and (*2.3.2.1-4), we have

$$T'_x :: T_y \models \mathcal{O}^{\mathsf{co}}_{i\omega}(W_x, S_x, \epsilon).$$

Thus we finish this proof. □

Lemma 11. For any $T, W, S, e, T_0, \mathbb{W}, \mathbb{S}$ and M,

if

1. $|T| = \omega$,
2. $T \models \mathcal{O}^{\mathsf{co}}_{i\omega}(w, S, e :: T_0)$,
3. $T \models (W, S) \precsim (\mathbb{W}, \mathbb{S}) \diamond M$,

then $\mathcal{O}^{\mathsf{co}}_{\omega}(\mathbb{W}, \mathbb{S}, e :: T_0)$.

Proof. By co-induction, we only need to prove:

there exist $\mathbb{T}, \mathbb{W}'$ and $\mathbb{S}'$ such that

$$(\mathbb{W}, \mathbb{S}) \overset{\mathbb{T}}{\longmapsto}{}^{+} (\mathbb{W}', \mathbb{S}'),$$
$$\mathsf{get\_obsv}(\mathbb{T}) = e,$$
$$\mathcal{O}^{\mathsf{co}}_{\omega}(\mathbb{W}', \mathbb{S}', T_0)$$

By premise 2, we have:

there exist $n, T_x, e, T_y, W_x, S_x, W_y$ and S_y such that

$$T = T_x :: e :: T_y,$$
$$(W, S) \overset{T_x}{\longmapsto}{}^{n} (W_x, S_x),$$
$$\mathsf{get\_obsv}(T_x) = \epsilon,$$
$$(W_x, S_x) \overset{e}{\longmapsto} (W_y, S_y), \tag{*2.3.3-0}$$
$$T_y \models \mathcal{O}^{\mathsf{co}}_{i\omega}(W_y, S_y, T_0), \tag{*2.3.3-1}$$
$$\mathsf{iso}(T_y).$$

By induction over n, we have following two cases.

- **Base case:** $n = 0$.

  Thus we have:

  $$(W, S) \overset{e}{\longmapsto} (W_y, S_y)$$

  By premise 3, we have there exist $\mathbb{T}, \mathbb{W}', \mathbb{S}'$ and M' such that

  $$(\mathbb{W}, \mathbb{S}) \overset{\mathbb{T}}{\longmapsto}{}^{+} (\mathbb{W}', \mathbb{S}'),$$
  $$\mathsf{get\_obsv}(\mathbb{T}) = e,$$
  $$T_y \models (W_y, S_y) \precsim (\mathbb{W}', \mathbb{S}') \diamond M' \tag{*2.3.3-2}$$

  Thus we only need to prove:

  $$\mathcal{O}^{\mathsf{co}}_{\omega}(\mathbb{W}', \mathbb{S}', T_0)$$

  By destructing whether T_0 is ϵ, we have following two cases.

(1) If $T_0 = \epsilon$.

Then by Lemma 9, (*2.3.3-1), (*2.3.3-2), we have:

$$\mathcal{O}^{\mathsf{co}}_{\omega}(\mathbb{W}', \mathbb{S}', \epsilon)$$

Thus we finish this case.

(2) If $T_0 \neq \epsilon$,then by co-induction hypothesis, (*2.3.3-1), (*2.3.3-2), we have:

$$\mathcal{O}^{\mathsf{co}}_{\omega}(\mathbb{W}', \mathbb{S}', T_0)$$

Thus we finish this case.

- **Inductive case:** $n = k + 1$.

We have:

$$(W, S) \overset{T_x}{\longmapsto}{}^{k+1} (W_x, S_x)$$

Thus there exist e', T'_x, W'_x and S'_x such that:

$$(W, S) \overset{e'}{\longmapsto} (W'_x, S'_x) \tag{*2.3.3-3}$$

$$(W'_x, S'_x) \overset{T'_x}{\longmapsto}{}^{k} (W_x, S_x) \tag{*2.3.3-4}$$

$$T_x = e' :: T'_x$$

$$\mathsf{get\_obsv}(e' :: T'_x) = \epsilon$$

By (*2.3.3-4), (*2.3.3-0) and (*2.3.3-1), we have:

$$T'_x :: e :: T_y \models \mathcal{O}^{\mathsf{co}}_{i\omega}(W'_x, S'_x, e :: t_0) \tag{*2.3.3-5}$$

By premise 3, we have there exist $T', \mathbb{W}', \mathbb{S}'$ and M' such that

$$(\mathbb{W}, \mathbb{S}) \overset{\mathbb{T}'}{\longmapsto}{}^{*} (\mathbb{W}', \mathbb{S}') \tag{*2.3.3-6}$$

$$\mathsf{get\_obsv}(\mathbb{T}) = \epsilon$$

$$T'_x :: e :: T_y \models (W'_x, S'_x) \precsim (\mathbb{W}', \mathbb{S}') \diamond M' \tag{*2.3.3-7}$$

By induction hypothesis, (*2.3.3-4), (*2.3.3-5) and (*2.3.3-7), we have:
there exist $\mathbb{T}'', \mathbb{W}''$ and $\mathbb{S}''$, such that

$$(\mathbb{W}', \mathbb{S}') \overset{\mathbb{T}''}{\longmapsto}{}^{+} (\mathbb{W}'', \mathbb{S}''),$$

$$\mathsf{get\_obsv}(\mathbb{T}'') = e,$$

$$\mathcal{O}^{\mathsf{co}}_{\omega}(\mathbb{W}'', \mathbb{S}'', T_0).$$

By (*2.3.3-6), we have:

$$(\mathbb{W}, \mathbb{S}) \overset{\mathbb{T}' :: \mathbb{T}''}{\longmapsto}{}^{+} (\mathbb{W}'', \mathbb{S}''),$$

$$\mathsf{get\_obsv}(\mathbb{T}' :: \mathbb{T}'') = e,$$
$$\mathcal{O}^{\mathsf{co}}_{\omega}(\mathbb{W}'', \mathbb{S}'', T_0).$$

Thus we finish this case.

Thus we have done. □

Lemma 12. For any $T, W, S, T_0, \mathbb{W}, \mathbb{S}$ and M,

if

1. $T \models \mathcal{O}^{\mathsf{co}}_{i\omega}(W, S, T_0)$,
2. $(W, S) \precsim (\mathbb{W}, \mathbb{S}) \diamond M$,

then $T \models (W, S) \precsim (\mathbb{W}, \mathbb{S}) \diamond M$.

Proof. By Lemma 13, we only need to prove:

$$(T_0, T) \in \mathcal{O}_{i\omega}[\![W, S]\!]$$

By Lemma 5 and premise 1, we prove it. □

Lemma 13. For any $T, T_0, W, S, \mathbb{W}, \mathbb{S}$ and M,

if

1. $(T, T_0) \in \mathcal{O}_{i\omega}[\![W, S]\!]$,
2. $(W, S) \precsim (\mathbb{W}, \mathbb{S}) \diamond M$,

then $T \models (W, S) \precsim (\mathbb{W}, \mathbb{S}) \diamond M$.

Proof. By co-induction,we need to prove the following (1)(2)(3)(4).

(1) If $dom(M) = \mathsf{activeThrds}(W) = \mathsf{activeThrds}(\mathbb{W})$.

Proof: By premise 2, we prove it directly.

(2) If $(W, S) \longmapsto (\mathbf{skip}, S')$ and $T = \epsilon$, then

there exist $\mathbb{T}$ and $\mathbb{S}'$ such that
$(\mathbb{W}, \mathbb{S}) \overset{\mathbb{T}}{\longmapsto}{}^{+} (\mathbf{skip}, \mathbb{S}')$ and
$\mathsf{get\_obsv}(\mathbb{T}) = \epsilon$.

Proof: By premise 2, we prove it directly.

(3) If $(W, S) \overset{e}{\longmapsto} \mathbf{abort}$ and $T = e :: \epsilon$, then ...

Proof: By premise 2, we prove it directly.

(4) If

$$(W, S) \overset{e}{\longmapsto} (W', S'), \qquad (*2.4\text{-}1)$$

and $T = e :: T'$, then

there exist $t, \mathbb{T}, \mathbb{W}', \mathbb{S}', M'$ and n such that

(a) $(\mathbb{W}, \mathbb{S}) \overset{\mathbb{T}}{\longmapsto}{}^{n} (\mathbb{W}', \mathbb{S}')$,

(b) $t = \mathsf{tid}(e)$, $\mathsf{get\_obsv}(e) = \mathsf{get\_obsv}(\mathbb{T})$, and
$(e = (t, \mathbf{term})) \implies (e = \mathsf{last}(\mathbb{T}))$,

(c) $T' \models (W', S') \precsim (\mathbb{W}', \mathbb{S}') \diamond M'$,

(d) If $n = 0$, then $M'(t) < M(t)$ and $M' \leq M$.

By premise 2 and (*2.4-1), we only need to prove:

$$T' \models (W', S') \precsim (\mathbb{W}', \mathbb{S}') \diamond M'$$

And we also have

$$(W', S') \precsim (\mathbb{W}', \mathbb{S}') \diamond M' \tag{*2.4-2}$$

By co-induction hypothesis, we need to prove:

$$(T', \mathsf{get\_obsv}(T')) \in \mathcal{O}_{i\omega}[\![W', S']\!], \text{ and}$$
$$(W', S') \precsim (\mathbb{W}', \mathbb{S}') \diamond M'$$

By (*2.4-2), we only need to prove:

$$(T', \mathsf{get\_obsv}(T')) \in \mathcal{O}_{i\omega}[\![W', S']\!]$$

By premise 1 and (*2.4-1), we prove it directly.

Thus we have done.

□

Definition 11 (Simulation for Task)**.** $R, G, I \models_t \{P\}(\Pi, C) \precsim (\Gamma, \mathbb{C})\{Q\}$ iff, for any σ_c, σ and Σ, if $(\sigma, \Sigma) \models P$, there exists a natural number M such that

$$R, G, I \models_t (\Pi, C, (\sigma_c, \sigma, \circ)) \precsim (\Gamma, \mathbb{C}, (\sigma_c, \Sigma, \circ)) \diamond M \Downarrow Q.$$

Here $R, G, I \models_t (\Pi, C, (\sigma_c, \sigma, \kappa)) \precsim (\Gamma, \mathbb{C}, (\sigma_c, \Sigma, \Bbbk)) \diamond M \Downarrow Q$ is coinductively defined as follows.

Whenever $R, G, I \models_t (\Pi, C, (\sigma_c, \sigma, \kappa)) \precsim (\Gamma, \mathbb{C}, (\sigma_c, \Sigma, \Bbbk)) \diamond M \Downarrow Q$ holds, then the following hold:

(1) $(C \neq \mathbf{skip}) \implies (\mathbb{C} \neq \mathbf{skip})$.

(2) If $C = \mathbf{skip}$, then $\mathbb{C} = \mathbf{skip}$ and $(\sigma, \Sigma) \models Q_t$.

(3) If $(C, (\sigma_c, \sigma \uplus \sigma_F, \kappa)) \xrightarrow{e}_{\mathsf{t},\Pi} \mathbf{abort}$ and $\Sigma \perp \Sigma_F$,
then $e = (t, \mathbf{clt}, \mathbf{abort})$ and there exists $\mathbb{T}$ such that $e = \mathsf{get\_obsv}(\mathbb{T})$
and $(\mathbb{C}, (\sigma_c, \Sigma \uplus \Sigma_F, \Bbbk)) \xrightarrow{\mathbb{T}}{}^{*}_{\mathsf{t},\Gamma} \mathbf{abort}$.

(4) For any σ_c', σ' and Σ', if $((\sigma, \Sigma), (\sigma', \Sigma')) \models R_t * \mathsf{Id}$,
then there exists M' such that
$R, G, I \models_t (\Pi, C, (\sigma_c', \sigma', \kappa)) \precsim (\Gamma, \mathbb{C}, (\sigma_c', \Sigma', \Bbbk)) \diamond M' \Downarrow Q$.

(5) If $(C, (\sigma_c, \sigma \uplus \sigma_F, \kappa)) \xrightarrow{e}_{\mathsf{t},\Pi} (C', (\sigma_c', \sigma'', \kappa'))$ and $\Sigma \perp \Sigma_F$,
then there exist $\sigma', n, \mathbb{T}, \mathbb{C}', \Sigma', \Bbbk'$ and M' such that

(a) $\sigma'' = \sigma' \uplus \sigma_F$,

(b) $(\mathbb{C}, (\sigma_c, \Sigma \uplus \Sigma_F, \Bbbk)) \xrightarrow{\mathbb{T}}{}^{n}_{\mathsf{t},\Gamma} (\mathbb{C}', (\sigma'_c, \Sigma' \uplus \Sigma_F, \Bbbk'))$,

(c) $\mathsf{get\_obsv}(e) = \mathsf{get\_obsv}(\mathbb{T})$ and $(e = (t, \mathbf{term})) \implies (e = \mathsf{last}(\mathbb{T}))$,

(d) $R, G, I \models_t (\Pi, C', (\sigma'_c, \sigma', \kappa')) \precsim (\Gamma, \mathbb{C}', (\sigma'_c, \Sigma', \Bbbk')) \diamond M' \Downarrow Q$,

(e) $((\sigma, \Sigma), (\sigma', \Sigma')) \models G_t * \mathsf{True}$,

(f) either $n > 0$, or $M' < M$.

Lemma 14 (Parallel Compositionality)**.** If there exist R, G, I and P, such that the following hold for any $t \in [1..n]$:

1. $R, G, I \models_t \{P\}(\Pi, C_t) \precsim (\Gamma, \mathbb{C}_t)\{P\}$,
2. $\forall t, t'.t \neq t' \implies (G_t \Rightarrow R_{t'})$,
3. $\forall t.I \rhd \{R_t, G_t\}$ and $P \Rightarrow I$,

then $\{\bigwedge_t P_t\}(\mathbf{let}\ \Pi\ \mathbf{in}\ C_1 \parallel \ldots \parallel C_n) \precsim (\mathbf{let}\ \Gamma\ \mathbf{in}\ \mathbb{C}_1 \parallel \ldots \parallel \mathbb{C}_n)$.

Proof. For any σ_c, σ and Σ, if $(\sigma, \Sigma) \models (\bigwedge_t P_t)$, from the premises and by sequential compositionality, we know: there exist M_1, ..., M_n such that the following holds for any $t \in [1..n]$:

$$R, G, I \models_t (\Pi, (C_t; \mathbf{end}), (\sigma_c, \sigma, \circ)) \precsim (\Gamma, (\mathbb{C}_t; \mathbf{end}), (\sigma_c, \Sigma, \circ)) \diamond M_t \Downarrow P$$

We want to show that there exists $\mathbb{M}$ such that

$$\begin{array}{l} ((\mathbf{let}\ \Pi\ \mathbf{in}\ (C_1; \mathbf{end}) \parallel \ldots \parallel (C_n; \mathbf{end}), (\sigma_c, \sigma, \circledcirc))) \\ \precsim \\ ((\mathbf{let}\ \Gamma\ \mathbf{in}\ (\mathbb{C}_1; \mathbf{end}) \parallel \ldots \parallel (\mathbb{C}_n; \mathbf{end}), (\sigma_c, \Sigma, \circledcirc))) \diamond \mathbb{M}. \end{array}$$

By Lemma 15, we prove it. □

Lemma 15. If

1. $(\sigma, \Sigma) \models I$,
2. for any $t \in [1..n]$, $R, G, I \models_t (\Pi, C_t, (\sigma_c, \sigma \uplus \sigma_t, \kappa_t)) \precsim (\Gamma, \mathbb{C}_t, (\sigma_c, \Sigma \uplus \Sigma_t, \Bbbk_t)) \diamond M_t \Downarrow P$,
3. $\forall t, t'.t \neq t' \implies (G_t \Rightarrow R_{t'})$,
4. $\forall t.I \rhd \{R_t, G_t\}$ and $P \Rightarrow I$,

then

$$(\mathbf{let}\ \Pi\ \mathbf{in}\ C_1 \parallel \ldots \parallel C_n, (\sigma_c, \sigma \uplus (\biguplus_t \sigma_t), K)) \precsim (\mathbf{let}\ \Gamma\ \mathbf{in}\ \mathbb{C}_1 \parallel \ldots \parallel \mathbb{C}_n, (\sigma_c, \Sigma \uplus (\biguplus_t \Sigma_t), \mathbb{K})) \diamond \mathbb{M}.$$

Here for any $t \in [1..n]$, $K(t) = \kappa_t$ and $\mathbb{K}(t) = \Bbbk_t$,

and the function $\mathbb{M}$ is defined as bellow:

- $dom(\mathbb{M}) = \mathsf{activeThrds}(\mathbf{let}\ \Pi\ \mathbf{in}\ C_1 \parallel \ldots \parallel C_n) = \{t | (C_t \neq \mathbf{skip})\}$,
- For any $t \in dom(\mathbb{M})$, $\mathbb{M}(t) = M_t$.

Proof. By co-induction, we need to prove following (1)(2)(3)(4).

Let

$$\mathbb{W} \stackrel{\mathsf{def}}{=} (\mathbf{let}\ \Pi\ \mathbf{in}\ C_1 \parallel \ldots \parallel C_n),$$

$$\mathbb{W} \stackrel{\mathsf{def}}{=} (\textbf{let } \Gamma \textbf{ in } \mathbb{C}_1 \parallel \ldots \parallel \mathbb{C}_n),$$
$$S \stackrel{\mathsf{def}}{=} (\sigma_c, \sigma \uplus (\biguplus_t \sigma_t), K),$$
$$\mathbb{S} \stackrel{\mathsf{def}}{=} (\sigma_c, \Sigma \uplus (\biguplus_t \Sigma_t), \mathbb{K}).$$

(1) $dom(\mathbb{M}) = \mathsf{activeThrds}(W) = \mathsf{activeThrds}(\mathbb{W})$.

Proof:

For any $t \in [1..n]$, from the premise, we have:

$$(C_t \neq \textbf{skip}) \iff (\mathbb{C}_t \neq \textbf{skip})$$

Thus

$$\mathsf{activeThrds}(\textbf{let } \Pi \textbf{ in } C_1 \parallel \ldots \parallel C_n) = \mathsf{activeThrds}(\textbf{let } \Gamma \textbf{ in } \mathbb{C}_1 \parallel \ldots \parallel \mathbb{C}_n)$$

By the premise, we also know $dom(\mathbb{M}) = \mathsf{activeThrds}(\textbf{let } \Pi \textbf{ in } C_1 \parallel \ldots \parallel C_n)$.

(2) If $(W, S) \longmapsto (\textbf{skip}, S')$, then there exist $\mathbb{T}$ and $\mathbb{S}'$ such that
$\mathsf{get\_obsv}(\mathbb{T}) = \epsilon$ and $(\mathbb{W}, \mathbb{S}) \stackrel{\mathbb{T}}{\longmapsto}{}^{+} (\textbf{skip}, \mathbb{S}')$.

Proof:

By the operational semantics, we know: for any $t \in [1..n]$, we have $C_t = \textbf{skip}$.

By the premise 2, we have $\mathbb{C}_t = \textbf{skip}$.

Thus we have $(\mathbb{W}, \mathbb{S}) \longmapsto (\textbf{skip}, \mathbb{S})$.

(3) If $(W, S) \stackrel{e}{\longmapsto} \textbf{abort}$, then there exist $\mathbb{T}$ and t such that
$e = (t, \textbf{clt}, \textbf{abort})$, $e = \mathsf{get\_obsv}(\mathbb{T})$
and $(\mathbb{W}, \mathbb{S}) \stackrel{\mathbb{T}}{\longmapsto}{}^{+} \textbf{abort}$.

Proof:

By the operational semantics, we know: there exists $t \in [1..n]$ such that

$$(C_t, (\sigma_c, \sigma \uplus (\biguplus_t \sigma_t), \kappa_t)) \stackrel{e}{\rightarrow}_{\mathtt{t},\Pi} \textbf{abort}$$

By premise 2, we know $e = (t, \textbf{clt}, \textbf{abort})$ and there exists $\mathbb{T}$ such that $e = \mathsf{get\_obsv}(\mathbb{T})$ and

$$(\mathbb{C}_t, (\sigma_c, \Sigma \uplus (\biguplus_t \Sigma_t), \Bbbk_t)) \stackrel{\mathbb{T}}{\rightarrow}{}^{+}_{\mathtt{t},\Gamma} \textbf{abort}$$

Thus $(\mathbb{W}, \mathbb{S}) \stackrel{\mathbb{T}}{\longmapsto}{}^{+} \textbf{abort}$.

(4) If $(W, S) \stackrel{e}{\longmapsto} (W', (\sigma_c', \sigma'', K'))$, then there exist $t, \mathbb{T}, \mathbb{W}', \mathbb{S}', \mathbb{M}'$ and n
such that all the following hold.

(a) $(\mathbb{W}, \mathbb{S}) \stackrel{\mathbb{T}}{\longmapsto}{}^{n} (\mathbb{W}', \mathbb{S}')$.

(b) $t = \mathsf{tid}(e)$, $\mathsf{get\_obsv}(e) = \mathsf{get\_obsv}(\mathbb{T})$, and
$(e = (t, \textbf{term})) \implies (e = \mathsf{last}(\mathbb{T}))$.

(c) $(W', (\sigma'_c, \sigma'', K')) \precsim (\mathbb{W}', \mathbb{S}') \diamond M'$.

(d) If $n = 0$, then $\mathbb{M}'(t) < \mathbb{M}(t)$ and $\mathbb{M}' \leq \mathbb{M}$.

Proof:

By the operational semantics, we know there exist t, C'_t and κ'_t such that

$$W' = (\textbf{let } \Pi \textbf{ in } C_1 \parallel \dots C'_t \dots \parallel C_n),$$
$$t = \mathsf{tid}(e),$$
$$(C_t, (\sigma_c, \sigma \uplus (\biguplus_t \sigma_t), \kappa_t)) \xrightarrow{e}_{\mathtt{t},\Pi} (C'_t, (\sigma'_c, \sigma'', \kappa'_t)),$$
$$K' = K\{t \rightsquigarrow \kappa'_t\}.$$

By premise 2, we know

then there exist $\sigma''', n, \mathbb{T}, \mathbb{C}'_t, \Sigma''', \Bbbk'_t$ and M'_t such that

(A) $\sigma'' = \sigma''' \uplus (\biguplus_{t' \neq t} \sigma_{t'})$,

(B) $(\mathbb{C}_t, (\sigma_c, \Sigma \uplus (\biguplus_t \Sigma_t), \Bbbk)) \xrightarrow{\mathbb{T}}{}^{n}_{\mathtt{t},\Gamma} (\mathbb{C}'_t, (\sigma'_c, \Sigma''' \uplus (\biguplus_{t' \neq t} \Sigma_{t'}), \Bbbk'_t))$,

(C) $\mathsf{get\_obsv}(e) = \mathsf{get\_obsv}(\mathbb{T})$ and $(e = (t, \textbf{term})) \implies (e = \mathsf{last}(\mathbb{T}))$,

(D) $R, G, I \models_t (\Pi, C'_t, (\sigma'_c, \sigma''', \kappa'_t)) \precsim (\Gamma, \mathbb{C}'_t, (\sigma'_c, \Sigma''', \Bbbk'_t)) \diamond M'_t \Downarrow P$,

(E) $((\sigma \uplus \sigma_t, \Sigma \uplus \Sigma_t), (\sigma''', \Sigma''')) \models G_t * \mathsf{True}$,

(F) either $n > 0$, or $M'_t < M_t$.

Since $(\sigma, \Sigma) \models I$ and $\forall t. I \rhd \{R_t, G_t\}$, we know there exist $\sigma', \sigma'_t, \Sigma'$ and Σ'_t such that

$$\sigma''' = \sigma' \uplus \sigma'_t, \quad \Sigma''' = \Sigma' \uplus \Sigma'_t,$$
$$(\sigma', \Sigma') \models I, \quad ((\sigma, \Sigma), (\sigma', \Sigma')) \models G_t.$$

For any $t' \neq t$, since $G_t \Rightarrow R_{t'}$, we have

$$((\sigma, \Sigma), (\sigma', \Sigma')) \models R_{t'}.$$

Thus we have

$$((\sigma \uplus \sigma_{t'}, \Sigma \uplus \Sigma_{t'}), (\sigma' \uplus \sigma_{t'}, \Sigma' \uplus \Sigma_{t'})) \models R_{t'} * \mathsf{Id}.$$

By $R, G, I \models_{t'} (\Pi, C_{t'}, (\sigma_c, \sigma \uplus \sigma_{t'}, \kappa_{t'})) \precsim (\Gamma, \mathbb{C}_{t'}, (\sigma_c, \Sigma \uplus \Sigma_{t'}, \Bbbk_{t'})) \diamond M_{t'} \Downarrow P$,
we know there exist $M'_{t'}$ such that

$$R, G, I \models_{t'} (\Pi, C_{t'}, (\sigma'_c, \sigma' \uplus \sigma_{t'}, \kappa_{t'}))$$
$$\precsim$$
$$(\Gamma, \mathbb{C}_{t'}, (\sigma'_c, \Sigma' \uplus \Sigma_{t'}, \Bbbk_{t'})) \diamond M'_{t'} \Downarrow P$$

Define the function $\mathbb{M}'$ as follow:

- $dom(\mathbb{M}') = \mathsf{activeThrds}(W')$,
- For any $t \in dom(\mathbb{M}')$, $\mathbb{M}'(t) = M'_t$.

Then by the co-induction hypothesis, we know

$$(W', (\sigma'_c, \sigma'', K')) \precsim (\mathbb{W}', \mathbb{S}') \diamond \mathbb{M}'.$$

Thus we are done. □

Lemma 16 (Lifting)**.** If $dom(\Pi) = dom(\Gamma)$ and $R, G, I \models \{P\}\Pi \precsim^{i\omega} \Gamma$, then for any t and C, we have $R, G, I \models_t \{P\}(\Pi, C) \precsim (\Gamma, C)\{P\}$.

Proof. By structural induction over C and by co-induction. □

C.3 Proof for ③

Definition 12. $\Pi \precsim_P \Gamma$ iff there exist R, G, I such that $R, G, I \models \{P\}\Pi \precsim \Gamma$ holds.

$R, G, I \models \{P\}\Pi \precsim \Gamma$ iff, for any $f \in dom(\Pi)$, for any σ and Σ, for any t, if $\Pi(f) = (x, C), \Gamma(f) = (y, \mathbb{C})$, and $((\sigma, \Sigma), \mathbf{skip}) \models P_t * \mathsf{own}(x) * \mathsf{own}(y) \wedge (x = y) * \mathsf{arem}(\mathbf{skip})$, then

$$R, G, I \models_t (C, \sigma) \precsim (\mathbb{C}, \Sigma) \Downarrow (P * \mathsf{own}(x) * \mathsf{own}(y) * \mathsf{arem}(\mathbf{skip}))$$

Here $R, G, I \models_t (C, \sigma) \precsim (\mathbb{C}, \Sigma) \Downarrow Q$ is co-inductively defined as follows.

Whenever $R, G, I \models_t (C, \sigma) \precsim (\mathbb{C}, \Sigma) \Downarrow Q$ holds, then the following hold:

(1) If $C = \mathbf{E}[\mathbf{return}\ E]$, then for any Σ_F such that $\Sigma \perp \Sigma_F$, there exist $\mathbb{E}$ and Σ' such that
   a. $(\mathbb{C}, \Sigma \uplus \Sigma_F) \rightarrowtriangle_{\mathsf{t}}^* (\mathbf{return}\ \mathbb{E}, \Sigma' \uplus \Sigma_F)$, and
   b. $((\sigma, \Sigma'), \mathbf{skip}) \models Q_t$ and $[\![E]\!]_{\sigma.s} = [\![\mathbb{E}]\!]_{\Sigma'.s}$, and
   c. $((\sigma, \Sigma), (\sigma, \Sigma')) \models G_t * \mathsf{True}$.

(2) If $C = \mathbf{E}[\mathbf{skip}]$, then for any Σ_F such that $\Sigma \perp \Sigma_F$, there exist $\mathbb{C}'$ and Σ' such that
   a. $(\mathbb{C}, \Sigma \uplus \Sigma_F) \rightarrowtriangle_{\mathsf{t}}^* (\mathbb{C}', \Sigma' \uplus \Sigma_F)$, and
   b. $((\sigma, \Sigma'), \mathbb{C}') \models Q_t$, and
   c. $((\sigma, \Sigma), (\sigma, \Sigma')) \models G_t * \mathsf{True}$.

(3) For any σ_F, $\neg((C, \sigma \uplus \sigma_F) \rightarrowtriangle_{\mathsf{t}} \mathbf{abort})$.

(4) $(C, \sigma) \Downarrow$.

(5) For any σ' and Σ', if $((\sigma, \Sigma), (\sigma', \Sigma')) \models R_t * \mathsf{Id}$, then $R, G, I \models_t (C, \sigma') \precsim (\mathbb{C}, \Sigma') \Downarrow Q$.

(6) For any C', σ'', σ_F and Σ_F, if $(C, \sigma \uplus \sigma_F) \rightarrowtriangle_{\mathsf{t}} (C', \Sigma'')$ and $\Sigma \perp \Sigma_F$, then there exist $\sigma', \mathbb{C}'$ and Σ' such that
   a. $\sigma'' = \sigma' \uplus \sigma_F$, and
   b. $(\mathbb{C}, \Sigma \uplus \Sigma_F) \rightarrowtriangle_{\mathsf{t}}^* (\mathbb{C}', \Sigma' \uplus \Sigma_F)$, and
   c. $R, G, I \models_t (C', \sigma') \precsim (\mathbb{C}', \Sigma') \Downarrow Q$, and
   d. $((\sigma, \Sigma), (\sigma', \Sigma')) \models G_t * \mathsf{True}$.

Definition 13 (Locality)**.** $\mathsf{Locality}(C)$ iff, for any σ_1 nad σ_2, let $\sigma = \sigma_1 \uplus \sigma_2$, then the following hold:

1. (Safety monotonicity) If $\neg((C, \sigma_1) \rightarrowtriangle_{\mathsf{t}}^* \mathbf{abort})$, then $\neg((C, \sigma) \rightarrowtriangle_{\mathsf{t}}^* \mathbf{abort})$.
2. (Termination monotonicity) If $\neg((C, \sigma_1) \rightarrowtriangle_{\mathsf{t}}^* \mathbf{abort})$ and $\neg((C, \sigma_1) \rightarrowtriangle_{\mathsf{t}}^{\omega} \cdot)$, then $\neg((C, \sigma) \rightarrowtriangle_{\mathsf{t}}^{\omega} \cdot)$.

3. (Frame property) For any n and σ', if $\neg((C, \sigma_1) \twoheadrightarrow_{\mathtt{t}}^{*} \textbf{abort})$ and $(C, \sigma) \twoheadrightarrow_{\mathtt{t}}^{n} (C', \sigma')$, then there exists σ_1' such that $\sigma' = \sigma_1' \uplus \sigma_2$ and $(C, \sigma_1) \twoheadrightarrow_{\mathtt{t}}^{n} (C', \sigma_1')$.

Lemma 17 (③ in Fig. 11)**.** If $R, G, I \models \{P\}\Pi \precsim \Gamma$, then $R, G, I \models \{P\}\Pi \precsim^{i\omega} \Gamma$.

Proof. By the following Lemma 18, we prove it directly. □

Lemma 18. If for any $R, G, I, C, \sigma, \mathbb{C}, \Sigma$ and Q, such that

1. $R, G, I \models_t (C, \sigma) \precsim (\mathbb{C}, \Sigma) \Downarrow Q$, and
2. C ends with a (**return** _) statement,

then there exists m, such that $R, G, I \models_t (C, \sigma) \precsim (\mathbb{C}, \Sigma)\Diamond m \Downarrow Q$.

Proof. By $R, G, I \models_t (C, \sigma) \precsim (\mathbb{C}, \Sigma) \Downarrow Q$, we know:

$$(C, \sigma) \Downarrow .$$

Thus we know, there exists m, such that for any n and σ', if $(C, \sigma) \twoheadrightarrow_{\mathtt{t}}^{n} (\mathbf{E}[\textbf{return } \_], \sigma')$, then $n \leq m$.

Then we prove:

$$R, G, I \models_t (C, \sigma) \precsim (\mathbb{C}, \Sigma)\Diamond m \Downarrow Q$$

By Lemma 19, we prove it. □

Lemma 19. If for any $C, \sigma, \mathbb{C}, \Sigma, m$ and Q, such that

1. $R, G, I \models_t (C, \sigma) \precsim (\mathbb{C}, \Sigma) \Downarrow Q$, and
2. for any n, if $(C, \sigma) \twoheadrightarrow_{\mathtt{t}}^{n} (\mathbf{E}[\textbf{return } \_], \_)$, then $n \leq m$, and
3. $(C, \sigma) \Downarrow$,

then $R, G, I \models_t (C, \sigma) \precsim (\mathbb{C}, \Sigma)\Diamond m \Downarrow Q$.

Proof. By co-induction, we have the co-induction hypothesis and need to prove following cases (1) (2) (3) and (4).

(1) If $C = \mathbf{E}[\textbf{return } E]$, then for any Σ_F such that $\Sigma \perp \Sigma_F$, there exist $\mathbb{E}$ and Σ' such that
   (a) $(\mathbb{C}, \Sigma \uplus \Sigma_F) \twoheadrightarrow_{\mathtt{t}}^{*} (\textbf{return } \mathbb{E}, \Sigma' \uplus \Sigma_F)$, and
   (b) $((\sigma, \Sigma'), \textbf{skip}) \models Q_t$ and $[\![E]\!]_{\sigma.s} = [\![\mathbb{E}]\!]_{\Sigma'.s}$, and
   (c) $((\sigma, \Sigma), (\sigma, \Sigma')) \models G_t * \mathsf{True}$.

   Proof: By premise 1, we can prove it directly.

(2) For any σ_F, $\neg((C, \sigma \uplus \sigma_F) \twoheadrightarrow_{\mathtt{t}} \textbf{abort})$.

   Proof: By premise 1, we can prove it directly.

(3) For any C', σ'', σ_F and Σ_F, if $(C, \sigma \uplus \sigma_F) \twoheadrightarrow_{\mathtt{t}} (C', \sigma'')$ and $\Sigma \perp \Sigma_F$, then there exist $\sigma', \mathbb{C}', \Sigma'$ and m' such that
   (a) $\sigma'' = \sigma' \uplus \sigma_F$, and
   (b) $(\mathbb{C}, \Sigma \uplus \Sigma_F) \twoheadrightarrow_{\mathtt{t}}^{n} (\mathbb{C}', \Sigma' \uplus \Sigma_F)$, and
   (c) $R, G, I \models_t (C', \sigma') \precsim (\mathbb{C}', \Sigma')\Diamond m' \Downarrow Q$, and
   (d) $((\sigma, \Sigma), (\sigma', \Sigma')) \models G_t * \mathsf{True}$, and

(e) either $n > 0$, or $m' < m$.

Proof. By premise 1 and $(C, \sigma \uplus \sigma_F) \rightarrowtriangle_{\mathsf{t}} (C', \sigma'')$ and $\Sigma \perp \Sigma_F$, we know there exist $\sigma', \mathbb{C}'$ and Σ', such that

(a′) $\sigma'' = \sigma' \uplus \sigma_F$, and

(b′) $(\mathbb{C}, \Sigma \uplus \Sigma_F) \rightarrowtriangle_{\mathsf{t}}^{*} (\mathbb{C}', \Sigma' \uplus \Sigma_F)$, and

(c′)

$$R, G, I \models_t (C', \sigma') \precsim \mathbb{C}', \Sigma' \Downarrow Q, \text{ and} \tag{*3.2.1}$$

(d′) $((\sigma, \Sigma), (\sigma', \Sigma')) \models G_t * \mathsf{True}$.

Thus we only need to prove: there exists m' such that

- $R, G, I \models_t (C', \sigma') \precsim (\mathbb{C}', \Sigma')\Diamond m' \Downarrow Q$, and
- either $n > 0$, or $m' < m$.

By premise 3 and $(C, \sigma \uplus \sigma_F) \rightarrowtriangle_{\mathsf{t}} (C', \sigma' \uplus \sigma_F)$ and $\mathsf{Locality}(C)$(by Lemma 20), we know

$$(C, \sigma) \rightarrowtriangle_{\mathsf{t}} (C', \sigma')$$

By premise 2, premise 3 and $(C, \sigma) \rightarrowtriangle_{\mathsf{t}} (C', \sigma')$, we know

$$m \geq 1$$

Let $m' = m - 1$, then we only need to prove:

$$R, G, I \models_t (C', \sigma') \precsim (\mathbb{C}', \Sigma')\Diamond(m-1) \Downarrow Q$$

By co-induction hypothesis, we need to prove:

(i) $R, G, I \models_t (C', \sigma') \precsim (\mathbb{C}', \Sigma') \Downarrow Q$.

Proof: By (*3.2.1), we prove it.

(ii) for any n, if $(C', \sigma') \rightarrowtriangle_{\mathsf{t}}^{n} (\mathbf{E}[\mathbf{return}\ \_], \_)$, then $n \leq m - 1$.

Proof: We prove it by contradiction.

Assuming there exists n, such that $(C', \sigma') \rightarrowtriangle_{\mathsf{t}}^{n} (\mathbf{E}[\mathbf{return}\ \_], \_)$ and $n > m - 1$.

Then by $(C, \sigma) \rightarrowtriangle_{\mathsf{t}} (C', \sigma')$, we know

$$(C, \sigma) \rightarrowtriangle_{\mathsf{t}}^{n+1} (\mathbf{E}[\mathbf{return}\ \_], \_) \wedge n + 1 > m$$

which contradict premise 2.

(iii) $(C', \sigma') \Downarrow$.

Proof: By $R, G, I \models_t (C', \sigma') \precsim (\mathbb{C}', \Sigma') \Downarrow Q$, we prove it directly.

Thus we finish this case. □

(4) For any σ' and Σ', if $((\sigma, \Sigma), (\sigma', \Sigma')) \models R_t * \mathsf{Id}$, then there exists m', such that $R, G, I \models_t (C, \sigma') \precsim (\mathbb{C}, \Sigma')\Diamond m' \Downarrow Q$.

Proof:

By premise 1 and $((\sigma, \Sigma), (\sigma', \Sigma')) \models R_t * \mathsf{Id}$, we have:

$$R, G, I \models_t (C, \sigma') \precsim (\mathbb{C}, \Sigma') \Downarrow Q \tag{*3.2.2}$$

By (*3.3.2), we know

$$(C, \sigma') \Downarrow \tag{*3.2.3}$$

Thus we have, there exists m', such that

$$\forall n.\ \text{if } (C, \sigma') \rightarrowtriangle_{\mathsf{t}}^{n} (\mathbf{E}[\mathbf{return}\ \_], \_),\ \text{then } n \leq m' \tag{*3.2.4}$$

By co-induction hypothesis, (*3.2.2), (*3.2.4), (*3.2.3), we get

$$R, G, I \models_t (C, \sigma') \precsim (\mathbb{C}, \Sigma')\Diamond m' \Downarrow Q$$

Thus we have done. □

Lemma 20. For any C, $\mathsf{Locality}(C)$.

We can prove it by induction on the structure of C.

C.4 Proof for ④

Definition 14 (Sequential Judgment Semantics)**.** $\models_{\mathsf{t}} [p]\ C\ [q]$ iff, for all σ, Σ and $\mathbb{C}$, for any t,

if $((\sigma, \Sigma), \mathbb{C}) \models p_t$, the followings are true:

1. for any σ', if $(C, \sigma) \rightarrowtriangle_{\mathsf{t}}^{*} (\mathbf{skip}, \sigma')$, then for any Σ_F such that $\Sigma \perp \Sigma_F$, there exist $\mathbb{C}'$ and Σ' such that
   (a) $(\mathbb{C}, \Sigma \uplus \Sigma_F) \rightarrowtriangle_{\mathsf{t}}^{*} (\mathbb{C}', \Sigma' \uplus \Sigma_F)$, and
   (b) $((\sigma', \Sigma'), \mathbb{C}') \models q_t$.
2. $(C, \sigma) \Downarrow$.

Definition 15 (Judgment Semantics)**.** $R, G, I \models_{\mathsf{t}} \{p\}\ C\ \{q\}$ iff, for any σ, Σ and $\mathbb{C}$, for any t,
if $((\sigma, \Sigma), \mathbb{C}) \models p_t$, then
$R, G, I \models_t (C, \sigma) \precsim (\mathbb{C}, \Sigma) \Downarrow q$.

Lemma 21 (④ in Fig. 11)**.** If $R, G, I \vdash \{P\}\Pi : \Gamma$, then $R, G, I \models \{P\}\Pi \precsim \Gamma$.

By the following lemma, we can prove it directly.

Lemma 22. If

1. $R, G, I \vdash_{\mathsf{t}} \{p\}\ C\ \{q\}$, and
2. for any t and t', if $t \neq t'$, then $G_t \Rightarrow R_{t'}$, and
3. for any t, $I \rhd \{R_t, G_t\}$,
   then $R, G, I \models_{\mathsf{t}} \{p\}\ C\ \{q\}$.

Proof. Induction over the derivation.

By Lemma 23, Lemma 27 and Lemma 28 (with the soundness proofs for other logic rules, which are straightforward and we omit here), we prove it. □

The While Rule

Lemma 23 (WHL-Sound)**.** If

1. $p \Rightarrow (B = B) * I$, and
2. $R, G, I \models_{\mathsf{t}} \{p \wedge B\}\ C\ \{p\}$, and
3. $\models_{\mathsf{t}} [p \wedge B]\ \mathbf{while}(B)\{C\}\ [p \wedge \neg B]$, and
4. $I \rhd \{R, G\}$ and $\mathsf{Sta}(p, R * \mathsf{Id})$, and
5. for any t and t', if $t \neq t'$, then $G_t \Rightarrow R_{t'}$,

then $R, G, I \models_{\mathsf{t}} \{p\}\ \mathbf{while}(B)\{C\}\ \{p \wedge \neg B\}$.

Proof. Below we need to prove: for any $\sigma, \Sigma, \mathbb{C}$, for any t, if $((\sigma, \Sigma), \mathbb{C}) \models p_t$, then

$$R, G, I \models_t (\mathbf{while}(B)\{C\}, \sigma) \precsim (\mathbb{C}, \Sigma) \Downarrow (p \wedge \neg B).$$

By co-induction, we need to prove following (1)(2)(3)(4)(5)(6)(7).

(1) If $\mathbf{while}(B)\{C\} = \mathbf{E}[\mathbf{return}\ E]$, ...

Proof: It is vacuously true.

(2) If $\mathbf{while}(B)\{C\} = \mathbf{skip}$, ...

Proof: It is vacuously true.

(3) For any σ_F, $\neg((\mathbf{while}(B)\{C\}, \sigma \uplus \sigma_F) \twoheadrightarrow_{\mathsf{t}} \mathbf{abort})$.

Proof:

By premise 1, we know $[\![B]\!]$ can not be *undefined*.

Thus we prove it.

(4) $(\mathbf{while}(B)\{C\}, \sigma) \Downarrow$.

Proof:

By premise 3 and $((\sigma, \Sigma), \mathbb{C}) \models p_t$, we have following two cases:

(a) If $[\![B]\!]_{\sigma.s} = \mathbf{true}$, then $((\sigma, \Sigma), \mathbb{C}) \models p_t \wedge B$.

Thus we have:

$$(\mathbf{while}(B)\{C\}, \sigma) \Downarrow .$$

(b) If $[\![B]\!]_{\sigma.s} = \mathbf{false}$, then we know:

$$(\mathbf{while}(B)\{C\}, \sigma) \twoheadrightarrow_{\mathsf{t}} (\mathbf{skip}, \sigma)$$

Thus $(\mathbf{while}(B)\{C\}, \sigma) \Downarrow$ holds.

(5) For any σ' and Σ', if $((\sigma, \Sigma), (\sigma', \Sigma')) \models R_t * \mathsf{Id}$, then

$$R, G, I \models_t (\mathbf{while}(B)\{C\}, \sigma') \precsim (\mathbb{C}, \Sigma') \Downarrow (p \wedge \neg B).$$

Proof:

By co-induction hypothesis, we only need to prove:

$$((\sigma', \Sigma'), \mathbb{C}) \models p_t$$

By $((\sigma, \Sigma), \mathbb{C}) \models p_t$, $((\sigma, \Sigma), (\sigma', \Sigma')) \models R_t * \mathsf{Id}$ and premise 4, we prove it.

(6) If $[\![B]\!]_{\sigma.s} = \mathbf{false}$ and

$(\mathbf{while}(B)\{C\}, \sigma \uplus \sigma_F) \rightarrowtriangle_{\mathsf{t}} (\mathbf{skip}, \sigma \uplus \sigma_F)$, then

(a) $(\mathbb{C}, \Sigma \uplus \Sigma_F) \rightarrowtriangle_{\mathsf{t}}^{*} (\mathbb{C}, \Sigma \uplus \Sigma_F)$, and

Proof: Trivailly hold.

(b) $R, G, I \models_t (\mathbf{skip}, \sigma) \precsim (\mathbb{C}, \Sigma) \Downarrow (p \wedge \neg B)$, and

Proof: By $((\sigma, \Sigma), \mathbb{C}) \models p_t \wedge \neg B$, we prove it.

(c) $((\sigma, \Sigma), (\sigma, \Sigma)) \models G_t * \mathsf{True}$.

Proof: By premise 4, we prove it.

(7) If $[\![B]\!]_{\sigma.s} = \mathbf{true}$ and

$(\mathbf{while}(B)\{C\}, \sigma \uplus \sigma_F) \rightarrowtriangle_{\mathsf{t}} (C; \mathbf{while}(B)\{C\}, \sigma \uplus \sigma_F)$, then

$$R, G, I \models_t (C; \mathbf{while}(B)\{C\}, \sigma) \precsim (\mathbb{C}, \Sigma) \Downarrow (p \wedge \neg B).$$

Proof:

By Lemma 24, we only need to prove:

(a) $R, G, I \models_{\mathsf{t}} \{p \wedge B\}\ C\ \{p\}$, and

(b) $p \Rightarrow (B = B) * I$, and

(c) $\mathsf{Sta}(p, R * \mathsf{Id})$, $I \rhd \{R, G\}$, and

(d) $\models_{\mathsf{t}} [p \wedge B]\ \mathbf{while}(B)\{C\}\ [p \wedge \neg B]$, and

(e) $R, G, I \models_t (C, \sigma) \precsim (\mathbb{C}, \Sigma) \Downarrow p$.

Thus we only need to prove: $R, G, I \models_t (C, \sigma) \precsim (\mathbb{C}, \Sigma) \Downarrow p$.

By $R, G, I \models_{\mathsf{t}} \{p \wedge B\}\ C\ \{p\}$ and $((\sigma, \Sigma), \mathbb{C}) \models p_t \wedge B$, we prove it.

Thus we have done. □

Lemma 24. If

1. $R, G, I \models_{\mathsf{t}} \{p \wedge B\}\ C_0\ \{p\}$, and
2. $p \Rightarrow (B = B) * I$, and
3. $I \rhd \{R, G\}$ and $\mathsf{Sta}(p, R * \mathsf{Id})$, and
4. $\models_{\mathsf{t}} [p \wedge B]\ \mathbf{while}(B)\{C_0\}\ [p \wedge \neg B]$, and
5. $R, G, I \models_t (C, \sigma) \precsim (\mathbb{C}, \Sigma) \Downarrow p$,

then $R, G, I \models_t (C; \mathbf{while}(B)\{C_0\}, \sigma) \precsim (\mathbb{C}, \Sigma) \Downarrow (p \wedge \neg B)$.

Proof. By co-induction, we only need to prove following (1)(2)(3)(4)(5)(6)(7).

(1) If $(C; \mathbf{while}(B)\{C_0\} = \mathbf{E}[\mathbf{return}\ E])$, ...

Proof: It is vacuously true.

(2) If $(C; \mathbf{while}(B)\{C_0\} = \mathbf{skip})$, ...

Proof: It is vacuously true.

(3) For any σ_F, $\neg((C; \mathbf{while}(B)\{C_0\}, \sigma \uplus \sigma_F) \rightarrow_{\mathsf{t}} \mathbf{abort})$.

Proof:

We have following cases:

(a) If $C = \mathbf{skip}$, then it trivially holds.

(b) If $C \neq \mathbf{skip}$, then by premise 5, we have:

$$\neg((C, \sigma) \rightarrow_{\mathsf{t}} \mathbf{abort})$$

By operational semantics, we prove it.

(4) $(C; \mathbf{while}(B)\{C_0\}, \sigma) \Downarrow$.

Proof:

By Lemma 25, premise 5, premise 4 and premise 2, we get:

$$(C; \mathbf{while}(B)\{C_0\}, \sigma) \Downarrow$$

(5) For any σ' and Σ', if $((\sigma, \Sigma), (\sigma', \Sigma')) \models R_t * \mathsf{Id}$, then

$$R, G, I \models_t (C; \mathbf{while}(B)\{C_0\}, \sigma') \precsim (\mathbb{C}, \Sigma') \Downarrow (p \wedge \neg B).$$

Proof:

By co-induciton hypothesis, we only need to prove:

$$R, G, I \models_t (C, \sigma') \precsim (\mathbb{C}, \Sigma') \Downarrow p$$

By premise 5 and $((\sigma, \Sigma), (\sigma', \Sigma')) \models R_t * \mathsf{Id}$, we prove it.

(6) If $C = \mathbf{skip}$, then we have

$(\mathbf{skip}; \mathbf{while}(B)\{C_0\}, \sigma \uplus \sigma_F) \rightarrow_{\mathsf{t}} (\mathbf{while}(B)\{C_0\}, \sigma \uplus \sigma_F)$, and we need to prove:

$$R, G, I \models_t (\mathbf{while}(B)\{C_0\}, \sigma) \precsim (\mathbb{C}, \Sigma) \Downarrow (p \wedge \neg B)$$

Proof:

By co-induction, we only need to prove following (a)(b)(c)(d)(e)(f)(g).

(a) If $\mathbf{while}(B)\{C_0\} = \mathbf{E}[\mathbf{return}\ E]$, ...

Proof: It is vacuously true.

(b) If $\mathbf{while}(B)\{C_0\} = \mathbf{skip}$, ...

Proof: It is vacuously true.

(c) For any σ_F, $\neg((\mathbf{while}(B)\{C_0\}, \sigma \uplus \sigma_F) \rightarrow_{\mathsf{t}} \mathbf{abort})$.

Proof:

By $R, G, I \models_t (\mathbf{skip}, \sigma) \precsim (\mathbb{C}, \Sigma) \Downarrow p$, we know there exist $\mathbb{C}'$ and Σ', such that

(I) $(\mathbb{C}, \Sigma \uplus \Sigma_F) \rightarrowtriangle_{\mathsf{t}}^{*} (\Sigma', \Sigma' \uplus \Sigma_F)$, and

(II)

$$((\sigma, \Sigma'), \mathbb{C}') \models p_t, \text{ and} \tag{*4.2.1.1}$$

(III) $((\sigma, \Sigma), (\sigma, \Sigma')) \models G_t * \mathsf{True}$.

By (*4.2.1.1) and $p \Rightarrow (B = B) * I$, we prove the goal.

(d) $(\mathbf{while}(B)\{C_0\}, \sigma) \Downarrow$.

Proof: by (*4.2.1.1) and $\models_{\mathsf{t}} [p \wedge B]\ \mathbf{while}(B)\{C_0\}\ [p \wedge \neg B]$, we prove it.

(e) For any σ' and Σ', if $((\sigma, \Sigma), (\sigma', \Sigma')) \models R_t * \mathsf{Id}$, then

$$R, G, I \models_t (\mathbf{while}(B)\{C_0\}, \sigma') \precsim (\mathbb{C}, \Sigma') \Downarrow (p \wedge \neg B)$$

Proof:

By co-induction hypothesis, we only need to prove:

$$R, G, I \models_t (\mathbf{skip}, \sigma') \precsim (\mathbb{C}, \Sigma') \Downarrow p$$

By $R, G, I \models_t (\mathbf{skip}, \sigma) \precsim (\mathbb{C}, \Sigma) \Downarrow p$ and

$((\sigma, \Sigma), (\sigma', \Sigma')) \models R_t * \mathsf{Id}$, we prove it.

(f) If $[\![B]\!]_{\sigma.s} = \mathbf{false}$ and

$(\mathbf{while}(B)\{C_0\}, \sigma \uplus \sigma_F) \rightarrowtriangle_{\mathsf{t}} (\mathbf{skip}, \sigma \uplus \sigma_F)$, then

$$R, G, I \models_t (\mathbf{skip}, \sigma) \precsim (\mathbb{C}, \Sigma) \Downarrow (p \wedge \neg B).$$

Proof:

By $R, G, I \models_t (\mathbf{skip}, \sigma) \precsim (\mathbb{C}, \Sigma) \Downarrow p$ and

$[\![B]\!]_{\sigma.s} = \mathbf{false}$, we prove it.

(g) If $[\![B]\!]_{\sigma.s} = \mathbf{true}$ and

$(\mathbf{while}(B)\{C_0\}, \sigma \uplus \sigma_F) \rightarrowtriangle_{\mathsf{t}} (C_0; \mathbf{while}(B)\{C_0\}, \sigma \uplus \sigma_F)$ and $\Sigma \perp \Sigma_F$,

then there exist $\mathbb{C}'$ and Σ', such that

(I) $(\mathbb{C}, \Sigma \uplus \Sigma_F) \rightarrowtriangle_{\mathsf{t}}^{*} (\mathbb{C}', \Sigma' \uplus \Sigma_F)$, and

(II) $R, G, I \models_t (C_0; \mathbf{while}(B)\{C_0\}, \sigma) \precsim (\mathbb{C}', \Sigma') \Downarrow (p \wedge \neg B)$, and

(III) $((\sigma, \Sigma), (\sigma, \Sigma')) \models G_t * \mathsf{True}$.

Proof:

By $R, G, I \models_t (\mathbf{skip}, \sigma) \precsim (\mathbb{C}, \Sigma) \Downarrow p$, we have

for any Σ_F such that $\Sigma \perp \Sigma_F$, there exist $\mathbb{C}'$ and Σ' such that

(I′) $(\mathbb{C}, \Sigma \uplus \Sigma_F) \rightarrowtriangle_{\mathsf{t}}^{*} (\mathbb{C}', \Sigma' \uplus \Sigma_F)$, and

(II′)

$$((\sigma, \Sigma'), \mathbb{C}') \models p, \text{ and} \tag{*4.2.1.2}$$

(III′) $((\sigma, \Sigma), (\sigma, \Sigma')) \models G_t * \mathsf{True}$.

Thus we only need to prove:

$$R, G, I \models_t (C_0; \mathbf{while}(B)\{C_0\}, \sigma) \precsim (\mathbb{C}', \Sigma') \Downarrow (p \wedge \neg B)$$

By the first co-induction hypothesis, we only need to prove:

$$R, G, I \models_t (C_0, \sigma) \precsim (\mathbb{C}', \Sigma') \Downarrow p$$

By (*4.2.1.2) and $[\![B]\!]_{\sigma.s} = \mathbf{true}$, we have:

$$((\sigma, \Sigma'), \mathbb{C}') \models p \wedge B \qquad (*4.2.1.3)$$

By premise 1 and (*4.2.1.3), we prove it.

Thus we finish this case.

(7) If $C \neq \mathbf{skip}$ and

$(C; \mathbf{while}(B)\{C_0\}, \sigma \uplus \sigma_F) \rightarrowtriangle_{\mathtt{t}} (C'; \mathbf{while}(B)\{C_0\}, \sigma'')$ and $\Sigma \perp \Sigma_F$,

then there exist $\sigma', \mathbb{C}'$ and Σ' such that

(a) $\sigma'' = \sigma' \uplus \sigma_F$, and

(b) $(\mathbb{C}, \Sigma \uplus \Sigma_F) \rightarrowtriangle^*_{\mathtt{t}} (\mathbb{C}', \Sigma' \uplus \Sigma_F)$, and

(c) $R, G, I \models_t (C'; \mathbf{while}(B)\{C_0\}, \sigma') \precsim (\mathbb{C}', \Sigma') \Downarrow (p \wedge \neg B)$, and

(d) $((\sigma, \Sigma), (\sigma', \Sigma')) \models G_t * \mathsf{True}$.

Proof:

By premise 5, we have if $(C, \sigma \uplus \sigma_F) \rightarrowtriangle_{\mathtt{t}} (C', \sigma'')$ and $\Sigma \perp \Sigma_F$,

then there exist $\sigma', \mathbb{C}'$ and Σ' such that

(a′) $\sigma'' = \sigma' \uplus \sigma_F$, and

(b′) $(\mathbb{C}, \Sigma \uplus \Sigma_F) \rightarrowtriangle^*_{\mathtt{t}} (\mathbb{C}', \Sigma' \uplus \Sigma_F)$, and

(c′)

$$R, G, I \models_t (C', \sigma') \precsim (\mathbb{C}', \Sigma') \Downarrow p, \text{ and} \qquad (*4.2.1.4)$$

(d′) $((\sigma, \Sigma), (\sigma', \Sigma')) \models G_t * \mathsf{True}$.

Thus we only need to prove:

$$R, G, I \models_t (C'; \mathbf{while}(B)\{C_0\}, \sigma') \precsim (\mathbb{C}', \Sigma') \Downarrow p \wedge \neg B$$

By co-induction hypothesis and (*4.2.1.4), we prove it.

Thus we have done.

□

Lemma 25. If

1. $R, G, I \models_t (C, \sigma) \precsim (\mathbb{C}, \Sigma) \Downarrow p$, and

2. $\models_{\mathsf{t}} [p \wedge B]\ \mathbf{while}(B)\{C_0\}\ [p \wedge \neg B]$, and
3. $p \Rightarrow (B = B) * I$,

then $(C; \mathbf{while}(B)\{C_0\}, \sigma) \Downarrow$.

Proof. By definition, we need to prove following (1)(2).

1. $\neg((C, \mathbf{while}(B)\{C_0\}, \sigma) \rightarrow_{\mathsf{t}}^{\omega} \cdot)$.

   Proof:

   We prove it by contradiction.

   Assuming

$$(C, \mathbf{while}(B)\{C_0\}, \sigma) \rightarrow_{\mathsf{t}}^{\omega} \cdot \tag{*4.2.2.1}$$

   By premise 1, we have:

$$(C, \sigma) \Downarrow$$

   Thus we know:

$$\neg((C, \sigma) \rightarrow_{\mathsf{t}}^{*} \mathbf{abort}) \text{ and } \neg((C, \sigma) \rightarrow_{\mathsf{t}}^{\omega} \cdot)$$

   Thus there exists σ', such that:

$$(C, \sigma) \rightarrow_{\mathsf{t}}^{*} (\mathbf{skip}, \sigma') \tag{*4.2.2.2}$$

   By (*4.2.2.1), we know

$$(\mathbf{while}(B)\{C_0\}, \sigma') \rightarrow_{\mathsf{t}}^{\omega} \cdot \tag{*4.2.2.3}$$

   By Lemma 26, premise 1 and (*4.2.2.3), we know there exist $\mathbb{C}'$ and Σ', such that:

   $(\mathbb{C}, \Sigma) \rightarrow_{\mathsf{t}}^{*} (\mathbb{C}', \Sigma')$, and

   $((\sigma', \Sigma'), \mathbb{C}') \models p$.

   By the value of $[\![B]\!]_{\sigma'.s}$, we need to prove following (a)(b).

   (a) If $[\![B]\!]_{\sigma'.s} = \mathbf{false}$, then

   $(\mathbf{while}(B)\{C_0\}, \sigma') \rightarrow_{\mathsf{t}} (\mathbf{skip}, \sigma')$

   which contradicts (*4.2.2.3).

   (b) If $[\![B]\!]_{\sigma'.s} = \mathbf{true}$, then we have

$$((\sigma', \Sigma'), \mathbb{C}') \models p \wedge B \tag{*4.2.2.4}$$

   By premise 2 and (*4.2.2.4), we have

$$(\mathbf{while}(B)\{C_0\}, \sigma') \Downarrow$$

   which contradicts (*4.2.2.3).

   Thus we finish this case.

2. $\neg((C; \textbf{while}(B)\{C_0\}, \sigma) \twoheadrightarrow_{\mathtt{t}}^{*} \textbf{abort})$.

Proof:

We can prove it in a similar way.

Thus we have done. □

Lemma 26. If for any n,

1. $R, G, I \models_t (C, \sigma) \precsim (\mathbb{C}, \Sigma) \Downarrow q$, and
2. $(C, \sigma) \twoheadrightarrow_{\mathtt{t}}^{n} (C', \sigma')$,

then for any Σ_F, if $\Sigma_F \perp \Sigma$, then there exist $\mathbb{C}'$ and Σ', such that

a. $(\mathbb{C}, \Sigma \uplus \Sigma_F) \twoheadrightarrow_{\mathtt{t}}^{*} (\mathbb{C}', \Sigma' \uplus \Sigma_F)$, and

b. $R, G, I \models_t (C', \sigma') \precsim (\mathbb{C}', \Sigma') \Downarrow q$.

Proof. Induction over n.

Base case: $n = 0$.

It is trivially holds.

Inductive case: $n = k + 1$.

By $(C, \sigma) \twoheadrightarrow_{\mathtt{t}}^{k+1} (C', \sigma')$, we know there exist σ'' and C'', such that

$$(C, \sigma) \twoheadrightarrow_{\mathtt{t}} (C'', \sigma''), \text{ and} \tag{*4.2.3.1}$$

$$(C'', \sigma'') \twoheadrightarrow_{\mathtt{t}}^{k} (C', \sigma') \tag{*4.2.3.2}$$

By $\mathsf{Locality}(C)$ and (*4.2.3.1), we have:

$$\forall \sigma_F.\ (C, \sigma \uplus \sigma_F) \twoheadrightarrow_{\mathtt{t}} (C'', \sigma'' \uplus \sigma_F) \tag{*4.2.3.3}$$

By premise 1 and (*4.2.3.3), we know, for any Σ_F, if $\Sigma \perp \Sigma_F$, then there exist $\mathbb{C}''$ and Σ'', such that

$$(\mathbb{C}, \Sigma \uplus \Sigma_F) \twoheadrightarrow_{\mathtt{t}}^{*} (\mathbb{C}'', \Sigma'' \uplus \Sigma_F), \text{ and} \tag{*4.2.3.a}$$

$$R, G, I \models_t (C'', \sigma'') \precsim (\mathbb{C}'', \Sigma'') \Downarrow q, \text{ and} \tag{*4.2.3.4}$$

$$((\sigma, \Sigma), (\sigma'', \Sigma'')) \models G_t * \mathsf{True}.$$

By induction hypothesis, (*4.2.3.4) and (*4.2.3.2), we have, for any Σ_F, if $\Sigma_F \perp \Sigma$,

then there exist $\mathbb{C}'$ and Σ', such that

$$(\mathbb{C}'', \Sigma'' \uplus \Sigma_F) \twoheadrightarrow_{\mathtt{t}}^{*} (\mathbb{C}', \Sigma' \uplus \Sigma_F), \text{ and} \tag{*4.2.3.5}$$

$$R, G, I \models_t (C', \sigma') \precsim (\mathbb{C}', \Sigma') \Downarrow q$$

Thus we only need to prove:

$$(\mathbb{C}, \Sigma \uplus \Sigma_F) \twoheadrightarrow_{\mathtt{t}}^{*} (\mathbb{C}', \Sigma' \uplus \Sigma_F)$$

By (*4.2.3.a) and (*4.2.3.5), we prove it. □

The ATOM Rule

Lemma 27 (ATOM-Sound)**.** If

1. $\models_{\mathsf{t}} [p]\ C\ [q]$, and
2. $p \ltimes q \Rightarrow G * \mathsf{True}$, and
3. $I \rhd G$, and
4. $p \vee q \Rightarrow I * \mathbf{true}$,

then $[I], G, I \models_{\mathsf{t}} \{p\}\ \langle C\rangle\ \{q\}$.

Proof. By definition, we need to prove, for any σ, Σ and $\mathbb{C}$, for any t,

if $((\sigma, \Sigma), \mathbb{C}) \models p_t$, then

$$[I], G, I \models_t (\langle C\rangle, \sigma) \precsim (\mathbb{C}, \Sigma) \Downarrow q$$

By co-induction, we only need to prove following (1)(2)(3)(4)(5)(6).

1. If $\langle C\rangle = \mathbf{E}[\mathbf{return}\ E]$, ...

   Proof: It is vacuously true.

2. If $\langle C\rangle = \mathbf{skip}$, ...

   Proof: It is vacuously true.

3. For any σ_F, $\neg((\langle C\rangle, \sigma \uplus \sigma_F) \twoheadrightarrow_{\mathsf{t}} \mathbf{abort})$.

   Proof:

   By $\models_{\mathsf{t}} [p]\ C\ [q]$ and $((\sigma, \Sigma), \mathbb{C}) \models p_t$, we know there exists σ', such that

   $$(C, \sigma) \twoheadrightarrow_{\mathsf{t}}^{*} (\mathbf{skip}, \sigma')$$

   By $\mathsf{Locality}(C)$, we know

   $$(C, \sigma \uplus \sigma_F) \twoheadrightarrow_{\mathsf{t}}^{*} (\mathbf{skip}, \sigma' \uplus \sigma_F)$$

   By operational semantics, we prove it.

4. $(\langle C\rangle, \sigma) \Downarrow$.

   Proof:

   By $\models_{\mathsf{t}} [p]\ C\ [q]$ and $((\sigma, \Sigma), \mathbb{C}) \models p_t$, we have;

   $$(C, \sigma) \Downarrow$$

   Thus we prove it.

5. For any σ' and Σ', if $((\sigma, \Sigma), (\sigma', \Sigma')) \models [I] * \mathsf{Id}$, then

   $[I], G, I \models_t (\langle C\rangle, \sigma') \precsim (\mathbb{C}, \Sigma') \Downarrow q$.

   Proof:

   By $((\sigma, \Sigma), (\sigma', \Sigma')) \models [I] * \mathsf{Id}$, we have:

   $$\sigma' = \sigma \text{ and } \Sigma' = \Sigma$$

   Thus we only need to prove:

   $$[I], G, I \models_t (\langle C\rangle, \sigma) \precsim (\mathbb{C}, \Sigma) \Downarrow q$$

   By co-induction hypothesis, we prove it.

6. For any σ'', σ_F and Σ_F,
   if $(\langle C\rangle, \sigma \uplus \sigma_F) \rightarrowtriangle_{\mathsf{t}} (\mathbf{skip}, \sigma'')$ and $\Sigma \perp \Sigma_F$,
   then there exist $\sigma', \mathbb{C}'$ and Σ', such that

$$\sigma'' = \sigma' \uplus \sigma_F, \text{ and}$$
$$(\mathbb{C}, \Sigma \uplus \Sigma_F) \rightarrowtriangle_{\mathsf{t}}^* (\mathbb{C}', \Sigma' \uplus \Sigma_F), \text{ and}$$
$$[I], G, I \models_t (\mathbf{skip}, \sigma') \precsim (\mathbb{C}', \Sigma') \Downarrow q, \text{ and}$$
$$((\sigma, \Sigma), (\sigma', \Sigma')) \models G_t * \mathsf{True}.$$

   Proof:
   By $\models_{\mathsf{t}} [p]\ C\ [q]$, we have:

$$(C, \sigma) \Downarrow \tag{*4.3-1}$$

   By $(\langle C\rangle, \sigma \uplus \sigma_F) \rightarrowtriangle_{\mathsf{t}} (\mathbf{skip}, \sigma'')$, we have:

$$(C, \sigma \uplus \sigma_F) \rightarrowtriangle_{\mathsf{t}}^* (\mathbf{skip}, \sigma'') \tag{*4.3-2}$$

   By $\mathsf{Locality}(C)$, (*4.3-2), (*4.3-1), we have: there exist σ', such that

$$\sigma'' = \sigma' \uplus \sigma_F, \text{ and} \tag{*4.3-4}$$
$$(C, \sigma) \rightarrowtriangle_{\mathsf{t}}^* (\mathbf{skip}, \sigma') \tag{*4.3-3}$$

   By $\models_{\mathsf{t}} [p]\ C\ [q]$ and (*4.3-3), we know for any Σ_F such that $\Sigma \perp \Sigma_F$,
   there exist $\mathbb{C}'$ and Σ' such that

$$(\mathbb{C}, \Sigma \uplus \Sigma_F) \rightarrowtriangle_{\mathsf{t}}^* (\mathbb{C}', \Sigma' \uplus \Sigma_F), \text{ and} \tag{*4.3-5}$$
$$((\sigma', \Sigma'), \mathbb{C}') \models q_t \tag{*4.3-6}$$

   By (*4.3-4) and (*4.3-5), we only need to prove:

$$[I], G, I \models_t (\mathbf{skip}, \sigma') \precsim (\mathbb{C}', \Sigma') \Downarrow q, \text{ and}$$
$$((\sigma, \Sigma), (\sigma', \Sigma')) \models G_t * \mathsf{True}.$$

   By $p \ltimes q \Rightarrow G * \mathsf{True}$, $((\sigma, \Sigma), \mathbb{C}) \models p_t$ and $((\sigma', \Sigma), \mathbb{C}') \models q_t$, we have:

$$((\sigma, \Sigma), (\sigma', \Sigma')) \models G_t * \mathsf{True}$$

   Thus we only need to prove:

$$[I], G, I \models_t (\mathbf{skip}, \sigma') \precsim (\mathbb{C}', \Sigma') \Downarrow q$$

   By $((\sigma', \Sigma'), \mathbb{C}') \models q_t$ and $I \rhd G$, we prove it directly.

Thus we have done. □

The Seq Rule

Lemma 28 (SEQ-Sound)**.** If

1. $R, G, I \models_{\mathsf{t}} \{p\}\ C_1\ \{r\}$, and
2. $R, G, I \models_{\mathsf{t}} \{r\}\ C_2\ \{q\}$,

then $R, G, I \models_{\mathsf{t}} \{p\}\ C_1; C_2\ \{q\}$.

Proof. Below we prove: for any σ, Σ and $\mathbb{C}$, for any t, if $((\sigma, \Sigma), \mathbb{C}) \models p_t$,

then $R, G, I \models_t (C_1; C_2, \sigma) \precsim (\mathbb{C}, \Sigma) \Downarrow q$.

By premise 1, we have

$$R, G, I \models_t (C_1, \sigma) \precsim (\mathbb{C}, \Sigma) \Downarrow r \tag{*4.4-1}$$

By Lemma 29, (*4.4-1) and premise 2, we prove it. □

Lemma 29. If

1. $R, G, I \models_t (C_1, \sigma) \precsim (\mathbb{C}, \Sigma) \Downarrow r$, and
2. $R, G, I \models_{\mathsf{t}} \{r\}\ C_2\ \{q\}$,

then $R, G, I \models_t (C_1; C_2, \sigma) \precsim (\mathbb{C}, \Sigma) \Downarrow q$.

Proof. By co-induction, we only need to prove following (1)(2)(3)(4)(5)(6)(7).

1. If $C_1; C_2 = \mathbf{E}[\mathbf{return}\ E]$, ...

   Proof: It is vacuously true.

2. If $C_1; C_2 = \mathbf{skip}$, ...

   Proof: It is vacuously true.

3. For any σ_F, $\neg((C_1; C_2, \sigma \uplus \sigma_F) \twoheadrightarrow_{\mathsf{t}} \mathbf{abort})$.

   Proof: By operational semantics and premise 1, we prove it.

4. $(C_1; C_2, \sigma) \Downarrow$.

   Proof:

   We need to prove following two cases.

   (I) $\neg((C_1; C_2, \sigma) \twoheadrightarrow_{\mathsf{t}}^{\omega} \cdot)$.

   Proof:

   By premise 1, we have:

   $$(C_1, \sigma) \Downarrow \tag{*4.4.1-1}$$

   By $(C_1, \sigma) \Downarrow$, we have

   $$\neg((C_1, \sigma) \twoheadrightarrow_{\mathsf{t}}^{*} \mathbf{abort}) \text{ and } \neg((C_1, \sigma) \twoheadrightarrow_{\mathsf{t}}^{\omega} \cdot) \tag{*4.4.1-2}$$

   Then we prove the goal by contradiction.

Assuming

$$(C_1; C_2, \sigma) \rightarrowtriangle_{\mathsf{t}}^{\omega} \cdot \tag{*4.4.1-3}$$

By (*4.4.1-3) and (*4.4.1-2), we know there exists σ', such that

$$(C_1, \sigma) \rightarrowtriangle_{\mathsf{t}}^{*} (\mathbf{skip}, \sigma'), \text{ and} \tag{*4.4.1-4}$$

$$(C_2, \sigma') \rightarrowtriangle_{\mathsf{t}}^{\omega} \cdot \tag{*4.4.1-5}$$

By Lemma 26, premise 1 and (*4.4.1-4), we have:

for any Σ_F, if $\Sigma_F \perp \Sigma$,

then there exist $\mathbb{C}'$ and Σ', such that

$$(\mathbb{C}, \Sigma \uplus \Sigma_F) \rightarrowtriangle_{\mathsf{t}}^{*} (\mathbb{C}', \Sigma' \uplus \Sigma_F), \text{ and} \tag{*4.4.1-6}$$

$$R, G, I \models_t (\mathbf{skip}, \sigma') \precsim (\mathbb{C}', \Sigma') \Downarrow r \tag{*4.4.1-7}$$

By (*4.4.1-7), we know for any Σ_F, if $\Sigma_F \perp \Sigma$,

then there exist $\mathbb{C}''$ and Σ'', such that

$$(\mathbb{C}', \Sigma' \uplus \Sigma_F) \rightarrowtriangle_{\mathsf{t}}^{*} (\mathbb{C}'', \Sigma'' \uplus \Sigma_F), \text{ and} \tag{*4.4.1-8}$$

$$((\sigma', \Sigma''), \mathbb{C}'') \models r_t \tag{*4.4.1-9}$$

By $R, G, I \models_{\mathsf{t}} \{r\}\ C_2\ \{q\}$ and (*4.4.1-9), we know:

$$R, G, I \models_t (C_2, \sigma) \precsim (\mathbb{C}'', \Sigma'') \Downarrow q$$

Thus we have:

$$(C_2, \sigma') \Downarrow,$$

which contradicts $(C_2, \sigma') \rightarrowtriangle_{\mathsf{t}}^{\omega} \cdot$ (the equation (*4.4.1-5)).

(II) $\neg((C_1; C_2, \sigma) \rightarrowtriangle_{\mathsf{t}}^{*} \mathbf{abort})$.

Proof: we can prove it in a similar way.

5. For any σ' and Σ', if $((\sigma, \Sigma), (\sigma', \Sigma')) \models R_t * \mathsf{Id}$, then

$$R, G, I \models_t (C_1; C_2, \sigma') \precsim (\mathbb{C}, \Sigma') \Downarrow q$$

Proof:

By co-induction hypothesis, we only need to prove

$$R, G, I \models_t (C_1, \sigma') \precsim (\mathbb{C}, \Sigma') \Downarrow r$$

By premise 1, we can prove it directly.

6. If $C_1 = \textbf{skip}$ and $(C_1; C_2, \sigma \uplus \sigma_F) \rightarrow_{\mathtt{t}} (C_2, \sigma \uplus \sigma_F)$
   and $\Sigma \perp \Sigma_F$,
   then there exist $\mathbb{C}'$ and Σ', such that

$$(\mathbb{C}, \Sigma \uplus \Sigma_F) \rightarrow_{\mathtt{t}}^* (\mathbb{C}', \Sigma' \uplus \Sigma_F), \text{ and}$$
$$R, G, I \models_t (C_2, \sigma) \precsim (\mathbb{C}', \Sigma') \Downarrow q.$$

   Proof:

   By premise 1, we have:

$$R, G, I \models_t (\textbf{skip}, \sigma) \precsim (\mathbb{C}, \Sigma) \Downarrow r$$

   Thus for any Σ_F, if $\Sigma \perp \Sigma_F$,
   then there exist $\mathbb{C}'$ and Σ', such that

$$(\mathbb{C}, \Sigma \uplus \Sigma_F) \rightarrow_{\mathtt{t}}^* (\mathbb{C}', \Sigma' \uplus \Sigma_F), \text{ and} \qquad \text{(*4.4.1-10)}$$
$$((\sigma, \Sigma'), \mathbb{C}') \models r_t$$

   By premise 2 and $((\sigma, \Sigma'), \mathbb{C}') \models r_t$, we have

$$R, G, I \models_t (C_2, \sigma) \precsim (\mathbb{C}', \Sigma') \Downarrow q \qquad \text{(*4.4.1-11)}$$

   By (*4.4.1-10) and (*4.4.1-11), we finish this proof.
7. If $C_1 \neq \textbf{skip}$ and $(C_1; C_2, \sigma \uplus \sigma_F) \rightarrow_{\mathtt{t}} (C_1'; C_2, \sigma'')$ and $\Sigma \perp \Sigma_F$,
   then there exist $\mathbb{C}', \Sigma'$ and σ', such that

$$\sigma'' = \sigma' \uplus \sigma_F, \text{ and}$$
$$(\mathbb{C}, \Sigma \uplus \Sigma_F) \rightarrow_{\mathtt{t}}^* (\mathbb{C}', \Sigma' \uplus \Sigma_F), \text{ and}$$
$$R, G, I \models_t (C_1'; C_2, \sigma') \precsim (\mathbb{C}', \Sigma') \Downarrow q, \text{ and}$$
$$((\sigma, \Sigma), (\sigma', \Sigma')) \models G_t * \mathsf{True}.$$

   Proof:

   By operational semantics, we have:

$$(C_1, \sigma \uplus \sigma_F) \rightarrow_{\mathtt{t}} (C_1', \sigma'').$$

   By premise 1 and $(C_1, \sigma \uplus \sigma_F) \rightarrow_{\mathtt{t}} (C_1', \sigma'')$, we only need to prove:

$$R, G, I \models_t (C_1'; C_2, \sigma') \precsim (\mathbb{C}', \Sigma') \Downarrow q$$

   And we have:

$$R, G, I \models_t (C_1', \sigma') \precsim (\mathbb{C}', \Sigma') \Downarrow r.$$

   By co-induction hypothesis, we prove it.

Thus we have done. □