Manifest Sharing with Session Types

STEPHANIE BALZER AND FRANK PFENNING

March 2017
CMU-CS-17-106

Computer Science Department
School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work supported by a Mozilla Research grant and partially sponsored by NSF Grant CNS-1423168: "Blameworthy Programs: Accountability via Deviance and Causal Determination". Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of Mozilla Research or NSF.
Keywords: Linear logic, Curry-Howard isomorphism, session types, message-passing concurrency, sharing
Abstract

Session-typed languages building on the Curry-Howard isomorphism between linear logic and session-typed communication guarantee session fidelity and deadlock freedom. Unfortunately, these strong guarantees exclude many naturally occurring programming patterns pertaining to shared resources. In this paper, we introduce sharing into a session-typed language where types are stratified into linear and shared layers with modal operators connecting the layers. The resulting language retains session fidelity but not the absence of deadlocks, which can arise from contention for shared processes. We illustrate our language on various examples, such as the dining philosophers problem, and show that sharing recovers the computational power of the untyped asynchronous $\pi$-calculus.
# Contents

1 Introduction .................................................. 1

2 Background .................................................... 2

3 Manifest Sharing ............................................. 4
   3.1 A Programming Perspective ................................. 4
   3.2 A Logic Perspective ......................................... 5
   3.3 Equi-Synchronizing Session Types .......................... 9

4 More Examples ................................................ 11
   4.1 Dining Philosophers ........................................... 11
   4.2 Atomicity ................................................... 12
   4.3 Nondeterminism .............................................. 13

5 Semantics .................................................... 13
   5.1 Configuration Typing ......................................... 14
   5.2 Preservation and Progress .................................... 15
   5.3 Asynchronous Dynamics ...................................... 16

6 Recovering the Computational Power of the Untyped $\pi$-calculus 17

7 Implementation ............................................... 19

8 Related Work ................................................ 21

9 Discussion and Future Work .................................. 22

A Abstract Syntax ............................................. 23

B Statics ....................................................... 23
   B.1 Signature Checking .......................................... 23
   B.2 Process Typing ............................................. 24
   B.3 Configuration Typing ...................................... 25

C Operational Semantics ...................................... 26

D Preservation and Progress .................................. 30
   D.1 Definitions, Lemmas, and Corollaries ..................... 30
      D.1.1 Definitions ........................................... 30
      D.1.2 Lemmas and Corollaries ............................... 30
   D.2 Preservation ............................................... 41
   D.3 Progress .................................................. 53
1 Introduction

Session types \cite{9,31} prescribe the communication protocols that arise in concurrent programming. Session types and session type libraries have found their ways into various practical programming languages \cite{18,33,34,44,53} to express such protocols and ensure their adherence at compile-time. Recently, message-passing concurrency has been put onto a firm logical foundation by exhibiting a Curry-Howard isomorphism between linear logic and session-typed communication \cite{8,9,57,62}. Programming languages \cite{26,58} based on this isomorphism not only guarantee session fidelity (preservation) but also a form of global progress, since the process graph forms a tree and is acyclic by construction.

Unfortunately, these strong guarantees preclude programming scenarios that naturally demand sharing, such as shared databases or output devices, or implementations that make use of sharing for performance considerations. The shared channels available through the exponential modality in linear logic have a copying semantics \cite{8,62} and therefore do not provide the correct tools in such applications. In this paper, shared channels and shared processes always refer to mutable resources.

In this paper, we contribute a session-typed programming language for message-passing concurrency that seamlessly integrates linear and shared processes. The language allows multiple aliases to a shared process to exist, but makes sure that any state-altering communication with such a process only happens once exclusive access to the process has been obtained. At this point, the process becomes linear and can become shared again once it is released, resulting in renunciation of exclusive access. The resulting language retains session fidelity but not the absence of deadlocks, which can arise from contention for shared processes.

A key novelty of our work is to go beyond supporting acquire-release as a mere language primitive, but to enrich the type system so that a session type prescribes at which points in the protocol acquisition and release must happen. We generalize the idea of type stratification introduced in \cite{49}, based on Benton’s LNL 1994 and Reed’s adjoint logic 2009 and stratify session types into a linear and shared layer and support two modalities going back and forth between them. We then interpret the modal operator shifting down from the shared to the linear layer as a release and the operator shifting up from the linear to the shared layer as an acquire. As a result, we obtain a type system where any form of synchronization, including the acquisition and release of a shared process, is manifest in the session type.

Now that types prescribe the acquisition and release points of shared processes, it is only a small step to making sure that the assumptions by a client attempting to acquire a shared process are actually met. When there is contention for a shared process and one client obtains access at type $A$ and then releases it again, the release must happen again at the same type $A$. This is necessary since the acquire/release cycle is invisible to all other clients. To capture this constraint statically we introduce the notion of an equi-synchronizing session type. A session type is equi-synchronizing if it satisfies the invariant that any release restores the session to the same type at which a preceding acquire occurred.

We illustrate our language on various examples, such as producer-consumer queues and dining philosophers, and also demonstrate how nondeterministic choice can be emulated in the resulting language thanks to shared processes. Moreover, we provide an encoding of the untyped asynchronous $\pi$-calculus into our language, recovering the computational power of the untyped $\pi$-calculus for session-typed, message-passing concurrency.

An interesting question is what the meta-theoretic consequences of the introduction of sharing are. The correspondence between linear logic and session-typed communication \cite{8,9,57,62} established for purely linear session-typed languages seems no longer to hold in its original form. Under this interpretation proofs correspond to processes and cut reduction to communication. With the introduction of sharing, on the other hand, shared channels upon which a process depends may not always be available. Such a computation state corresponds to an incomplete proof. Overall, computation is then an interleaving of proof construction (acquiring a resource), proof reduction (communication), and proof deconstruction (releasing a resource). The fact that computation may deadlock is always a failure of proof construction, never communication.

The principal contributions of this paper are:

- the introduction of sharing into session-typed, message-passing, concurrent programming such that sharing is manifest in the type structure via adjoint modalities;
- its elaboration in the programming language SILL5, resulting in type system, synchronous operational semantics,
and proofs of session fidelity (preservation) and a modified form of progress that characterizes possible deadlocks;
• the notion of an equi-synchronizing session type to guarantee session fidelity without the need for run-time type checking when acquiring a process;
• an encoding of the untyped asynchronous $\pi$-calculus into $SILL_5$, reclaiming the expressiveness of the untyped $\pi$-calculus;
• an extension of the formal system to accommodate an asynchronous dynamics, using a novel transformation derived from logic;
• a prototype implementation of manifest sharing in Concurrent C0.

The main part of this paper is structured as follows: Section 2 provides a brief introduction to linear session types. Section 3 introduces manifest sharing. Section 4 illustrates manifest sharing on various examples. Section 5 details the semantics of $SILL_5$, including preservation and progress. Section 6 gives the encoding of the untyped asynchronous $\pi$-calculus into $SILL_5$. Section 7 provides a brief overview of our implementation. Section 8 summarizes the related work, and Section 9 concludes the main part of this paper with a discussion and some remarks about future work. The appendix gives the complete statics and dynamics of $SILL_5$, proofs of preservation and progress as well as of supporting lemmas and corollaries, and further examples.

## 2 Background

In this section, we provide a short introduction to linear session-typed message-passing concurrency based on the functional language $SILL$ [26, 49, 58] built on the Curry-Howard isomorphism between intuitionistic linear logic and session-typed concurrency. $SILL$ incorporates processes into a functional core via a linear contextual monad that isolates session-typed concurrency. In this introduction we focus on the linear process layer of $SILL$, which we extend with manifest sharing in Section 3.

Linear logic [24] is a substructural logic that restricts the structural rules of weakening and contraction to propositions of the form $!A$, where $!$ is a so-called exponential modality. As result, purely linear propositions (that is, propositions without an exponential modality) can be viewed as resources that must be used exactly once in a proof. We adopt the intuitionistic version of linear logic, which yields the following sequent [13]

$$A_1, \ldots, A_n \vdash A$$

where $A_1, \ldots, A_n$ are linear antecedents and $A$ is the succedent.

Under the Curry-Howard isomorphism for intuitionistic linear logic, propositions are related to session types, proofs to processes, and cut reduction in proofs to communication. Appealing to this correspondence, we assign a process term $P$ to the above judgment and label each hypothesis as well as the conclusion with a channel:

$$x_1 : A_1, \ldots, x_n : A_n \vdash P :: (x : A)$$

The resulting judgment states that process $P$ provides a service of session type $A$ along channel $x$, using the services of session types $A_1, \ldots, A_n$ provided along channels $x_1, \ldots, x_n$. The assignment of a channel to the conclusion is convenient because, unlike functions, processes do not evaluate to a value but continue to communicate along their providing channel once they have been created. For the judgment to be well-formed, all the channel names have to be distinct. In particular, the channel name to the right of the turnstile cannot appear to its left. This intuitionistic interpretation of linear logic avoids the need for explicit dualization [29, 30, 62] of a session type. Whether a session type is used or provided is determined by its positioning to the left or right, respectively, of the turnstile.

The balance between providing and using a session is established by the two fundamental rules of the sequent calculus that are independent of all logical connectives: cut and identity. Cut states that if $P$ provides service $A$ along channel $x$, then $Q$ can use the service along the same channel at the same type. Identity states that, if we are a client of a service $A$ we can always directly provide $A$.

$$\Delta \vdash P_x :: (x : A) \quad \Delta', x : A \vdash Q_x :: (z : C)$$

$$\Delta, \Delta' \vdash x \leftarrow P_x ; Q_x :: (z : C) \quad \text{(T-Cut)}$$

$$y : A \vdash \text{fwd } x y :: (x : A) \quad \text{(T-Id)}$$
Operationally, the process $x \gets P_x : Q_x$ creates a globally fresh channel $c$, spawns a new process $[c/x]P_x$ providing
along $c$, and continues as $[c/x]Q_x$. Conversely, the process $\text{fwd} \ c \ d$ terminates after directly identifying channels $c$
and $d$. Here, we have adopted the convention to use $x$, $y$, and $z$ for channel variables and $c$ and $d$ for channels.
Channels are created at run-time and substituted for channel variables in process terms. For type-checking purposes,
the distinction between variables and channels is negligible, even though they obey slightly different invariants (see
Section B.2); we hence use the metavariables $x$, $y$, and $z$ to stand for either of them when type-checking process
terms.

The Curry-Howard correspondence gives each connective of linear logic an interpretation as a session type. This
session type prescribes the kind of message that must be sent or received along a channel of this type and at
which type the session continues after the exchange. Table 1 provides an overview of the session types arising from
linear logic and their operational meaning. We generalize internal $A \oplus B$ and external choice $A \& B$ to n-ary
labeled choices $\odot \{ \Gamma : A \}$ and $\& \{ \Gamma : A \}$, respectively, where we use the overline-notation to denote a sequence, as is
usual. We require external and internal choice to comprise at least one label. Otherwise, there would exist a linear
channel without observable interaction along it, which is computationally not really interesting and furthermore
would complicate our proofs. Because we adopt the intuitionistic version of linear logic, session types are expressed
from the point of view of the provider. In the first line of each connective, Table 1 provides the point of view of
the provider and in the second line the point of view of the client. For each connective, its session type before the
exchange (Session type current) and after the exchange (Session type continuation) is given. Likewise,
the implementing process term is indicated before the exchange (Process term current) and after the exchange
(Process term continuation). Table 1 shows that the process terms of a provider and a client for a connective
come in matching pairs. Both participants’ view of the session changes consistently. The process typing rules for the
connectives shown in Table 1 can be found in Figure 3. We defer the discussion of the process typing judgment to
Section 3.2.

<table>
<thead>
<tr>
<th>Session type current</th>
<th>Process term current</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$c : \odot { \Gamma : A }$</td>
<td>$c : A_h$</td>
<td>provider sends label $l_h$ along $c$</td>
</tr>
<tr>
<td>$c : &amp; { \Gamma : A }$</td>
<td>$c : A_h$</td>
<td>client receives label $l_h$ along $c$</td>
</tr>
<tr>
<td>$c : A \oplus B$</td>
<td>$c : B$</td>
<td>provider receives label $l_h$ along $c$</td>
</tr>
<tr>
<td>$c : A \rightarrow B$</td>
<td>$c : B$</td>
<td>client sends label $l_h$ along $c$</td>
</tr>
<tr>
<td>$c : 1$</td>
<td>-</td>
<td>provider sends “end” along $c$</td>
</tr>
</tbody>
</table>

Table 1: Overview of linear session types together with their operational meaning.

As an illustration, we consider a protocol on how to interact with a provider of a queue data structure that contains
elements of some variable type $A$\footnote{Polymorphism is orthogonal to the investigation of this paper, so we adopt it for the examples without formal treatment, which can be found in the literature \cite{20,37}.}

The session type prescribes that a process providing a service of type $\text{queue} \ A$, gives a client the choice to either
enqueue ($\text{enq}$) or dequeue ($\text{deq}$) an element of type $A$. Upon receipt of the label $\text{enq}$, the providing process expects
to receive a channel of type $A$ to be enqueued and recurs. Upon receipt of the label $\text{deq}$, the providing process
either indicates that the queue is empty (none), in which case it terminates, or that there is a channel stored in

\[
\begin{align*}
\text{queue} \ A &= \& \{ \text{enq} : A \rightarrow \text{queue} \ A, \\
&\phantom{=} \text{deq} : \odot \{ \text{none} : 1, \ \text{some} : A \otimes \text{queue} \ A \} \}
\end{align*}
\]
the queue *(some)*, in which case it dequeues this element, sends it to the client, and recurs. We adopt an *equi-recursive* [14] interpretation for recursive session types, which requires recursive session types to be *contractive* [22]. This interpretation guarantees that there are no messages associated with the unfolding of a recursive type.

Figure 1 shows two process definitions *empty* and *elem* implementing the session type *queue* *A*. In SILL, we declare the type of a defined process *X* with *X* : { *A* ← *A*₁, ..., *A*_ₙ}, indicating that the process provides a service of type *A*, using channels of type *A*₁, ..., *A*_ₙ. The definition of the process is then given by *x* ← *X* ← *y_1*, ..., *y_n* = *P* where *P* is a process term satisfying *y_1* : *A*_₁, ..., *y_n* : *A*_ₙ ⊢ *P* : (*x* : *A*). A new process *X* providing along *x* is spawned with an expression of the form *x* ← *X* ← *y_1*, ..., *y_n* ; *Q*_x, where *Q*_x is the continuation binding *x*. The channels *y_1*, ..., *y_n* are passed to *X* and hence no longer available to *Q*_x.

```
| enq → y ← recv q ; % x : A, t : qu A, y : A ⊢ q : qu A
t.enq ; send t y ; % x : A, t : qu A ⊢ q : qu A
q ← elem ← x, t |
| deq → q.some ; % x : A, t : qu A ⊢ q : A ⊗ qu A
send q x ; % t : qu A ⊢ q : qu A
fwd q t |
```

```
| enq → x ← recv q ; % x : A ⊢ q : qu A
eq ← empty ; % x : A, e : qu A ⊢ q : qu A
q ← elem ← x, e |
| deq → q.none ; % ⊢ q : 1
close q |
```

Figure 1: Processes implementing linear session type *queue* *A*.

The queue in Figure 1 is implemented as a sequence of *elem* processes, ending in an *empty* process. The recursive process *elem* provides a queue along channel *q* and uses a channel *x* : *A* (the element in front of the queue) as well as a channel *t* : *queue* *A* (the tail of the queue). If it receives an *enq* label and then a channel *y*, it simply enqueues *y* in the tail *t*. If it receives a *deq* label it responds with *some*, followed by the channel *x* it holds, and then forwards all future communication along *q* to the tail *t*. The implementation is highly parallel; in particular, many enqueuing operations can be in flight at the same time. Process *empty*, on the other hand, builds a singleton queue from an element received to be enqueued and returns *none* and terminates when asked to dequeue. Perhaps the most unusual aspect of writing session-typed programs is that the type of channels changes during interactions, as already indicated in Table 1. To make this explicit we annotate the code in Figure 1 with the types of all channels at the various points in a process definition. We abbreviate *queue* *A* to *qu* *A* in those comments.

### 3 Manifest Sharing

In this section, we extend the linear process language of the previous section with the capability to share a process among several clients. The shared channels introduced previously [8, 62] via the exponential modality in linear logic have a copying semantics and therefore do not allow sharing of mutable resources as pursued in this paper. We first approach the support of shared processes programatically, by introducing acquire-release as a primitive to our language. We then derive those primitives as modalities from logic in a stratified system of session types. Lastly, we develop the notion of an equi-synchronizing session type.

#### 3.1 A Programming Perspective

In the intuitionistic linear setting of Section 2 processes form a tree at run-time, guaranteeing that a client of a process is the only client of that process. With the introduction of *shared processes* this invariant no longer holds because there may exist multiple clients that refer to the process by a *shared channel*. To uphold session fidelity, communication along a shared channel must only be possible once exclusive access to the process providing along that channel has been obtained. To this end, we impose an *acquire-release* discipline on shared processes, where an acquire yields exclusive access to a shared process, if the process is available, and a release relinquishes exclusive access. As a result, processes can alternate between linear and shared, where a successful acquire of a shared process turns the process into a linear one, and conversely, a release of a linear process turns the process into a shared one. This view of a process undergoing phases requires an identification of a process with a thread
of control, which is extremely natural in intuitionistic linear logic since we can identify a process with the channel along which it provides a service.

We illustrate the programmatic working of the acquire-release primitives on a schematic producer-consumer scenario in Figure 2. For now, we assume for both processes that the shared channel \( q \) is provided by a shared process of session type \( \text{queue } A \) that stores shared elements \( x \) of type \( A \). In program code, we typeset shared channels as well as shared session types in red and bold font to make them distinguishable from linear channels and session types, which we typeset in black and regular font. Moreover, we assume that the session type \( \text{queue } A \) recurs rather than terminates upon dequeueing, if the queue is empty, which is more appropriate for a producer-consumer context. In Section 3.2 we clarify how to change the type specification to accommodate these assumptions.

Processes \textit{produce} and \textit{consume} in Figure 2 attempt to communicate with the queue by issuing corresponding acquire and release statements. Process \textit{produce}, for example, issues the statement \( q' \leftarrow \text{acquire } q \), which, if successful, yields the queue’s linear channel \( q' \) along which the process can enqueue the element. Before the process recurs, it releases the now linear \textit{queue} process providing along \( q' \) by issuing \( q \leftarrow \text{release } q' \). This yields the queue’s shared channel \( q \) and gives turn to another producer or consumer.

\begin{align*}
\text{produce} &: \{1 \leftarrow A, \text{queue } A\} \\
&\quad c \leftarrow \text{produce } \leftarrow x, q = \\
&\quad q' \leftarrow \text{acquire } q ; \\
&\quad q'.\text{enq} ; \\
&\quad \text{send } q' \times ; \\
&\quad q \leftarrow q' ; \\
&\quad c \leftarrow \text{produce } \leftarrow x, q
\end{align*}

\begin{align*}
\text{consume} &: \{1 \leftarrow \text{queue } A\} \\
&\quad c \leftarrow \text{consume } \leftarrow q = \\
&\quad q' \leftarrow \text{acquire } q ; \\
&\quad q'.\text{deq} ; \\
&\quad \text{case } q' \text{ of} \\
&\quad \mid \text{some } \rightarrow x \leftarrow \text{recv } q' ; \\
&\quad \quad q \leftarrow q' ; \\
&\quad \quad c \leftarrow \text{consume } \leftarrow q \\
&\quad \mid \text{none } \rightarrow q \leftarrow q' ; \\
&\quad \quad c \leftarrow \text{consume } \leftarrow q
\end{align*}

Figure 2: Acquire-release primitives illustrated on producer-consumer, programatically. Shared channels are typeset in red and bold font, linear channels in black and regular font. See Section 3.2 for definition of shared session type \( \text{queue } A \).

### 3.2 A Logic Perspective

Like send and receipt of a message, acquire and release denote synchronization points in the communication between processes. If we were to introduce acquire and release as operational primitives only, session types would no longer accurately prescribe the protocols of communication. To restore the descriptive power of session types, we enrich the type system so that the type of a process dictates at which points in the communication acquire and release must happen.

The key idea in pursuit of this goal is to generalize the notion of type stratification introduced in [49], based on Benton’s LNL 1994 and Reed’s adjoint logic 2009, and to stratify session types into a linear and shared layer. We then connect these layers with modalities that go back and forth between them. In [Pfenning and Griffith 2015] the modes are U, F, and L for unrestricted, affine, and linear session types, respectively. In this paper, we focus on the interplay between the modes S and L, pertaining to shared and linear session types, respectively. An integration with the remaining modes U and F is straightforward.

The stratification arises from a difference in structural properties that exist for session types at a mode — or propositions, when viewed through the lens of the Curry-Howard correspondence. For example, shared propositions can be weakened, contracted, and exchanged, whereas linear propositions can only be exchanged. The difference in structural properties entails a hierarchy between modes such that a mode with fewer structural properties is at the bottom. The hierarchy for the modes S and L is:

\[ S > L \]

The independence principle for modes states that proofs of a proposition of a stronger mode (with more structural properties) may not depend on hypotheses of a strictly weaker mode (with fewer structural properties). This is
because a client of a stronger proposition may, for example, reuse the proposition, which would implicitly reuse the weaker proposition on which it depends. More technically, on the logical side, cut elimination would fail without this restriction. As a result, we get separate\footnote{We could have chosen an combined judgment with a combined context and corresponding projections onto each mode, as employed in \cite{DBLP:conf/esop/Heule19} for a richer structure of modes. For this paper, we have chosen separate judgments and contexts for clarity of presentation.} hypothetical judgments for shared and linear processes which, by definition, obey the independence principle:

$$
\Gamma \vdash_{\Sigma} P :: (x_5 : A_5)
$$

$$
\Gamma; \Delta \vdash_{\Sigma} P :: (x_1 : A_1)
$$

The subscripts denote the respective mode of a channel or session type, and the contexts $\Gamma$ and $\Delta$ consist of hypotheses on the typing of shared and linear channels, respectively. The judgments depend on a signature $\Sigma$ that is populated with all process definitions prior to type-checking, allowing for recursive process definitions.

Given the two layers, we can now define the modality $\downarrow_{\text{S}} A_5$, which shifts a shared proposition (session type) to a linear one, and the modality $\uparrow_{\text{L}} A_1$, which shifts a linear proposition (session type) to a shared one. The resulting strata restricted to session types (propositions) at the modes $\text{S}$ and $\text{L}$ are\footnote{Shared counterparts of all the linear connectives can be defined at the shared level as well, but for the purposes of this paper we will keep the shared layer as simple as possible.}

$$
A_5 \quad \triangleq \quad \uparrow_{\text{L}} A_1
$$

$$
A_1, B_1 \quad \triangleq \quad A_1 \otimes B_1 \mid 1 \mid \oplus \{l : A_1\} \mid \exists A_5, B_5 \mid \exists l : A_5, B_5 \mid & \{l : A_1\} \mid \downarrow_{\text{S}} A_5
$$

We review the new connectives and their operational meaning in Table\footnote{We could have chosen an combined judgment with a combined context and corresponding projections onto each mode, as employed in \cite{DBLP:conf/esop/Heule19} for a richer structure of modes. For this paper, we have chosen separate judgments and contexts for clarity of presentation.}. Together with Table\footnote{We could have chosen an combined judgment with a combined context and corresponding projections onto each mode, as employed in \cite{DBLP:conf/esop/Heule19} for a richer structure of modes. For this paper, we have chosen separate judgments and contexts for clarity of presentation.} this table defines the connectives supported in $\text{SILL}_S$. Besides the new connectives to accommodate acquire-release, which we discuss in more detail below, we introduce the connectives $\exists A_5, B_5$ and $\exists l : A_5$ to support shared channel input and output, respectively. These connectives of mixed mode are based on the dependent session type connectives introduced in \cite{DBLP:conf/esop/Heule19} \cite{DBLP:conf/esop/Lawvere18}, yet at the present stage our language does not make use of the potentially dependent nature of these connectives. The process typing rules for the connectives of $\text{SILL}_S$, excluding the acquire-release connectives, which we discuss below, can be found in Figure\footnote{We could have chosen an combined judgment with a combined context and corresponding projections onto each mode, as employed in \cite{DBLP:conf/esop/Heule19} for a richer structure of modes. For this paper, we have chosen separate judgments and contexts for clarity of presentation.}. A complete listing of all the process typing rules can be found in Figure\footnote{We could have chosen an combined judgment with a combined context and corresponding projections onto each mode, as employed in \cite{DBLP:conf/esop/Heule19} for a richer structure of modes. For this paper, we have chosen separate judgments and contexts for clarity of presentation.} and Figure\footnote{We could have chosen an combined judgment with a combined context and corresponding projections onto each mode, as employed in \cite{DBLP:conf/esop/Heule19} for a richer structure of modes. For this paper, we have chosen separate judgments and contexts for clarity of presentation.} in the appendix.

<table>
<thead>
<tr>
<th>Session type</th>
<th>Process term</th>
<th>Continuation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$c_1 : \exists A_5, B_5$</td>
<td>$c_l : B_l$</td>
<td>$\text{send } c_1 \mid d_5 \mid P$</td>
<td>$P$</td>
</tr>
<tr>
<td>$c_1 : \exists A_5, B_5$</td>
<td>$c_l : B_l$</td>
<td>$y_5 \leftarrow \text{recv } c_1 \mid Q_{y_5}$</td>
<td>$[d_5/y_5] Q_{y_5}$</td>
</tr>
<tr>
<td>$c_1 : \downarrow_{\text{S}} A_5$</td>
<td>$c_5 : A_5$</td>
<td>$c_5 \leftarrow \text{detach } c_1 \mid P_{c_5}$</td>
<td>$[c_5/x_5] P_{c_5}$</td>
</tr>
<tr>
<td>$c_5 : \uparrow_{\text{L}} A_1$</td>
<td>$c_l : A_l$</td>
<td>$x_5 \leftarrow \text{release } c_1 \mid Q_{x_5}$</td>
<td>$[c_5/x_5] Q_{x_5}$</td>
</tr>
</tbody>
</table>

Table 2: Overview of shared session types together with their operational meaning. See Table\footnote{We could have chosen an combined judgment with a combined context and corresponding projections onto each mode, as employed in \cite{DBLP:conf/esop/Heule19} for a richer structure of modes. For this paper, we have chosen separate judgments and contexts for clarity of presentation.} for linear connectives.
an acquire and a detach initiates a release. We review each pair of rules in turn, along with their operational semantics:

The typing of the pair acquire-accept is defined by the following rules:

\[
\frac{\Gamma, x_3 : \uparrow x_3 A; \Delta, x_1 : A \vdash Q_{\alpha_1} :: (z_1 : C_1)}{\Gamma, y_3 : \uparrow x_3 A; \Delta \vdash_{\Sigma} x_3 \leftarrow \text{acquire } x_3 : Q_{\alpha_1} :: (z_1 : C_1)} \quad \text{(T-\uparrow)}
\]

\[
\frac{\Gamma, \cdot \vdash_{\Sigma} P_{\alpha} :: (x_1 : A_{\alpha})}{\Gamma \vdash_{\Sigma} x_1 \leftarrow \text{accept } x_3 : P_{\alpha} :: (x_3 : \uparrow x_3 A)} \quad \text{(T-\uparrow^R)}
\]

An acquire is applied to the shared channel \(x_3\) along which the shared process offers and yields the process’ linear channel \(x_1\), when successful. The shared channel \(x_3\) is still available to the continuation \(Q_{\alpha_1}\). By accepting an acquire request by a client along its shared channel \(x_3\), a shared process transitions to a linear process, now offering along its linear channel \(x_1\). Since the independence principle forbids a shared process to depend on linear channels, the new linear process starts out with an empty linear context.
(D-Id₁) \[ \text{proc}(a, \text{fwd } a, b_1) \rightarrow a = b_1, a_3 = b_5 \]
(D-Id₂) \[ \text{proc}(a, \text{fwd } a, b_2) \rightarrow \text{unavail}(a), a_3 = b_5 \]
(D-Spawn₄) \[ \text{proc}(a, x_1 \leftarrow X_1 \leftarrow \tau / \tau_1, \tau_2; Q_{a}) \rightarrow \text{proc}(a, [b / x_1] Q_{a}), \text{proc}(b, [b / x_1], \tau_1 / \tau, \tau_2 / \tau) P_{\tau_1 / \tau_2, \tau_1}, \text{unavail}(b) \]
for \( x_1' : A_1 \leftarrow X_1 \leftarrow \tau_2 : B_1, \tau_2 : B_2 = P_{\tau_1 / \tau_2, \tau_1} \in \Sigma \) and \( b \) fresh

(D-Spawn₅) \[ \text{proc}(a, x_2 \leftarrow X_2 \leftarrow \tau; Q_{a}) \rightarrow \text{proc}(a, [b / x_2] Q_{a}), \text{proc}(b, [b / x_2], \tau / \tau) P_{\tau / \tau}, \text{unavail}(b) \]
for \( x_2' : A_2 \leftarrow X_2 \leftarrow \tau : B_2 = P_{\tau / \tau} \in \Sigma \) and \( b \) fresh

(D-Spawn₆) \[ \text{proc}(a, x_3 \leftarrow X_3 \leftarrow \tau; Q_{a}) \rightarrow \text{proc}(a, [b / x_3] Q_{a}), \text{proc}(b, [b / x_3], \tau / \tau) P_{\tau / \tau}, \text{unavail}(b) \]
for \( x_3' : A_3 \leftarrow X_3 \leftarrow \tau : B_3 = P_{\tau / \tau} \in \Sigma \) and \( b \) fresh

(D-1) \[ \text{proc}(a, \text{wait } a; Q), \text{proc}(a, \text{close } a) \rightarrow \text{proc}(a, Q) \]
(D-⊙/Ξ) \[ \text{proc}(a, y \leftarrow \text{recv } a; Q_a), \text{proc}(a, \text{send } a, b; P) \rightarrow \text{proc}(a, [b / y] Q_a), \text{proc}(a, P) \]
(D-→/Π) \[ \text{proc}(a, \text{send } a, b; Q), \text{proc}(a, y \leftarrow \text{recv } a; P) \rightarrow \text{proc}(a, Q), \text{proc}(a, [b / y] P) \]
(D-⊙) \[ \text{proc}(a, \text{case } a \text{ of } I \Rightarrow Q), \text{proc}(a, a, a_a, P) \rightarrow \text{proc}(a, Q), \text{proc}(a, P) \]
(D-⊙) \[ \text{proc}(a, a_a; Q), \text{proc}(a, a, a_a; P) \rightarrow \text{proc}(a, Q), \text{proc}(a, P) \]

Figure 4: Remaining multiset rewriting rules not shown inline.

Operationally, we capture the dynamics of SILL₅ by \textit{multiset rewriting rules} [11]. A multiset rewriting rule is generally of the form \( S_1, \ldots, S_n \rightarrow T_1, \ldots, T_m \) and denotes a transition from \( S_1, \ldots, S_n \) to the \( T_1, \ldots, T_m \), where each \( S_i \) and \( T_j \) is a formula capturing some aspect of the current state of the computation. In our setting, we use the rules to capture a transition in the configuration of processes that arise from a program. As we discuss in Section 5.1, we use the predicates \( \text{proc}(c_m, P) \) and \( \text{unavail}(a) \) to define the states of a configuration. The former denotes a process with process term \( P \) that provides along channel \( c_m \) at mode \( m \), the latter acts as a placeholder for a shared channel providing along channel \( a \) that is currently not available. Multiset rewriting rules are local in that they only mention the parts of a configuration they rewrite. The synchronous dynamics of the pair acquire-accept is given by the following rule:

\[ \text{proc}(a, x \leftarrow \text{acquire } a; Q_a), \text{proc}(a, x \leftarrow \text{accept } a; P_a) \rightarrow \text{proc}(a, [a / x] Q_a), \text{proc}(a, [a / x] P_a), \text{unavail}(a) \]  

(D-\( \rightarrow \))

The above rule indicates that, at run-time, for every process there exists one channel, \( a \), with two modes, a linear one, \( a_1 \), and a shared one, \( a_2 \). When a process shifts between modes, it switches between the two modes of its offering channel. This channel is substituted at the appropriate mode for the variables occurring within process terms. The typing rules (T-\( \rightarrow \)) and (T-\( \leftrightarrow \)) create a fresh variable \( x_1 \), for which the already existing channel \( a \) at mode \( L \) is substituted. The offering channel together with its two modes is created when a process is spawned.

Figure 4 gives the dynamics of the remaining connectives in SILL₅. A complete listing of all the multiset rewriting rules can be found in Figure 2 in the appendix. The side condition \( b \) \textit{fresh} indicates allocation of a globally fresh channel and the equality \( a = b \) expresses that \( b \) is substituted for \( a \) in the entire configuration. For convenience, we write multiset rewriting rules such that a providing process appears to the right of its client. Multiset rewriting rules, however, are unordered.

The typing of the pair release-detach is defined by the following rules:

\[ \Gamma, x_5 : A; \Delta \vdash \Sigma Q_{x_5} :: (z_5 : C_5) \quad \Gamma \vdash \Sigma P_{x_5} :: (x_5 : A_5) \quad (T-\check{\rightarrow}^L) \]

\[ \Gamma; \Delta, x_5 : \check{\rightarrow}^L A_5 \vdash \Sigma, x_5 \leftarrow \text{release } x_5 ; Q_{x_5} :: (z_5 : C_5) \quad (T-\check{\rightarrow}^L_R) \]

The rules are essentially inverse to the typing rules of acquire-release; we point out that rule (T-\( \check{\rightarrow}^L_R \)) requires the linear context to be empty, to satisfy the independence principle. Operationally, the rules have the following semantics:

\[ \text{proc}(a, x_5 \leftarrow \text{release } a; Q_a), \text{proc}(a, x_5 \leftarrow \text{detach } a; P_{x_5}), \text{unavail}(a) \rightarrow \text{proc}(a, [a / x_5] Q_{x_5}), \text{proc}(a, [a / x_5] P_{x_5}) \]  

(D-\( \check{\rightarrow} \))

This time the rules shift the process from \textit{S} to \textit{L}, by switching the offering channel from \( a \) to \( a_5 \) and by substituting the channel \( a_5 \) for the variable \( x_5 \).

Let’s now return to the producer-consumer example and work out what the type specifications have to be. The processes \textit{produce} and \textit{consume} in Figure 2 have been devised under the assumption that the channel \( q \) is a shared
channel to a shared queue and that the shared queue process recurs rather than terminates upon dequeueing, if the queue is empty. For this to be the case, we change the session type queue from Section 2 as follows:

\[
\text{queue } A_5 = \uparrow^t \Pi \text{queue } A_5, \downarrow^t \text{queue } A_5, \text{some : } \exists A_5, \downarrow^t \text{queue } A_5\}
\]

With this change, the code in Figure 2 is type-correct as it is written. The new definition of session type queue uses the previously introduced dependent linear session types \(\Pi_{A_5, B_5}\) and \(\exists A_5, B_5\) for shared channel input and output, respectively, and prescribes the following synchronization pattern: When a process of type queue \(A_5\) is spawned, it starts out as a shared process that first must be acquired. Any of the defined sequences of inputs and outputs then are executed while the process is linear. After such an exchange, the process recurs at type \(\downarrow^t \text{queue } A_5\). Since queue \(A_5\) is defined as \(\uparrow^t \Pi \text{queue } A_5\), the type \(\downarrow^t \text{queue } A_5\) amounts to the type \(\downarrow^t \Pi \text{queue } A_5\). This means that in its recursion, the process will first need to be released to become a shared process of type \(\downarrow^t \text{queue } A_5\). Comparing this shared version of session type queue with its linear version in Section 2, we note that the shared version does no longer require the elements stored in the queue to be linear. The elements can either be of a shared type \(A_5\) or of a shifted linear type \(\uparrow^t A_5\). This choice is not available for a linear queue because the queue can only be consumed if all the elements stored in it can be consumed too. For the same reason it is now also possible for the shared queue to recur upon dequeueing rather than terminating, if the queue is empty.

### 3.3 Equi-Synchronizing Session Types

So far we have achieved that a client communicates with a shared process in mutual exclusion from other clients and that the acquire and release points of a shared process manifest in its session type. There remains a last threat
to session fidelity that we need to address: erroneous assumptions by a client on a shared process’ type. These can come about, for example, in the following scenario: two clients $Q_1$ and $Q_2$ are trying to acquire access to the same shared channel $c_i$ at type $\uparrow_i^A A_i$. Let’s assume that $Q_1$ succeeds and then later releases $c_i$ to a different type $\uparrow_i^B B_i$. Once $Q_2$ finally obtains access to $c_i$, $Q_2$ and the provider will disagree on the type of the channel $c_i$: the provider will think that $c_i : B_i$, while $Q_2$ will think that $c_i : A_i$, thereby violating session fidelity.

To guarantee preservation without resorting to run-time checks, we introduce the notion of an equi-synchronizing session type. A session type is equi-synchronizing if it imposes the invariant on a process to be preserved without resorting to run-time checks. We formally define the notion of an equi-synchronizing session type in Figure 6, giving a coinductive definition. For example, our shared queue $A_s$ from Section 3.2 is equi-synchronizing because, in each branch, it releases a channel back to type queue $A_s$, which is the type at which the channel must have been acquired.

We say that the type $A$ equi-synchronizes to $\hat{D}$ or that $\hat{D}$ is $A$’s equi-synchronizing constraint. Underlying the coinductive definition of an equi-synchronizing session type is the notion of a continuation type. To check that a type $A$ equi-synchronizes to the type $\uparrow_i^D D_i$, the rules in Figure 6 transitively step through $A$’s continuation (starting from $(A, \top)$) until the first acquisition point $\uparrow_i^B B_i$ is encountered. At this point, the type $\uparrow_i^B B_i$ is set to be the equi-synchronizing constraint, and the rules transitively step through each continuation of $B_i$ until the first release point $\uparrow_i^C C_i$ is encountered. The session type is equi-synchronizing, if it holds that $C_i = \uparrow_i^D D_i$ at each such release point.

Let’s exercise the rules in Figure 6 on our shared queue $A_s$. We start out with $\vdash (\text{queue } A_s, \top)$ sync. Since session types are interpreted equi-recursively and are contractive [22], we can “silently” replace queue $A_s$ with its definition, which means we have to check $\vdash (\uparrow_i^\downarrow \text{queue } A_s, \top)$ sync.
According to rule \((T\text{-ESYNC}_\uparrow)\), we set the equi-synchronizing constraint to \(\text{queue} \ A_s\), requiring us to check for the continuation that

\[ \vdash \Sigma (\&\{\text{enq} : \ldots \text{deq} : \ldots\}, \text{queue} \ A_s) \ esync \]

According to rule \((T\text{-ESYNC}_\downarrow)\), we are required to check for each continuation that

\[ \vdash \Sigma (\Pi A_s.\downarrow^\downarrow\text{queue} \ A_s, \text{queue} \ A_s) \ esync \]

\[ \vdash \Sigma (\oplus\{\text{none} : \downarrow^\downarrow\text{queue} \ A_s, \ \text{some} : \exists A_s.\downarrow^\downarrow\text{queue} \ A_s\}, \text{queue} \ A_s) \ esync \]

Let’s consider the first branch. According to rule \((T\text{-ESYNC}_\Pi)\) we must check that

\[ \vdash \Sigma (\downarrow^\downarrow\text{queue} \ A_s, \text{queue} \ A_s) \ esync \]

which, according to rule \((T\text{-ESYNC}_\downarrow^\downarrow)\), amounts to the check

\[ \vdash \Sigma (\text{queue} \ A_s, \top) \ esync \]

This is the check we started out with, allowing us to succeed on this branch since our rules are interpreted coinductively. Since the same holds true for all branches, we conclude that the session type \(\text{queue} \ A_s\) is equi-synchronizing, unfolding type definitions where necessary.

Not all branches must actually release. For example, the variant

\[
\text{queue} \ A_s = \uparrow^\uparrow \&\{\text{enq} : \Pi A_s.\downarrow^\downarrow\text{queue} \ A_s, \\
\text{deq} : \oplus\{\text{none} : \downarrow^\downarrow, \ \text{some} : \exists A_s.\downarrow^\downarrow\text{queue} \ A_s\}\}
\]

of the shared queue above is equi-synchronizing even though the queue terminates upon dequeuing in case of an empty queue. In that case, the queue can effectively no longer be acquired.

As we will show in more detail in Section 5.2 the equi-synchronizing invariants are at the core of the preservation proof, requiring us to show that each process maintains its equi-synchronizing constraint along all possible transitions. The three possible constraints \(D\), namely \(\top\), \(\uparrow^\uparrow A_i\), and \(\bot\), are related by the following partial order, for any \(A_i\):

\[ \top \geq \uparrow^\uparrow A_i \geq \bot \]

This relationship becomes relevant for substitutions, where we allow substituting a channel of a smaller type for variables or channels of a bigger type at the client side (see Section 5.2).

When checking the signature \(\Sigma\), recursive session type definitions are checked to be both contractive and equi-synchronizing and process definitions are checked to provide an equi-synchronizing session type. The check is initiated with \(\top\) as a constraint to convey that any initial release is unconstrained. A purely linear session type \(A_i\) with neither acquire nor release points will thus satisfy the constraint \(\vdash \Sigma (A_i, \top) \ esync\) and also the even stronger condition \(\vdash \Sigma (A_i, \bot) \ esync\).

4 More Examples

In this section, we illustrate manifest sharing on several examples. Section E provides additional examples, including an “imperative” style of a queue implementation that maintains a reference to the back of the queue.

4.1 Dining Philosophers

The dining philosophers problem [19] is a prime example designed to illustrate the issues of enforcing mutual exclusion in the presence of circular dependencies among processes. It’s precisely because of circularity that the dining philosophers problem cannot be modelled in the purely linear language presented in Section 2. With sharing at our disposal, however, we are now able to model the dining philosophers problem. The result is given in Figure 7.
The implementation defines the mutually dependent session types \( \text{return} \) and \( \text{fork} \) and the session type \( \text{phil} \), representing a fork and a philosopher, respectively. In support of the spirit of the example, the former allow perpetual acquire-release cycles and are implemented by process \( \text{fork} \). Session type \( \text{phil} \), on the other hand, denotes a trivial linear session, which is implemented by the processes \( \text{thinking} \) and \( \text{eating} \). As the names suggest, process \( \text{thinking} \) represents a philosopher that is thinking, whereas process \( \text{eating} \) represents a philosopher that is eating. A thinking philosopher has shared channel references to the forks on their left and right. Once the philosopher is done thinking, they attempt to acquire their right and left fork and transition to eating, if successful. An eating philosopher, on the other hand, has linear channel references to the forks on their left and right, which they release, once they are done eating and before transitioning to thinking. We can set up a table of 4 philosophers using the following lines of code:

\[
\begin{align*}
\text{f0} &\leftarrow \text{fork}\_\text{proc} ; \\
\text{f1} &\leftarrow \text{fork}\_\text{proc} ; \\
\text{f2} &\leftarrow \text{fork}\_\text{proc} ; \\
\text{f3} &\leftarrow \text{fork}\_\text{proc} ; \\
\text{p0} &\leftarrow \text{thinking} \leftarrow \text{f0}, \text{f1} ; \\
\text{p1} &\leftarrow \text{thinking} \leftarrow \text{f1}, \text{f2} ; \\
\text{p2} &\leftarrow \text{thinking} \leftarrow \text{f2}, \text{f3} ; \\
\text{p3} &\leftarrow \text{thinking} \leftarrow \text{f3}, \text{f0} ;
\end{align*}
\]

The above setup faithfully matches the circular table and can lead to a deadlock, as pointed out by Dijkstra, if every philosopher picks up the fork on their left and then blocks, waiting for the fork on their right. We can avoid this deadlock by following Dijkstra’s originally proposed solution to impose a partial order on the forks and acquiring the forks in ascending order. This can be achieved by reversing the order of the arguments in the last line to \( p3 \leftarrow \text{thinking} \leftarrow f0, f3 \).

### 4.2 Atomicity

Another benefit of making the acquire and release points of a process manifest in the type structure is that atomic sections \([21]\) become explicit. Since the statements between an up- and a downshift are executed while the process is linear, they are guaranteed to be executed without interference.

We illustrate atomicity on the example of printing to standard out from a concurrent program. To make sure that the print statements will be issued to standard out in the order that they appear in a given thread, we represent the standard output stream by a shared process that obeys the mutually recursive session types \( \text{s\_stdout} \) and \( \text{l\_stdout} \) in Figure 8. The protocol defined by those session types requires a client to acquire standard out before being able to print to it and then to release it upon completion. The processes \( p \) and \( v \) implement the session types \( \text{s\_stdout} \) and \( \text{l\_stdout} \), respectively. We have chosen their names in reminiscence of Dijkstra’s semaphore operations \( \text{P} \) and \( \text{V} \). The lines of code below demonstrate how a client interacts with atomic standard out for printing, assuming the channel \( \text{out} \) of type \( \text{s\_stdout} \) to be available as a system service:

\[
\begin{align*}
\text{out’} &\leftarrow \text{acquire out} ; \text{out’}\_\text{enter} ; \\
\text{out’}\_\text{print} &\leftarrow \text{send out’ “Hello”} ; \\
\text{out’}\_\text{print} &\leftarrow \text{send out’ “happy”} ; \\
\text{out’}\_\text{print} &\leftarrow \text{send out’ “world!”} ; \\
\text{out’}\_\text{leave} &\leftarrow \text{out} \leftarrow \text{release out’} ;
\end{align*}
\]

In session type \( \text{l\_stdout} \), we take the liberty to use the connective \( \triangleright \), a connective introduced in \([26, 58]\) to support value input. The type “\( \text{string} \triangleright \text{l\_stdout} \)” describes as session that receives a value of type \( \text{string} \) and then continues as a session of type \( \text{l\_stdout} \). Toninho et al. \([58]\) show how to safely integrate a functional layer with a process layer.
Figure 8: Atomic standard output. The connective \( \triangleright \) denotes value input, an orthogonal concept introduced in [26, 58].

by means of a linear contextual monad. Those results are orthogonal to sharing and generalize to our language. The statement \( \textit{print} \) in process \( v \), lastly, abstracts the actual print primitive on a given platform. To prevent races on this primitive, processes \( p \) and \( v \) are internal, and the only way for users to interact with standard out is via the system service \( \textit{out} \).

4.3 Nondeterminism

Acquire-release introduces \textit{nondeterminism} into our language because it is unknown which client among several clients that acquire a shared process will succeed. We use this property to implement binary nondeterministic choice in our language.

Figure 9 gives the definition of session type \textit{coin} and its implementing, mutually recursive processes \textit{coin\_head} and \textit{coin\_tail}. Session type \textit{coin} indicates which side of the coin is currently facing up. In the implementation each interaction flips the coin to its opposite side.

![Figure 9: Session type coin with implementing processes coin\_head and coin\_tail.](image)

Figure 10 shows the process \textit{nd\_choice} which nondeterministically sends \textit{yes} or \textit{no} and then terminates. Process \textit{nd\_choice} achieves nondeterminism by reading a coin that it shares with process \textit{coin\_flipper}. Since both processes try to acquire the coin concurrently and the coin switches sides when read, the value read by \textit{nd\_choice} depends on the order in which the coin is acquired. For a client of this service, see Figure 11 where it is used to model nondeterminism inherent in the (untyped) asynchronous \( \pi \)-calculus.

5 Semantics

In this section, we complete the discussion of the semantics of \textsc{SILL}$_5$, by giving the configuration typing rules as well as elaborating on preservation and progress. A complete listing of \textsc{SILL}$_5$’s abstract syntax, statics, and dynamics as well as proofs of preservation and progress can be found in the appendix. In the last subsection, we sketch an asynchronous dynamics for \textsc{SILL}$_5$, which relies on a novel transformation derived from logic.
\[\text{nd_choice} : \{\oplus\{\text{yes} : 1, \text{no} : 1\}\}\]
\[d \leftarrow \text{nd_choice} = \]
\[\begin{align*}
& c \leftarrow \text{coin.head} ; \\
& f \leftarrow \text{coin.flipper} \leftarrow c ; \\
& c' \leftarrow \text{acquire} c ; \\
& \text{case} c' \text{ of} \\
& \quad | \text{head} \rightarrow c \leftarrow \text{release} c' ; d \text{yes} ; \text{wait} f ; \text{close} d \\
& \quad | \text{tail} \rightarrow c \leftarrow \text{release} c' ; d \text{no} ; \text{wait} f ; \text{close} d
\end{align*}\]

\[\text{coin.flipper} : \{1 \leftarrow \text{coin}\}\]
\[d \leftarrow \text{coin.flipper} \leftarrow e = \]
\[\begin{align*}
& c' \leftarrow \text{acquire} c ; \\
& \text{case} c' \text{ of} \\
& \quad | \text{head} \rightarrow c \leftarrow \text{release} c' ; \text{close} d \\
& \quad | \text{tail} \rightarrow c \leftarrow \text{release} c' ; \text{close} d
\end{align*}\]

Figure 10: Binary nondeterministic choice.

5.1 Configuration Typing

At run-time, a SILL\textsubscript{S} program evolves into a number of linear and shared processes as well as placeholders for formerly shared processes that are currently linear. To type the resulting configuration \(\Omega\), we divide the configuration into a linear part \(\Theta\) and a shared part \(\Lambda\), subject to the following well-formedness conditions:

\[\begin{align*}
\Omega & \triangleq \cdot | \Lambda; \Theta \\
\Lambda & \triangleq | \text{proc}(a, P_{a_k}), \Lambda' | \text{unavail}(a), \Lambda' \\
\Theta & \triangleq | \text{proc}(a, P_{a_k}), \Theta'
\end{align*}\]

\((\forall a. \text{proc}(a, \_)) \in \Theta \implies \text{unavail}(a) \in \Lambda)\\n(\text{proc}(a, \_), \text{unavail}(a) \text{ not in } \Lambda')\\n(\text{proc}(a, \_) \text{ not in } \Theta')

The side conditions make sure that no other process (or placeholder) exists yet in the configuration that provides along the same channel and that for every linear process there exists a placeholder along the shared mode of the channel. The division is justified by the hierarchy between mode \(S\) and \(L\), making sure that shared processes cannot depend on linear processes. We use the following typing judgment to type a configuration:

\[\Gamma \vdash_{\Sigma} \Lambda; \Theta :: \Gamma; \Delta\]

The judgment expresses that the configuration \(\Lambda; \Theta\) provides the shared channels in \(\Gamma\) and the linear channels in \(\Delta\). To permit cyclic dependencies along shared channels, a configuration is type-checked relative to all shared channels, which is the reason why \(\Gamma\) appears to the left of the turnstile. The typing of a configuration is defined by the following rule:

\[\begin{align*}
\frac{
\Gamma \vdash_{\Sigma} \Lambda :: \Gamma \\
\Gamma \vdash_{\Sigma} \Theta :: \Delta
}{
\Gamma \vdash_{\Sigma} \Lambda; \Theta :: \Gamma; \Delta}
\end{align*}\]

\((T-\Omega)\)

The rule relies on the judgment \(\Gamma \vdash_{\Sigma} \Theta :: \Delta\) for typing \(\Theta\) and the judgment \(\Gamma \vdash_{\Sigma} \Lambda :: \Gamma\) for typing \(\Lambda\). The judgment \(\Gamma \vdash_{\Sigma} \Theta :: \Delta\) expresses that the configuration \(\Theta\) provides the linear channels in \(\Delta\), using the shared channels in \(\Gamma\).

The typing of \(\Theta\) is defined by the following two rules:

\[\begin{align*}
\frac{
\Gamma \vdash_{\Sigma} (\cdot) :: (\cdot) \\
\Gamma \vdash_{\Sigma} (\text{proc}(a, P_{a_k}), \Theta :: (\Delta, a_k : A_k))
}{
\Gamma \vdash_{\Sigma} (\text{proc}(a, P_{a_k}), \Theta :: (\Delta, a_k : A_k))
}
\end{align*}\]

\((T-\Theta_1)\)

\[\begin{align*}
\frac{
\Gamma \vdash_{\Sigma} (A_k, \hat{B}) \text{ sync} \\
\Gamma; \Delta' \vdash_{\Sigma} P_{a_k} :: (a_k : A_k) \\
\Gamma \vdash_{\Sigma} \Theta :: \Delta, \Delta'
}{
\Gamma \vdash_{\Sigma} (\text{proc}(a, P_{a_k}), \Theta :: (\Delta, a_k : A_k))
}
\end{align*}\]

\((T-\Theta_2)\)

Rule \((T-\Theta_2)\) is of particular interest as it imposes an order on linear configurations. By requiring that all the linear channels \(\Delta'\) used by \(\text{proc}(a, P_{a_k})\) are provided by the remaining configuration \(\Theta\), the rule “flattens” the linear process tree such that for any process the providers of the channels used by the process are to the right of the process in the configuration. We maintain this order only for typing purposes, at run-time any permutations of a well-typed configuration are permissible. The rule also enforces that a linear configuration only provides the channels that are not used internally to the configuration. For example, the channels \(\Delta'\) consumed by \(\text{proc}(a, P_{a_k})\) are no longer provided as part of the resulting configuration \(\text{proc}(a, P_{a_k}), \Theta\). An initial configuration \(\Lambda; \Theta\) would be typed as \(\Gamma \vdash_{\Sigma} \Lambda; \Theta :: (\Gamma; a_1 : 1)\), where the process providing along channel \(a_1\) is the main program thread and \(\Lambda\) may provide some pre-defined shared system services such a out as in Section 4.2. The premises \((a_5 : \hat{B}) \in \Gamma\) and \(\vdash_{\Sigma} (A_k, \hat{B}) \text{ sync}\) of rule \((T-\Theta_2)\), constrain the type to which \(\text{proc}(a, P_{a_k})\) must be released to.
Unlike the typing rules for $\Theta$, the typing rules for $\Lambda$ do not impose any order on the shared processes. Any attempt would be futile anyway because the reference structure along shared channels may not adhere to any pattern and could, for example, be cyclic. We use the judgment $\Gamma \vdash_\Sigma \Lambda :: \Gamma'$ to type such configurations, expressing that $\Lambda$ offers the shared channels in $\Gamma'$, using the shared channels in $\Gamma$. The typing rules for $\Lambda$ are:

\[
\begin{align*}
\text{(T-\Lambda_1)} \\
\Gamma \vdash_\Sigma (\cdot) :: (\cdot) \quad &\quad \Gamma \vdash_\Sigma (\Sigma^\top \Lambda, \top) \text{ esync} \quad \Gamma \vdash_\Sigma (P_{a_5} :: (a_5 : \Sigma^\top \Lambda)) \\
\text{(T-\Lambda_2)} \\
\Gamma \vdash_\Sigma \text{ proc}(a_5, P_{a_5}) :: (a_5 : \Sigma^\top \Lambda) \\
\Gamma \vdash_\Sigma \Lambda :: \Gamma' \quad \Gamma \vdash_\Sigma \Lambda' :: \Gamma'' \\
\text{(T-\Lambda_4)} \\
\Gamma \vdash_\Sigma \text{ unavail}(a_5) :: (a_5 : \top)
\end{align*}
\]

Rule (T-\Lambda_4) permits breaking up a configuration $\Lambda$ into its subparts at any point. Rule (T-\Lambda_2) carries again an equi-synchronizing invariant as a premise, indicating that the type to which $\text{proc}(a_5, P_{a_5})$ must be released is not yet significant.

### 5.2 Preservation and Progress

In this section, we state preservation and progress for $\text{SILL}_S$ and review the key issues that had to be adressed to prove preservation and progress. The proofs of preservation and progress can be found in Section 1.

The challenges that arise from extending the linear system discussed in Section 2 with manifest sharing are twofold. For preservation, we need to make sure that clients will encounter shared processes at the type they would like to acquire them. For progress, we need to account for the possibility of deadlock due to cyclic dependencies along shared channels or termination of a process providing a shared service, while ruling out other forms of failure of progress.

To address the first challenge, we have introduced the notion of an equi-synchronizing session type in Section 3.3, which statically imposes the invariant that each shared channel is released to the same session type at which it was acquired (if at all). The preservation proof shows that this invariant is maintained for each channel along any possible transition, as captured in the corresponding premises of rules (T-\Theta_2) and (T-\Lambda_2). Key are the three form of type constraints $\bar{D}$ with $\vdash_\Sigma (A, \bar{D}) \text{ esync}$ where $A$ is the current type of a linear process providing along $a_i$:

1. $\bar{D} = \top$, indicating that there is no constraint on a future release of $a_i$ because $a_i$ has never been shared. $\bar{D} = \top$ holds initially, when a linear process is spawned, and continues to hold until the process is released for the first time to become shared. Processes which remain linear throughout their lifetime will never be subject to an equi-synchronizing constraint.

2. $\bar{D} = D_s$, indicating that if there is a future release of $a_i$ to a shared channel $a_s$, then $a_s$ must have type $D_s$. Preservation holds since we have statically checked that $\vdash_\Sigma (A, \bar{D}) \text{ esync}$ and this property is maintained along all continuations of $A$.

3. $\bar{D} = \bot$, expressing that $a_s$ must never be released, which means that any client attempting to acquire $a_s$ will be blocked forever. The need for $\bot$ is subtle. Imagine we forward between two linear channels $\text{fwd} a_i b_i$. The forward has to identify not only $a_i$ and $b_i$, but also the underlying shared channels $a_s$ and $b_s$, because releasing one now amounts to releasing the other:

\[
\text{proc}(a_i, \text{fwd} a_i b_i) \rightarrow a_i = b_i, a_s = b_s
\]

### D-ID$_k$

While the types of $a_i$ and $b_i$ must be at the same $A$, it is possible that the constraints on the releases of $a_i$ and $b_i$ are $\vdash (A, D_s) \text{ esync}$ and $\vdash (A, D'_s) \text{ esync}$ for $D_s \neq D'_s$. This can arise because $a_i$ and $b_i$ may have different histories. Preservation still holds in this case because there can not be a down shift in any continuation of $A$ (shown by coinduction on the definition of esync), so neither $a_i$ nor $b_i$ could ever be released. Formally, this is conveniently expressed as $\vdash_\Sigma (A, \bot) \text{ esync}$.

The introduction of $\bot$ requires us to generalize all the typing rules where a process uses a shared channel. For example, we change rule (T-\Lambda^{\top}_1) as follows:

\[
\begin{align*}
\bar{B} &\leq \Sigma^\top \Lambda \\
\Gamma, x_5 : \bar{B}; \Delta, x_1 : A_1 \vdash_\Sigma Q_{a_5} :: (z_1 : C_1)
\end{align*}
\]

\[
\text{(T-\Lambda^{\top}_4)}
\]

\[
\Gamma, x_5 : \bar{B}; \Delta \vdash_\Sigma \text{ acquire} x_5; Q_{a_5} :: (z_1 : C_1)
\]
In contrast to the rule introduced in Section 3.2, the above rule accounts for the possibility of a shared process to be of type \( \bot \). In this case, a client can freely choose the type of the process to be acquired because it will never succeed in acquiring that process. As can be seen in Figure 3, the rules (T-\text{ID}_S), (T-\text{SPAWN}_LL), (T-\text{SPAWN}_LS), (T-\text{SPAWN}_{SS}), (T-\exists_R), and (T-\Pi_L) require an analogous treatment.

We can finally state the preservation theorem. It expresses that the types of the providing linear channels are maintained along transitions and that new shared channels may be allocated.

**Theorem 1** (Preservation). If \( \Gamma \models \Sigma; \Lambda; \Theta :: \Gamma; \Delta \), then \( \Gamma' \models \Sigma; \Lambda'; \Theta' :: \Gamma'; \Delta \), for some \( \Lambda', \Theta' \), and \( \Gamma' \).

**Proof.** Preservation is proved by induction on the dynamics, constructing a derivation of a well-typed configuration \( \Gamma' \models \Sigma; \Lambda''; \Theta'' :: \Gamma'; \Delta \), where \( \Lambda'' \) and \( \Theta'' \) are permutations of \( \Lambda' \) and \( \Theta' \), respectively, and using a variety of substitution lemmas and inversion. Note that the linear context \( \Delta \) remains the same: freshly spawned linear channels have both a provider and client and are therefore not part of the interface. The set of shared channels however can grow.

Our progress theorem is based on the notion of a poised process introduced in [49]. A proc\((a, P_a)\) is poised if it is communicating along its providing channel. The poised forms of processes in \( \text{SILL}_S \) are:

**Receiving**

\[
\begin{align*}
\text{proc}(a_y, y \leftarrow \text{recv } a_i; P_y) & \quad \text{proc}(a_x, \text{close } a_i) \\
\text{proc}(a_i, \text{case } a_i \text{ of } l \Rightarrow P) & \quad \text{proc}(a_i, a_i; P) \\
\text{proc}(a_i, x_i \leftarrow \text{accept } a_i; P_{x_i}) & \quad \text{proc}(a_i, x_i \leftarrow \text{detach } a_i; P_{x_i})
\end{align*}
\]

**Sending**

\[
\begin{align*}
\text{proc}(a_y, \text{send } a_y; P) & \\
\text{proc}(a_i, a_i.l_i; P) & \\
\text{proc}(a_x, x_i \leftarrow \text{recv } a_i; P_{x_i}) & \\
\text{proc}(a_x, x_i \leftarrow \text{detach } a_i; P_{x_i}) & \\
\end{align*}
\]

A linear configuration \( \Theta \) is poised if all proc\((a_i, P_{a_i}) \in \Theta \) are poised and a shared configuration \( \Lambda \) is poised if all proc\((a_i, P_{a_i}) \in \Lambda \) are poised.

To account for the possibility of deadlock, we introduce the notion of a blocked process. We say that a process is blocked along \( a_i \) if it has the form proc\((a_i, x_i \leftarrow \text{acquire } a_i; Q_{a_i})\). We then state the progress theorem such as to express that being blocked is the only way the whole configuration may be stuck [27]. Case (2-c) captures the scenario where a blocked process cannot proceed because the shared channel is unavailable. A successful acquire, on the other hand, is represented as part of case (2-a).

**Theorem 2** (Progress). If \( \Gamma \models \Sigma; \Lambda; \Theta :: \Gamma; \Delta \), then either

1. \( \Lambda \rightarrow \Lambda' \), for some \( \Lambda' \), or
2. \( \Lambda \) is poised and
   (a) \( \Lambda; \Theta \rightarrow \Lambda'; \Theta' \), for some \( \Lambda' \) and \( \Theta' \), or
   (b) \( \Theta \) is poised, or
   (c) some process in \( \Theta \) is blocked along \( a_i \) and unavail\((a_i) \in \Lambda \).

**Proof.** Progress is proved by induction on the typing of the configurations \( \Lambda \) and \( \Theta \).

At the top level, we have \( \Delta = (c_0 : 1) \), which means that if \( \Theta \) is poised then it and all subcomputations must be finished, trying to close \( c_0 \). If it cannot transition, then the remaining possibility is that some process in \( \Theta \) is blocked along a shared channel. A blocked process may wait indefinitely in case of a deadlock, or because the underlying shared process has terminated, or may never be released. Dining philosophers (Figure 7), for instance, is an example leading to a classic deadlock due to a cyclic dependency along the shared forks. Section E.2 gives another example.

### 5.3 Asynchronous Dynamics

The synchronous operational semantics we have provided for \( \text{SILL}_S \) is simple, but not realistic in many applications. Fortunately, we can easily model asynchronous output in the existing language in a logically meaningful way. In
order to explain this, we reintroduce the general form of cut (spawn) which is not tied to process definitions, and remind the reader of the identity (forward) rule. For simplicity, we restrict the presentation to the linear case; the shown technique directly generalizes to the shared case.

\[
\frac{\Delta \vdash P_x : (x : A)}{\Delta', x : A \vdash Q_x : (z : C)} \quad (\text{T-Cut})
\]

\[
\Delta, \Delta' \vdash x \sslash P_x; Q_x : (z : C)
\]

\[
y : A \vdash \text{fwd } x \ y : (x : A)
\]

To asynchronously send a channel \(y\) along \(x\) we spawn a new process which carries the message \(y\), immediately followed by forwarding.

\[
\text{send } x \ y : P \quad \approx \quad x' \leftarrow (\text{send } x \ y : \text{fwd } x' \ x) ; [x'/x]P
\]

Intuitively, the spawned process \((\text{send } x \ y : \text{fwd } x' \ x)\) represents the message \(y\) sent along \(x\) with fresh continuation channel \(x'\). The continuation channel is necessary so that multiple messages sent along the same channel are guaranteed to arrive in the correct order. It is easy to see that, if the synchronous form on the left is well-typed, then so is the asynchronous form on the right. Logically, we can obtain the proof of the left from the proof of the right by a commuting conversion and reduction of cut with identity.

Operationally, the single synchronous reduction

\[
\text{proc}(c, \text{send } a \ b ; P), \text{proc}(a, y \leftarrow \text{recv } a : Q_y)
\]

\[
\rightarrow \text{proc}(c, P), \text{proc}(a, [b/y]Q_y)
\]

is now decomposed into several steps, where \(P\) can proceed with its continuation before \(b\) is received.

\[
\text{proc}(c, x' \leftarrow (\text{send } a \ b : \text{fwd } x' \ a) ; [x'/a]P), \text{proc}(a, y \leftarrow \text{recv } a : Q_y)
\]

\[
\rightarrow \text{proc}(c, [a'/a]P), \text{proc}(a', \text{send } a \ b : \text{fwd } a' \ a), \text{proc}(a, y \leftarrow \text{recv } a : Q_y) \quad (\text{spawn, } a' \text{ fresh})
\]

\[
\rightarrow \text{proc}(c, [a'/a]P), \text{proc}(a', \text{fwd } a' \ a), \text{proc}(a, [b/y]Q_y) \quad (\text{receive})
\]

\[
\rightarrow \text{proc}(c, [a'/a]P), \text{proc}(a', [a'/a][b/y]Q_y) \quad (\text{forward})
\]

Since \(a'\) is chosen globally fresh and \(a\) is linear, the result is an \(\alpha\)-variant of the synchronous outcome. This technique can be applied to all send operations of the semantics. Effectively, this allows a program written in the synchronous style to be executed fully asynchronously.

The caveat is that we would not want to translate acquire in this manner even though the logical semantics dictates it must be a send operation \(^{11}\). The reason is that a process would no longer block when trying to acquire a shared channel. Instead it would continue until the corresponding linear channel is actually used to receive a message, which is not the intended meaning. In the implementation (see Section \(^7\)) all sends are asynchronous, using a more efficient message buffer instead of explicit continuation channels, except for acquire which blocks until the shared channel becomes available.

Alternatively, we could directly provide an asynchronous semantics for all the operations and use an additional acknowledgment step (a “double shift” \(^{11}\)) to ensure that acquiring a shared resource is synchronous. For this paper, we have chosen the former route because it simplifies the operational semantics and therefore our theorems: without loss of expressiveness, we do not have to explicitly deal with messages or message queues.

### 6 Recovering the Computational Power of the Untyped \(\pi\)-calculus

When we view Howard’s original isomorphism between typed \(\lambda\)-calculus and intuitionistic natural deduction \(^{32}\) as a type assignment system for untyped \(\lambda\)-terms, we lose much of the computational power of the untyped \(\lambda\)-calculus. For example, normalization for natural deduction implies termination of computation on well-typed \(\lambda\)-terms, while arbitrary \(\lambda\)-terms may not have a normal form. However, there is a simple way we can embed all untyped \(\lambda\)-terms if we add recursive types. In linear instances of the Curry-Howard correspondence, just adding recursion appears insufficient to recover the computational power of the asynchronous \(\pi\)-calculus \(^{62}\), and so far there has been no logically motivated and fully satisfactory way to do so.\(^4\)

\(^4\)Other recent work in this direction in the setting of classical linear logic by Atkey et al. \(^2\) uses quite different techniques from ours.
In this section, we give an encoding of the asynchronous, untyped \(\pi\)-calculus into SILL\(_5\), demonstrating that shared channels recover the computational power of the untyped \(\pi\)-calculus. The key points to address in the encoding are that (i) \(\pi\)-calculus channels may connect arbitrarily many processes, (ii) messages sent along a \(\pi\)-calculus channel may arrive in arbitrary order, and (iii) \(\pi\)-calculus channels are untyped. Furthermore, since the \(\pi\)-calculus permits deadlock, it is important here that SILL\(_5\) also admits deadlock.

The basic idea of our encoding is to translate \(\pi\)-calculus processes to linear SILL\(_5\) processes of type 1, and \(\pi\)-calculus channels to shared SILL\(_5\) processes of a universal shared type \(\mathcal{U}_d\). The latter are unordered buffers and obey the following protocol:

\[
\mathcal{U}_d = \frac{\text{ins} : \Pi \mathcal{U}_d, \downarrow^s \mathcal{U}_d,}{\downarrow^s (\mathcal{U}_d)} \cup \{\text{del} : \oplus (\text{none} : \downarrow^s \mathcal{U}_d), \text{some} : \exists \mathcal{U}_d, \downarrow^s \mathcal{U}_d\}
\]

Type \(\mathcal{U}_d\) provides the choice to either send (\text{ins}) or receive (\text{del}) a channel. In the latter case, it communicates whether the buffer is empty (\text{none}) or not empty (\text{some}) and delivers a channel in the buffer in the latter case. Figure 11 shows the processes \text{empty} and \text{elem} that implement session type \(\mathcal{U}_d\). To guarantee that the resulting buffer is unordered, process \text{elem} nondeterministically inserts the received channel at an arbitrary point in the buffer, using \text{nd}._\text{choice} defined in Figure 10. It is also possible and slightly more complicated to postpone the nondeterministic choice to the deletion operation.

\begin{align*}
\text{empty} : \{\mathcal{U}_d\} & \quad \text{elem} : \{\mathcal{U}_d \leftarrow \mathcal{U}_d, \mathcal{U}_d\} \\
\text{c} & \leftarrow \text{empty} = \\
\text{case } \text{c} \text{ of} & \\
\mid \text{ins} \rightarrow x & \leftarrow \text{recv } \text{c} \; ; \\
\quad \text{e} & \leftarrow \text{empty} ; \\
\quad \text{c} & \leftarrow \text{detach } \text{c} ; \text{c} \leftarrow \text{elem} \leftarrow x, e \\
\mid \text{del} \rightarrow \text{c}.\text{none} ; & \\
\quad \text{c} & \leftarrow \text{detach } \text{c} ; \text{c} \leftarrow \text{empty} \\
\end{align*}

Figure 11: Processes \text{empty} and \text{elem} implement session type \(\mathcal{U}_d\), representing a \(\pi\)-calculus channel. To guarantee that the resulting buffer is unordered, process \text{elem} nondeterministically inserts the received channel at an arbitrary point in the buffer, using process \text{nd}._\text{choice} defined in Figure 10

The linear SILL\(_5\) processes representing \(\pi\)-calculus processes now simply amount to “producers” and “consumers” of shared channels of type \(\mathcal{U}_d\). Any number of such processes can communicate along a \(\pi\)-calculus channel by acquiring the shared SILL\(_5\) channel of universal type.

We are now ready to give the encoding of processes. We first review the syntax of the asynchronous monadic \(\pi\)-calculus \cite{154,52}, defining the set \(P^\pi\) of \(\pi\)-calculus process terms. We follow the presentation in \cite{13}:

\[
P \overset{\Delta}{=} 0 \mid \tau(y) \mid x(y).P \mid \nu x P \mid P_1 \mid P_2 \mid !P
\]

0 denotes an inactive process. \(\tau(y)\) represents an asynchronous send of \(y\) along channel \(x\). \(x(y).P\) represents the receiving of a channel along channel \(x\), after which the process continues with executing \(P\) with the received channel bound to \(y\) in \(P\). The action prefix \(x(y)\) acts as a guard, making sure that \(P\) can only become active once the
input has occurred. \( \nu x \, P \) introduces a new channel \( x \) that is bound in \( P \). \( P_1 \mid P_2 \) denotes parallel composition of \( P_1 \) and \( P_2 \) and \( !P \) replication of \( P \).

Our translation shown in Figure 12 yields for each \( \pi \)-calculus process term \( P^\pi \) a corresponding linear process \( \llbracket P^\pi \rrbracket_a \) in SILL\(_S\), satisfying the typing judgment

\[
\Gamma; \mid \Sigma \vdash \llbracket P^\pi \rrbracket_a :: (a_1 : 1)
\]

where \( \Gamma \) consists of declarations \( x_a : \mathcal{U}_a \) for every shared channel in the overall process configuration. We use type \( 1 \) since all communication goes through \( \pi \)-calculus channels, which are mapped to shared channels in \( \Gamma \). This is also the reason why there are no linear channels in the context. Of course, as shared channels are acquired when send or receive operations are modeled, we communicate with the buffer along a linear channel until it is released again.

\[
\begin{align*}
\llbracket 0 \rrbracket_a &= \text{close } a & \text{snd} : \{ (\Pi \mathcal{U}_a, 1) \leftarrow \mathcal{U}_a \} \\
\llbracket x \rrbracket_a &= p \leftarrow \text{snd } c ; \\
& \quad \text{send } p \, b ; \\
& \quad \text{wait } p ; \\
& \quad \text{close } a & \text{d} \leftarrow \text{snd } c = \text{x} \leftarrow \text{recv } d ; \\
& \quad \text{c} \leftarrow \text{acquire } c ; \\
& \quad \text{c}.\text{ins} ; \\
& \quad \text{send } c'.x ; \\
& \quad \text{c} \leftarrow \text{release } c' ; \\
& \quad \text{close } d
\end{align*}
\]

\[
\begin{align*}
\llbracket \pi (b) \rrbracket_a &= p \leftarrow \text{poll } \text{recv } c \leftarrow c ; \\
& \quad \text{b} \leftarrow \text{recv } p ; \\
& \quad \text{wait } p ; \\
& \quad a \leftarrow [b/x] \llbracket P \rrbracket_a \quad \text{poll}_\text{recv} : \{ ([\mathcal{U}_a, 1] \leftarrow \mathcal{U}_a) \} \\
\llbracket c(x).P \rrbracket_a &= p \leftarrow \text{poll } \text{recv } c \leftarrow c ; \\
& \quad \text{b} \leftarrow \text{recv } p ; \\
& \quad \text{wait } p ; \\
& \quad a \leftarrow [b/x] \llbracket P \rrbracket_a \\
\llbracket \nu x \, P \rrbracket_a &= e \leftarrow \text{empty} ; \\
& \quad a \leftarrow [e/x] \llbracket P \rrbracket_a \\
\llbracket P_1 \mid P_2 \rrbracket_a &= b \leftarrow \llbracket P_1 \rrbracket_b ; \\
& \quad c \leftarrow \llbracket P_2 \rrbracket_c ; \\
& \quad \text{wait } b ; \\
& \quad \text{wait } c ; \\
& \quad \text{close } a \quad \text{d} \leftarrow \text{poll}_\text{recv } c \leftarrow c ; \\
& \quad \text{c} \leftarrow \text{release } c' ; \\
& \quad \text{d} \leftarrow \text{poll}_\text{recv } c \leftarrow c ; \\
& \quad \text{c} \leftarrow \text{release } c' ; \\
& \quad \text{d} \leftarrow \text{poll}_\text{recv } c \leftarrow c \leftarrow \text{recv } c' ; \\
& \quad \text{c} \leftarrow \text{release } c' ; \\
& \quad \text{d} \leftarrow \text{poll}_\text{recv } c \leftarrow c
\end{align*}
\]

\[
\llbracket !P \rrbracket_a = \text{Rec}_P^\pi, \quad \text{where} \\
\begin{align*}
\text{Rec}_P^\pi &= b \leftarrow \llbracket P \rrbracket_b ; \\
& \quad c \leftarrow \text{Rec}_P^\pi ; \\
& \quad \text{wait } b ; \\
& \quad \text{wait } c ; \\
& \quad \text{close } a
\end{align*}
\]

\[
\text{empty} : \{ \mathcal{U}_a \} \text{ is defined in Figure 11}
\]

Figure 12: Translation from untyped asynchronous \( \pi \)-calculus processes to SILL\(_S\) and auxiliary processes \( \text{snd} \) and \( \text{poll}_\text{recv} \).

Because of the different semantic basis (asynchronous \( \pi \)-calculus on one hand and multiset rewriting on the other), and the question what precisely is observable about a computation, the precise nature of the correspondence between traces in the source and target is difficult to formulate and prove and left to future work (see Section 9 for further remarks).

## 7 Implementation

We briefly describe our implementation of manifest sharing in the context of a type-safe C-like imperative language with session types called Concurrent C0 [65], which is an extension of C0 [1, 48] designed for and used in an introductory imperative programming course [50]. Because session-typed programming follows a monadic style, this imperative implementation is semantically adequate for exploration of the expressive power and programming style for manifest sharing. We have transliterated all the examples in this papers into Concurrent C0 and they will be made available with the implementation artifact should this submission be accepted. Besides an occasional
illustrative use of imperative language features (e.g., loops in place of recursion, or mutable arrays instead of sequences), the only significant difference is the lack of parametric polymorphism in Concurrent C0. Examples have therefore been modified to use either base types such as int, or ad hoc polymorphism in the form of void* which engenders tagging of values with their dynamic type to ensure type safety. The implementation uses asynchronous message passing, as described in Section 5.3. Moreover, the downshift modality ↓S↓ has no explicit syntax but implicitly precedes every upshift ↑S↑. This is adequate since, just as in this paper, the only constructor of shared mode is an upshift so there is no other possible continuation.

The compiler translates C0 source to C. Each logical thread of control is implemented as an operating system thread as provided by the pthread library. Message passing is implemented via shared memory. Each channel is therefore a data structure in shared memory that can progress through linear and shared phases. Figure 13 provides a schematic overview of this data structure. While linear, access is shared between a provider and a client. The channel contains a current direction of communication and a message queue implemented as a ring buffer whose size is calculated from the session type. Access to the buffer for send and receive operations is protected by a mutex and associated condition variable. In the shared phase, there will be zero or one provider and an arbitrary number of clients. The channel therefore contains a flag that indicates whether the channel is currently available to be acquired. This flag is turned off when the channel is acquired by one of the clients and remains off until the client has been detached and the provider is ready to accept another client. Access to this flag is protected by a separate mutex and condition variable. The operating system scheduler will then nondeterministically select one of the clients.

As might be expected from the theory, the most difficult aspect of the implementation is forwarding. For forwarding between two linear channels, fwd cd, we send a message FWD c along d, or FWD d along c, depending on the current direction of communication. Then the thread executing the forward terminates. When the FWD e message arrives (where e is either c or d, depending on the direction), the recipient changes its internal reference to the shared channel to e, effectively now continuing communication along e. For more details and some failed alternatives, see [65].

Unfortunately, this strategy fails for forwarding between two shared channels, fwd cd, because there is no effective way to notify all clients of c to now communicate along d via a message. Instead, before terminating, the provider installs a forwarding pointer from c to d and marks the availability of c. Attempts to acquire c will follow the forwarding pointer to d. A potential client may have to follow a whole chain of such forwarding pointers. However, each client has to do so at most once.

Returning to a linear forward: when we execute fwd cd for linear channels c and d that where once shared, the semantics requires that we also forward between the underlying shared channels. For example, if the client replaces references to c by references to d and d is eventually released, then subsequent attempts to acquire c should obtain access to d. In order to account for this scenario, we also install the forwarding pointer from c to d upon a linear
forward if the channel has ever been a shared channel with possibly multiple waiting clients.

The current implementation of Concurrent C0 does not deallocate channels that were shared at any point during the program execution. We conjecture that manifest sharing admits an effective reference counting garbage collector by transforming the typing derivation to make implicit applications of weakening and contraction explicit. This is one of the immediately planned items of future work.

8 Related Work

Our work is situated in the family of works on session types [22, 29, 30, 31] among which it extends work based on the Curry-Howard isomorphism between linear logic and session-typed communication [8, 9, 67, 58, 62] with manifest sharing. We have already summarized that work in Section 2 and have pointed out that the shared channels available through the exponential modality in linear logic have a copying semantics and therefore cannot accommodate the examples presented in this paper. Perhaps most closely related is work by Atkey et al. [2] which proceeds by conflating dual pairs of types in classical linear logic, whereas in this paper we maintain the original interpretation of propositions as session types, but provide an alternative operational semantics for a shared layer of channels separated from the linear types by a pair of adjoint modalities.

From the point of view of protocol expression, our work is related to the line of research that uses typestate [56] for protocol checking [5, 15, 20, 40] or program verification [45]. Whereas first approaches [15] support a rather restricted set of aliasing patterns to facilitate modular protocol checking, subsequent approaches lift some of the imposed restrictions, notably by combining aliasing information with type-state [5, 63] or rely-guarantee-based reasoning [40]. Most closely related to our work is Fähndrich’s and DeLine’s work [2002] on adoption and focus for protocol checking in an object-oriented language. In the resulting language, linear and non-linear objects coexist such that every non-linear object (adoptee) has a linear adopter. Aliases are permitted to adoptees, as long as access goes through the adopter and mutating access happens in a temporary scope, called focus. While an aliased object is in focus, access to the object via another alias is disabled by capability tracking. From this aspect, a focus scope bears resemblance to a critical section arising between acquire and release points in our system, even though adoption and focus are employed in a purely sequential setting. Whilst capabilities are treated as resources, the underlying type system is not linear, but the required semantics is achieved by threading the capabilities through program execution.

From the point of view of allowing controlled aliasing in a concurrent setting, our work is related to permission-based logics [6, 28, 39, 54] and concurrent separation logic [7, 36, 46, 59, 60]. Permission-based logics maintain a distinction between read and write access to a shared memory location, allowing read access even if only a fractional permission [6] is held, whereas write access requires the entire permission. From a session type perspective, this distinction is less relevant because any communication, input (write) and output (read) alike, amounts to a change in protocol state and thus must be protected sufficiently. Separation logic shares with linear logic the separating conjunction to reason about resource consumption, but uses a Hoare-style reasoning approach that is extrinsic to the type system, whereas resource-awareness is intrinsic to our type system via the Curry-Howard correspondence. Moreover, both permission-based logics and concurrent separation logic target shared-memory concurrency, whereas our work is situated in the realm of message-passing concurrency, offering a different level of abstraction.

Linear types have also found various applications in systems programming. [Walker and Watkins 2001], for example, combine linear types with regions [23], and Smith et al. relax the operational “use-once” semantics of linear types [61] to exploit pointer aliasing for destructive operations. Similar observations have been made by Castegren and Wrigstad [2016] in the context of implementing lock-free algorithms. Our work differs from these approaches in that it is based on a richer semantics of linearity derived from the Curry-Howard isomorphism between linear logic and session-typed communication. Moreover, our work employs a message-passing approach to concurrency rather than a shared-memory-based approach. From this perspective, our work has closer ties with the Rust systems programming language [42], which supports message-passing concurrency in an affine setting. Shared data in Rust is normally immutable, but Rust also supports various abstractions (e.g., mutexes) that support the safe mutation of shared data. We have found that the programming patterns arising in SILL readily translate into Rust code with mutexes. Rust mutexes, however, are dynamic notions only, and Rust does furthermore not support protocol expression.
9 Discussion and Future Work

We have presented an extension of logic-based session-typed message-passing concurrency by permitting shared resources encapsulated in processes. This allows elegant expression of examples such as queues with multiple producers and multiple consumers, dining philosophers, shared databases, shared input and output devices, or nondeterministic choice. In fact, all of the asynchronous $\pi$-calculus can now be embedded in a statically typed framework satisfying session fidelity by modeling $\pi$-calculus channels as shared processes maintaining a nondeterministic message buffer. We were able to maintain the view of linear propositions as session types, sequent proofs as processes, and linear proof reduction as communication. To accommodate shared processes, we had to generalize the usual Curry-Howard correspondence and allow interleaved proof construction (acquire), proof reduction (communication), and proof deconstruction (release). Proof construction may fail, which manifests operationally as deadlock. Key insights are the decomposition of the exponential modality $!A$ into $\downarrow S^L_1 A \uparrow S^L_1$ inspired by adjoint logic and the insistence on equi-synchronizing types which guarantees that a shared process is always released at the same type it was acquired. The former makes sharing manifest in the type; the latter guarantees session fidelity without runtime checking of types.

On the theory side, we plan to consider how to overlay a likely very different type system or static analysis in order to recover absence of deadlocks. Some recent promising work in this direction \cite{37, 38} in a different context may be adaptable to our situation. We are also interested in relaxing the restriction on equi-synchronization. A first avenue to pursue is to extend our definitions to support subtyping, along the lines of Gay and Hole \cite{22}. Another possibility is to complement the static approach with run-time type-checking to maintain session fidelity \cite{35}, particularly in a distributed setting. On the implementation side, we would like to develop the proof-theoretic foundation of a reference counting implementation so that resources associated with shared processes that are no longer accessible can be released.

Finally, the embedding of the asynchronous $\pi$-calculus into SILL$_S$ raises the interesting question of how precise the modeling is. While we can easily relate computation traces, other traditional notions of concurrency theory such as bisimulation do not immediately apply since our semantics is given as a multiset rewriting system. We conjecture that a slightly modified interpretation with late application of nondeterministic choice describes a bisimulation, according to the definitions mapped out by Deng et al. \cite{2016}.
## A Abstract Syntax

Table 3 defines the abstract syntax of SILL. As is usual, we use the overline-notation to denote a sequence. For example, $\oplus \{ l : A_l \}$ stands for $\oplus \{ l_1 : A_{l_1}, \ldots, l_n : A_{l_n} \}$. By convention, lines without a left-hand side are separated by $|$ from their preceding line.

<table>
<thead>
<tr>
<th>Sort</th>
<th>Abstract Form</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metavariables</td>
<td>$x_m, y_m, \ldots$</td>
<td>variable (or channel)</td>
</tr>
<tr>
<td></td>
<td>$a_m, b_m, c_m, d_m$</td>
<td>channel</td>
</tr>
<tr>
<td>Modes $m$</td>
<td>$S</td>
<td>L$</td>
</tr>
<tr>
<td>Constraint $A, B, C, D$</td>
<td>$\bot$</td>
<td>no yet detached</td>
</tr>
<tr>
<td></td>
<td>$\pm { l : A_l }$</td>
<td>can no longer be acquired</td>
</tr>
<tr>
<td>Session types $A_m, B_m, C_m, D_m$</td>
<td>$\uparrow S L$</td>
<td>constraint on which type must be released to</td>
</tr>
<tr>
<td></td>
<td>$\pm { l : A_l }$</td>
<td>internal choice, at least one label</td>
</tr>
<tr>
<td></td>
<td>$A_l \bowtie B_l$</td>
<td>external choice, at least one label</td>
</tr>
<tr>
<td></td>
<td>$A_l \rightarrow B_l$</td>
<td>linear channel output</td>
</tr>
<tr>
<td></td>
<td>$\exists A_{l_k} B_{l_k}$</td>
<td>linear channel input</td>
</tr>
<tr>
<td></td>
<td>$\Pi A_{l_k} B_{l_k}$</td>
<td>shared channel output</td>
</tr>
<tr>
<td></td>
<td>$1_L$</td>
<td>shared channel input</td>
</tr>
<tr>
<td></td>
<td>$\downarrow S L$</td>
<td>termination</td>
</tr>
<tr>
<td></td>
<td>$\uparrow S L$</td>
<td>downshift</td>
</tr>
<tr>
<td></td>
<td>$\uparrow Y_m$</td>
<td>upshift</td>
</tr>
<tr>
<td></td>
<td>$\uparrow Y_m$</td>
<td>type variable</td>
</tr>
<tr>
<td>Definition $X_m, Y_m$</td>
<td>$x_m : A_m \leftarrow X_m \leftarrow y:B = P_{x_m,y}$</td>
<td>process definition</td>
</tr>
<tr>
<td></td>
<td>$Y_m = A_m$</td>
<td>recursive session type definition</td>
</tr>
<tr>
<td>Process $P, Q$</td>
<td>$x_i \downarrow ; P$</td>
<td>label output</td>
</tr>
<tr>
<td></td>
<td>$case x_i of l \Rightarrow P$</td>
<td>label input</td>
</tr>
<tr>
<td></td>
<td>$send x_i y_m ; P$</td>
<td>channel output</td>
</tr>
<tr>
<td></td>
<td>$y_m \leftarrow recv x_i ; P_{y_m}$</td>
<td>channel input</td>
</tr>
<tr>
<td></td>
<td>$close x_i$</td>
<td>terminate process</td>
</tr>
<tr>
<td></td>
<td>$wait x_i ; Q$</td>
<td>wait for process to terminate</td>
</tr>
<tr>
<td></td>
<td>$fwd x_m y_m$</td>
<td>forward $x$ to $y$</td>
</tr>
<tr>
<td></td>
<td>$x_m \leftarrow X_m \leftarrow y:B = Q_{x_m}$</td>
<td>spawn</td>
</tr>
<tr>
<td></td>
<td>$x_5 \leftarrow detach x_i ; P_{x_5}$</td>
<td>detach (i.e., shift for $\uparrow^1 ! R$)</td>
</tr>
<tr>
<td></td>
<td>$x_5 \leftarrow release x_i ; Q_{x_5}$</td>
<td>release (i.e., shift for $\downarrow^1 ! R$)</td>
</tr>
<tr>
<td></td>
<td>$x_i \leftarrow acquire x_5 ; Q_{x_5}$</td>
<td>acquire (i.e., shift for $\uparrow^1 ! L$)</td>
</tr>
<tr>
<td></td>
<td>$x_i \leftarrow accept x_5 ; P_{x_5}$</td>
<td>accept (i.e., shift for $\downarrow^1 ! L$)</td>
</tr>
</tbody>
</table>

Table 3: Abstract syntax.

## B Statics

### B.1 Signature Checking

A well-formed signature $\Sigma$ consists of a finite set of process definitions and recursive session type definitions. A process definition $x_m : A_m \leftarrow X_m \leftarrow y:B = P_{x_m,y}$ associates a name $X$ with a process term $P$ and indicates the name and type of the process’ providing channel and the names and types of its argument channels. A recursive session type definition $Y_m = A_m$ associates a name $Y$ with a type term $A$:

$$
\Sigma \triangleq \ldots
\begin{align*}
  &x_m : A_m \leftarrow X_m \leftarrow y:B = P_{x_m,y}, \Sigma' \quad (X_m \text{ not in } \Sigma') \\
  &Y_m = A_m, \Sigma' \quad (Y_m \text{ not in } \Sigma')
\end{align*}
$$
We assume that the signature $\Sigma$ is populated prior to type-checking. Each process definition $x_m : A_m \leftarrow X_m \leftarrow y : B = P_{x_m,y}$ gives rise to a corresponding persistent predicate $\text{def}(x_m : A_m \leftarrow X_m \leftarrow y : B = P_{x_m,y})$ with variables $x_m$ and $y$ bound by $P$ that are subject to $\alpha$-variance to guarantee freshness. We use the subscript notation to separate the linear $\underline{m}$ from the shared $\overline{m}$ part of the arguments $\overline{y}$.

The rules for type-checking the signature are given in Figure 14, Figure 15, and Figure 16. For recursive session types, we adopt the *equi-recursive* interpretation developed by Gay and Hole 2005, requiring recursive session types to be *contractive*. This requirement is stipulated in rule $(T-\Sigma_3)$ and defined by the rules shown in Figure 15. Moreover, we require session types to be *equi-synchronizing*, a property we introduce in this paper (see Section 3.3) to guarantee that a process is *released* to the *same* type at which it was *acquired*. The property of equi-synchronizing establishes session fidelity without the need for run-time checks at acquisition points.

\[
\begin{align*}
\Gamma \vdash \Sigma (\cdot) \text{ sig} \\
\frac{\text{refl}}{\vdash \Sigma (x_m : A_m) \text{ esync}} \quad \frac{\vdash \Sigma (A_m, \Gamma) \text{ esync}}{\vdash \Sigma \Sigma' \text{ sig} (T-\Sigma_2)} \\
\frac{\vdash \Sigma \text{ contr} A_m \quad \vdash \Sigma (A_m, \Gamma) \text{ esync}}{\vdash \Sigma \Sigma' \text{ sig} (T-\Sigma_3)}
\end{align*}
\]

Figure 14: Signature checking.

\[
\begin{align*}
\frac{\vdash \Sigma \text{ contr} \{T : A_i\}}{\vdash \Sigma \text{ contr} \{T : A_i\}} \quad \frac{\vdash \Sigma \text{ contr} \{T : A_i\}}{\vdash \Sigma \text{ contr} \{T : A_i\}} \\
\frac{\vdash \Sigma \text{ contr} A_i \rightarrow B_i}{\vdash \Sigma \text{ contr} A_i \rightarrow B_i} \quad \frac{\vdash \Sigma \text{ contr} \exists A_i B_i}{\vdash \Sigma \text{ contr} \exists A_i B_i} \\
\frac{\vdash \Sigma \text{ contr} \Pi A_i B_i}{\vdash \Sigma \text{ contr} \Pi A_i B_i} \quad \frac{\vdash \Sigma \text{ contr} \Delta_i A_r}{\vdash \Sigma \text{ contr} \Delta_i A_r} \\
\frac{\vdash \Sigma \text{ contr} \Delta_i A_m}{\vdash \Sigma \text{ contr} \Delta_i A_m}
\end{align*}
\]

Figure 15: Contractive recursive session type.

### B.2 Process Typing

To type *process terms*, we use the judgments:

\[
\Gamma \vdash \Sigma P :: (x_s : A_i)
\]

\[
\Gamma ; \Delta \vdash \Sigma P :: (x_s : A_i)
\]

The judgments rely on the signature $\Sigma$ and on the contexts $\Gamma$ and $\Delta$ to type shared and linear channels, respectively. The judgment indicates that the process $P$ provides a service of session type $A_m$ along channel $x_m$, given the typing of services provided by processes along the channels in $\Delta$ (and $\Gamma$). Since channels are substituted for variables at run-time, we allow the metavariables $x_m, y_m, z_m$ to stand for both variables and channels.

The context $\Gamma$ is a *structural* context that consists of a finite set of assumptions of the form $x_{si} : A_{si}$, associating with each shared variable or channel a session type. A *well-formed* structural context is defined as follows:

\[
\Gamma \triangleq \cdot \mid \Gamma', \ x_s : \hat{A} \quad (x_s \text{ not in } \Gamma')
\]

24
The side-condition makes sure that the variable or channel name is unique within the context. When concatenating a context \( \Gamma \) with a context \( \Gamma' \), variables or channels \( x_i : A_i \) that are shared between \( \Gamma \) and \( \Gamma' \) are contracted, i.e., reduced to one occurrence.

The context \( \Delta \), on the other hand, is a linear context that consists of a finite set of assumptions of the form \( x_{i,1} : A_{i,1} \), associating with each linear variable or channel a session type. A well-formed linear context is defined as follows:

\[
\Delta \triangleq \cdot \mid \Delta', \quad x_i : A_i \quad (x_i \text{ not in } \Delta')
\]

Again, the side-condition makes sure that the variable or channel name is unique within the context. We define the projections \( \text{dom}(\Gamma) \) and \( \text{dom}(\Delta) \) to project onto the variable or channel names in \( \Gamma \) and \( \Delta \), respectively, yielding the empty set in case the context is empty.

The well-formedness of a process typing judgment imposes slightly different invariants on variables and channels. Whereas variables are always unique by \( \alpha \)-conversion, uniqueness holds only for linear channels, but not shared channels. For a linear process typing judgment to be well-formed, the following condition must hold:

\[
\Gamma; \Delta \vdash \Sigma \quad P :: (x_i : A_i) \quad (x_i \text{ not in } \Delta)
\]

The same condition holds only for shared variables in shared process typing judgments:

\[
\Gamma \vdash \Sigma \quad P :: (x_i : A_i) \quad (x_i \text{ not in } \Gamma, \text{ if } x_i \text{ is a variable})
\]

Since the same shared channel can be substituted for different shared variables, giving rise to the possibility of cycles among shared channels (see Section 5.2), the offering channel of a shared process can already occur in its shared context. We point out that no ambiguity arises in that case between the provision and use of a shared channel because SILL\(_5\) introduces separate constructs for each direction. For example, \( a_5 \in x_i \leftarrow \text{accept} a_5 : P_\Delta \) denotes the offering channel whereas it denotes a used channel in \( x_i \leftarrow \text{acquire} a_5 : Q_\Delta \).

The typing rules for process terms are given in Figure 16 and Figure 17. Due to the difference in invariants shared variables and channels have to obey, a context of the form \( \Gamma, x_5 : \hat{A} \) conveys the information that \( x_5 \) is fresh, if \( x \) is a variable.

### B.3 Configuration Typing

Figure 19 gives the typing rules for a SILL\(_5\) configuration \( \Omega \). A configuration \( \Omega \) is divided into a a linear part \( \Theta \) and a shared part \( \Lambda \), subject to the following well-formedness conditions:
\[
\begin{align*}
\Gamma; y_0 & : A_0 \vdash \text{fwd } x_0 : y_0 :: (x_0 : A_0) & \quad (T-\text{Id}_L) \\
\Gamma, y_0 & : A_0 \vdash \text{fwd } x_0 : A_0 & \quad (T-\text{Id}_S)
\end{align*}
\]

\[
\begin{align*}
\Gamma = \frac{y_0 : B_0}{B \leq B_0} \\
\Gamma', \Delta, \Delta' \vdash \text{fwd } x_0 & : y_0 :: (x_0 : A_0) \\
(\Gamma' : x_0 = x_0 & : y_0 :: B_0 = P_{x_0,y_0}) \in \Sigma & \quad \Delta = \frac{y_0 : B_0}{B \leq B_0} \\
\Gamma, \Gamma'; \Delta', \Delta'' \vdash \text{fwd } x_0 & : A_0; \Delta \vdash \Sigma Q_{x_0} :: (z_0 : C_0) \\
\Gamma = \frac{y_0 : B_0}{B \leq B_0} \quad (\text{SPAWN}_L) \\
\Gamma, \Gamma', \Delta, \Delta' \vdash \text{fwd } x_0 & : y_0 :: (x_0 : A_0) \\
(\Gamma' : x_0 = x_0 & : y_0 :: B_0 = P_{x_0,y_0}) \in \Sigma & \quad \Delta = \frac{y_0 : B_0}{B \leq B_0} \\
\Gamma, \Gamma', \Delta' \vdash \text{fwd } x_0 & : A_0; \Delta \vdash \Sigma Q_{x_0} :: (z_0 : C_0) \\
\Gamma = \frac{y_0 : B_0}{B \leq B_0} \quad (\text{SPAWN}_S) \\
\Gamma, \Gamma', \Delta, \Delta' \vdash \text{fwd } x_0 & : y_0 :: (x_0 : A_0) \\
(\Gamma' : x_0 = x_0 & : y_0 :: B_0 = P_{x_0,y_0}) \in \Sigma & \quad \Delta = \frac{y_0 : B_0}{B \leq B_0} \\
\Gamma, \Gamma', \Delta' \vdash \text{fwd } x_0 & : A_0; \Delta \vdash \Sigma Q_{x_0} :: (z_0 : C_0) \\
\Gamma = \frac{y_0 : B_0}{B \leq B_0} \quad (\text{SPAWN}_S)
\end{align*}
\]

Figure 17: Process typing for identity and spawn (cut).

\[
\begin{align*}
\Omega & \triangleq \begin{array}{c}
\Lambda; \Theta \\
\Lambda & \triangleq \begin{array}{c}
\text{proc}(a_0, P_{a_0}), \Lambda' \\
\text{unavail}(a_0), \Lambda'
\end{array} \\
\Theta & \triangleq \begin{array}{c}
\text{proc}(a_0, P_{a_0}), \Theta' \\
\text{proc}(a_0, \_), \Theta'
\end{array}
\end{array} \\
(\forall a. \text{proc}(a, \_) \in \Theta \implies \text{unavail}(a) \in \Lambda) \\
(\text{proc}(a_0, \_), \text{unavail}(a_0) \text{ not in } \Lambda') \\
(\text{proc}(a_0, \_), \text{not in } \Theta')
\end{align*}
\]

We provide further explanations on the configuration typing in Section 5.1 but point out that Rule (T-Ω) permits cyclic dependencies along shared channels by type-checking a configuration relative to all shared channels. Moreover, the rules adhere to the convention to use the metavariables \(x\), \(y\), and \(z\) to stand for variables and the metavariables \(a\), \(b\), \(c\), and \(d\) to stand for channels. Channels are run-time artifacts, and thus it is known at this stage whether a metavariable denotes a variable or a channel.

\section*{C Operational Semantics}

Figure 20 gives the operational semantics of \(\text{SILL}_S\) using \textit{multiset rewriting rules} \[11\]. The semantics is \textit{synchronous}. Section 5.3 sketches how to transform this synchronous semantics into an asynchronous one using cut and identity. A multiset rewriting rule is of the form

\[
S_1, \ldots, S_n \rightarrow T_1, \ldots, T_m
\]

indicating that the state consisting of \(S_1, \ldots, S_n\) transitions to the one consisting of \(T_1, \ldots, T_m\). The \(\rightarrow\) denotes the state transition, substates are separated by \(\rightarrow\). The rule only mentions the part of the state that it rewrites.

We use the following predicates to denote states:

- \(\text{proc}(a_m, P_m)\), for a process providing along channel \(a_m\) and executing the process term \(P_m\);
- \(\text{unavail}(a)\), as a placeholder for a shared process providing along channel \(a\) that is currently not available;
- \(!\text{def}(x_m : A_m \leftarrow X_m \leftarrow \overline{y} : B = P_{x_m,y})\), for each \((x_m : A_m \leftarrow X_m \leftarrow \overline{y} : B = P_{x_m,y}) \in \Sigma\).

Even though multiset rewriting rules are unordered, we write the rules such that a providing process appears to the right of its client, for ease of reading.

We use the side-condition \((b \text{ fresh})\) in

\[
S \rightarrow T \quad (b \text{ fresh})
\]

to allocate a globally \textit{fresh} channel. The freshly allocated channel may occur in \(T\) but not yet in \(S\).
Lastly, we use the equation $a = b$ in

$$S \rightarrow T, a = b$$

for the global substitution of $b$ for $a$ in the entire post-configuration. The channels $a$ and $b$ may occur in $S$.  

---

**Figure 18:** Process typing for shifts and propositional rules.
(aS : ˆB) ∈ Γ ⊢Σ (AL, ˆB) esync Λ ⊢Σ PaL :: (aL : AL) Γ ⊢Σ Θ :: Δ, Δ′ (T-Θ2)

Γ ⊩Σ (aL, PaL), Θ :: (Δ, aL : AL) (T-Λ1)

Γ ⊩Σ (aS, PaS) :: (aS : ↑SAL) (T-Λ2)

Γ ⊩Σ unavail(aS) :: (aS : ˆAL) (T-Λ3)

Γ ⊩Σ AL :: Γ′ Γ ⊩Σ AL′ :: Γ″ (T-Λ4)

Γ ⊩Σ Λ :: Γ Γ ⊩Σ Θ :: Δ (T-Ω)

Figure 19: Configuration typing.
proc(a, fwd a, b)  
→ aₜ = bₜ, aₛ = bₛ  
(D-Idₜ)

proc(aₛ, fwd aₛ bₛ)  
→ unavail(aₛ), aₛ = bₛ  
(D-Idₛ)

proc(aₜ, xₜ ← Xₜ ← cₜ, cₛ; Qₛₜ), !def(xₜ⁺ : Aₜ ← Xₜ ← yₜ : Bₜ ; yₛ : Bₛ = Pₛₜ₊, Pₛₜ₋)  
→ proc(aₜ, [bₛ/xₛ]Qₛₜ), proc(bₛ, [bₛ/xₛ, cₛ/yₛ]Pₛₜ₊, Pₛₜ₋), unavail(bₛ)  
(b fresh)  
(D-SpawnLL)

proc(aₛ, xₛ ← Xₛ ← cₛ; Qₛₙ), !def(xₛ₊ : Aₛ ← Xₛ ← yₛ : Bₛ = Pₛₙ₊, Pₛₙ₋)  
→ proc(aₛ, [bₛ/xₛ]Qₛₙ), proc(bₛ, [bₛ/xₛ, cₛ/yₛ]Pₛₙ₊, Pₛₙ₋)  
(b fresh)  
(D-SpawnLS)

proc(aₛ, xₛ ← Xₛ ← cₛ; Qₛₙ), !def(xₛ⁺ : Aₛ ← Xₛ ← yₛ : Bₛ = Pₛₙ₊, Pₛₙ₋)  
→ proc(aₛ, [bₛ/xₛ]Qₛₙ), proc(bₛ, [bₛ/xₛ, cₛ/yₛ]Pₛₙ₊, Pₛₙ₋)  
(b fresh)  
(D-SpawnSS)

proc(aₛ, xₛ ← release aₛ ; Qₛₙ), proc(aₛ, xₛ ← detach aₛ ; Pₛₙ), unavail(aₛ)  
→ proc(aₛ, [aₛ/xₛ]Qₛₙ), proc(aₛ, [aₛ/xₛ]Pₛₙ)  
(D-[ₕ]ₘ – release/detach)

proc(aₛ, xₛ ← acquire aₛ ; Qₛₙ), proc(aₛ, xₛ ← accept aₛ ; Pₛₙ)  
→ proc(aₛ, [aₛ/xₛ]Qₛₙ), proc(aₛ, [aₛ/xₛ]Pₛₙ), unavail(aₛ)  
(D-[ₕ]ₘ – acquire/accept)

proc(aₛ, wait aₛ ; Qₛₙ), proc(aₛ, close aₛ)  
→ proc(aₛ, Q)  
(D-1)

proc(aₛ, y ← recv aₛ ; Qₚₙ), proc(aₛ, send aₛ b ; P)  
→ proc(aₛ, [b/y]Qₚₙ), proc(aₛ, P)  
(D-⊙/∃)

proc(aₛ, send aₛ b ; Qₚₙ), proc(aₛ, y ← recv aₛ ; Pₚₙ)  
→ proc(aₛ, Qₚₙ), proc(aₛ, [b/y]Pₚₙ)  
(D-→ /II)

proc(aₛ, case aₛ of T⇒ Qₛₚₙ), proc(aₛ, aₛ ; Pₛₚₙ)  
→ proc(aₛ, Qₛₚₙ), proc(aₛ, Pₛₚₙ)  
(D-⊙)

proc(aₛ, aₛ ; Qₛₚₙ), proc(aₛ, case aₛ of T⇒ Pₛₚₙ)  
→ proc(aₛ, Qₛₚₙ), proc(aₛ, Pₛₚₙ)  
(D- &)  

Figure 20: Multiset rewriting system defining synchronous operational dynamics.
D Preservation and Progress

D.1 Definitions, Lemmas, and Corollaries

D.1.1 Definitions

Definition 1 (Configuration Substitution). Substitution in configurations is defined as follows:

\[
\begin{align*}
[b_i/a_i] (\cdot) & \triangleq (\cdot) \\
[b_i/a_i] (\text{proc}(c_i, Q, \Theta)) & \triangleq \text{proc}(c_i, [b_i/a_i] Q), [b_i/a_i] \Theta \quad (\text{where } a_i \neq c_i) \\
[b_s/a_s] (\cdot) & \triangleq (\cdot) \\
[b_s/a_s] (\text{proc}(c_s, Q, \Theta)) & \triangleq \text{proc}(c_s, [b_s/a_s] Q), [b_s/a_s] \Theta \\
[b_s/a_s] (\text{proc}(c_s, Q, \Lambda)) & \triangleq \text{proc}(c_s, [b_s/a_s] Q), [b_s/a_s] \Lambda \quad (\text{where } a_s \neq c_s) \\
[b_s/a_s] (\text{unavail}(c_s), \Lambda) & \triangleq \text{unavail}(c_s), [b_s/a_s] \Lambda
\end{align*}
\]

For a well-typed configuration \( \Gamma \vdash \Sigma \text{proc}(a_i, [b_i/a_i] Q), [b_i/a_i] \Theta :: \Delta \) where \( a_i \) occurs in \( Q \), it follows by induction on the configuration typing that \( [b_i/a_i] \Theta = \Theta \). In order for \( a_i \) to be used in \( Q \) it must be offered by the sub-configuration \( \Theta \) and hence cannot be used by any process in \( \Theta \). Both side-conditions are easily met in all cases Definition 1 is used.

Definition 2 (Concretization). A concretization is a partial order on structural contexts \( \Gamma \) and is inductively defined by the following rules, relying on the partial order \( \bot \leq \top \leq C_i \leq \top \), for any \( C_i \):

\[
\begin{align*}
\text{(T-} \langle \cdot \rangle) & \quad \text{(T-} \langle \cdot \rangle) \\
\Gamma \langle \cdot \rangle & \quad \Gamma' \langle \Gamma \rangle \\
\text{\( A \leq B \) } & \quad \text{\( \Gamma' \times A, \Gamma, x : A \leq \top \) }
\end{align*}
\]

Definition 3 (Poised Process and Configuration). A proc\((a, P_a)\) is poised if it is communicating along its providing channel. The poised processes in SILL\(_S\) are:

Receiving
\[
\text{proc}(a, y \leftarrow \text{recv } a; P_y)
\]
Sending
\[
\text{proc}(a, \text{send } b; P) \\
\text{proc}(a, \text{close } a) \\
\text{proc}(a, \text{case } a \text{ of } \Gamma \Rightarrow P) \\
\text{proc}(a, \text{accept } a; P_a)
\]

A configuration \( \Theta \) is poised if and only if all proc\((a, P_a)\) in \( \Theta \) are poised. A configuration \( \Lambda \) is poised if and only if all proc\((a, P_a)\) in \( \Lambda \) are poised.

Definition 4 (Blocked Process). A process is blocked along \( a_s \) if it has the form proc\((c_i, x_s \leftarrow \text{acquire } a_s; Q_{a_s})\).

D.1.2 Lemmas and Corollaries

Lemma 1 (Process Term Substitution). Given the partial order \( \bot \leq \top C_i \leq \top \), for any \( C_i \), the following substitutions are type-preserving and thus admissible:

1. If \( \Gamma; \Delta \vdash \Sigma P :: (x_i : A_i) \), then, for any fresh \( y_i : A_i \), \( \Gamma; \Delta \vdash \Sigma [y_i/x_i] P :: (y_i : A_i) \).
2. If \( \Gamma; \Delta, y_k : B \vdash \Sigma P \vdash : (x_i : A_i) \), then, for any fresh \( z_k : B \), \( \Gamma; \Delta, z_k : B \vdash \Sigma [z_k/y_k] P \vdash : (x_i : A_i) \).

3. If \( \Gamma; y_k : B; \Delta \vdash \Sigma P \vdash : (x_i : A_i) \), then, for any fresh \( z_k : C \) such that \( C \leq B \), \( \Gamma, z_k : C; \Delta \vdash \Sigma [z_k/y_k] P \vdash : (x_i : A_i) \).

4. If \( \Gamma, y_k : C, y'_k : C; \Delta \vdash \Sigma P \vdash : (x_i : A_i) \), then \( \Gamma, y_k : C; \Delta \vdash \Sigma [y_k/y'_k] P \vdash : (x_i : A_i) \).

5. If \( \Gamma \vdash P \vdash : (z_k : A_k) \), then, for any fresh \( y_k : A_k \), \( \Gamma, y_k : A_k \vdash \Sigma [y_k/x_k] P \vdash : (y_k : A_k) \).

6. If \( \Gamma, x_k: A_k, x'_k : A_k \vdash \Sigma P \vdash : (x_k : A_k) \), then \( \Gamma, x_k : A_k \vdash \Sigma [x_k/x'_k] P \vdash : (x_k : A_k) \).

7. If \( \Gamma, y_k : B; \Delta \vdash \Sigma P \vdash : (x_i : A_i) \), then, for any fresh \( z_k : C \) such that \( C \leq B \), \( \Gamma, z_k : C; \Delta \vdash \Sigma [z_k/y_k] P \vdash : (x_i : A_i) \).

8. If \( \Gamma, y_k : C, y'_k : C; \Delta \vdash \Sigma P \vdash : (x_i : A_i) \), then \( \Gamma, y_k : C; \Delta \vdash \Sigma [y_k/y'_k] P \vdash : (x_i : A_i) \).

**Proof.** We prove each case in turn:

**Lemma 4.4** By \( \alpha \)-equivalence.

**Lemma 4.5** By \( \alpha \)-equivalence.

**Lemma 4.6 and 4.7** By simultaneous induction on \( \Gamma, y_k : B; \Delta \vdash \Sigma P \vdash : (x_i : A_i) \) and \( \Gamma, y_k : B \vdash \Sigma P \vdash : (x_i : A_i) \):

* \( \Gamma, y_k : B; y_k : A_k \vdash \Sigma \) fvd \( x_k, y_k \vdash : (x_i : A_i) \)
  - (since \( y_k \) does not occur in the process term)

* \( \Gamma, z_k : \hat{C}; y_k : A_k \vdash \Sigma \) fvd \( x_k, y_k \vdash : (x_i : A_i) \)
  - for some fresh \( z_k : \hat{C} \) such that \( \hat{C} \leq B \)

* \( \Gamma, y_k : B \vdash \Sigma \) fvd \( x_k, y_k : (x_i : A_i) \) and \( B \leq B \)
  - (by (T-Ids) and since \( B \) \leq \( B \) transitivity of \( \leq \))

* \( \Gamma, x'_k, \hat{A}, y_k : B \vdash \Sigma \) fvd \( x_k, x'_k \vdash : (x_i : A_i) \) and \( \hat{A} \leq B \)
  - (since \( y_k \) does not occur in the process term)

* \( \Gamma, x'_k ; \hat{A}, z_k : \hat{C} \vdash \Sigma \) fvd \( x_k, x'_k \vdash : (x_i : A_i) \)
  - for some fresh \( z_k : \hat{C} \) such that \( \hat{C} \leq B \)

* \( \Gamma, \Gamma', y_k : B; \Delta, \Delta' \vdash \Sigma \) fvd \( x_k \vdash : (x_i : A_i) \)
  - (by (T-SPAWN\_LL))

* \( \Gamma, \Gamma', y_k : B; \Delta, \Delta' \vdash \Sigma \) fvd \( x_k \vdash : (x_i : A_i) \)
  - (by (T-SPAWN\_LL))

* \( \Gamma, \Gamma', y_k : B; \Delta, \Delta' \vdash \Sigma \) fvd \( x_k \vdash : (x_i : A_i) \)
  - (by (T-SPAWN\_LL))
\[
\begin{align*}
\text{Γ, Γ', y_s : } & B; \Gamma' \vdash_\Sigma x'_s \leftarrow X_s \leftarrow w; \text{ } Q_{x'_s} :: (x_s : A_s) \\
\text{where } y_s \notin w & \\
\begin{array}{l}
(x''_s : A'_s \leftarrow X_s \leftarrow w'_s : B'_s = P_{x'_s,w'_s}) \in \Sigma \\
\end{array} \\
B \leq B'_s & \text{ and } \Gamma = w : B \\
\text{Γ, Γ', y_s : } & B, x'_s : A_s; \text{ } \Delta \vdash_\Sigma Q_{x'_s} :: (x_s : A_s) \\
\text{Γ, Γ', z_s : } & \hat{C}, x'_s : A_s; \text{ } \Delta \vdash_\Sigma [z_s/y_s] Q_{x'_s} :: (x_s : A_s) \\
\text{for some fresh } z_s : \hat{C} & \text{ such that } \hat{C} \leq B \\
\text{Γ, Γ', z_s : } & \hat{C}; \text{ } \Delta \vdash_\Sigma x'_s \leftarrow X_s \leftarrow w; \text{ } [z_s/y_s] Q_{x'_s} :: (x_s : A_s) \\
\text{by (T-SPAWN ЛS)} & \\
\text{Γ, Γ', y_s : } & B \vdash_\Sigma x'_s \leftarrow X_s \leftarrow w; \text{ } Q_{x'_s} :: (x_s : A_s) \\
\begin{array}{l}
(x''_s : A'_s \leftarrow X_s \leftarrow w'_s : B'_s, y'_s : B'_s = P_{x'_s,w'_s,y'_s}) \in \Sigma \\
\end{array} \\
B \leq B'_s & \text{ and } \Gamma = w : B \\
\text{Γ, Γ', y_s : } & B, x'_s : A'_s; \text{ } \Delta \vdash_\Sigma Q_{x'_s} :: (x_s : A_s) \\
\text{Γ, Γ', z_s : } & \hat{C}, x'_s : A'_s; \text{ } \Delta \vdash_\Sigma [z_s/y_s] Q_{x'_s} :: (x_s : A_s) \\
\text{for some fresh } z_s : \hat{C} & \text{ such that } \hat{C} \leq B \\
\text{Γ, Γ', z_s : } & \hat{C}; \text{ } \Delta \vdash_\Sigma x'_s \leftarrow X_s \leftarrow w; \text{ } [z_s/y_s] Q_{x'_s} :: (x_s : A_s) \\
\text{by (T-SPAWN SS)} & \\
\text{Γ, y_s : } & \hat{B}; \text{ } \Delta \vdash_\Sigma x'_s \leftarrow \text{acquire } y_s; \text{ } Q_{x'_s} :: (x_s : A_s) \\
B & \leq \uparrow^s C_a \\
\text{Γ, y_s : } & \hat{B}, x'_s : C_i; \text{ } \Delta \vdash_\Sigma Q_{x'_s} :: (x_s : A_i) \\
\text{Γ, z_s : } & \hat{C}, x'_s : C_i; \text{ } \Delta \vdash_\Sigma [z_s/y_s] Q_{x'_s} :: (x_s : A_i) \\
\text{for some fresh } z_s : \hat{C} & \text{ such that } \hat{C} \leq B \\
\text{Γ, z_s : } & \hat{C}; \text{ } \Delta \vdash_\Sigma x'_s \leftarrow \text{acquire } z_s; \text{ } [z_s/y_s] Q_{x'_s} :: (x_s : A_i) \\
\text{(by transitivity of \leq)} & \text{by (T-↑^s_s L(L))} \\
\text{Γ, y_s : } & \hat{B}, y'_s : \hat{D}; \text{ } \Delta \vdash_\Sigma x'_s \leftarrow \text{acquire } y'_s; \text{ } Q_{x'_s} :: (x_s : A_i) \\
\text{Γ, y_s : } & \hat{B}, y'_s : \hat{D}, x'_s : C_i; \text{ } \Delta \vdash_\Sigma Q_{x'_s} :: (x_s : A_i) \\
\text{Γ, z_s : } & \hat{C}, y'_s : \hat{D}; \text{ } \Delta \vdash_\Sigma x'_s : C_i; \text{ } \Delta \vdash_\Sigma [z_s/y_s] Q_{x'_s} :: (x_s : A_i) \\
\text{for some fresh } z_s : \hat{C} & \text{ such that } \hat{C} \leq B \\
\text{Γ, z_s : } & \hat{C}, y'_s : \hat{D}; \text{ } \Delta \vdash_\Sigma x'_s \leftarrow \text{acquire } y'_s; \text{ } [z_s/y_s] Q_{x'_s} :: (x_s : A_i) \\
\text{(by (T-↑^s_s L(L)))} & \\
\text{Γ, y_s : } & \hat{B}; \text{ } \Delta \vdash_\Sigma x'_s \leftarrow \text{accept } x_s; \text{ } P_{x'_s} :: (x_s : \uparrow^s_s A_k) \\
\text{Γ, y_s : } & \hat{B}; \text{ } \Delta \vdash_\Sigma P_{x'_s} :: (x_s : A_i) \\
\text{Γ, z_s : } & \hat{C}; \text{ } \Delta \vdash_\Sigma [z_s/y_s] P_{x'_s} :: (x_s : A_i) \\
\text{for some fresh } z_s : \hat{C} & \text{ such that } \hat{C} \leq B \\
\text{Γ, z_s : } & \hat{C}; \text{ } \Delta \vdash_\Sigma x'_s \leftarrow \text{accept } x_s; \text{ } [z_s/y_s] P_{x'_s} :: (x_s : \uparrow^s_s A_i) \\
\text{(by (T-↑^s_s R))} & \\
\text{Γ, y_s : } & \hat{B}; \text{ } \Delta \vdash_\Sigma x'_s \leftarrow \text{release } x'_s; \text{ } Q_{x'_s} :: (x_s : A_i) \\
\text{Γ, y_s : } & \hat{B}; \text{ } \Delta \vdash_\Sigma Q_{x'_s} :: (x_s : A_i) \\
\text{Γ, z_s : } & \hat{C}; \text{ } \Delta \vdash_\Sigma [z_s/y_s] Q_{x'_s} :: (x_s : A_i) \\
\text{for some fresh } z_s : \hat{C} & \text{ such that } \hat{C} \leq B \\
\text{Γ, z_s : } & \hat{C}; \text{ } \Delta \vdash_\Sigma x'_s \leftarrow \text{release } x'_s; \text{ } [z_s/y_s] P_{x'_s} :: (x_s : \uparrow^s_s A_i) \\
\text{(by (T-↑^s_s R))} & \\
32
\end{align*}
\]
\begin{align*}
\Gamma, y_b : B; x'_b : A_b; & \quad \Delta \vdash_{\Sigma} Q_{y_b'} :: (x_i : A_i) \\
\Gamma, z_b : C; x'_b : A_b; & \quad \Delta \vdash_{\Sigma} \left[ z_b/y_b \right] Q_{y_b'} :: (x_i : A_i) \\
& \quad \text{for some fresh } z_b : C \text{ such that } \hat{C} \leq \hat{B} \\
\Gamma, z_b : C; & \quad \Delta, x'_l \vdash \left[ z_b/y_b \right] A_b \vdash_{\Sigma} \text{release } x'_i \vdash \left[ z_b/y_b \right] Q_{y_b'} :: (x_i : A_i) & \text{(by (T-\$^L_B))}
\end{align*}

\begin{align*}
\Gamma, y_b : B; & \quad \vdash_{\Sigma} x_b \leftarrow \text{detach } x_b : P_{z_b} :: (x_i : A_i) \\
\Gamma, y_b : B; & \quad \vdash_{\Sigma} P_{z_b} :: (x_i : A_i) \\
\Gamma, z_b : C; & \quad \Delta \vdash_{\Sigma} z_b/y_b \left[ z_b/y_b \right] P_{z_b} :: (x_i : A_i) \\
& \quad \text{for some fresh } z_b : C \text{ such that } \hat{C} \leq \hat{B} \\
\Gamma, z_b : C; & \quad \Delta, x'_i \vdash \text{detach } x_i : \left[ z_b/y_b \right] P_{z_b} :: (x_i : A_i) & \text{(by (T-\$^R_B))}
\end{align*}

\begin{align*}
\Gamma, y_b : B; & \quad \Delta, y_b : 1 \vdash_{\Sigma} \text{wait } y_b : Q :: (x_i : A_i) \\
\Gamma, y_b : B; & \quad \vdash_{\Sigma} Q :: (x_i : A_i) \\
\Gamma, z_b : C; & \quad \Delta \vdash_{\Sigma} z_b/y_b \left[ z_b/y_b \right] Q :: (x_i : A_i) \\
& \quad \text{for some fresh } z_b : C \text{ such that } \hat{C} \leq \hat{B} \\
\Gamma, z_b : C; & \quad \Delta, y_b : 1 \vdash_{\Sigma} \text{wait } y_b : \left[ z_b/y_b \right] Q :: (x_i : A_i) & \text{(by (T-1L))}
\end{align*}

\begin{align*}
\Gamma, y_b : B; & \quad \vdash_{\Sigma} \text{close } x_i :: (x_i : 1) \\
\Gamma, z_b : C; & \quad \vdash_{\Sigma} \text{close } x_i :: (x_i : 1) \\
& \quad \text{for some fresh } z_b : C \text{ such that } \hat{C} \leq \hat{B} \\
\Gamma, y_b : \hat{B}; & \quad \Delta, x'_b : B_b \otimes C_b \vdash_{\Sigma} \text{recv } x'_i : Q_{y_b} :: (x_i : A_i) \\
\Gamma, y_b : \hat{B}; & \quad \vdash_{\Sigma} x'_b : C_b, y_b : B_b \vdash_{\Sigma} Q_{y_b} :: (x_i : A_i) \\
\Gamma, z_b : C; & \quad \Delta, x'_b : C_b, y_b : B_b \vdash_{\Sigma} z_b/y_b \left[ z_b/y_b \right] Q_{y_b} :: (x_i : A_i) \\
& \quad \text{for some fresh } z_b : C \text{ such that } \hat{C} \leq \hat{B} \\
\Gamma, z_b : C; & \quad \Delta, x'_b : B_b \otimes C_b \vdash_{\Sigma} \text{recv } x'_i : \left[ z_b/y_b \right] Q_{y_b} :: (x_i : A_i) & \text{(by (T-\otimes_L))}
\end{align*}

\begin{align*}
\Gamma, y_b : \hat{B}; & \quad \Delta, y_b : A_i \vdash_{\Sigma} \text{send } x_i : P :: (x_i : A_i \otimes B_i) \\
\Gamma, y_b : \hat{B}; & \quad \vdash_{\Sigma} P :: (x_i : B_i) \\
\Gamma, z_b : C; & \quad \Delta \vdash_{\Sigma} \left[ z_b/y_b \right] P :: (x_i : B_i) \\
& \quad \text{for some fresh } z_b : C \text{ such that } \hat{C} \leq \hat{B} \\
\Gamma, z_b : C; & \quad \Delta, y_b : A_i \vdash_{\Sigma} \text{send } x_i : \left[ z_b/y_b \right] P :: (x_i : A_i \otimes B_i) & \text{(by (T-\otimes_R))}
\end{align*}

\begin{align*}
\Gamma, y_b : \hat{B}; & \quad \Delta, x'_b : (\exists A_b, B_b) \vdash_{\Sigma} y'_b \leftarrow \text{recv } x'_i : Q_{y_b'} :: (x_i : A_i) \\
\Gamma, y_b : \hat{B}, y'_b : A_b; & \quad \Delta, x'_b : B_b \vdash_{\Sigma} Q_{y_b'} :: (x_i : A_i) \\
\Gamma, z_b : C; & \quad y'_b : A_b; \quad \Delta, x'_b : B_b \vdash_{\Sigma} z_b/y_b \left[ z_b/y_b \right] Q_{y_b'} :: (x_i : A_i) \\
& \quad \text{for some fresh } z_b : C \text{ such that } \hat{C} \leq \hat{B} \\
\Gamma, z_b : C; & \quad \Delta, x'_b : (\exists A_b, B_b) \vdash_{\Sigma} y'_b \leftarrow \text{recv } x'_i : \left[ z_b/y_b \right] Q_{y_b'} :: (x_i : A_i) & \text{(by (T-\exists_L))}
\end{align*}

\begin{align*}
\Gamma, y_b : \hat{B}; & \quad \Delta \vdash_{\Sigma} \text{send } x_i : P :: (x_i : (\exists B_b, A_i)) \\
\Gamma, y_b : \hat{B}; & \quad \vdash_{\Sigma} P :: (x_i : A_i) \text{ and } \hat{B} \leq B_b \\
\Gamma, z_b : C; & \quad \Delta \vdash_{\Sigma} \left[ z_b/y_b \right] P :: (x_i : A_i) \\
& \quad \text{for some fresh } z_b : C \text{ such that } \hat{C} \leq \hat{B} \\
\hat{C} \leq B_b & \quad \text{(by transitivity of } \leq \text{)} \\
\Gamma, z_b : C; & \quad \Delta \vdash_{\Sigma} \text{send } x_i : \left[ z_b/y_b \right] P :: (x_i : (\exists B_b, A_i)) & \text{(by (T-\exists_R))}
\end{align*}

\begin{align*}
\Gamma, y_b : \hat{B}, y'_b : A; & \quad \Delta \vdash_{\Sigma} \text{send } x_i : P :: (x_i : (\exists A_a, B_b)) \\
\Gamma, y_b : \hat{B}, y'_b : A; & \quad \Delta \vdash_{\Sigma} P :: (x_i : B_b) \text{ and } \hat{A} \leq A_a \\
\Gamma, z_b : C; & \quad y'_b : A; \quad \Delta \vdash_{\Sigma} \left[ z_b/y_b \right] P :: (x_i : B_b) \\
& \quad \text{for some fresh } z_b : C \text{ such that } \hat{C} \leq \hat{B}
\end{align*}
\[ \Gamma, z_5 : \hat{C}, y'_5 : \hat{A} \mid \Delta \vdash \Sigma \ \text{send} \ x_i, y'_5; [z_5/y_5] \ P :: (x_i : (\exists A_5.B_i)) \]  
(by (T-\exists_R))

- \[ \Gamma, y_5 : \hat{B}; \Delta, x'_i : A_i \rightarrow B_i, y_i : A_i \mid \Sigma \ \text{send} \ x'_i, y_i; Q :: (x_i : A_i) \]  
(by (T-\rightarrow_R))

- \[ \Gamma, y_5 : \hat{B}; \Delta, x'_i : B_i \mid \Sigma \ Q :: (x_i : A_i) \]  
(by (T-\rightarrow_L))

- \[ \Gamma, z_5 : \hat{C}; \Delta, x'_i : B_i \mid \Sigma \ [z_5/y_5] Q :: (x_i : A_i) \]  
(by (I.H.))

- \[ \Gamma, z_5 : \hat{C}; \Delta, x'_i : A_i \rightarrow B_i, y_i : A_i \mid \Sigma \ \text{send} \ x'_i, y_i; [z_5/y_5] Q :: (x_i : A_i) \]  
(by (T-\rightarrow_L))

- \[ \Gamma, y_5 : \hat{B}; \Delta, x'_i : (\Pi B_i.\hat{C}_i) \mid \Sigma \ \text{send} \ x'_i, y'_5; Q :: (x_i : A_i) \]  
(by T-IDL)}

\[ \Gamma, y_5 : \hat{B}; \Delta, x'_i : \hat{A}; \Delta, x'_i : B_i \mid \Sigma \ Q :: (x_i : A_i) \]  
(by (T-\rightarrow_L))

\[ \Gamma, z_5 : \hat{C}, y'_5 : \hat{A}; \Delta, x'_i : B_i \mid \Sigma \ [z_5/y_5] Q :: (x_i : A_i) \]  
(by I.H.)

\[ \Gamma, z_5 : \hat{C}; \Delta, x'_i : (\Pi B_i.\hat{C}_i) \mid \Sigma \ \text{send} \ x'_i, y'_5; [z_5/y_5] Q :: (x_i : A_i) \]  
(by (T-\rightarrow_L))

\[ \Gamma, y_5 : \hat{B}; \Delta, x'_i : (\Pi A_5.B_i) \mid \Sigma \ \text{send} \ x'_i, y'_5; Q :: (x_i : A_i) \]  
(by T-IDL)}

\[ \Gamma, y_5 : \hat{B}; \Delta, x'_i : A_i; \Delta, x'_i : B_i \mid \Sigma \ Q :: (x_i : A_i) \]  
(by I.H.)

\[ \Gamma, z_5 : \hat{C}, y'_5 : \hat{A}; \Delta, x'_i : B_i \mid \Sigma \ [z_5/y_5] Q :: (x_i : A_i) \]  
(by I.H.)

\[ \Gamma, z_5 : \hat{C}; \Delta, x'_i : (\Pi B_i.\hat{C}_i) \mid \Sigma \ \text{send} \ x'_i, y'_5; [z_5/y_5] Q :: (x_i : A_i) \]  
(by (T-\rightarrow_L))

\[ \Gamma, y_5 : \hat{B}; \Delta, x'_i : \hat{A}; \Delta, x'_i : B_i \mid \Sigma \ P :: (x_i : A_{i.h}) \]  
(by I.H.)

\[ \Gamma, z_5 : \hat{C}; \Delta, x'_i : B_i \mid \Sigma \ [z_5/y_5] P :: (x_i : A_{i.h}) \]  
(by I.H.)

\[ \Gamma, z_5 : \hat{C}; \Delta, x'_i : [z_5/y_5] P :: (x_i : A_{i.h}) \]  
(by I.H.)

\[ \Gamma, z_5 : \hat{C}; \Delta, x'_i : \hat{A}; \Delta, x'_i : B_i \mid \Sigma \ [z_5/y_5] Q :: (x_i : A_i) \]  
(by I.H.)

\[ \Gamma, z_5 : \hat{C}; \Delta, x'_i : B_i \mid \Sigma \ Q :: (x_i : A_i) \]  
(by I.H.)
\[\Gamma, y_b : \hat{B}; \Delta \vdash \Sigma \text{ case } x_i \text{ of } \hat{l} = \hat{P} :: (x_i : \& \{\Gamma, \Lambda_i\}) \quad \text{(this case)}\]

\[(\forall i) \quad \Gamma, y_b : \hat{B}; \Delta \vdash \Sigma \quad P_i :: (x_i : A_{\Lambda_i}) \quad \text{(this case)}\]

\[(\forall i) \quad \Gamma, z_a : \hat{C}; \Delta \vdash \Sigma \quad [z_a/y_b] P_i :: (x_i : A_{\Lambda_i}) \quad \text{(by I.H.)}\]

for some fresh \(z_a : \hat{C}\) such that \(\hat{C} \leq \hat{B}\)

\[\Gamma, z_a : \hat{C}; \Delta \vdash \Sigma \text{ case } x_i \text{ of } \hat{l} = [z_a/y_b] \hat{P} :: (x_i : \& \{\Gamma, \Lambda_i\}) \quad ((T-\&R))\]

\[\text{Lemma [??]} \quad \text{By contraction.}\]

\[\text{Lemma [??]} \quad \text{By } \alpha\text{-equivalence.}\]

\[\text{Lemma [??]} \quad \text{By contraction.}\]

\[\text{Lemma [??]} \quad \text{By contraction.}\]

\[\text{Lemma 2 (Configuration Substitution). Writing } Q\langle a \rangle \text{ for a process term } Q \text{ with an occurrence of a channel } a \text{ and given the partial order } \bot \leq \uparrow_t C_i \leq \top, \text{ for any } C_i, \text{ the following substitutions are type-preserving and thus admissible:}\]

1. If \(\Gamma \vdash \Sigma \Theta \vdash (\Delta, \Delta_1, a_i : A_i)\), then, for any \(\Theta'\) such that \(\Gamma \vdash \Sigma \Theta' \vdash (\Delta, \Delta_1, b_i : A_i)\), \(\Gamma \vdash \Sigma \Theta' \vdash [b_i/a_i] Q\langle a_i \rangle\), \(\Theta' \vdash \Delta\).

2. If \(\Gamma, a_s : \hat{A}, b_s : \hat{B} \vdash \Sigma \Theta \vdash \Delta \text{ and } \hat{B} \leq \hat{A}\), then \(\Gamma, a_s : \hat{A}, b_s : \hat{B} \vdash \Sigma [b_s/a_s] \Theta \vdash \Delta\).

3. If \(\Gamma, a_s : \hat{A}, b_s : \hat{B} \vdash \Sigma \Lambda \text{ and } \text{proc}(a_s, \_ \neq \Lambda \text{ and } \text{unavail}(a_s) \neq \Lambda \text{ and } \hat{B} \leq \hat{A}\), then \(\Gamma, a_s : \hat{A}, b_s : \hat{B} \vdash \Sigma [b_s/a_s] \Lambda \vdash \Gamma_1\).

\[\text{Proof. We prove each case in turn:}\]

1. By induction on \(\Gamma \vdash \Sigma \Theta \vdash (\Delta, \Delta_1, a_i : A_i)\), \(\Theta' \vdash \Delta\):

   - \(\Gamma \vdash \Sigma \Theta \vdash (\Delta, \Delta_1, a_i : A_i)\)
   - \(\Theta' \vdash \Delta\)
   - \(\Gamma \vdash \Sigma \Theta' \vdash (\Delta, \Delta_1, b_i : A_i)\)
   - \(\Gamma \vdash \Sigma \Theta' \vdash [b_i/a_i] Q\langle a_i \rangle\), \(\Theta' \vdash \Delta\)

2. By induction on \(\Gamma, a_s : \hat{A}, b_s : \hat{B} \vdash \Sigma \Theta \vdash \Delta\):

   - \(\Gamma, a_s : \hat{A}, b_s : \hat{B} \vdash \Sigma \Theta \vdash (\cdot, A_i : A_i)\)
   - \(\Gamma, a_s : \hat{A}, b_s : \hat{B} \vdash \Sigma (\cdot, A_i : A_i)\)

3. By induction on \(\Gamma, a_s : \hat{A}, b_s : \hat{B} \vdash \Sigma \Lambda \vdash \Gamma_1\):
   - \(\Gamma, a_s : \hat{A}, b_s : \hat{B} \vdash \Sigma (\cdot, \_ \neq (\cdot, \_ \neq A_i : A_i)\)
   - \(\Gamma, a_s : \hat{A}, b_s : \hat{B} \vdash \Sigma (\cdot, \_ \neq (\cdot, \_ \neq A_i : A_i)\)
   - \(\Gamma, a_s : \hat{A}, b_s : \hat{B} \vdash \Sigma \Theta \vdash (\cdot, A_i : A_i)\)

\[\text{Lemma [??]} \quad \text{By Definition [??]}\]

\[\text{Lemma [??]} \quad \text{By Definition [??]}\]

\[\text{Lemma [??]} \quad \text{By Definition [??]}\]
Proof.\quad type-preserving and thus admissible:

1. By induction on $\Gamma$

   - $\Gamma, a_s : \check{A}, b_s : \check{B} \vdash \Sigma P_{a_s} :: (c_s : t_C)$ (by Lemma 16)
   - $\Gamma, b'_s : \check{B}, b_s : \check{B} \vdash \Sigma [b'_s/a_s] P_{a_s} :: (c_s : t_C)$ (by Lemma 15 and weakening)

   for some fresh $b'_s : \check{B}$

   - $\Gamma, a_s : \check{A}, b_s : \check{B} \vdash \Sigma [b'_s/b'_s] ([b'_s/a_s] P_{a_s}) :: (c_s : t_C)$ (by Lemma 15 and weakening)
   - $\Gamma, a_s : \check{A}, b_s : \check{B} \vdash \Sigma \text{proc}(c_s, [b'_s/a_s] P_{a_s}) :: (c_s : t_C)$ (by (T-A2))

2. $\Gamma, a_s : \check{A}, b_s : \check{B} \vdash \Sigma \text{avail}(c_s) :: (c_s : C)$ and $\check{B} \leq \check{A}$ and $a_s \neq c_s$

   - $\Gamma, a_s : \check{A}, b_s : \check{B} \vdash \Sigma \text{avail}(c_s) :: (c_s : C)$ (by Definition 1)

   for some $\check{A}, \check{B}, \check{B}_1, \check{B}_2, b : \check{B}$ and proc$(a_s, \_ ) \notin \check{A}, \check{B}_1$ and unavail$(a_s) \notin \check{A}, \check{B}_1$

   (this case)

   - $\check{B} \leq \check{A}$ (this case)
   - $\Gamma, a_s : \check{A}, b_s : \check{B} \vdash \Sigma \check{A}_1 \check{B}_2 :: \check{B}_1, \check{B}_2, b : \check{B}$ (this case)

   for some $\check{A}_1, \check{B}_2, \check{B}_1, \check{B}_2$ and $\check{B}_1, \check{B}_2, b : \check{B}$ (this case)

   - $\Gamma, a_s : \check{A}, b_s : \check{B} \vdash \Sigma \check{A}_1 \check{B}_2 :: \check{B}_1, \check{B}_2, b : \check{B}$ (by I.H.)

Lemma 3 (Update of $\Gamma$). Given the partial order $\bot \leq t_C \leq T$, for any $C_i$, the following substitutions are type-preserving and thus admissible:

1. If $\Gamma, a_s : \check{A} \vdash \Sigma \Theta :: \Delta$, then, for any $C_i$ such that $\vdash \Sigma (C_i, \check{A}) \text{esync}$ and for any $\check{B}$ such that $\check{B} \leq \check{A}$ and $\vdash \Sigma (C_i, \check{B}) \text{esync}$, $\Gamma, a_s : \check{B} \vdash \Sigma \Theta :: \Delta$.

2. If $\Gamma, a_s : \check{A} \vdash \Sigma \Lambda :: \Gamma_1$, with proc$(a_s, P) \notin \Lambda$ and unavail$(a_s) \notin \Lambda$, then, for any $C_i$ such that $\vdash \Sigma (C_i, \check{A}) \text{esync}$ and for any $\check{B}$ such that $\check{B} \leq \check{A}$ and $\vdash \Sigma (C_i, \check{B}) \text{esync}$, $\Gamma, a_s : \check{B} \vdash \Sigma \Lambda :: \Gamma_1$.

Proof. We prove each case in turn:

1. By induction on $\Gamma$, $a_s : \check{A} \vdash \Sigma \Theta :: \Delta$:

   - $\Gamma, a_s : \check{A} \vdash \Sigma (\cdot) :: (\cdot)$ (this case)

   for some $C_i$ such that $\vdash \Sigma (C_i, \check{A}) \text{esync}$ and for any $\check{B}$ such that $\check{B} \leq \check{A}$

   - $\Gamma, a_s : \check{B} \vdash \Sigma (\cdot) :: (\cdot)$ (this case)

   (since $a_s$ does not occur in the configuration)

   for some $C_i$ such that $\vdash \Sigma (C_i, \check{A}) \text{esync}$ and for any $\check{B}$ such that $\check{B} \leq \check{A}$

   - $\Gamma, a_s : \check{A} \vdash \Sigma \text{proc}(c_s, P_{c_s}), \Theta :: (\Delta, c_s : D_c)$ (this case)

   ($c_s : D_c) \in \Gamma$ and $\vdash \Sigma (D_c, D_c) \text{esync}$

   - $\Gamma, a_s : \check{A} \vdash \Sigma (\Delta', D_c) :: (c_s : D_c)$ (this case)

   for some fresh $a'_s : \check{B}$

   - $\Gamma, a_s : \check{B} : \vdash \Sigma (\Delta', [a'_s/a_s]) P_{c_s} :: (c_s : D_c)$ (by Lemma 15 and weakening)

   for some fresh $a'_s : \check{B}$

   - $\Gamma, a_s : \check{B} : \vdash \Sigma (\Delta', [a'_s/a_s]) (\Delta', c_s : D_c) :: (c_s : D_c)$ (by (T-\Theta_2))

2. By induction on $\Gamma, a_s : \check{A} \vdash \Sigma \Lambda :: \Gamma_1$:

   - $\Gamma, a_s : \check{A} \vdash \Sigma (\cdot) :: (\cdot)$ and proc$(a_s, \_ ) \notin (\cdot)$ and unavail$(a_s) \notin (\cdot)$ (this case)

   for some $C_i$ such that $\vdash \Sigma (C_i, \check{A}) \text{esync}$ and for any $\check{B}$ such that $\check{B} \leq \check{A}$

   - $\Gamma, a_s : \check{B} \vdash \Sigma (\cdot) :: (\cdot)$ (this case)

   (since $a_s$ does not occur in the configuration)

   for some $C_i$ such that $\vdash \Sigma (C_i, \check{A}) \text{esync}$ and for any $\check{B}$ such that $\check{B} \leq \check{A}$

   - $\Gamma, a_s : \check{A} \vdash \Sigma \text{proc}(c_s, P_{c_s}), \Theta :: (\Delta, c_s : D_c)$ (this case)

   $\vdash \Sigma (\Delta', D_c) \text{esync}$

   - $\Gamma, a_s : \check{A} \vdash \Sigma P_{c_s} :: (c_s : t_D)$ (this case)

   (case 1)

   - $\Gamma, a_s : \check{B} \vdash \Sigma [b'_s/a_s] P_{c_s} :: (c_s : t_D)$ (by Lemma 17 and weakening)

   for some fresh $b'_s : \check{B}$ and $C_i$ such that $\vdash \Sigma (C_i, \check{A}) \text{esync}$ and $\check{B} \leq \check{A}$

   - $\Gamma, a_s : \check{B} \vdash \Sigma [b'_s/a_s] ([b'_s/a_s] P_{c_s}) :: (c_s : t_D)$ (by Lemma 15 and weakening)

   (by (T-A2))
Lemma 4 (Equi-Synchronizing and ⊥). If \( \vdash_\Sigma (C_i, \uparrow_i^i A_i) \) \( \esync \) and \( \vdash_\Sigma (C_i, \uparrow_i^i B_i) \) \( \esync \), for any \( C_i, \uparrow_i^i A_i, \uparrow_i^i B_i \) such that \( A_i \neq B_i \), then \( \vdash_\Sigma (C_i, \bot) \) \( \esync \).

Proof. For the presentation of the proof, we switch to a set-based formulation of \( \esync \) to allow for a more natural formulation of the coinductive proof. The assertion \( \vdash_\Sigma (D, D) \esync \) then is expressed as \( (D, D) \in \esync \). Given the monotone generating function \( \mathcal{F} \) arising from the rules defined in Figure 16, we obtain that \( \esync \subseteq \mathcal{F}(\esync) \), since \( \esync \) is \( \mathcal{F} \)-consistent.

Next, we define the set \( \esync' \) as

\[
\esync' \overset{\text{def}}{=} \esync \cup \esync_{\bot}
\]

where \( \esync_{\bot} \) is defined as:

\[
\esync_{\bot} \overset{\text{def}}{=} \{(C_i, \bot) \mid \exists A_i, B_i . (C_i, \uparrow_i^i A_i) \in \esync \land (C_i, \uparrow_i^i B_i) \in \esync \land A_i \neq B_i\}
\]

To prove Lemma 4 it suffices to show that \( \esync' \) is \( \mathcal{F} \)-consistent, i.e., that \( \esync' \subseteq \mathcal{F}(\esync') \). Thus, we have to show the following two cases:

(i) \( \esync \subseteq \mathcal{F}(\esync') \) and
(ii) \( \esync_{\bot} \subseteq \mathcal{F}(\esync') \)

We first show (i) and then (ii):

(i) \( \esync \subseteq \esync' \) (by definition of \( \esync' \))

\[
\mathcal{F}(\esync) \subseteq \mathcal{F}(\esync')
\]

\( \esync \subseteq \mathcal{F}(\esync) \) (by monotonicity of \( \mathcal{F} \))

\( \esync \subseteq \mathcal{F}(\esync') \) (by transitivity of \( \subseteq \))

(ii) We consider each syntactic form of \( C_i \) in turn:

• \( (\top \{ t : C_i \}, \bot) \in \esync' \) (this case)

\[
(\top \{ t : C_i \}, \uparrow_i^i A_i) \in \esync \text{ and } (\top \{ t : C_i \}, \uparrow_i^i B_i) \in \esync
\]

for some \( A_i \) and \( B_i \) such that \( A_i \neq B_i \) (this case)

• \( (\forall i \{ t : C_i \}, \bot) \in \esync_{\bot} \) (by inversion on \( \text{T-Esync}_{\bot} \))

\[
(\forall i \{ t : C_i \}, \uparrow_i^i A_i) \in \esync \text{ and } (\forall i \{ t : C_i \}, \uparrow_i^i B_i) \in \esync
\]

for some \( A_i \) and \( B_i \) such that \( A_i \neq B_i \) (by definition of \( \esync_{\bot} \))

\( \forall i \{ t : C_i \}, \bot \in \esync_{\bot} \) (since \( \esync_{\bot} \subseteq \esync' \)) (by \( \text{T-Esync}_{\bot} \))

\( (\forall i \{ t : C_i \}, \bot) \in \mathcal{F}(\esync') \) (by \( \text{T-Esync}_{\bot} \))

• \( (\land \{ t : C_i \}, \bot) \in \esync' \) (this case)

\[
(\land \{ t : C_i \}, \uparrow_i^i A_i) \in \esync \text{ and } (\land \{ t : C_i \}, \uparrow_i^i B_i) \in \esync
\]

for some \( A_i \) and \( B_i \) such that \( A_i \neq B_i \) (this case)

• \( (\land \{ t : C_i \}, \bot) \in \esync_{\bot} \) (by inversion on \( \text{T-Esync}_{\&} \))

\[
(\land \{ t : C_i \}, \uparrow_i^i A_i) \in \esync \text{ and } (\land \{ t : C_i \}, \uparrow_i^i B_i) \in \esync
\]

for some \( A_i \) and \( B_i \) such that \( A_i \neq B_i \) (by definition of \( \esync_{\bot} \))

\( \forall i \{ t : C_i \}, \bot \in \esync_{\bot} \) (since \( \esync_{\bot} \subseteq \esync' \)) (by \( \text{T-Esync}_{\&} \))

\( (\land \{ t : C_i \}, \bot) \in \mathcal{F}(\esync') \) (by \( \text{T-Esync}_{\&} \))
By well-formedness of $\Lambda; \Theta$ (see Section B.3) it follows that

$\vdash_{\text{sync}_\bot} (C \otimes C', \bot) \in \text{sync}_\bot$

$\vdash_{\text{sync}_\bot} (C \otimes C', \bot, A_i) \in \text{sync} \quad \text{for some } A_i \text{ and } B_i \text{ such that } A_i \neq B_i$

$\vdash_{\text{sync}_\bot} (C, \bot) \in \text{sync}_\bot$

$\vdash_{\text{sync}_\bot} (C', \bot) \in \text{sync}_\bot$

$\vdash_{\text{sync}_\bot} (C, \bot) \in \text{sync}_\bot'$

$\vdash_{\text{sync}_\bot} (C', \bot) \in \text{sync}_\bot'$

$\vdash_{\text{sync}_\bot} (C \rightarrow C', \bot) \in \text{sync}_\bot$

$\vdash_{\text{sync}_\bot} (C \rightarrow C', \bot, A_i) \in \text{sync} \quad \text{for some } A_i \text{ and } B_i \text{ such that } A_i \neq B_i$

$\vdash_{\text{sync}_\bot} (C', \bot) \in \text{sync}_\bot$

$\vdash_{\text{sync}_\bot} (C', \bot) \in \text{sync}_\bot'$

$\vdash_{\text{sync}_\bot} (C \rightarrow C', \bot) \in \mathcal{F}(\text{sync}_\bot)$

If the configuration $\Lambda; \Theta$ is well-formed, then, for any $\text{proc}(a, \bot)$ in $\Lambda$, there does not exist a $\text{proc}(a, \bot)$ in $\Theta$.

Proof. By well-formedness of $\Lambda; \Theta$ (see Section B.3) it follows that $\text{unavail}(a) \notin \Lambda$ and that $\forall a. \text{proc}(a, \bot) \in \Theta \implies \text{unavail}(a) \in \Lambda$. Then, by the contrapositive, it follows that $\text{proc}(a, \bot) \notin \Theta$.

Corollary 1 (Balance between $\Lambda$ and $\Theta$). If the configuration $\Lambda; \Theta$ is well-formed, then, for any $\text{proc}(a, \bot)$ in $\Lambda$, there does not exist a $\text{proc}(a, \bot)$ in $\Theta$.

Proof. By well-formedness of $\Lambda; \Theta$ (see Section B.3) it follows that $\text{unavail}(a) \notin \Lambda$ and that $\forall a. \text{proc}(a, \bot) \in \Theta \implies \text{unavail}(a) \in \Lambda$. Then, by the contrapositive, it follows that $\text{proc}(a, \bot) \notin \Theta$.

Lemma 5 (Permutation of $\Theta$). Writing $Q(a_i)$ for a process term $Q$ with an occurrence of a linear channel $a_i$, the following permutation is admissible:

If $\Gamma \vdash_\Theta \Theta_1, \text{proc}(a_i, Q(a_i)), \Theta_2, \text{proc}(a_i, P_{a_i}), \Theta_3 :: \Delta$, then $\Gamma \vdash_\Sigma \Theta_1, \text{proc}(a_i, Q(a_i)), \text{proc}(a_i, P_{a_i}), \Theta_2, \Theta_3 :: \Delta$.

Proof. In the given typing derivation, $\text{proc}(a_i, P_{a_i})$ provides $a_i : A_i$ for some $A_i$ to $\Theta_1$, $\text{proc}(a_i, Q(a_i))$, $\Theta_2$. Well-formedness of a configuration (see Section B.3) guarantees that $a_i$ is unique within a configuration, and hence there can be no other process in $\Theta_2$ that provides a service along $a_i$. Moreover, channel $a_i$ cannot be consumed by $\Theta_2$.
because channels are linear and \( a_i \) occurs in \( \text{proc}(c_i, Q(a_i)) \). Any channels used by \( \text{proc}(a_i, P_{a_i}) \) will continue to be available if we move the process to the left.

\[ \square \]

**Lemma 6 (Truncate \( \Theta \)).** If \( \Gamma \models_{\Sigma} \Theta_1, \text{proc}(a_i, P_{a_i}), \Theta_2 :: \Delta \), then there exists an \( A_i \) and \( \Delta' \) such that \( \Gamma \models_{\Sigma} \text{proc}(a_i, P_{a_i}), \Theta_2 :: (\Delta', \alpha_i : A_i) \).

**Proof.** By induction on \( \Gamma \models_{\Sigma} \Theta :: \Delta :: (\text{this case}) \):

- \( \Gamma \models_{\Sigma} (\cdot) :: (\cdot) \)
  - Holds vacuously.

- \( \Gamma \models_{\Sigma} \text{proc}(c_i, P_{c_i}), \Theta :: \Delta \)
  - (this case)\( \Gamma \models_{\Sigma} \Delta_2 \models_{\Sigma} P_{c_i} :: (c : C_i) \)
  - (this case)\( \text{for some } \Delta_2, \Delta_1, \text{ and } C_i \text{ such that } \Delta = (\Delta_1, c : C_i) \)
  - (this case)\( \Gamma \models_{\Sigma} \Theta :: \Delta_1, \Delta_2 \)
  - (this case)\( \Theta_1 = (\cdot) \) and \( \text{proc}(a_i, P_{a_i}), \Theta_2 = \text{proc}(c_i, P_{c_i}), \Theta \)
  - (this subcase)\( \Gamma \models_{\Sigma} \text{proc}(c_i, P_{c_i}), \Theta :: (\Delta_1, c : C_i) \)
  - (this subcase)\( \Theta = \text{proc}(a_i, P_{a_i}), \Theta_2 = \text{proc}(c_i, P_{c_i}), \Theta_2 \text{ for some } \Theta'_i \text{ such that } \Theta = \Theta'_i, \text{proc}(a_i, P_{a_i}), \Theta_2 \)

\( \Gamma \models_{\Sigma} \text{proc}(a_i, P_{a_i}), \Theta_2 :: (\Delta_3, \alpha_i : A_i) \)
- (by I.H.)\( \text{for some } \Delta_3 \text{ and } A_i \)

\[ \square \]

**Lemma 7 (Linear Process Terms are Stable under Concretization).** If \( \Gamma_1, \Gamma_2; \Delta \models_{\Sigma} P :: (\alpha_i : A_i) \) and \( \Gamma'_2 < \Gamma_2 \), then \( \Gamma_1, \Gamma'_2; \Delta \models_{\Sigma} P :: (\alpha_i : A_i) \).

**Proof.** By induction on \( \Gamma'_2 < \Gamma_2 :: (\text{this case}) \):

- \( \Gamma'_2 < (\cdot) \)
  - (this case)\( \Gamma_1; \Delta \models_{\Sigma} P :: (\alpha_i : A_i) \)
  - (by assumption)\( \Gamma_1, \Gamma'_2; \Delta \models_{\Sigma} P :: (\alpha_i : A_i) \)

- \( \Gamma'_3, x_3 : \hat{A} < \Gamma_3, x_3 : \hat{B} \) and \( \Gamma'_3 < \Gamma_3 \) and \( \hat{A} < \hat{B} \)
  - (this case)\( \text{where } \Gamma_2 = \Gamma_3, x_3 : \hat{B} \)
  - (by assumption)\( \Gamma_1, \Gamma_3, x_3 : \hat{B}; \Delta \models_{\Sigma} P :: (\alpha_i : A_i) \)
  - (by I.H.)\( \Gamma_1, \Gamma'_3, x_3 : \hat{B}; \Delta \models_{\Sigma} P :: (\alpha_i : A_i) \)

- \( \Gamma'_3, x'_3 : \hat{A}; \Delta \models_{\Sigma} [x'_3/x_3] P :: (\alpha_i : A_i) \)
  - (by Lemma 13)\( \text{where } x'_3 \text{ fresh} \)
  - (by Lemma 14 and weakening)\( \Gamma_1, \Gamma'_3, x_3 : \hat{A}; \Delta \models_{\Sigma} [x'_3/x_3] [x'_3/x_3] P :: (\alpha_i : A_i) \)

\[ \square \]

**Lemma 8 (Invariant Sub-Configuration in \( \Theta \)).** If \( \Gamma \models_{\Sigma} \Theta_1, \Theta_2 :: \Delta \) and \( \Gamma \models_{\Sigma} \Theta_2 :: \Delta' \), then, for any \( \Gamma' \) and \( \Theta'_2 \) such that \( \Gamma' \models_{\Sigma} \Theta'_2 :: \Delta' \) and \( \Gamma' \models_{\Sigma} \Theta_1, \Theta'_2 :: \Delta \).

**Proof.** By induction on \( \Gamma \models_{\Sigma} \Theta :: \Delta :: (\text{this case}) \):

- \( \Gamma \models_{\Sigma} (\cdot) :: (\cdot) \)
  - Holds vacuously.

- \( \Gamma \models_{\Sigma} \text{proc}(c_i, P_{c_i}), \Theta :: \Delta \)
  - (this case)\( \Gamma \models_{\Sigma} \Delta_2 \models_{\Sigma} P_{c_i} :: (c : C_i) \) and \( (c_2 : \hat{B}) \in \Gamma \) and \( \models_{\Sigma} (C_i, \hat{B}) \text{esync} \)
  - (this case)\( \text{for some } \Delta_2, \Delta_1, C_i, \text{ and } \hat{B} \text{ such that } \Delta = (\Delta_1, c : C_i) \)
  - (this case)\( \Gamma \models_{\Sigma} \Theta :: \Delta_1, \Delta_2 \)

\[ 39 \]

\[ \square \]
(a) \( \Theta_1 = (\cdot) \) and \( \Theta_2 = \text{proc}(c, P_{a_\delta}), \Theta \) and \( \Gamma \vdash_\Sigma \text{proc}(c, P_{a_\delta}), \Theta :: \Delta \) (this subcase)

\[ \Gamma' \triangleright \Gamma \] (by assumption)

\( \Gamma' \vdash_\Sigma \Theta_2' :: \Delta \) (by assumption)

(b) \( \Theta_1 = \text{proc}(c, P_{a_\delta}), \Theta_1' \) and \( \Gamma \vdash_\Sigma \Theta_2 :: \Delta' \) (this subcase)

for some \( \Theta_1' \) such that \( \Theta = \Theta_1', \Theta_2 \)

\[ \Gamma' \vdash_\Sigma \Theta_2 :: \Delta' \] (by assumption)

\[ \Gamma' \triangleright \Gamma \] (by assumption)

\( \Gamma' \vdash_\Sigma \Theta_1', \Theta_2' :: \Delta_1, \Delta_2 \) (by I.H.)

\( \Gamma'; \Delta_2 \vdash_\Sigma P_{\delta_\delta} :: (c : C_{1}) \) (by Lemma 7)

\( \Gamma' \vdash_\Sigma \text{proc}(c, P_{a_\delta}), \Theta_1', \Theta_2' :: \Delta \) (by (T-Θ2))

\( \square \)

**Lemma 9** (Existence of Process for Offered Linear Channel). If \( \Gamma \vdash_\Sigma \Theta :: \Delta \), then, for all \( a_\delta \in \text{dom}(\Delta) \), there exists exactly one \( \text{proc}(a_\delta, P_{a_\delta}) \), for some \( P \), in \( \Theta \).

**Proof.** We prove Lemma 9 by induction \( \Gamma \vdash_\Sigma \Theta :: \Delta \):

- \( \Gamma \vdash_\Sigma (\cdot) :: (\cdot) \) (this case)
  
  Holds vacuously.

- \( \Gamma \vdash_\Sigma \text{proc}(a_\delta, P_{a_\delta}), \Theta :: (\Delta, a_\delta : A_{\delta}) \) (this case)

\[ \Gamma; \Delta' \vdash_\Sigma P_{\delta_\delta} :: (a_\delta : A_{\delta}) \] (this case)

for some \( \Delta' \)

\[ \Gamma \vdash_\Sigma \Theta :: (\Delta, \Delta') \] (this case)

For all \( b_\delta \in \text{dom}(\Delta, \Delta') \), there exists exactly one \( \text{proc}(b_\delta, Q_{\delta_\delta}) \), for some \( Q \), in \( \Theta \). (by I.H.)

There exists exactly one \( \text{proc}(a_\delta, P_{a_\delta}) \) in \( \text{proc}(a_\delta, P_{a_\delta}), \Theta \) that offers along \( a_\delta \). (by well-formedness of configuration)

\( \square \)

**Lemma 10** (Existence of Provider). Writing \( Q(a_{m}) \) for a process term \( Q \) with an occurrence of a channel \( a_{m} \), the following hold:

1. If \( \Gamma \vdash_\Sigma \Lambda; \text{proc}(c_{1}, Q(a_{\delta})), \Theta_1 :: \Gamma; \Delta, \) then either there exists a \( \text{proc}(a_{\delta}, P_{\delta_\delta}) \) in \( \Lambda, \) for some \( P \), or there exists an \( \text{unavail}(a_{\delta}) \) in \( \Lambda \).

2. If \( \Gamma \vdash_\Sigma \Lambda; \text{proc}(c_{1}, Q(a_{\delta})), \Theta_1 :: \Gamma; \Delta, \) then there exists exactly one \( \text{proc}(a_{\delta}, P_{\delta_\delta}) \), for some \( P \), in \( \Theta_1 \).

**Proof.** We prove each case in turn:

1. \( \Gamma \vdash_\Sigma \Lambda; \text{proc}(c_{1}, Q(a_{\delta})), \Theta_1 :: \Gamma; \Delta \) (by assumption)

\[ \Gamma \vdash_\Sigma \Lambda :: \Gamma \text{ and } \Gamma \vdash_\Sigma \text{proc}(c_{1}, Q(a_{\delta})), \Theta_1 :: \Delta \] (by inversion on (T-Ω))

\[ (a_\delta : \hat{A}) \in \Gamma \] (by the meaning of the configuration and process typing judgment)

for some \( \hat{A} \)

\[ \Gamma \vdash_\Sigma \Lambda_1 :: (a_\delta : \hat{A}) \text{ and } \Gamma \vdash_\Sigma \Lambda_2 :: \Gamma_2 \] (by inversion on (T-Λ4))

for some \( \Lambda_1, \Lambda_2, \) and \( \Gamma_1 \) such that \( \Gamma = \Gamma_2, a_\delta : \hat{A} \)

Either \( \Lambda_1 = \text{unavail}(a_{\delta}) \) or \( \Lambda_1 = \text{proc}(a_{\delta}, P_{\delta_\delta}) \) (by inversion on (T-Λ2) and (T-Λ2))

for some \( P \)

2. \( \Gamma \vdash_\Sigma \Lambda; \text{proc}(c_{1}, Q(a_{\delta})), \Theta_1 :: \Gamma; \Delta \) (by assumption)

\[ \Gamma \vdash_\Sigma \text{proc}(c_{1}, Q(a_{\delta})), \Theta_1 :: \Delta \] (by inversion on (T-Ω))

\[ \Gamma; \Delta', a_\delta : A_{\delta} \vdash_\Sigma Q :: (c_{1} : C_{1}) \text{ and } \Gamma \vdash_\Sigma \Theta_1 :: \Delta_1, \Delta', a_\delta : A_{\delta} \] (by inversion on (T-Θ2) and meaning of process typing judgment)

for some \( \Delta', \Delta_1, A_{\delta}, \) and \( C_{1} \) such that \( \Delta = \Delta_1, c_{1} : C_{1} \)

There exists exactly one \( \text{proc}(a_{\delta}, P_{\delta_\delta}) \), for some \( P \), in \( \Theta_1 \) (by Lemma 9)

\( \square \)
### D.2 Preservation

The preservation theorem expresses that the types of the providing linear channels are maintained along transitions and that new shared channels may be allocated and the types of existing shared channels concretized.

**Theorem 3** (Preservation). If \( \Gamma \vdash \Sigma \: \Lambda; \Theta \vdash \Gamma; \Delta \) and \( \Lambda; \Theta \rightarrow \Lambda'; \Theta' \), then \( \Gamma' \vdash \Sigma; \Lambda'; \Theta' \vdash \Delta' \), for some \( \Lambda' \), \( \Theta' \), and \( \Gamma' \) such that \( \Gamma' < \Gamma \).

**Proof.** We prove preservation by induction on the dynamics, constructing a derivation of a well-formed and well-typed configuration \( \Gamma' \vdash \Sigma \: \Lambda''; \Theta'' \vdash \Delta' \), where \( \Lambda'' \) and \( \Theta'' \) are permutations of \( \Lambda' \) and \( \Theta' \), respectively:

**Case:**

\[
\text{proc}(a_i, \text{fwd} \ a_i, b_i) \quad \text{(D-Id)}
\]

\[\Gamma \vdash \Sigma \: \text{unavail}(a_5), \text{unavail}(b_5), \Lambda_1; \Theta_1, \text{proc}(a_i, \text{fwd} \ a_i, b_i), \Theta_2, \text{proc}(b_i, P), \Theta_3 :: \Gamma; \Delta \]

for some \( \Lambda_1, \Theta_1, \Theta_2, \Theta_3 \), and \( \text{proc}(b_i, P) \) (by assumption and Lemma \ref{lemma:proc_1})

\[\Gamma \vdash \Sigma \: \text{unavail}(a_5), \text{unavail}(b_5), \Lambda_1; \Theta_1, \text{proc}(a_i, \text{fwd} \ a_i, b_i), \Theta_2, \text{proc}(b_i, P), \Theta_3 :: \Gamma; \Delta \]

for some \( \Lambda_1, \Theta_1, \Theta_2, \Theta_3 \) (by Lemma \ref{lemma:proc_2})

\[\text{unavail}(a_5), \text{unavail}(b_5), \Lambda_1; \Theta_1, \text{proc}(a_i, \text{fwd} \ a_i, b_i), \Theta_2, \Theta_3 :: \Gamma; \Delta \]

\[\rightarrow \text{unavail}(a_5), \text{unavail}(b_5), [b_5/a_5] \Lambda_1; [b_5/a_5, b_5/a_i] \Theta_1, \text{proc}(b_i, P), [b_5/a_5] (\Theta_2, \Theta_3) \]

\[\Gamma \vdash \Sigma \: \text{unavail}(a_5), \text{unavail}(b_5), \Lambda_1 :: \Gamma \]

\[\Gamma \vdash \Sigma \: \text{unavail}(a_5), \Lambda_1; \Theta_1, \text{proc}(a_i, \text{fwd} \ a_i, b_i), \Theta_2, \Theta_3 :: \Delta \]

\[\Gamma = \Theta = \Lambda_1 \]

\[\Gamma \vdash \Sigma \: \text{unavail}(a_5), \Lambda_1; \Theta_1, \text{proc}(a_i, \text{fwd} \ a_i, b_i), \Theta_2, \Theta_3 :: \Delta \]

\[\Gamma_1 = a_5 : \hat{A} \text{ and } \Gamma_2 = b_5 : \hat{B} \]

\[\Gamma \vdash \Sigma \: \text{proc}(a_i, \text{fwd} \ a_i, b_i), \Theta_2, \Theta_3 :: \Delta \]

\[\Gamma \vdash \Sigma \: \text{proc}(a_i, \text{fwd} \ a_i, b_i), \text{proc}(b_i, P), \Theta_2, \Theta_3 :: \Delta \]

\[\Gamma_1 = \Delta_1 \vdash \text{fwd} \ a_i, b_i :: (a_i : C_i) \]

\[\Gamma \vdash \Sigma : (\Delta_1, a_i : C_i) \]

\[\Delta_1' = b_i : C_i \]

\[\Gamma \vdash \Sigma : (\Delta_1, b_i : C_i) \]

\[\Gamma_1 = \Delta_1' \vdash \text{sync} \quad \text{(by inversion on (T-\text{Id}))} \]

\[\Gamma \vdash \Sigma : (\Delta_1, B_i) \]

\[\Gamma_1 = \Delta_1' \vdash \text{sync} \quad \text{(by inversion on (T-\text{Id}))} \]

\[\Gamma \vdash \Sigma : (\Delta_1', B_i) \]

Since \( a_5 = \hat{A} \) and \( b_5 = \hat{B} \) there are 9 combinations of 2 out of \( \bot, \top, \text{and } \tau \), and \( \tau^* \text{A}_i / \tau^* \text{B}_i \), for some \( \text{A}_i \) and \( \text{B}_i \). We consider each case, collating several cases that have the same proof:

**Subcases:** \( \hat{A} \geq \hat{B} \)

- \( a_5 : \bot \text{ and } b_5 : \bot \)
- \( a_5 : \tau^* \text{A}_i \text{ and } b_5 : \bot \)
- \( a_5 : \tau^* \text{A}_i \text{ and } b_5 : \tau^* \text{B}_i \text{ and } \text{A}_i = \text{B}_i \)
- \( a_5 : \top \text{ and } b_5 : \bot \)
- \( a_5 : \top \text{ and } b_5 : \tau^* \text{B}_i \)
- \( a_5 : \top \text{ and } b_5 : \top \)

\[\Gamma \vdash \Sigma [b_5/a_5] (\Theta_2, \Theta_3) :: (\Delta_1, \Delta_1') \]

\[\Gamma \vdash \Sigma \: \text{proc}(b_i, P), [b_5/a_5] (\Theta_2, \Theta_3) :: (\Delta_1, b_i : C_i) \]

\[\Gamma \vdash \Sigma \: [b_5/a_5, b_5/a_i] \Theta_1, \text{proc}(b_i, P), [b_5/a_5] (\Theta_2, \Theta_3) :: \Delta \]

\[\text{(by Lemma \ref{lemma:proc_1} and Lemma \ref{lemma:proc_2})} \]
\[\Gamma \vdash [b_b/a_s] \Lambda_1 :: \Gamma_3 \quad \text{(by Lemma 2.3 since } \text{proc}(a_s, \bot) \notin \Lambda_1 \text{ and } \text{unavail}(a_s) \notin \Lambda_1)\]
\[\Gamma \vdash \text{unavail}(a_s), \text{unavail}(b_s), [b_b/a_s] \Lambda_1 :: \Gamma \quad \text{(by (T-\Lambda))}\]
\[\Gamma \vdash \text{unavail}(a_s), \text{unavail}(b_s), [b_b/a_s] \Lambda_1; [b_b/a_s, b_b/a_s] \Theta_1, \text{proc}(b_s, P), [b_b/a_s] (\Theta_2, \Theta_3) :: \Gamma; \Delta \quad \text{(by (T-\Omega) and well-formedness maintained)}\]

**Subcase:** \(a_s : \uparrow^s A_1 \) and \(b_s : \uparrow^s B_1 \) and \(A_i \neq B_i\)

\[
\Gamma' \vdash (C_i, \bot) \text{sync} \quad \text{(by Lemma 3.2 since } \Gamma' \vdash \text{sync}(C_i, \uparrow^s B_1) \text{, } \Gamma' \vdash \text{sync}(C_i, \bot) \text{ sync), } \bot \leq \uparrow^s B_1, \text{ proc} (b_s, \bot) \notin \Lambda_1, \text{ and unavail}(b_s) \notin \Lambda_1)\]

\[\Gamma' \vdash [b_b/a_s] (\Theta_2, \Theta_3) :: (\Delta_1, \Delta''_s) \quad \text{(by Lemma 3.1)}\]

\[
\Gamma' = [b_b : \bot/b_s : \uparrow^s B_1] \Delta' \quad \text{(by Definition 2 since } \prec \text{ is reflexive)}\]

\[\Gamma' \vdash \text{unavail}(a_s), \text{unavail}(b_s), [b_b/a_s] \Lambda_1 :: \Gamma' \quad \text{(by (T-\Lambda))}\]

\[\Gamma' \vdash \text{unavail}(a_s), \text{unavail}(b_s), [b_b/a_s] \Lambda_1; [b_b/a_s, b_b/a_s] \Theta_1, \text{proc}(b_s, P), [b_b/a_s] (\Theta_2, \Theta_3) :: \Gamma'; \Delta \quad \text{(by (T-\Omega) and well-formedness maintained)}\]

**Subcases: \(\hat{A} \leq \hat{B} \)**

\[
a_s : \bot \quad \text{and} \quad b_s : \uparrow^s B_1 \quad \text{(by Lemma 3.1)}\]

\[
a_s : \bot \quad \text{and} \quad b_s : \top \quad \text{(by (T-\Omega))}\]

\[
a_s : \uparrow^s A_1 \quad \text{and} \quad b_s : \top \quad \text{(by (T-\Omega))}\]

\[\Gamma' \vdash (\Theta_2, \Theta_3) :: (\Delta_1, \Delta''_s) \quad \text{(by Lemma 3.1)}\]

\[
\Gamma' = [b_b : \hat{A}/b_s : \hat{B}] \Gamma \quad \text{(by Definition 2 since } \prec \text{ is reflexive)}\]

\[\Gamma' \vdash \Lambda_1 :: \Gamma_3 \quad \text{(by Lemma 3.2 since } \Gamma' \vdash \text{sync}(C_i, \hat{B}) \text{ sync, } \Gamma' \vdash \text{sync}(C_i, \hat{A}) \text{ sync, and } \hat{A} \leq \hat{B})\]

\[\Gamma' \vdash [b_b/a_s] (\Theta_2, \Theta_3) :: (\Delta_1, \Delta''_s) \quad \text{(by (T-\Omega))}\]

\[
[b'_s : \hat{A}/b_s : \hat{B}] \Gamma' \vdash \text{sync}(C_i, \hat{A}) \quad \text{(by Definition 2 since } \prec \text{ is reflexive)}\]

\[\Gamma' \vdash \text{proc}(b_s, P), [b_b/a_s] (\Theta_2, \Theta_3) :: (\Delta_1, b_s : \Lambda_1) \quad \text{(by (T-\Omega))}\]

\[\Gamma' \vdash \text{proc}(b_s, P), [b_b/a_s] (\Theta_2, \Theta_3) :: (\Delta, \hat{B}) \quad \text{(by Lemma 3.1)}\]

\[\Gamma' \vdash \text{proc}(b_s, P), [b_b/a_s] (\Theta_2, \Theta_3) :: (\Delta, \hat{A}) \quad \text{(by (T-\Omega))}\]

\[\Gamma' \vdash \text{unavail}(a_s), \text{unavail}(b_s), [b_b/a_s] \Lambda_1; [b_b/a_s, b_b/a_s] \Theta_1, \text{proc}(b_s, P), [b_b/a_s] (\Theta_2, \Theta_3) :: \Gamma'; \Delta \quad \text{(by (T-\Omega) and well-formedness maintained)}\]

**Case:**

\[
\text{proc}(a_s, \text{fwd} a_s b_s) \quad \text{(D-ID)}
\]

\[
\rightarrow \text{unavail}(a_s), a_s = b_s
\]

42
Γ ⊨ Σ proc(\(a_s, \text{fwd} \ a_s \ b_s\)), \(\Lambda_1; \Theta :: \Gamma; \Delta\) (by assumption)
for some \(\Lambda_1\)

Γ ⊨ Σ proc(\(a_s, \text{fwd} \ a_s \ b_s\)), \(\Lambda_1; \Theta :: \Gamma; \Delta\) is well-formed (by I.H.)

\[ \text{proc}(a_s, \text{fwd} \ a_s \ b_s), \Lambda_1; \Theta \rightarrow \text{unavail}(a_s), \ [b_s/a_s] \Lambda_1; \ [b_s/a_s] \Theta \] (this case)

Γ ⊨ Σ proc(\(a_s, \text{fwd} \ a_s \ b_s\)), \(\Lambda_1 :: \Gamma\) (by inversion on (T-Ω))

Γ ⊨ Σ proc(\(a_s, \text{fwd} \ a_s \ b_s\)) :: \(\Gamma_1\) and Γ ⊨ Σ \(\Lambda_1 :: \Gamma_2\) (by inversion on (T-Λ\(\_A_1\)))
for some \(\Gamma_1\) and \(\Gamma_2\) such that Γ = \(\Gamma_1, \Gamma_2\)

\(\Gamma_1 = a_s : \uparrow^s A_i\) and Γ ⊨ Σ \(a_s \ b_s :: (a_s : \uparrow^s A_i)\) and ⊨ Σ (\(\uparrow^s A_i, \top\)) esync for some \(A_k\)
(b_\(s : \hat{B}\) ⊆ Γ and \(\hat{B} \leq \uparrow^s A_i\) (by inversion on (T-Ids\(\_S\)))
for some \(\hat{B}\)

**Subcase:** \(b_s : \bot\)
(\(\Lambda \leq \uparrow^s A_i\) and \(\text{proc}(a_s, \bot) \notin \Lambda_1\) and \(\text{unavail}(a_s) \notin \Lambda_1\))

Γ ⊨ Σ \([b_s/a_s] \Lambda_1 :: \Gamma_2\) (by Lemma 23 since \(\bot \leq \uparrow^s A_i\) and \(\text{proc}(a_s, \bot) \notin \Lambda_1\) and \(\text{unavail}(a_s) \notin \Lambda_1\))

Γ ⊨ Σ \(\text{unavail}(a_s) :: (a_s : \uparrow^s A_i)\) (by (T-Λ\(\_A_3\)))

Γ ⊨ Σ \(\text{unavail}(a_s), \ [b_s/a_s] \Lambda_1 :: \Gamma\) (by (T-Λ\(\_A_4\)))

Γ ⊨ Σ \(\Theta :: \Delta\) (by inversion on (T-Ω))

Γ ⊨ Σ \([b_s/a_s] \Theta :: \Delta\) (by Lemma 23 since \(\bot \leq \uparrow^s A_i\))

Γ ⊨ Σ \(\text{unavail}(a_s), \ [b_s/a_s] \Lambda_1; \ [b_s/a_s] \Theta :: \Gamma; \Delta\) (by (T-Ω) and well-formedness maintained)

**Subcase:** \(b_s : \uparrow^s A_i\)
(\(\uparrow^s A_i \leq \uparrow^s A_i\) and \(\text{proc}(a_s, \bot) \notin \Lambda_1\) and \(\text{unavail}(a_s) \notin \Lambda_1\))

Γ ⊨ Σ \([b_s/a_s] \Lambda_1 :: \Gamma_2\) (by Lemma 23 since \(\uparrow^s A_i \leq \uparrow^s A_i\) and \(\text{proc}(a_s, \bot) \notin \Lambda_1\) and \(\text{unavail}(a_s) \notin \Lambda_1\))

Γ ⊨ Σ \(\text{unavail}(a_s) :: (a_s : \uparrow^s A_i)\) (by (T-Λ\(\_A_3\)))

Γ ⊨ Σ \(\text{unavail}(a_s), \ [b_s/a_s] \Lambda_1 :: \Gamma\) (by (T-Λ\(\_A_4\)))

Γ ⊨ Σ \(\Theta :: \Delta\) (by inversion on (T-Ω))

Γ ⊨ Σ \([b_s/a_s] \Theta :: \Delta\) (by Lemma 23 since \(\uparrow^s A_i \leq \uparrow^s A_i\))

Γ ⊨ Σ \(\text{unavail}(a_s), \ [b_s/a_s] \Lambda_1; \ [b_s/a_s] \Theta :: \Gamma; \Delta\) (by (T-Ω) and well-formedness maintained)

**Case:**

\[ \text{proc}(a_s, x_i \leftarrow X_i \leftarrow \overline{r_i}, \overline{s_i} :: Q_{\bar{x}}), \ !\text{def}(x'_i :: A_i \leftarrow X_i \leftarrow y_i :: B_i :: y_i :: \overline{B}_i = \overline{P}_{x'_i, \overline{y}_i, \overline{B}_i}) \] (D-SPAWN\(\_\_L\))

\[ \rightarrow \text{proc}(b_s, \ [h_i/x'_i] Q_{\bar{x}}), \ \text{proc}(b_s, \ [h_i/x'_i, \overline{r_i}/\overline{y}_i, \overline{s_i}/\overline{y}_i] \overline{P}_{x'_i, \overline{y}_i, \overline{B}_i}), \ \text{unavail}(b_s) \] (b fresh)

Γ ⊨ Λ; \(\Theta_1, \ \text{proc}(a_s, x_i \leftarrow X_i \leftarrow \overline{r_i}, \overline{s_i} :: Q_{\bar{x}}), \ \Theta_2 :: \Gamma; \Delta\) (by assumption)
for some \(\Theta_1\) and \(\Theta_2\), and where \(!\text{def}(x'_i :: A_i \leftarrow X_i \leftarrow y_i :: B_i :: y_i :: \overline{B}_i = \overline{P}_{x'_i, \overline{y}_i, \overline{B}_i})\)

Γ ⊨ Λ; \(\Theta_1, \ \text{proc}(a_s, x_i \leftarrow X_i \leftarrow \overline{r_i}, \overline{s_i} :: Q_{\bar{x}}), \ \Theta_2 :: \Gamma; \Delta\) is well-formed (by I.H.)

\(\Lambda; \Theta_1, \ \text{proc}(a_s, x_i \leftarrow X_i \leftarrow \overline{r_i}, \overline{s_i} :: Q_{\bar{x}}), \ \Theta_2 \rightarrow \text{unavail}(b_s), \ \Lambda; \Theta_1, \ \text{proc}(a_s, \ [h_i/x_i] Q_{\bar{x}}), \ \text{proc}(b_s, \ [h_i/x'_i, \overline{r_i}/\overline{y}_i, \overline{s_i}/\overline{y}_i] \overline{P}_{x'_i, \overline{y}_i, \overline{B}_i}), \ \Theta_2\) (this case)

Γ ⊨ Λ :: \(\Gamma\) (by inversion on (T-Ω))

Γ ⊨ Λ; \(\Theta_1, \ \text{proc}(a_s, x_i \leftarrow X_i \leftarrow \overline{r_i}, \overline{s_i} :: Q_{\bar{x}}), \ \Theta_2 :: \Delta\) (by inversion on (T-Ω))

Γ ⊨ Π \(\Theta_1, \ \text{proc}(a_s, x_i \leftarrow X_i \leftarrow \overline{r_i}, \overline{s_i} :: Q_{\bar{x}}), \ \Theta_2 :: (\Delta_1, a_i : C_i)\) (by Lemma 6)
for some \(\Delta_1\) and \(C_i\)

Γ; \(\Delta'_1 \vdash x_i \leftarrow X_i \leftarrow \overline{r_i}, \overline{s_i} :: Q_{\bar{x}} :: (a_i : C_i)\) (by inversion on (T-Θ_2))
for some \(\Delta'_1\)

\(a_s : \hat{D}\) ∈ Γ and ⊨ Σ \((C_i, \hat{D})\) esync (by inversion on (T-Θ_2))
for some $\hat{D}$

$$(x'_1 : A_1 \leftarrow X_1 \leftarrow \hat{y}_1 : B_1, \hat{y}_1 : B_1 = P_{x'_1[B_1]} ) \in \Sigma$$

(by inversion on (T-SPAWNLL) and since $\text{def}(x'_1 : A_1 \leftarrow X_1 \leftarrow \hat{y}_1 : B_1, \hat{y}_1 : B_1 = P_{x'_1[B_1]})$)

$\Gamma ; \Delta_2, x_1 : A_1 \vdash \Sigma Q_{x_1} :: (a_1 : C_1)$

where $\Delta_2 = \Delta'_1 = \Gamma$ and $\hat{c}_2 : \bar{B}$ and $\bar{c}_2 : \bar{B} \subseteq \Gamma$ for some $\bar{B}$ such that $\bar{B} \leq \bar{B}_s$

$\Gamma \vdash \Sigma \Theta_2 :: \Delta_1, \Delta'_1$ (by inversion on (T-Theta))

$\vdash (A_1, \top) \text{ esync}$

$\bar{y}_2 : B_2, \bar{y}_2 : B_2 = P_{x'_2[B_2]}$ (by (T-Sigma))

$\Gamma \vdash \Delta_2, b_1 : A_1 \vdash \Sigma [x'_2/\bar{y}_2, \bar{y}_2/x'_2, \bar{c}_2/\bar{c}_2] P_{x'_2[B_2]} :: (b_1 : A_1)$

where $\bar{c}_2 : \bar{B}$ and $\bar{c}_2 : \bar{B} \subseteq \Gamma$ for some $\bar{B}$ such that $\bar{B} \leq \bar{B}_s$

$\Gamma' \vdash \Sigma \Theta_1 :: \Delta, \Theta_2 :: \Delta_1, \Delta_2, b_1 : A_1$ (by Lemma 1-1 and weakening and since $\bar{c}_2 : \bar{B} \subseteq \Gamma$

$\Gamma' \vdash \Sigma \Theta_2 :: \Delta, \Theta_2 :: \Delta_1, \Delta_2, b_1 : A_1$ (by (T-Theta) and weakening)

$\Gamma' \vdash \Sigma \Theta_2 :: \Delta, \Theta_2 :: \Delta_1, \Delta_2, b_1 : A_1$

(\text{by Definition 2} since $<$ is reflexive)

Case:

$$\text{proc}(a_1, x_2 \leftarrow X_2 \leftarrow \bar{c}_2 : Q_{x_2}), !\text{def}(x'_2 : A_1 \leftarrow X_2 \leftarrow \bar{y}_2 : B_2 = P_{x'_2[B_2]} )$$

(D-SPAWNLS)

\begin{equation}
\Gamma \vdash \Sigma \Lambda ; \Theta_1, \text{proc}(a_1, x_2 \leftarrow X_2 \leftarrow \bar{c}_2 : Q_{x_2}), \Theta_2 :: \Delta \quad (b \text{ fresh})
\end{equation}

(by assumption)

$\Gamma \vdash \Sigma \Lambda ; \Theta_1, \text{proc}(a_1, x_2 \leftarrow X_2 \leftarrow \bar{c}_2 : Q_{x_2}), \Theta_2 :: \Delta$ (by I.H.)

$\Lambda ; \Theta_1, \text{proc}(a_1, x_2 \leftarrow X_2 \leftarrow \bar{c}_2 : Q_{x_2}), \Theta_2 :: \Delta$ (this case)

(by inversion on (T-Theta))

(by inversion on (T-Theta))

(by Lemma 6)

$\Gamma \vdash \Sigma \Theta_1 :: \Delta, \text{proc}(a_1, x_2 \leftarrow X_2 \leftarrow \bar{c}_2 : Q_{x_2}), \Theta_2 :: \Delta$ (by inversion on (T-Theta))

$\Gamma \vdash \Sigma \Theta_1 :: \Delta, \text{proc}(a_1, x_2 \leftarrow X_2 \leftarrow \bar{c}_2 : Q_{x_2}), \Theta_2 :: \Delta$ (by inversion on (T-Theta))

$\Gamma \vdash \Sigma \Theta_1 :: \Delta, \text{proc}(a_1, x_2 \leftarrow X_2 \leftarrow \bar{c}_2 : Q_{x_2}), \Theta_2 :: \Delta$ (by inversion on (T-Theta))

(by inversion on (T-SPAWNLL) and since $\text{def}(x'_1 : A_1 \leftarrow X_1 \leftarrow \hat{y}_1 : B_1, \hat{y}_1 : B_1 = P_{x'_1[B_1]})$)

$\Gamma, x_1 : A_1 ; \Delta'_1 \vdash Q_{x_1} :: (a_1 : C_1)$

(by inversion on (T-SPAWNLL))

$\Gamma \vdash \Sigma \Theta_2 :: \Delta_1, \Delta'_1$ (by inversion on (T-Theta))
\[\vdash_{\Sigma} (A_5, T) \text{ sync} \]

\[\frac{y_b : B_b, \vdash_{\Sigma} P_{x'_5, \overline{y_b}} :: (x'_5 : A_5)}{\vdash_{\Sigma} P_{x'_5, \overline{y_b}} :: (x'_5 : A_5)} \text{ (by inversion on } (T-\Sigma_2)) \]

\[c'_5 : \overline{B}, b_5 : A_5 \vdash_{\Sigma} \left[ \frac{b_5/x'_5, \overline{c'_5/\overline{y_b}}}{P_{x'_5, \overline{y_b}}} \right] :: (b_5 : A_5) \text{ (by Lemma 11 and weakening and since } \overline{c'_5} : \overline{B} \subseteq \Gamma) \]

\[\Gamma, b_5 : A_5 \vdash_{\Sigma} \left[ \frac{\overline{c'_5/c'_5}}{(b_5/x'_5, \overline{c'_5/\overline{y_b}}) P_{x'_5, \overline{y_b}}} \right] :: (b_5 : A_5) \text{ (by Lemma 13 and weakening and since } \overline{c'_5} : \overline{B} \subseteq \Gamma) \]

\[\Gamma, b_5 : A_5, \Delta' \vdash_{\Sigma} \left[ \frac{b_5/x_5}{Q_{x_5}} \right] :: (a_t : C_t) \text{ (by (T-\Theta_2) and weakening)} \]

\[\Gamma' \not\in \Gamma \text{ (by Definition 2 since } \not\in \text{ is reflexive)} \]

\[\Gamma' \vdash_{\Sigma} \Theta_1, \text{ proc}(a_t, [b_5/x_5]Q_{x_5}), \Theta_2 :: \Delta \text{ (by Lemma 8 since } \Gamma' \not\in \Gamma) \]

\[\Gamma' \vdash_{\Sigma} \text{ proc}(b_5, [b_5/x'_5, \overline{c'_5/\overline{y_b}}] P_{x'_5, \overline{y_b}}), \text{ L} :: \Gamma' \text{ (by (T-A_4) and weakening)} \]

\[\Gamma' \vdash_{\Sigma} \text{ proc}(b_5, [b_5/x'_5, \overline{c'_5/\overline{y_b}}] P_{x'_5, \overline{y_b}}), \text{ L} : \Theta_1, \text{ proc}(a_t, [b_5/x_5]Q_{x_5}), \Theta_2 :: \Gamma' ; \Delta \text{ (by (T-\Omega) and well-formedness maintained)} \]

**Case:**

\[\text{proc}(a_t, x_t \leftarrow X_t \leftarrow \overline{c_t} ; Q_{x_t}), \text{ !def}(x'_5 : A_5 \leftarrow X_t \leftarrow \overline{y_b} : \overline{B_b} = P_{x'_5, \overline{y_b}}) \text{ (D-SPAWN\Sigma_5 \Sigma)} \]

\[\rightarrow \text{proc}(a_t, [b_5/x_5]Q_{x_5}), \text{ proc}(b_5, [b_5/x'_5, \overline{c'_5/\overline{y_b}}] P_{x'_5, \overline{y_b}}) \text{ (by assumption)} \]

\[\Gamma \vdash_{\Sigma} \text{proc}(a_t, x_t \leftarrow X_t \leftarrow \overline{c_t} ; Q_{x_t}), \text{ L} : \Theta :: \Gamma ; \Delta \text{ (by I.H.)} \]

\[\Gamma \vdash_{\Sigma} \text{proc}(b_5, [b_5/x'_5, \overline{c'_5/\overline{y_b}}] P_{x'_5, \overline{y_b}}), \text{ L} : \Theta :: \Gamma ; \Delta \text{ (this case)} \]

\[\Gamma \vdash_{\Sigma} \Theta :: \Delta \text{ (by inversion on } (T-\Omega)) \]

\[\Gamma \vdash_{\Sigma} \text{proc}(a_t, x_t \leftarrow X_t \leftarrow \overline{c_t} ; Q_{x_t}) :: \Gamma_1 \text{ and } \Gamma \vdash_{\Sigma} \Lambda_1 :: \Gamma_2 \text{ (by inversion on } (T-A_4)) \]

\[\Gamma_1 = a_t : \overline{c_1}_t \text{ and } \Gamma \vdash_{\Sigma} x_t \leftarrow X_t \leftarrow \overline{c_t} ; Q_{x_5} :: (a_t : \overline{c_1}_t C_t) \text{ and } \vdash_{\Sigma} (\overline{c_1}_t C_t, T) \text{ sync (by inversion on } (T-A_2)) \]

\[\text{for some } C_t \text{ (by inversion on } (T-\text{SPAWN\Sigma_5 \Sigma}) \text{ and since } \text{!def}(x'_5 : A_5 \leftarrow X_t \leftarrow \overline{y_b} : \overline{B_b} = P_{x'_5, \overline{y_b}})) \]

\[\Gamma, x_5, A_5 \vdash_{\Sigma} Q_{x_5} :: (a_t : \overline{c_1}_t C_t) \text{ and } \overline{c_t} : \overline{B} \subseteq \Gamma \text{ for some } \overline{B} \text{ such that } \overline{B} \subseteq \overline{B_5} \text{ (by inversion on } (T-\text{SPAWN\Sigma_5 \Sigma}) \text{ (by inversion on } (T-\Sigma_2)) \text{ (by inversion on } (T-\Sigma_2)) \text{ (by Lemma 11 and weakening and since } \overline{c}_5 : \overline{B} \subseteq \Gamma) \]

\[\vdash_{\Sigma} (A_5, T) \text{ sync} \]

\[\frac{y_b : B_b, \vdash_{\Sigma} P_{x'_5, \overline{y_b}} :: (x'_5 : A_5)}{\vdash_{\Sigma} P_{x'_5, \overline{y_b}} :: (x'_5 : A_5)} \text{ (by inversion on } (T-\Sigma_2)) \]

\[c'_5 : \overline{B}, b_5 : A_5 \vdash_{\Sigma} \left[ \frac{b_5/x'_5, \overline{c'_5/\overline{y_b}}}{P_{x'_5, \overline{y_b}}} \right] :: (b_5 : A_5) \text{ (by Lemma 17) \text{ (by (T-A_2))}} \]

\[\Gamma', \theta \in \Gamma \text{ (by Definition 2 since } \theta \not\in \text{ is reflexive)} \]

\[\Gamma' \vdash_{\Sigma} \text{proc}(b_5, [b_5/x'_5, \overline{c'_5/\overline{y_b}}] P_{x'_5, \overline{y_b}}), \text{ L} :: (\Gamma_2, b_5 : A_5) \text{ (by (T-A_4) and weakening)} \]

\[\Gamma' \vdash_{\Sigma} \text{proc}(a_t, [b_5/x_5]Q_{x_5}) :: (a_t : \overline{c_1}_t C_t) \text{ (by (T-A_2))} \]
\[ \Gamma' \vdash \text{proc}(a_2, [a_3/x_2] Q_{x_3}), \text{proc}(b_2, [b_3/x_3', \overline{x_3}/y_3] P_{x_3}, y_3), \Lambda_1 \vdash \Gamma' \] (by (T-A_4))

\[ \Gamma' \vdash \text{proc}(a_2, [a_3/x_2] Q_{x_3}), \text{proc}(b_2, [b_3/x_3', \overline{x_3}/y_3] P_{x_3}, y_3), \Lambda_1; \Theta \vdash \Gamma'; \Delta \] (by (T-\Omega) and weakening and well-formedness maintained)

**Case:**

\[
\text{proc}(c_1, \ x_3 \leftarrow \text{release} \ a_1; \ Q_{x_3}), \ \text{proc}(a_2, \ x_3 \leftarrow \text{detach} \ a_1; \ P_{x_3}), \ \text{unavail}(a_3)
\]

\[ \rightarrow \ \text{proc}(c_1, [a_3/x_3] Q_{x_3}), \ \text{proc}(a_2, [a_3/x_3] P_{x_3}) \] (D-\(\downarrow^5_i\) - release/detach)

\[ \Gamma \vdash \text{unavail}(a_3), \ \Lambda_1; \ \Theta_1, \ \text{proc}(c_1, \ x_3 \leftarrow \text{release} \ a_1; \ Q_{x_3}), \ \Theta_2, \ \text{proc}(a_2, \ x_3 \leftarrow \text{detach} \ a_1; \ P_{x_3}), \ \Theta_3 \vdash \Gamma, \ \Delta \] (by assumption)

\[ \Gamma \vdash \text{unavail}(a_3), \ \Lambda_1; \ \Theta_1, \ \text{proc}(c_1, \ x_3 \leftarrow \text{release} \ a_1; \ Q_{x_3}), \ \Theta_2, \ \text{proc}(a_2, \ x_3 \leftarrow \text{detach} \ a_1; \ P_{x_3}), \ \Theta_3 \vdash \Gamma, \ \Delta \] is well-formed (by I.H.)

\[ \Gamma \vdash \text{unavail}(a_3), \ \Lambda_1; \ \Theta_1, \ \text{proc}(c_1, \ x_3 \leftarrow \text{release} \ a_1; \ Q_{x_3}), \ \text{proc}(a_2, \ x_3 \leftarrow \text{detach} \ a_1; \ P_{x_3}), \ \Theta_2, \ \Theta_3 \vdash \Gamma, \ \Delta \] (by Lemma 5)

\[ \text{unavail}(a_3), \ \Lambda_1; \ \Theta_1, \ \text{proc}(c_1, \ x_3 \leftarrow \text{release} \ a_1; \ Q_{x_3}), \ \text{proc}(a_2, \ x_3 \leftarrow \text{detach} \ a_1; \ P_{x_3}), \ \Theta_2, \ \Theta_3 \vdash \] (this case)

\[ \Gamma \vdash \text{unavail}(a_3), \ \Lambda_1 \vdash \Gamma \] (by inversion on (T-\Omega))

\[ \Gamma \vdash \text{unavail}(a_3) \vdash \Gamma_1 \text{ and } \Gamma \vdash \Lambda_1 \vdash \Gamma_2 \] (by inversion on (T-A_4))

\[ \Gamma_1 = a_3; \ \tilde{B} \] (by inversion on (T-A_3))

\[ \Gamma \vdash \Theta_1, \ \text{proc}(c_1, \ x_3 \leftarrow \text{release} \ a_1; \ Q_{x_3}), \ \text{proc}(a_2, \ x_3 \leftarrow \text{detach} \ a_1; \ P_{x_3}), \ \Theta_2, \ \Theta_3 \vdash \Delta \] (by inversion on (T-\Omega))

\[ \Gamma \vdash \Theta_1, \ \text{proc}(c_1, \ x_3 \leftarrow \text{release} \ a_1; \ Q_{x_3}), \ \text{proc}(a_2, \ x_3 \leftarrow \text{detach} \ a_1; \ P_{x_3}), \ \Theta_2, \ \Theta_3 \vdash (\Delta_1, c_1 : C_1) \] (by Lemma 6)

\[ \Gamma \vdash \text{unavail}(a_3), \ \Lambda_1 \vdash \Gamma \] (by inversion on (T-\Omega))

\[ \text{proc}(c_1, \ x_3 \leftarrow \text{release} \ a_1; \ Q_{x_3}), \ \text{proc}(a_2, \ x_3 \leftarrow \text{detach} \ a_1; \ P_{x_3}), \ \Theta_2, \ \Theta_3 \vdash \] (by Lemma 5)

\[ \Gamma ; \ \Delta'_1 \vdash x_3 \leftarrow \text{release} \ a_1; \ Q_{x_3} : (c_1 : C_1) \text{ and } (c_3 : \tilde{D}) \vdash \Gamma \text{ and } \vdash \text{sync}(C_1, \tilde{D}) \] (by inversion on (T-\Theta_2))

\[ \text{for some } \Delta'_1 \text{ and } \tilde{D} \text{ and } \Delta'_2 \vdash \text{sync}(C_1, \tilde{D}) \text{ is impossible according to the rules in Figure 5} \]

\[ \Delta'_1 = \Delta_2, a_1: \downarrow^5_i A_3 \text{ and } \Gamma, x_3 : A_3 ; \Delta_2 \vdash \text{sync}(c_1 : C_1) \] (by inversion on (T-\downarrow^5_i L))

\[ \Gamma \vdash \text{proc}(a_1, \ x_3 \leftarrow \text{detach} \ a_1; \ P_{x_3}), \ \Theta_2, \ \Theta_3 \vdash (\Delta_1, \Delta_2, \ a_1 : \downarrow^5_i A_4) \] (by inversion on (T-\Theta_2))

\[ \Gamma ; \ \Delta'_1 \vdash x_3 \leftarrow \text{detach} \ a_1; \ P_{x_3} : (a_1 : \downarrow^5_i A_3) \text{ and sync}(\downarrow^5_i A_3, \tilde{B}) \text{ sync} \] (by inversion on (T-\Theta_2) and since \((a_3 : \tilde{B}) \in \Gamma\))

\[ \Delta'_2 = \vdash \text{sync}(\downarrow^5_i A_3, \bot) \text{ sync} \text{ is impossible according to the rules in Figure 16} \]

**Subcase:** \(\tilde{B} = \uparrow^5_i B_k\), for some \(B_k\), or \(\tilde{B} = \top\)

Then, \(\vdash \text{sync}(\downarrow^5_i A_3, \uparrow^5_i B_k)\) sync. Consequently, the type \(A_3\) of the continuation \(P_{x_3}\) must be \(\uparrow^5_i B_k\).

\[ A_3 = \uparrow^5_i B_k \] (by \(\vdash \text{sync}(\downarrow^5_i A_3, \tilde{B})\) sync)

\[ \vdash \text{sync}(\downarrow^5_i B_k, \top) \text{ sync} \] (by inversion on (T-ESYNC_{\downarrow^5_i})) since \(\vdash \text{sync}(\downarrow^5_i A_3, \uparrow^5_i B_k)\) sync

\[ \Gamma, a'_2 : \uparrow^5_i B_k \vdash [a'_2/x_3] P_{x_3} : (a'_2 : \uparrow^5_i B_k) \] (by Lemma 5)

\[ \text{where } a'_2 \text{ fresh} \] (by inversion on (T-\nearrow^5_i-1) since \(\vdash \text{sync}(\downarrow^5_i A_3, \uparrow^5_i B_k)\) sync)

\[ \Gamma \vdash \text{proc}(a_2, [a_2/x_3] P_{x_3}) : (a_2 : \uparrow^5_i B_k) \] (by Lemma 5)

\[ \Gamma \vdash \text{proc}(a_2, [a_3/x_3] P_{x_3}) : (a_3 : \uparrow^5_i B_k) \] (by (T-A_4) and since \(\text{proc}(a_3, \bot) \notin \Lambda_1\) by well-formedness of \(\Lambda\))

46
Subcase: $\bar{B} = \top$
Then, $\vdash_{\Sigma} (\downarrow_i A_s, \top) \text{ sync}$. Consequently, $\Gamma$ must be updated as follows: $[a_s : A_s/a_s : \top] \Gamma$.

(by induction on rules in Figure 16 rule (T-ESYNC;i=1) in particular)

\[ \Gamma \vdash_{\Sigma} \Theta_2, \Theta_3 :: (\Delta_1, \Delta_2) \text{ and } \Gamma' \vdash_{\Sigma} \Lambda_1 :: \Gamma_2 \]

(by Lemma 3 and 32 since $\vdash_{\Sigma} (\downarrow_i A_s, \top) \text{ sync}$ and $\vdash_{\Sigma} (\downarrow_i A_s, A_s) \text{ sync}$)

(by Definition 2 since $\prec$ is reflexive)

(by Lemma 15 and weakening)

(by Lemma 16 since $(a_s : A_s) \in \Gamma'$)

(by inversion on (T-ESYNC;i=2) since $\vdash_{\Sigma} (\downarrow_i A_s, \top) \text{ sync}$)

(by (T-A2))

(by (T-A4) and since $\vdash_{\Sigma} (\downarrow_i A_s, \top) \text{ sync}$)

(by (T-\Theta_2) and weakening)

(by Lemma 8 since $\Gamma' \prec \Gamma$)

(by (T-\Theta_3) and weakening)

(by Lemma 8 since $\Gamma' \prec \Gamma$)

(by (T-\Theta_3) and weakening)

Case:

\[ \text{proc}(c_i, x_i \leftarrow \text{acquire } a_s; Q_{x_i}), \text{proc}(a_s, x_i \leftarrow \text{acquire } a_s; P_{x_i}) \]

\[ \longrightarrow \text{proc}(c_i, [a_s/x_i] Q_{x_i}), \text{proc}(a_s, [a_s/x_i] P_{x_i}), \text{unavail}(a_s) \]

(by assumption)

\[ \Gamma \vdash_{\Sigma} \text{proc}(c_i, x_i \leftarrow \text{acquire } a_s; P_{x_i}), \Lambda_1 : \Theta_1, \text{proc}(c_i, x_i \leftarrow \text{acquire } a_s; Q_{x_i}), \Theta_2 : \Gamma \]

(by I.H.)

\[ \text{proc}(a_s, x_i \leftarrow \text{acquire } a_s; P_{x_i}), \Lambda_1 : \Theta_1, \text{proc}(c_i, x_i \leftarrow \text{acquire } a_s; Q_{x_i}), \Theta_2 \]

\[ \longrightarrow \text{unavail}(a_s), \Lambda_1 : \Theta_1, \text{proc}(c_i, [a_s/x_i] Q_{x_i}), \text{proc}(a_s, [a_s/x_i] P_{x_i}), \Theta_2 \]

(by inversion on (T-\Omega))

(by inversion on (T-A4))

(by inversion on (T-A2))
for some $A_i$

$\Gamma; \vdash_\Sigma P_{a_i} :: (x_i : A_i)$ (by inversion on $\langle T-\langle a_i \rangle \rangle$)

$\Gamma \vdash_\Sigma \text{unavail}(a_i) :: (a_i : \langle a_i \rangle A_i)$ (by Lemma 4)

$\Gamma \vdash_\Sigma \text{unavail}(a_i), A_1 :: \Gamma$ (by $\langle T-\Lambda_4 \rangle$ and since $\text{unavail}(a_i) \notin A_1$ by well-formedness of $\Lambda$)

$\Gamma \vdash_\Sigma \Theta_1, \text{proc}(c_i, x_i \leftarrow \text{acquire } a_i : Q_{a_i}), \Theta_2 :: \Delta$ (by inversion on $\langle T-\Omega \rangle$)

$\Gamma \vdash_\Sigma \text{proc}(c_i, x_i \leftarrow \text{acquire } a_i : Q_{a_i}), \Theta_2 :: (\Delta_1, c_i : C_i)$ (by Lemma 6)

for some $\Delta_1$ and $C_i$

$\Gamma; \Delta_1 \vdash_\Sigma x_i \leftarrow \text{acquire } a_i : Q_{a_i} :: (c_i : C_i)$ and $(c_i : \bar{D}) \in \Gamma$ and $\vdash_\Sigma (C_i, \bar{D}) \text{ esync}$ (by inversion on $\langle T-\Theta_2 \rangle$)

for some $\Delta_1'$ and $\bar{D}$

$\Gamma \vdash_\Sigma \Theta_1 :: (\Delta_1, \Delta_1')$ (by inversion on $\langle T-\Theta_2 \rangle$)

$\Gamma; \Delta_1', x_i : A_i \vdash_\Sigma Q_{a_i} :: (c_i : C_i)$ (by inversion on $\langle T-\langle a_i \rangle \rangle$ and since $(a_i : \langle a_i \rangle A_i) \in \Gamma$)

$\vdash_\Sigma (A_i, \langle a_i \rangle A_i) \text{ esync}$ (by Lemma 11 and Corollary 1)

$\Gamma \vdash_\Sigma \text{proc}(a_i, [a_i/x_i] P_{a_i}), \Theta_2 :: (\Delta_1, \Delta_1', a_i : A_i)$ (by $\langle T-\Theta_2 \rangle$ and Corollary 1)

$\Gamma; \Delta_1', a_i : A_i \vdash_\Sigma [a_i/x_i] Q_{a_i} :: (c_i : C_i)$ (by Lemma 12 and Corollary 1)

$\Gamma \vdash_\Sigma \text{proc}(c_i, [a_i/x_i] Q_{a_i}), \text{proc}(a_i, [a_i/x_i] P_{a_i}), \Theta_2 :: \Delta$ (by Lemma 8)

$\Gamma \vdash_\Sigma \text{unavail}(a_i), \Lambda_1; \Theta_1, \text{proc}(c_i, [a_i/x_i] Q_{a_i}), \text{proc}(a_i, [a_i/x_i] P_{a_i}), \Theta_2 :: \Gamma; \Delta$ (by $\langle T-\Omega \rangle$ and well-formedness is maintained)

Case:

\[ \text{proc}(c_i, \text{wait } a_i : Q), \text{proc}(a_i, \text{close } a_i) \]

\[ \longrightarrow \text{proc}(c_i, Q) \] (D-1) (by assumption)

$\Gamma \vdash_\Sigma \Lambda; \Theta_1, \text{proc}(c_i, \text{wait } a_i : Q), \Theta_2, \text{proc}(a_i, \text{close } a_i), \Theta_3 :: \Gamma; \Delta$

for some $\Theta_1$, $\Theta_2$, and $\Theta_3$ (by I.H.)

$\Gamma \vdash_\Sigma \Lambda; \Theta_1, \text{proc}(c_i, \text{wait } a_i : Q), \text{proc}(a_i, \text{close } a_i), \Theta_2, \Theta_3 :: \Delta$ (by Lemma 5)

$\Lambda; \Theta_1, \text{proc}(c_i, \text{wait } a_i : Q), \text{proc}(a_i, \text{close } a_i), \Theta_2, \Theta_3 \longrightarrow \Lambda; \Theta_1, \text{proc}(a_i, Q), \Theta_2, \Theta_3$

(this case)

$\Gamma \vdash_\Sigma \Lambda :: \Gamma$ (by inversion on $\langle T-\Omega \rangle$)

$\Gamma \vdash_\Sigma \Theta_1, \text{proc}(c_i, \text{wait } a_i : Q), \text{proc}(a_i, \text{close } a_i), \Theta_2, \Theta_3 :: \Delta$ (by inversion on $\langle T-\Omega \rangle$)

$\Gamma \vdash_\Sigma \text{proc}(c_i, \text{wait } a_i : Q), \text{proc}(a_i, \text{close } a_i), \Theta_2, \Theta_3 :: (\Delta_1, c_i : C_i)$ (by Lemma 6)

for some $\Delta_1$ and $C_i$

$\Gamma; \Delta_1 \vdash_\Sigma \text{wait } a_i : Q :: (c_i : C_i)$ and $(c_i : \bar{D}) \in \Gamma$ and $\vdash_\Sigma (C_i, \bar{D}) \text{ esync}$ (by inversion on $\langle T-\Theta_2 \rangle$)

for some $\Delta_1'$ and $\bar{D}$

$\Gamma; \Delta_2 \vdash_\Sigma \text{Q} :: (c_i : C_i)$ (by inversion on $\langle T-\langle a_i \rangle \rangle$)

$\Gamma \vdash_\Sigma \text{proc}(a_i, \text{close } a_i), \Theta_2, \Theta_3 :: (\Delta_1, \Delta_2, a_i : 1)$ (by inversion on $\langle T-\Theta_2 \rangle$)

$\Gamma; \Delta_3 \vdash_\Sigma \text{close } a_i :: (a_i : 1)$ and $(a_i : \bar{B}) \in \Gamma$ and $\vdash_\Sigma (1, \bar{B}) \text{ esync}$ (by inversion on $\langle T-\Theta_2 \rangle$)

for some $\Delta_3$ and $\bar{B}$

$\Delta_3 = ()$ (by inversion on $\langle T-\langle a_i \rangle \rangle$)

$\Gamma \vdash_\Sigma \Theta_2, \Theta_3 :: (\Delta_1, \Delta_2)$ (by $\langle T-\Theta_2 \rangle$)

$\Gamma \vdash_\Sigma \text{proc}(c_i, Q), \Theta_2, \Theta_3 :: (\Delta_1, c_i : C_i)$ (by Lemma 8)

$\Gamma \vdash_\Sigma \Lambda; \Theta_1, \text{proc}(c_i, Q), \Theta_2, \Theta_3 :: \Gamma; \Delta$ (by $\langle T-\Omega \rangle$ and well-formedness is maintained)
Case:
\[ \text{proc}(a, y \leftarrow \text{recv} \ a; Q_{y}), \text{proc}(a, \text{send} \ a, b; P) \] (D-\[\star\])
\[ \rightarrow \text{proc}(a, [b_k/y_k] Q_{y}), \text{proc}(a, P) \]

\[ \Gamma \vdash \Sigma \Lambda; \Theta_1, \text{proc}(a, y \leftarrow \text{recv} \ a; Q_{y}), \Theta_2, \text{proc}(a, \text{send} \ a, b; P), \Theta_3 :: \Gamma; \Delta \]
for some \( \Theta_1, \Theta_2, \) and \( \Theta_3 \)
(by assumption)

\[ \Gamma \vdash \Sigma \Lambda; \Theta_1, \text{proc}(a, y \leftarrow \text{recv} \ a; Q_{y}), \Theta_2, \text{proc}(a, \text{send} \ a, b; P), \Theta_3 :: \Gamma; \Delta \]
is well-formed
(by I.H.)

\[ \Gamma \vdash \Sigma \Lambda; \Theta_1, \text{proc}(a, y \leftarrow \text{recv} \ a; Q_{y}), \text{proc}(a, \text{send} \ a, b; P), \Theta_2, \Theta_3 :: \Gamma; \Delta \]
(by Lemma 5)

\[ \Lambda; \Theta_1, \text{proc}(a, y \leftarrow \text{recv} \ a; Q_{y}), \text{proc}(a, \text{send} \ a, b; P), \Theta_2, \Theta_3 \]
\[ \rightarrow \Lambda; \Theta_1, \text{proc}(a, [b_k/y_k] Q_{y}), \text{proc}(a, P), \Theta_2, \Theta_3 \]
(this case)

\[ \Gamma \vdash \Sigma \Lambda :: \Gamma \]
(by inversion on (T-\[\Omega\]))

\[ \Gamma \vdash \Sigma \Theta_1, \text{proc}(a, y \leftarrow \text{recv} \ a; Q_{y}), \text{proc}(a, \text{send} \ a, b; P), \Theta_2, \Theta_3 :: \Delta \]
(by inversion on (T-\[\Omega\]))

\[ \Gamma \vdash \Sigma \text{proc}(a, y \leftarrow \text{recv} \ a; Q_{y}), \text{proc}(a, \text{send} \ a, b; P), \Theta_2, \Theta_3 :: \Delta \]
for some \( \Delta \) and \( \Theta \)
(by Lemma 5)

\[ \Gamma \vdash \Sigma \text{proc}(a, y \leftarrow \text{recv} \ a; Q_{y}), \text{proc}(a, \text{send} \ a, b; P), \Theta_2, \Theta_3 :: \Delta \]
for some \( \Delta \) and \( \Theta \)
(by Lemma 5)

\[ \Gamma \vdash \Sigma \text{proc}(a, y \leftarrow \text{recv} \ a; Q_{y}), \text{proc}(a, \text{send} \ a, b; P), \Theta_2, \Theta_3 :: \Delta \]
for some \( \Delta \) and \( \Theta \)
(by Lemma 6)

\[ \Gamma \vdash \Sigma \Lambda; \Theta_1, \text{proc}(a, y \leftarrow \text{recv} \ a; Q_{y}), \text{proc}(a, \text{send} \ a, b; P), \Theta_2, \Theta_3 :: \Gamma; \Delta \]
(by (T-\[\Omega\]) and well-formedness is maintained)

Case:
\[ \text{proc}(a, y \leftarrow \text{recv} \ a; Q_{y}), \text{proc}(a, \text{send} \ a, b; P) \]
(D-\[\Xi\])
\[ \rightarrow \text{proc}(a, [b_k/y_k] Q_{y}), \text{proc}(a, P) \]
\[ \Gamma \vdash \Sigma \Lambda; \Theta_1, \text{proc}(a, y \leftarrow \text{recv} \ a; Q_{y}), \Theta_2, \text{proc}(a, \text{send} \ a, b; P), \Theta_3 :: \Gamma; \Delta \]
for some \( \Theta_1, \Theta_2, \) and \( \Theta_3 \)
(by assumption)

\[ \Gamma \vdash \Sigma \Lambda; \Theta_1, \text{proc}(a, y \leftarrow \text{recv} \ a; Q_{y}), \Theta_2, \text{proc}(a, \text{send} \ a, b; P), \Theta_3 :: \Gamma; \Delta \]
is well-formed
(by I.H.)

\[ \Gamma \vdash \Sigma \Lambda; \Theta_1, \text{proc}(a, y \leftarrow \text{recv} \ a; Q_{y}), \text{proc}(a, \text{send} \ a, b; P), \Theta_2, \Theta_3 :: \Gamma; \Delta \]
(by Lemma 5)

\[ \Lambda; \Theta_1, \text{proc}(a, y \leftarrow \text{recv} \ a; Q_{y}), \text{proc}(a, \text{send} \ a, b; P), \Theta_2, \Theta_3 \]
\[ \rightarrow \Lambda; \Theta_1, \text{proc}(a, [b_k/y_k] Q_{y}), \text{proc}(a, P), \Theta_2, \Theta_3 \]
(this case)

\[ \Gamma \vdash \Sigma \Lambda :: \Gamma \]
(by inversion on (T-\[\Omega\]))

\[ \Gamma \vdash \Sigma \Theta_1, \text{proc}(a, y \leftarrow \text{recv} \ a; Q_{y}), \text{proc}(a, \text{send} \ a, b; P), \Theta_2, \Theta_3 :: \Delta \]
(by inversion on (T-\[\Omega\]))

\[ \Gamma \vdash \Sigma \text{proc}(a, y \leftarrow \text{recv} \ a; Q_{y}), \text{proc}(a, \text{send} \ a, b; P), \Theta_2, \Theta_3 :: \Delta \]
(by Lemma 5)
for some $\Delta_1$ and $C_i$

$\Gamma; \Delta'_1 \vdash \Sigma; y_b \gets \text{recv } a_i; Q_{y_b} :: (c_i : C_i)$ and $(c_b : \hat{D}) \in \Gamma$ and $\vdash \Sigma; (C_i, \hat{D}) \text{ esync}$

(by inversion on (T-Θ_2))

$\Gamma; y_b : A_i; \Delta_2, a_i : B_i \vdash \Sigma; Q_{y_b} :: (c_i : C_i)$

(by inversion on (T-∃_L))

$\Gamma \vdash \Sigma; \text{proc}(a_i, \text{send } a_b ; P), \Theta_2, \Theta_3 :: (\Delta_1, \Delta_2, a_i : \exists A_i.B_i)$

(by inversion on (T-Θ_2))

$\Gamma; \Delta_3 \vdash \Sigma; \text{send } a_i, b_i ; P :: (a_i : \exists A_i.B_i) \text{ and } (a_i : \hat{A}) \in \Gamma$ and $\vdash \Sigma; (\exists A_i.B_i, \hat{A}) \text{ esync}$

(by inversion on (T-Θ_2))

$\Gamma; \Delta_3 \vdash \Sigma; P :: (a_i : B_i)$ and $(b_i : \hat{B}) \in \Gamma$ and $\hat{B} \leq A_i$

(by inversion on (T-∃_R))

$\Gamma \vdash \Sigma; \Theta_2, \Theta_3 :: (\Delta_1, \Delta_2, \Delta_3)$

(by inversion on (T-Θ_2))

$\vdash \Sigma; (B_i, \hat{A}) \text{ esync}$

(by inversion on (T-Θ_2))

$\Gamma \vdash \Sigma; \text{proc}(a_i, P), \Theta_2, \Theta_3 :: (\Delta_1, \Delta_2, a_i : B_i)$

(by (T-Θ_2))

$\Gamma, b'_i : \hat{B}; \Delta_2, a_i : B_i \vdash \Sigma; b'_i[y_b] Q_{y_b} :: (c_i : C_i)$

where $b'_i$ fresh

(by Lemma 13 since $(b_i : \hat{B}) \in \Gamma$)

$\Gamma \vdash \Sigma; \text{proc}(a_i, [b_i/y_b] Q_{y_b}), \Theta_2, \Theta_3 :: (\Delta_1, c_i : C_i)$

(by (T-Θ_2))

$\Gamma \vdash \Sigma; \Theta_1, \text{proc}(a_i, [b_i/y_b] Q_{y_b}), \text{proc}(a_i, P), \Theta_2, \Theta_3 :: \Delta$

(by Lemma S)

$\Gamma \vdash \Sigma; \Lambda; \text{proc}(a_i, [b_i/y_b] Q_{y_b}), \Theta_2, \Theta_3 :: \Gamma; \Delta$

(by (T-Ω) and well-formedness is maintained)

Case:

$$\text{proc}(a, \text{send } a_b ; Q), \text{proc}(a, y_k \gets \text{recv } a_i; P_{y_k})$$

(by assumption)

$$\rightarrow \text{proc}(a_i, Q), \text{proc}(a_i, [b_i/y_b] P_{y_b})$$

(by assumption)

(by inversion on (T-Ω))

(by inversion on (T-Ω))

(by inversion on (T-Θ_2))

(by inversion on (T-Θ_2))

(by inversion on (T-Θ_2))

(by inversion on (T-Θ_2))

(by inversion on (T-Θ_2))

(by inversion on (T-Θ_2))

(by inversion on (T-Θ_2))

(by inversion on (T-Θ_2))

(by inversion on (T-Θ_2))

(by inversion on (T-Θ_2))

(by inversion on (T-Θ_2))
\[
\Gamma \vdash \Sigma. \text{proc}(a_1, [b_5/y_5]P_{y_5}), \Theta_2, \Theta_3 :: (\Delta_1, \Delta_2, a_1 : B_1) \quad \text{(by \text{T-\Theta}_2)}
\]
\[
\Gamma \vdash \Sigma. \text{proc}(a_3, Q), \text{proc}(a_1, [b_5/y_5]P_{y_5}), \Theta_2, \Theta_3 :: (\Delta_1, a_1 : C_1) \quad \text{(by \text{T-\Theta}_2)}
\]
\[
\Gamma \vdash \Sigma. \text{proc}(a_3, Q), \text{proc}(a_1, [b_5/y_5]P_{y_5}), \Theta_2, \Theta_3 :: \Delta \quad \text{(by \text{Lemma} 5)}
\]
\[
\Gamma \vdash \Sigma. \text{proc}(a_3, Q), \text{proc}(a_1, [b_5/y_5]P_{y_5}), \Theta_2, \Theta_3 :: \Gamma; \Delta \quad \text{(by \text{T-\Omega}) and well-formedness is maintained}
\]

Case:

\[
\begin{align*}
\text{proc}(a_1, \text{send} a_5 b_5 ; Q), \text{proc}(a_1, y_5 \leftarrow \text{recv} a_1 ; P_{y_5}) & \quad \text{(D-II)} \\
\rightarrow \text{proc}(a_1, Q), \text{proc}(a_1, [b_5/y_5]P_{y_5}) & \\
\end{align*}
\]

\[
\Gamma \vdash \Sigma. \Lambda; \Theta_1, \text{proc} (a_1, \text{send} a_5 b_5 ; Q), \Theta_2, \Theta_3 :: \Gamma; \Delta \\
\text{for some } \Theta_1, \Theta_2, \text{ and } \Theta_3 
\]

\[
\Gamma \vdash \Sigma. \Lambda; \Theta_1, \text{proc} (a_1, \text{send} a_5 b_5 ; Q), \Theta_2, \text{proc} (a_1, y_5 \leftarrow \text{recv} a_1 ; P_{y_5}), \Theta_3 :: \Gamma; \Delta \text{ is well-formed} \\
\text{(by \text{I.H.})}
\]

\[
\Gamma \vdash \Sigma. \Lambda; \Theta_1, \text{proc} (a_1, \text{send} a_5 b_5 ; Q), \Theta_2, \Theta_3 :: \Gamma; \Delta \\
\text{for \text{(by \text{I.H.})}}
\]

\[
\Lambda; \Theta_1, \text{proc} (a_1, \text{send} a_5 b_5 ; Q), \text{proc} (a_1, y_5 \leftarrow \text{recv} a_1 ; P_{y_5}), \Theta_2, \Theta_3 \\
\rightarrow \Lambda; \Theta_1, \text{proc} (a_1, Q), \text{proc} (a_1, [b_5/y_5]P_{y_5}), \Theta_2, \Theta_3 \\
\text{(this case)}
\]

\[
\Gamma \vdash \Sigma. \Lambda :: \Gamma \\
\text{(by inversion on \text{T-\Theta}_2)}
\]

\[
\Gamma \vdash \Sigma. \Lambda; \Theta_1, \text{proc} (a_1, \text{send} a_5 b_5 ; Q), \text{proc} (a_1, y_5 \leftarrow \text{recv} a_1 ; P_{y_5}), \Theta_2, \Theta_3 :: \Gamma; \Delta \\
\text{(by inversion on \text{T-\Theta}_2)}
\]

\[
\Gamma \vdash \Sigma. \text{proc} (a_1, \text{send} a_5 b_5 ; Q), \text{proc} (a_1, y_5 \leftarrow \text{recv} a_1 ; P_{y_5}), \Theta_2, \Theta_3 :: (\Delta_1, a_1 : C_1) \\
\text{for some } \Delta_1 \text{ and } C_1 \\
\text{(by \text{Lemma} 5)}
\]

\[
\begin{align*}
\Gamma; \Delta_1 & \vdash \text{send} a_5 b_5 ; Q :: (a_5, C_1) \text{ and } (c_5, C_1) \in \Gamma \text{ and } \vdash \Sigma; (c_5, C_1) \text{ \text{esync}} & \text{(by inversion on \text{T-\Theta}_2)} \\
\text{for some } \Delta_1 \text{ and } C_1 & \\
\end{align*}
\]

\[
\begin{align*}
\Gamma; \Delta_2, a_1 : B_1 & \vdash \Sigma; Q :: (a_1, C_1) \text{ and } (b_5, C_1) \in \Gamma \text{ and } \hat B \leq A_5 & \text{(by inversion on \text{T-\Pi}_L)} \\
\text{for some } \Delta_2, B, A_5 \text{ and } B_5 & \text{ such that } \Delta'_1 = \Delta_1 = \Delta_2, a_1 : \Pi A_5. B_1 & \text{(by inversion on \text{T-\Theta}_2)} \\
\Gamma \vdash \Sigma; \text{proc} (a_1, y_5 \leftarrow \text{recv} a_1 ; P_{y_5}), \Theta_2, \Theta_3 :: (\Delta_1, a_1 : \Pi A_5. B_1) & \text{(by inversion on \text{T-\Theta}_2)} \\
\Gamma; \Delta_3 & \vdash y_5 \leftarrow \text{recv} a_1 ; P_{y_5} :: (a_5, C_1) \text{ and } (a_5, C_1) \in \Gamma \text{ and } \vdash \Sigma; (\Pi A_5. B_1, C_1) \text{ \text{esync}} & \text{(by inversion on \text{T-\Theta}_2)} \\
\text{for some } \Delta_3 \text{ and } \hat A & \\
\Gamma, y_5 : A_5, \Delta_3 & \vdash \Sigma; P_{y_5} :: (a_5, C_1) & \text{(by inversion on \text{T-\Pi}_R)} \\
\Gamma \vdash \Sigma; \Theta_2, \Theta_3 :: (\Delta_1, \Delta_2, \Delta_3) & \text{(by inversion on \text{T-\Theta}_2)} \\
\text{(by \text{Lemma} 13)} \\
\Gamma; \Delta_3 & \vdash \Sigma; (b_5/y_5) [b_5/y_5] P_{y_5} :: (a_5, C_1) & \text{(by \text{Lemma} 13 \text{ since } (b_5, C_1) \in \Gamma)} \\
\text{(by inversion on \text{T-E\text{SYNC}_{\Pi}I})} & \text{(by \text{T-\Theta}_2)} \\
\Rightarrow \Sigma; (B_1, A) \text{ \text{esync}} & \text{(by \text{T-\Theta}_2)} \\
\Gamma \vdash \Sigma; \text{proc} (a_1, [b_5/y_5]P_{y_5}), \Theta_2, \Theta_3 :: (\Delta_1, a_1 : B_1) & \text{(by \text{T-\Theta}_2)} \\
\Gamma \vdash \Sigma; \text{proc} (a_1, Q), \text{proc} (a_1, [b_5/y_5]P_{y_5}), \Theta_2, \Theta_3 :: (\Delta_1, a_1 : C_1) & \text{(by \text{T-\Theta}_2)} \\
\Gamma \vdash \Sigma; \Theta_1, \text{proc} (a_1, Q), \text{proc} (a_1, [b_5/y_5]P_{y_5}), \Theta_2, \Theta_3 :: \Delta & \text{(by \text{Lemma} 5)} \\
\Gamma \vdash \Sigma; \Lambda; \Theta_1, \text{proc} (a_1, Q), \text{proc} (a_1, [b_5/y_5]P_{y_5}), \Theta_2, \Theta_3 :: \Gamma; \Delta & \text{(by \text{T-\Omega}) and well-formedness is maintained}
\]

Case:

\[
\begin{align*}
\text{proc} (a_1, \text{case } a_1 \text{ of } \Gamma \Rightarrow \Sigma), \text{proc} (a_1, a_1, l_n ; P) & \quad \text{(D-\Theta)} \\
\rightarrow \text{proc} (a_1, Q_k), \text{proc} (a_1, P) & \\
\end{align*}
\]

\[
\Gamma \vdash \Sigma; \Lambda; \Theta_1, \text{proc} (a_1, \text{case } a_1 \text{ of } \Gamma \Rightarrow \Sigma), \Theta_2, \text{proc} (a_1, a_1, l_n ; P), \Theta_3 :: \Gamma; \Delta \\
\text{for some } \Theta_1, \Theta_2, \text{ and } \Theta_3 & \text{ (by \text{assumption})} \\
\Gamma \vdash \Sigma; \Lambda; \Theta_1, \text{proc} (a_1, \text{case } a_1 \text{ of } \Gamma \Rightarrow \Sigma), \Theta_2, \text{proc} (a_1, a_1, l_n ; P), \Theta_3 :: \Gamma; \Delta & \text{ is well-formed} & \text{(by \text{I.H.})}
\]

51
\(\Gamma \vdash \Sigma; \Theta_1, \text{proc}(e_i, \text{case } a_i \text{ of } I =\rightarrow Q), \text{proc}(a_i, a_h, P), \Theta_2, \Theta_3 :: \Gamma; \Delta\) 
(by Lemma 5)

\(\Lambda; \Theta_1, \text{proc}(e_i, \text{case } a_i \text{ of } I =\rightarrow Q), \text{proc}(a_i, a_h, P), \Theta_2, \Theta_3 \rightarrow \Lambda; \Theta_1, \text{proc}(c_i, Q_h), \text{proc}(a_i, P), \Theta_2, \Theta_3\) 
(this case)

\(\Gamma \vdash \Sigma; \Lambda :: \Gamma\) 
(by inversion on (T-\(\varnothing\))

\(\Gamma \vdash \Sigma; \Theta_1, \text{proc}(e_i, \text{case } a_i \text{ of } I =\rightarrow Q), \text{proc}(a_i, a_h, P), \Theta_2, \Theta_3 :: \Delta\) 
(by inversion on (T-\(\varnothing\))

\(\Gamma \vdash \Sigma; \text{proc}(c_i, \text{case } a_i \text{ of } I =\rightarrow Q), \text{proc}(a_i, a_h, P), \Theta_2, \Theta_3 :: (\Delta_1, c_i : C_i)\) 
(by inversion on (T-\(\varnothing\))

for some \(\Delta_1\) and \(C_i\)

\(\Gamma; \Delta_1 \vdash_{C_i} \text{case } a_i \text{ of } I =\rightarrow Q :: (c_i : C_i)\) and \((c_i : D) \in \Gamma\) and \(\Gamma \vdash (\Sigma; C_i, D)\) esync 
(by inversion on (T-\(\varnothing\))

for some \(\Delta_1\) and \(D\)

\((\forall i) \Gamma; \Delta_2, a_i : A_{L_i} \vdash_{\Sigma} Q_i :: (c_i : C_i)\) 
(by inversion on (T-\(\varnothing\))

for some \(\Delta_2\) and \(A_i\) such that \(\Delta_2 = \Delta_2, a_i : \{I : A_i\}\)

\(\Gamma \vdash \Sigma; \text{proc}(a_i, P), \Theta_2, \Theta_3 :: (\Delta_1, \Delta_2, a_i : \{I : A_i\})\) 
(by inversion on (T-\(\varnothing\))

\(\Gamma; \Delta_3 \vdash_{C_i} a_h, P :: (a_i : \{I : A_i\})\) and \((a_i : A) \in \Gamma\) and \(\Gamma \vdash (\Sigma; a_i, A)\) esync 
(by inversion on (T-\(\varnothing\))

for some \(\Delta_3\) and \(\hat{A}\)

\(\Gamma; \Delta_3 \vdash_{\Sigma} P :: (a_i : A_h)\) 
(by inversion on (T-\(\varnothing\))

\(\Gamma \vdash \Sigma; \Theta_2, \Theta_3 :: (\Delta_1, \Delta_2, \Delta_3)\) 
(by inversion on (T-\(\varnothing\))

\((\forall i) \Gamma \vdash (\Sigma; A_i, \hat{A})\) esync 
(by inversion on (T-\(\text{ESYNC}_\varnothing\))

\(\Gamma \vdash \Sigma; \Theta_2, \Theta_3 :: (\Delta_1, \Delta_2, a_i : A_h)\) 
(by inversion on (T-\(\varnothing\))

\(\Gamma \vdash \Sigma; \text{proc}(a_i, P), \Theta_2, \Theta_3 :: (\Delta_1, c_i : C_i)\) 
(by inversion on (T-\(\varnothing\))

\(\Gamma \vdash \Sigma; \Theta_1, \text{proc}(c_i, Q_h), \text{proc}(a_i, P), \Theta_2, \Theta_3 :: \Delta\) 
(by inversion on (T-\(\varnothing\))

\(\Gamma \vdash \Sigma; \Lambda; \Theta_1, \text{proc}(e_i, Q_h), \text{proc}(a_i, P), \Theta_2, \Theta_3 :: \Gamma; \Delta\) 
(by (T-\(\varnothing\)) and well-formedness is maintained)

Case:

\[\text{proc}(a_i, a_h, Q), \text{proc}(a_i, \text{case } a_i \text{ of } I =\rightarrow P)\] 
(D-\&)

\(\Gamma \vdash \Sigma; \Lambda; \Theta_1, \text{proc}(e_i, a_h, Q), \text{proc}(a_i, \text{case } a_i \text{ of } I =\rightarrow P), \Theta_3 :: \Gamma; \Delta\) 
(by assumption)

\(\Gamma \vdash \Sigma; \Lambda :: \Gamma\) 
(by inversion on (T-\(\varnothing\))

\(\Gamma \vdash \Sigma; \Theta_1, \text{proc}(e_i, a_h, Q), \text{proc}(a_i, \text{case } a_i \text{ of } I =\rightarrow P), \Theta_3 :: \Gamma; \Delta\) is well-formed 
(by I.H.)

\(\Gamma \vdash \Sigma; \Lambda; \Theta_1, \text{proc}(e_i, a_h, Q), \text{proc}(a_i, \text{case } a_i \text{ of } I =\rightarrow P), \Theta_2, \Theta_3 :: \Gamma; \Delta\) 
(by Lemma 5)

\(\Lambda; \Theta_1, \text{proc}(e_i, a_h, Q), \text{proc}(a_i, \text{case } a_i \text{ of } I =\rightarrow P), \Theta_2, \Theta_3 \rightarrow \Lambda; \Theta_1, \text{proc}(a_i, P), \Theta_2, \Theta_3\) 
(this case)

\(\Gamma \vdash \Sigma; \Lambda :: \Gamma\) 
(by inversion on (T-\(\varnothing\))

\(\Gamma \vdash \Sigma; \Theta_1, \text{proc}(e_i, a_h, Q), \text{proc}(a_i, \text{case } a_i \text{ of } I =\rightarrow P), \Theta_2, \Theta_3 :: \Gamma; \Delta\) 
(by inversion on (T-\(\varnothing\))

\(\Gamma \vdash \Sigma; \text{proc}(e_i, a_h, Q), \text{proc}(a_i, \text{case } a_i \text{ of } I =\rightarrow P), \Theta_2, \Theta_3 :: (\Delta_1, c_i : C_i)\) 
(by inversion on (T-\(\varnothing\))

for some \(\Delta_1\) and \(C_i\)

\(\Gamma; \Delta_1 \vdash_{C_i} a_h, Q :: (c_i : C_i)\) and \((c_i : D) \in \Gamma\) and \(\Gamma \vdash (\Sigma; C_i, D)\) esync 
(by inversion on (T-\(\varnothing\))

for some \(\Delta_1\) and \(D\)

\(\Gamma; \Delta_2, a_i : A_{L_i} \vdash_{\Sigma} Q :: (c_i : C_i)\) 
(by inversion on (T-\(\varnothing\))

for some \(\Delta_2\) and \(A_i\) such that \(\Delta_2 = \Delta_2, a_i : \{I : A_i\}\)

\(\Gamma \vdash \Sigma; \text{proc}(a_i, \text{case } a_i \text{ of } I =\rightarrow P), \Theta_2, \Theta_3 :: (\Delta_1, \Delta_2, a_i : \{I : A_i\})\) 
(by inversion on (T-\(\varnothing\))

\(\Gamma; \Delta_3 \vdash_{C_i} \text{case } a_i \text{ of } I =\rightarrow P :: (a_i : \{I : A_i\})\) and \((a_i : A) \in \Gamma\) and \(\Gamma \vdash (\Sigma; a_i, A)\) esync 
(by inversion on (T-\(\varnothing\))

for some \(\Delta_3\) and \(A\)

\((\forall i) \Gamma; \Delta_3 \vdash_{\Sigma} P_i :: (a_i : A_{L_i})\) 
(by inversion on (T-\(\varnothing\))

\(\Gamma \vdash \Sigma; \Theta_2, \Theta_3 :: (\Delta_1, \Delta_2, \Delta_3)\) 
(by inversion on (T-\(\varnothing\))

52
(∀i) ⊢_Σ (A_L, Ā) esync  
Γ ⊢_Σ proc(a_i, P) :: (Δ_1, Δ_2, a_i : A_L) (by inversion on (T-ESYNC))  
Γ ⊢_Σ proc(c_i, Q), proc(a_i, P), Θ_2, Θ_3 :: (Δ_1, c_i : C_i) (by (T-Θ_2))  
Γ ⊢_Σ Θ_1, proc(c_i, Q), proc(a_i, P), Θ_2, Θ_3 :: Δ (by Lemma 3)  
Γ ⊢_Σ Λ, Θ_1, proc(c_i, Q), proc(a_i, P), Θ_2, Θ_3 :: Γ; Δ (by (T-Ω) and well-formedness is maintained)

□

D.3 Progress

The progress theorem relies on the notions of a poised and blocked process (see Definition 3 and Definition 4) and expresses that being blocked is the only way the whole configuration may be stuck [27]. Case (2-c) captures the scenario where a blocked process cannot proceed because the shared channel is unavailable. A successful acquire, on the other hand, is represented as part of case (2-a).

Theorem 4 (Progress). If Γ ⊢_Σ Λ; Θ :: Γ; Δ, then either

1. Λ → Λ', for some Λ', or
2. Λ is poised and
   (a) Λ; Θ → Λ'; Θ', for some Λ' and Θ', or
   (b) Θ is poised, or
   (c) some process in Θ is blocked along a_s and unavail(a_s) ∈ Λ.

Proof.

Γ ⊢_Σ Λ; Θ :: Γ; Δ (by assumption)  
Γ ⊢_Σ Λ :: Γ and Γ ⊢_Σ Θ :: Δ (by inversion on (T-Ω))

We first show that either Λ → Λ', for some Λ', or that Λ is poised. We proceed by induction on Γ ⊢_Σ Λ :: Γ_1, where Γ_1 ⊆ Γ:

Case: Γ ⊢_Σ (·) :: (·)

(·) is poised (by Definition 3)

Case: Γ ⊢_Σ proc(a_s, P_{as}) :: (a_s : ↑_i A_s), for some a_s, P_{as}, and A_s

We proceed by case analysis on Γ ⊢_Σ P_{as} :: (a_s : ↑_i A_s):

Subcase: Γ ⊢_Σ fwd a_s b_s :: (a_s : ↑_i A_s), for some (b_s : Ā) ∈ Γ such that Ā ≤ ↑_i A_s

proc(a_s, fwd a_s b_s), Λ_1 → unavail(a_s), [b_s/a_s] Λ_1

(by D-ID_b)

Subcase: Γ ⊢_Σ x_s ← X_s ← x_s ; Q_{xs} :: (a_s : ↑_i A_s)

proc(a_s, x_s ← X_s ← x_s ; Q_{xs}), Λ_1 → proc(a_s, [b_s/x_s] Q_{xs}), proc(b_s, [b_s/x_s', b_s/y] Q_{xs}), Λ_1

where b fresh (by D-SPAWN)

Subcase: Γ ⊢_Σ x_s ← accept a_s ; P_{as} :: (a_s : ↑_i A_s)

proc(a_s, x_s ← accept a_s ; P_{as}), Λ_1 is poised (by Definition 3)

Case: Γ ⊢_Σ unavail(a_s) :: (a_s : Ā), for some a_s and Ā

53
unavail(a_s) is poised \hspace{1cm} \text{(by Definition 3)}

Case: $\Gamma \vdash_{\Sigma} \Lambda_1, \Lambda_2 :: \Gamma_1, \Gamma_2$, for some $\Lambda_1, \Lambda_2, \Gamma_1$, and $\Gamma_2$, such that $\Gamma = \Gamma_1, \Gamma_2$

Either $\Lambda_1 \rightarrow \Lambda_1' \Gamma$, for some $\Lambda_1'$, or $\Lambda_1$ is poised, or $\Lambda_2 \rightarrow \Lambda_2' \Gamma$, for some $\Lambda_2'$, or $\Lambda_2$ is poised. \hspace{1cm} \text{(by I.H.)}

Subcase: $\Lambda_1 \rightarrow \Lambda_1'$, for some $\Lambda_1'$ and $\Lambda_2$ is poised

$\Lambda_1, \Lambda_2 \rightarrow \Lambda_1', \Lambda_2$

Subcase: $\Lambda_1 \rightarrow \Lambda_1'$, for some $\Lambda_1'$ and $\Lambda_2 \rightarrow \Lambda_2'$, for some $\Lambda_2'$

$\Lambda_1, \Lambda_2 \rightarrow \Lambda_1', \Lambda_2'$

Subcase: $\Lambda_1$ is poised and $\Lambda_2 \rightarrow \Lambda_2'$, for some $\Lambda_2'$

$\Lambda_1, \Lambda_2 \rightarrow \Lambda_1, \Lambda_2'$

Subcase: $\Lambda_1$ is poised and $\Lambda_2$ is poised

$\Lambda_1, \Lambda_2$ is poised

Having proved that either $\Lambda \rightarrow \Lambda'$, for some $\Lambda'$, or that $\Lambda$ is poised, we assume that $\Lambda$ is poised and proceed by induction on $\Gamma \vdash_{\Sigma} \Theta :: \Delta$.

Case: $\Gamma \vdash_{\Sigma} \Theta :: \Theta$

$\Theta$ is poised \hspace{1cm} \text{(by Definition 3)}

Case: $\Gamma \vdash_{\Sigma} \text{proc}(a_s, P_{a_s}), \Theta_1 :: \Delta_1, a_s : A_s$, for some $a_s, P_{a_s}, \Theta_1, \Delta_1, \text{and } A_s$

$\Gamma; \Delta_1 \vdash_{\Sigma} P_{a_s} :: (a_s : A_s)$ and $\Gamma \vdash_{\Sigma} \Theta_1 :: \Delta_1, \Delta_1'$ \hspace{1cm} \text{(by inversion on (T-Θ_2))}

Either $\Lambda; \Theta_1 \rightarrow \Lambda'; \Theta_1'$, for some $\Lambda'$ and $\Theta'$, or $\Theta_1$ is poised or some process in $\Theta_1$ is blocked along $a_s$ and unavail($a_s$) $\in \Lambda$. \hspace{1cm} \text{(by I.H.)}

Subcase: $\Lambda; \Theta_1 \rightarrow \Lambda'; \Theta_1'$

$\Lambda; \text{proc}(a_s, P_{a_s}), \Theta_1 \rightarrow \Lambda'; \text{proc}(a_s, P_{a_s}), \Theta_1'$

Subcase: $\Theta_1$ is poised

We proceed by case analysis on $\Gamma; \Delta_1 \vdash_{\Sigma} P_{a_s} :: (a_s : A_s)$:

Subsubcase: $\Gamma; \Delta_1 \vdash_{\Sigma} \text{fwd} a_s b_s :: (a_s : A_s)$, for some $b_s : A_s$ such that $\Delta_1 = a_s : A_s$

$\Lambda; \text{proc}(a_s, \text{fwd} a_s b_s), \Theta_1 \rightarrow [b_s/a_s] \Lambda; [b_s/a_s] \Theta_1$ \hspace{1cm} \text{(by D-ID_λ)}

Subsubcase: $\Gamma; \Delta_1 \vdash_{\Sigma} x_1 \leftarrow X_1 \leftarrow \overline{b}; \Theta_1 \rightarrow \text{unavail}(b_s), \Lambda; \text{proc}(a_s, [b_s/\overline{x_1}]Q_{x_1}), \text{proc}(b_s, [b_s/\overline{x'_1}, \overline{b}/\overline{y}]P_{x'_1\overline{y}}), \Theta_1$

\hspace{1cm} \text{where } b \text{ fresh} \hspace{1cm} \text{(by D-SPAWN_L)}

Subsubcase: $\Gamma; \Delta_1 \vdash_{\Sigma} x_2 \leftarrow X_2 \leftarrow \overline{b}; \Theta_1 \rightarrow \Lambda; \text{proc}(a_s, [b_s/\overline{x_2}]Q_{x_2}), \text{proc}(b_s, [b_s/\overline{x'_2}, \overline{b}/\overline{y}]P_{x'_2\overline{y}}), \Theta_1$

\hspace{1cm} \text{where } b \text{ fresh} \hspace{1cm} \text{(by D-SPAWN_{LS})}

Subsubcase: $\Gamma; \Delta_1 \vdash_{\Sigma} \text{acquire } c_s : Q_{a_s} :: (a_s : A_s)$, for some $(c_s : \overline{C}) \in \Gamma$ such that $\overline{C} \leq \overline{\overline{x'_s B_s}}$, for some $B_s$

Either there exists a proc($c_s, P_{c_s}$) in $\Lambda$ or an unavail($c_s$) in $\Lambda$. \hspace{1cm} \text{(by Lemma 10-1)}

Subsubsubcase: There exists a $\Lambda_1$ such that $\Lambda = \text{proc}(c_s, P_{c_s}), \Lambda_1$;
\[ \text{Subsubcase:} \] There exists a \( \Lambda \) such that \( \Lambda = \text{unavail}(c_1) \), \( \Lambda \):
\[ \text{proc}(c_1, x_2 \leftarrow \text{acquire } c_1) \text{ in } \Theta \text{ is blocked along } c_1 \text{ and } \text{unavail}(c_1) \in \Lambda \] (by Definition 3)
\[ \text{proc}(c_1, P_{c_1}) \text{ is poised} \] (by Definition 3 since \( \Lambda \) is poised)
\[ \text{proc}(c_1, x_2 \leftarrow \text{accept } c_2, P_{c_1}^1) \] (by Definition 3)
\[ \text{proc}(c_1, x_2 \leftarrow \text{acquire } c_3, Q_{c_3}, \Theta_1) \rightarrow \text{unavail}(c_1), \Lambda_1; \text{proc}(c_1, x_2 \leftarrow \text{acquire } c_3, Q_{c_3}, \Theta_1) \] (by D-\( \uparrow^s \) - acquire/accept)
\[ \text{Subsubcase:} \] There exist \( \Theta_1, \Theta_2 \), and \( \text{proc}(c_1, P_{c_1}) \) such that \( \Theta_1 = \Theta_2, \text{proc}(c_1, P_{c_1}), \Theta_2 \) and
\[ \text{unavail}(c_1), \Lambda_1; \text{proc}(c_1, x_2 \leftarrow \text{release } c_1, Q_{c_1}, \Theta_2, \text{proc}(c_1, x_2 \leftarrow \text{detach } c_1, P_{c_1}^2), \Theta_2' \rightarrow \text{proc}(c_1, [c_1/x_2] P_{c_2}^2, \Lambda_1; \text{proc}(c_1, [c_1/x_2] Q_{c_1}, \Theta_2, \Theta_2') \] (by Lemma 10.2 and inversion on process typing)
\[ \text{Subsubcase:} \] \( \Gamma; \Delta_2, c_1 : \|_{\Sigma}^1 C_2 \vdash x_2 \leftarrow \text{detach } c_1 : P_{c_2}^2 \) (by Definition 3 and inversion on process typing)
\[ \text{unavail}(c_1), \Lambda_1; \text{proc}(c_1, x_2 \leftarrow \text{release } c_1, Q_{c_1}, \Theta_2, \text{proc}(c_1, x_2 \leftarrow \text{detach } c_1, P_{c_2}^2), \Theta_2' \rightarrow \text{proc}(c_1, [c_1/x_2] P_{c_2}^2, \Lambda_1; \text{proc}(c_1, [c_1/x_2] Q_{c_1}, \Theta_2, \Theta_2') \] (by D-\( \downarrow^s \) - release/detach)
\[ \text{Subsubcase:} \] \( \Gamma; \Delta_2, c_1 : 1 \vdash \Sigma \text{ wait } c_1 : Q :: (a_1 : A_1) \) for some \( \Delta_2 \) such that \( \Delta_1' = \Delta_2, c_1 : 1 \)
\[ \text{proc}(c_1, P_{c_1}) \text{ is poised} \] (by Lemma 10.2)
\[ \text{proc}(c_1, P_{c_1}) = \text{proc}(c_1, x_2 \leftarrow \text{detach } c_1 : P_{c_2}^2) \] (by Definition 3 since \( \Theta_1 \) is poised)
\[ \text{Subsubcase:} \] \( \Gamma; \Delta_2, c_1 : B_2 \otimes C_2 \vdash y_2 \leftarrow \text{recv } c_1, Q_{c_2} :: (a_1 : A_1) \), for some \( B_2, C_2, \) and \( \Delta_2 \) such that \( \Delta_1' = \Delta_2, c_1 : B_2 \otimes C_2 \)
\[ \text{unavail}(c_1), \Lambda_1; \text{proc}(c_1, x_2 \leftarrow \text{release } c_1, Q_{c_1}, \Theta_2, \text{proc}(c_1, x_2 \leftarrow \text{detach } c_1, P_{c_2}^2), \Theta_2' \rightarrow \text{proc}(c_1, [c_1/x_2] P_{c_2}^2, \Lambda_1; \text{proc}(c_1, [c_1/x_2] Q_{c_1}, \Theta_2, \Theta_2') \] (by D-\( \downarrow^s \) - release/detach)
\[ \text{Subsubcase:} \] \( \Gamma; \Delta_2, c_1 : 1 \vdash \Sigma \text{ close } a_1 :: (a_1 : 1) \)
\[ \text{proc}(c_1, \text{close } a_1) \text{ is poised} \] (by Definition 3 since \( \Theta_1 \) is poised)
\[ \text{Subsubcase:} \] \( \Gamma; \Delta_2, c_1 : B_2 \otimes C_2 \vdash y_2 \leftarrow \text{travel } c_1, Q_{c_2} :: (a_1 : A_1) \), for some \( B_2, C_2, \) and \( \Delta_2 \) such that \( \Delta_1' = \Delta_2, c_1 : B_2 \otimes C_2 \)
\[ \text{proc}(c_1, P_{c_1}) \text{ is poised} \] (by Lemma 10.2)
\[ \text{proc}(c_1, P_{c_1}) = \text{proc}(c_1, \text{send } c_1, b_2 : P') \text{, for some } c_1 : B_2 \] (by Definition 3 and inversion on process typing)
\[ \text{Λ: proc}(a_1, y_2 \leftarrow \text{recv } a_1, Q_{c_2}, \Theta_2, \text{proc}(a_1, \text{send } c_1, b_2 : P'), \Theta_2' \rightarrow \text{Λ: proc}(a_1, b_2 : P'), \Theta_2, \text{proc}(a_1, P'), \Theta_2' \] (by D-\( \otimes/3 \))
\[ \text{Subsubcase:} \] \( \Gamma; \Delta_2, b_1 : B_2 \vdash \Sigma \text{ send } a_1, b_1 : P :: (a_1 : B_2 \otimes C_2) \), for some \( B_2, C_2, \) and \( \Delta_2 \) such that \( \Delta_1' = \Delta_2, b_1 : B_2 \)
\[ \text{proc}(c_1, \text{send } a_1, b_1 : P), \Theta_1 \text{ is poised} \] (by Definition 3 since \( \Theta_1 \) is poised)
\[ \text{Subsubcase:} \] \( \Gamma; \Delta_2, c_1 : (\exists B_2, C_2) \vdash y_2 \leftarrow \text{recv } c_1, Q_{y_2} :: (a_1 : A_1) \), for some \( B_2, C_2, \) and \( \Delta_2 \) such that \( \Delta_1' = \Delta_2, c_1 : \exists B_2, C_2 \)
\[ \text{proc}(c_1, \text{send } a_1, b_1 : P), \Theta_1 \text{ is poised} \] (by Lemma 10.2)
\[ \text{proc}(c_1, P_{c_1}) \text{ is poised} \] (by Definition 3 since \( \Theta_1 \) is poised)
\[ \text{proc}(c_1, P_{c_1}) = \text{proc}(c_1, \text{send } c_1, b_2 : P'), \text{ for some } b_2 : B_2 \] (by Definition 3 and inversion on process typing)
\[ \text{Λ: proc}(a_1, y_2 \leftarrow \text{recv } c_1, Q_{y_2}, \Theta_2, \text{proc}(a_1, \text{send } c_1, b_2 : P'), \Theta_2' \rightarrow \text{Λ: proc}(a_1, [b_2/y_2] Q_{y_2}, \Theta_2, \text{proc}(a_1, P'), \Theta_2' \] (by D-\( \otimes/3 \))
\[ \text{Subsubcase:} \] \( \Gamma; \Delta_1' \vdash \Sigma \text{ send } a_1, b_1 : P :: (a_1 : (\exists B_2, C_2)) \), for some \( B_2, C_2, \) and \( (b_2 : B \in \Gamma) \) such that \( A_1 = \exists B_2, C_2 \) and \( \hat{B} \leq B_2 \)
\[ \text{proc}(a_1, \text{send } a_1, b_1 : P), \Theta_1 \text{ is poised} \] (by Definition 3 since \( \Theta_1 \) is poised)
\[ \text{Subsubcase:} \] \( \Gamma; \Delta_2, c_1 : B_2 \rightarrow C_2, b_1 : B_2 \vdash \Sigma \text{ send } c_1, b_1 : Q :: (a_1 : A_1) \), for some \( B_2, C_2, \) and \( \Delta_2 \) such that \( \Delta_1' = \Delta_2, c_1 : B_2 \otimes C_2, b_1 : B_2 \)

55
There exist $\Theta_2$, $\Theta'_2$, and $\text{proc}(\alpha_i, P_{\alpha_i})$ such that $\Theta_1 = \Theta_2$, $\text{proc}(\alpha_i, P_{\alpha_i}), \Theta'_2$.

(by Lemma 10.2)

$\text{proc}(\alpha_i, P_{\alpha_i})$ is poised

(by Definition 3 since $\Theta_1$ is poised)

$\text{proc}(\alpha_i, P_{\alpha_i}) = \text{proc}(\alpha_i, y_k \leftarrow \text{recv} \alpha_i : P'_{y_k})$

(by Definition 3 and inversion on process typing)

$\Lambda: \text{proc}(\alpha_i, \text{send} c_i b_i : Q), \Theta_2, \text{proc}(\alpha_i, y_k \leftarrow \text{recv} \alpha_i : P'_{y_k}), \Theta'_2$

$\rightarrow \Lambda: \text{proc}(\alpha_i, Q), \Theta_2, \text{proc}(\alpha_i, [b_i/y_k] P'_{y_k}), \Theta'_2$

(by D-$\Theta$ /II)

**Subcase:** $\Gamma; \Delta_1 \vdash \Sigma y_k \leftarrow \text{recv} \alpha_i : P_{y_k} :: (\alpha_i : B_{i} \rightarrow C_{i})$, for some $B_{i}, C_{i}$ such that $A_{i} = B_{i} \rightarrow C_{i}$

$\text{proc}(\alpha_i, y_k \leftarrow \text{recv} \alpha_i : P_{y_k}), \Theta_1$ is poised

(by Definition 3 since $\Theta_1$ is poised)

$\text{proc}(\alpha_i, P_{\alpha_i})$ is poised

(by Definition 3 since $\Theta_1$ is poised)

$\text{proc}(\alpha_i, P_{\alpha_i}) = \text{proc}(\alpha_i, y_k \leftarrow \text{recv} \alpha_i : P'_{y_k})$

(by Definition 3 and inversion on process typing)

$\Lambda: \text{proc}(\alpha_i, \text{send} c_i b_i : Q), \Theta_2, \text{proc}(\alpha_i, y_k \leftarrow \text{recv} \alpha_i : P'_{y_k}), \Theta'_2$

$\rightarrow \Lambda: \text{proc}(\alpha_i, Q), \Theta_2, \text{proc}(\alpha_i, [b_i/y_k] P'_{y_k}), \Theta'_2$

(by D-$\Theta$ /II)

**Subcase:** $\Gamma; \Delta_1 \vdash \Sigma y_k \leftarrow \text{recv} \alpha_i : P_{y_k} :: (\alpha_i : (\Pi B_{i} C_{i}))$, for some $B_{i}, C_{i}$ such that $A_{i} = \Pi B_{i} C_{i}$

$\text{proc}(\alpha_i, y_k \leftarrow \text{recv} \alpha_i : P_{y_k}), \Theta_1$ is poised

(by Definition 3 since $\Theta_1$ is poised)

$\text{proc}(\alpha_i, P_{\alpha_i})$ is poised

(by Definition 3 since $\Theta_1$ is poised)

$\text{proc}(\alpha_i, P_{\alpha_i}) = \text{proc}(\alpha_i, c_i : \Delta_1)$

(by Definition 3 and inversion on process typing)

$\Lambda: \text{proc}(\alpha_i, \text{case} c_i \text{ of } \Gamma \Rightarrow Q :: (\alpha_i : A_{i})), \Theta_2, \text{proc}(\alpha_i, c_i : \Delta_1), \Theta'_2$

$\rightarrow \Lambda: \text{proc}(\alpha_i, Q), \Theta_2, \text{proc}(\alpha_i, \Delta_1), \Theta'_2$

(by D-$\Theta$)

**Subcase:** $\Gamma; \Delta_1 \vdash \Sigma a_i : \{\Gamma; B_i\}$ case $a_i$ of $\Gamma \Rightarrow Q :: (\alpha_i : A_{i})$, for some $B_{i}$ and $\Delta_2$ such that $\Delta'_1 = \Delta_2, c_i : \{\Gamma; B_i\}$

There exist $\Theta_2$, $\Theta'_2$, and $\text{proc}(\alpha_i, P_{\alpha_i})$ such that $\Theta_1 = \Theta_2, \text{proc}(\alpha_i, P_{\alpha_i}), \Theta'_2$.

(by Lemma 10.2)

$\text{proc}(\alpha_i, P_{\alpha_i})$ is poised

(by Definition 3 since $\Theta_1$ is poised)

$\text{proc}(\alpha_i, P_{\alpha_i}) = \text{proc}(\alpha_i, c_i : \Delta_1)$

(by Definition 3 and inversion on process typing)

$\Lambda: \text{proc}(\alpha_i, \text{case} c_i \text{ of } \Gamma \Rightarrow Q :: (\alpha_i : A_{i})), \Theta_2, \text{proc}(\alpha_i, c_i : \Delta_1), \Theta'_2$

$\rightarrow \Lambda: \text{proc}(\alpha_i, Q), \Theta_2, \text{proc}(\alpha_i, \Delta_1), \Theta'_2$

(by D-$\Theta$)

**Subcase:** $\Gamma; \Delta_1 \vdash \Sigma a_i : \{\Gamma; B_i\}$ case $a_i$ of $\Gamma \Rightarrow Q :: (\alpha_i : \{\Gamma; B_i\})$, for some $B_{i}$ and $\Delta_2$ such that $\Delta'_1 = \Delta_2, c_i : \{\Gamma; B_i\}$

There exist $\Theta_2$, $\Theta'_2$, and $\text{proc}(\alpha_i, P_{\alpha_i})$ such that $\Theta_1 = \Theta_2, \text{proc}(\alpha_i, P_{\alpha_i}), \Theta'_2$.

(by Lemma 10.2)

$\text{proc}(\alpha_i, P_{\alpha_i})$ is poised

(by Definition 3 since $\Theta_1$ is poised)

$\text{proc}(\alpha_i, P_{\alpha_i}) = \text{proc}(\alpha_i, \text{case} a_i \text{ of } \Gamma \Rightarrow P :: (\alpha_i : \{\Gamma; B_i\}))$

(by Definition 3 and inversion on process typing)

$\Lambda: \text{proc}(\alpha_i, a_i : \{\Gamma; B_i\}), \Theta_2, \text{proc}(\alpha_i, \text{case} a_i \text{ of } \Gamma \Rightarrow P :: (\alpha_i : \{\Gamma; B_i\})), \Theta'_2$

$\rightarrow \Lambda: \text{proc}(\alpha_i, Q), \Theta_2, \text{proc}(\alpha_i, P'_{\alpha_i}), \Theta'_2$

(by D-$\Theta$)

**Subcase:** $\Gamma; \Delta_1 \vdash \Sigma \text{case } a_i \text{ of } \Gamma \Rightarrow P :: (\alpha_i : \{\Gamma; B_i\})$, for some $B_{i}$ such that $A_{i} = \{\Gamma; B_i\}$

$\text{proc}(\alpha_i, \text{case } a_i \text{ of } \Gamma \Rightarrow P), \Theta_1$ is poised

(by Definition 3 since $\Theta_1$ is poised)

**Subcase:** Some process in $\Theta_1$ is blocked along $a_{\theta}$ and $\text{unavail}(a_{\theta}) \in \Lambda$

Some process in $\text{proc}(\alpha_i, P_{\alpha_i})$, $\Theta_1$ is blocked along $a_{\theta}$ and $\text{unavail}(a_{\theta}) \in \Lambda$

□
E.1 “Imperative” Queue

Linearity prohibits a more “imperative” style of a queue implementation that maintains a reference to the back of the queue for direct insertion of an element. In this section, we give an implementation of a queue with direct access to both the front and back of the queue; the result is shown in Figure 21.

Figure 21: Imperative queue: has access to both the front and the end of the queue.

As is common for imperative queue implementations, the queue consists of a head that maintains a reference to the front and back of a linked list that comprises the elements of the queue. The session type $\text{queue } A_5$ defines the protocol of the queue, which is the protocol we introduced earlier for the queue in the producer-consumer example. For convenience, we repeat the protocol definition in Figure 21. Process $\text{head}$ implements this protocol. The session type $\text{list } A_5$ defines the protocol of the linked list that is used internally by process $\text{head}$ to store the elements of the queue. Session type $\text{list } A_5$ is implemented by the processes $\text{empty}$ and $\text{elem}$. Process $\text{empty}$ represents an empty list, process $\text{elem}$ represents a non-empty list. The list thus consists of a sequence of $\text{elem}$ processes, ended by an $\text{empty}$ process. An empty queue is created by the following lines of code

\begin{verbatim}
  e ← empty;
  q ← head ← e, e;
\end{verbatim}

These lines illustrate that sharing arises in case of an empty queue between the $\text{front}$ and the $\text{back}$ channel because they both point to the same list element. For this reason, process $\text{head}$ defines the channels $\text{front}$ and $\text{back}$ to be of the shared session type $\text{list } A_5$. Sharing also arises in case of a non-empty queue between a list’s $\text{next}$ channel...
and the head’s back channel because both point to the same element in case of the last element in the list. For this reason, process elem defines the channel next to be of the shared session type list \( A \). Process head uses the acquire-release primitives to communicate with the list. It acquires channel back upon receiving an enq request and channel front upon receiving a deq request and then releases both channels upon successful insertion into or deletion from the list.

### E.2 Cycles and Deadlocks

In the dining philosophers example (Figure 7), the circular dependency among shared channels is created by shared channel process arguments. Alternatively, the circularity can be introduce by shared channel input and output. Figure 22 gives an example that leads to a classic deadlock. The cycle is created by process client, which spawns a new shared process deadlock and then sends a “self-reference” to that very process after acquiring it. The deadlock occurs once the newly spawned and now linear process attempts to acquire itself.

```plaintext
\begin{align*}
\text{cycle} &= \{↑[\text{cycle}]\} \\
\text{client} : \{1\} & \quad \text{deadlock} : \{\text{cycle}\} \\
\text{c} & \leftarrow \text{client} = \text{deadlock} = \text{c} \leftarrow \text{accept} \text{c} ; \\
\text{d} & \leftarrow \text{deadlock} ; \text{self} \leftarrow \text{recv} \text{c} ; \\
\text{d'} & \leftarrow \text{acquire} \text{d} ; \\
\text{send} \text{d'} \text{d} ; & \quad \text{send} \text{self} \text{self} ; \\
\text{wait} \text{d'} ; & \quad \text{wait} \text{self'} ; \\
\text{close} \text{c} & \quad \text{close} \text{c'}
\end{align*}
```

Figure 22: Processes creating a cycle along channel self, causing a deadlock.

### E.3 Cycles and Blocking

Another form of blocking can arise from circularity that is caused by forwarding rather than by a classic deadlock. Figure 23 shows a variation of the previous example where the offering process terminate forwards itself to itself, resulting in a configuration in which no process exists anymore along either channel. As a result, the client will block when attempting to re-acquire the process.

```plaintext
\begin{align*}
\text{cycle} &= \{↑[\text{cycle}]\} \& \{\text{input : \text{cycle}, dealloc : 1}\} \\
\text{client} : \{1\} & \quad \text{terminate} : \{\text{cycle}\} \\
\text{c} & \leftarrow \text{client} = \text{terminate} = \text{c} \leftarrow \text{accept} \text{c} ; \\
\text{d} & \leftarrow \text{terminate} ; \text{c} \leftarrow \text{detach} \text{c} ; \\
\text{d'} & \leftarrow \text{acquire} \text{d} ; \\
\text{d'}.\text{input} & \leftarrow \text{send} \text{d'} \text{d} ; \\
\text{d} & \leftarrow \text{release} \text{d'} ; \\
\text{d'} & \leftarrow \text{acquire} \text{d} ; \quad \text{send} \text{self} \text{self} ; \text{(* blocks here *)} \\
\text{d'}.\text{dealloc} & \leftarrow \text{wait} \text{d'} ; \\
\text{close} \text{c} & \quad \text{fwd} \text{c self} \quad \text{fwd} \text{c self}
\end{align*}
```

Figure 23: Client-side blocking caused by circular forwarding.

### E.4 Linear Forwarding

In the linear forwarding case of the preservation proof, the following 9 subcases for the types of \( a \) and \( b \) are considered, categorized as shown:

\[
\hat{B} \leq \hat{A} : \quad a : T \quad \text{and} \quad b : T \\
\text{a : T} \quad \text{and} \quad b : ↑[\text{a}]B
\]
Next, we will provide examples for some of the cases above. As in Section 4.2, we use the connective ⊃ [20[58] to support value input. The type “int ⊃ int ⊃ 1”, for example, describes a session that receives a value of type int and then continues as a session that expects to receive a value of type int before terminating. As a reminder, the process predicate with the forwarding term is proc(aₖ, fwd aₖ bₖ).

In the first 3 cases, aₖ : T guarantees that the channel aₖ does not yet occur in any process terms in the configuration. In that case, substitution does actually not have any effect. An example for aₖ : T and bₖ : ⊥ is:

\[
\begin{align*}
\text{supertype} &= \text{int} \triangleright \text{int} \triangleright 1 \\
\text{subtype} &= \text{int} \triangleright 1 \\
\text{main} : \{1\} &\quad \text{super} : \{\text{supertype}\} &\quad \text{sub} : \{\text{subtype}\} \\
\text{c} \leftarrow \text{main} &\quad \text{a} \leftarrow \text{super} = x \leftarrow \text{recv} a ; \\
\text{s} \leftarrow \text{super} ; &\quad \text{b} \leftarrow \text{sub} = x \leftarrow \text{recv} b ; \\
\text{send} s \; 6 ; \text{send} s \; 6 ; &\quad \text{fwd} \; a \; b \\
\text{wait} \; s ; \text{close} \; c &\quad \text{close} \; b \\
\end{align*}
\]

An example for aₖ : T and bₖ : ⊤₁Bₖ is:

\[
\begin{align*}
\text{supertype} &= \text{int} \triangleright \text{int} \triangleright 1 \\
\text{subtype} &= \text{int} \triangleright 1 \\
\text{main} : \{1\} &\quad \text{super} : \{\text{supertype}\} &\quad \text{sub} : \{\text{subtype}\} \\
\text{c} \leftarrow \text{main} = a \leftarrow \text{super} = b \leftarrow \text{sub} = \\
\text{s} \leftarrow \text{super} ; &\quad \text{a} \leftarrow \text{supertyp}e = x \leftarrow \text{recv} \; a ; \\
\text{send} s \; 6 ; \text{send} s \; 6 ; &\quad \text{b} \leftarrow \text{sub} = b' \leftarrow \text{accept} \; b ; \\
\text{wait} \; s ; \text{close} \; c &\quad \text{close} \; b' \\
\end{align*}
\]

An example for aₖ : ⊤₁Aₖ and bₖ : ⊤₁Bₖ and Aₖ ≠ Bₖ is:

\[
\begin{align*}
\text{supertype} &= \text{int} \triangleright 1 \triangleright \text{int} \triangleright 1 \\
\text{subtype} &= \text{int} \triangleright 1 \\
\text{main} : \{1\} &\quad \text{super} : \{\text{supertype}\} &\quad \text{sub} : \{\text{subtype}\} \\
\text{c} \leftarrow \text{main} = a \leftarrow \text{super} = b \leftarrow \text{sub} = \\
\text{s} \leftarrow \text{super} ; &\quad \text{a} \leftarrow \text{super} = x \leftarrow \text{recv} \; a ; \\
\text{s'} \leftarrow \text{acquire} \; s ; &\quad \text{b} \leftarrow \text{sub} = b' \leftarrow \text{accept} \; b ; \\
\text{send} s' \; 6 ; \text{send} s' \; 6 ; &\quad \text{b} \leftarrow \text{sub} = x \leftarrow \text{recv} \; b' ; \\
\text{wait} \; s' ; \text{close} \; c &\quad \text{close} \; b' \\
\end{align*}
\]

An example for aₖ : ⊤₁Aₖ and bₖ : ⊥ is:

\[
\begin{align*}
\text{supertype} &= \text{int} \triangleright 1 \triangleright \text{int} \triangleright 1 \\
\text{subtype} &= \text{int} \triangleright 1 \\
\text{main} : \{1\} &\quad \text{super} : \{\text{supertype}\} &\quad \text{sub} : \{\text{subtype}\} \\
\text{a} \leftarrow \text{main} = b \leftarrow \text{super} = c \leftarrow \text{sub} = \\
\text{b} \leftarrow \text{super} = b' \leftarrow \text{accept} \; b ; \\
\text{b} \leftarrow \text{super} = x \leftarrow \text{recv} \; b' ; \\
\text{s} \leftarrow \text{sub} = s' \leftarrow \text{acquire} \; s ; \\
\text{fwd} \; a \; b' &\quad \text{fwd} \; b' \; s' \\
\end{align*}
\]
Acknowledgements  The authors would like to thank Peter Thiemann, Philip Wadler, and other participants for comments on a preliminary talk on this work at the Dagstuhl Seminar on Theory and Applications of Behavioural Types, January 29 – February 3, 2017. The authors would also like to thank Bob Harper for discussions on process calculi and coinduction. This material is based upon work supported by a Mozilla Research grant and partially sponsored by NSF Grant CNS-1423168: ”Blameworthy Programs: Accountability via Deviance and Causal Determination”. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of Mozilla Research or NSF.
References


62


