

# Resource Sharing via Capability-Based Multiparty Session Types <sup>\*</sup>

A. Laura Voinea<sup>[0000-0003-4482-205X]</sup>, Ornela Dardha<sup>[0000-0001-9927-7875]</sup>, and  
Simon J. Gay<sup>[0000-0003-3033-9091]</sup>

School of Computing Science, University of Glasgow, United Kingdom  
a.voinea.1@research.gla.ac.uk  
{Ornela.Dardha, Simon.Gay}@glasgow.ac.uk

**Abstract.** *Multiparty Session Types (MPST)* are a type formalism used to model communication protocols among components in distributed systems, by specifying *type* and *direction* of data transmitted. It is standard for multiparty session type systems to use access control based on *linear* or *affine* types. While useful in offering strong guarantees of communication safety and session fidelity, linearity and affinity run into the well-known problem of inflexible programming, excluding scenarios that make use of shared channels or need to store channels in shared data structures.

In this paper, we develop *capability-based resource sharing* for multiparty session types. In this setting, channels are split into two entities, the channel itself and the capability of using it. This gives rise to a more flexible session type system, which allows channel references to be shared and stored in persistent data structures. We illustrate our type system through a producer-consumer case study. Finally, we prove that the resulting language satisfies type safety.

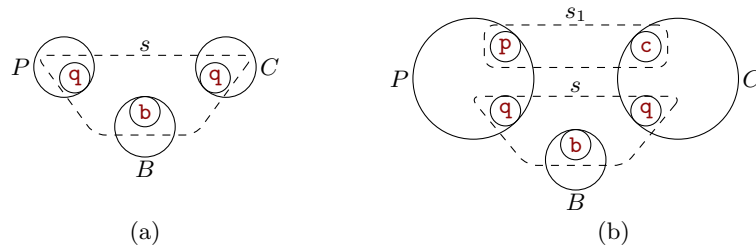
**Keywords:** session types · sharing · concurrent programming

## 1 Introduction

In the present era of communication-centric software systems, it is increasingly recognised that the structure of communication is an essential aspect of system design. *(Multiparty) session types* [18,19,32] allow communication structures to be codified as type definitions in programming languages, which can be exploited by compilers, development environments and runtime systems, for compile-time analysis or runtime monitoring. A substantial and ever-growing literature on session types and, more generally, behavioural types [20] provides a rich theoretical foundation, now being applied to a range of programming languages [1,16].

---

<sup>\*</sup> Supported by the UK EPSRC grant EP/K034413/1, “From Data Types to Session Types: A Basis for Concurrency and Distribution (ABCD)”, by the EU HORIZON 2020 MSCA RISE project 778233 “BehAPI: Behavioural Application Program Interfaces”, and by an EPSRC PhD studentship.



**Fig. 1.** Producer-consumer system: Producer— $P$  and Consumer— $C$  sharing access to Buffer— $B$  by implementing the same role  $q$ . (a)  $P$  and  $C$  communicate with  $B$  in session  $s$ ; (b)  $P$  and  $C$  exchange the capability to use channel  $s[q]$  in session  $s_1$  and then use it to communicate with  $B$  in session  $s$

Session type systems must control *aliasing* of the endpoints of communication channels, in order to avoid race conditions. If agents  $A$  and  $B$  both think they are running the client side of a protocol with the same server  $S$ , then a message sent by  $A$  advances the session state without  $B$ 's knowledge, which interferes with  $B$ 's attempt to run the protocol.

In order to guarantee unique ownership of channel endpoints and eliminate aliasing, most session type systems use strict *linear typing*. For more flexibility, some others use *affine typing*, which allows channels to be discarded, but they still forbid aliasing. It is possible to allow a session-typed channel to become sharable in the special case in which the session type reaches a point which is essentially stateless. However, in such systems, channels are *linearly typed* for the most interesting parts of their lifetimes—we discuss these possibilities in § 6.

This leads us to our research questions:

- Q1** *Are session types intrinsically related to linearity or affinity?*
- Q2** *Can we define session type systems without linear types?*
- Q3** *How can we check resource (channel) sharing and aliasing, to guarantee communication safety and session fidelity, i.e., type safety?*

The goal of this paper is to investigate questions **Q1–Q3**. To give a more flexible approach to resource sharing and access control, we propose a system of multiparty session types (MPST) that includes techniques from the Capability Calculus [11], and from Walker et al.'s work on alias types [36]. The key idea is to split a communication channel into two entities: (1) the channel itself, and (2) its usage *capability*. Both entities are first-class and can be referred to separately. Channels can now be shared, or stored in shared data structures, and aliasing is allowed. However, in order to guarantee communication safety and session fidelity, i.e., type safety, capabilities are used linearly so that only one alias can be used at a time.

This approach has several benefits, and improves on the state of the art: (i) for the first time, it is now possible for a system to have a communication structure defined by shared channels, with the capabilities being transferred from process to process as required; (ii) a capability can be implemented as a simple token,

whereas delegation of channels requires a relatively complex implementation, thus making linearity of capabilities more lightweight than linearity of channels.

*Example 1 (Producer-Consumer Fig. 1).* Producer P and consumer C communicate via buffer B in session  $\mathbf{s}$ , given in Fig. 1 (a). P and C implement *role*  $\mathbf{q}$ , and B implements *role*  $\mathbf{b}$ . *Shared access* to buffer B is captured by the fact that both P and C implement the same *role*  $\mathbf{q}$  and use the same channel  $\mathbf{s}[\mathbf{q}]$  to communicate with B.

Following MPST theory, we start by defining a *global type*, describing communications among *all* participants:

$$G_0 = \mathbf{q} \rightarrow \mathbf{b} : \text{add}(\text{Int}). \mathbf{q} \rightarrow \mathbf{b} : \text{request}(). \mathbf{b} \rightarrow \mathbf{q} : \text{send}(\text{Int}). G_0$$

In  $G_0$ , protocol proceeds as follows: P (playing  $\mathbf{q}$ ) sends an `add` message to B (playing  $\mathbf{b}$ ), to add data. In sequence, C (playing  $\mathbf{q}$ ) sends a `request` message to B, to ask for data. B replies with a `send` message, sending data to C (playing  $\mathbf{q}$ ), and the protocol repeats as  $G_0$ . *Projecting* the global protocol to each role gives us a local session type. In particular, for B, implementing *role*  $\mathbf{b}$ , we obtain:

$$S_{\mathbf{b}} = \mathbf{q} ? \text{add}(\text{Int}). \mathbf{q} ? \text{request}(). \mathbf{q} ! \text{send}(\text{Int}). S_{\mathbf{b}}$$

where the  $\mathbf{q}$  annotations show the other role participating in each interaction. For the shared access by P and C (*role*  $\mathbf{q}$ ), we obtain:

$$S_{\mathbf{q}} = \mathbf{b} ! \text{add}(\text{Int}). S'_{\mathbf{q}} \quad S'_{\mathbf{q}} = \mathbf{b} ? \text{request}(). \mathbf{b} ? \text{send}(\text{Int}). S_{\mathbf{q}}$$

Finally, the definitions of processes are as follows—we will detail the syntax in §2.

$$\begin{aligned} P\langle v \rangle &= \mathbf{s}[\mathbf{q}][\mathbf{b}] \oplus \langle \text{add}(v) \rangle . P\langle v + 1 \rangle \\ C\langle \rangle &= \mathbf{s}[\mathbf{q}][\mathbf{b}] \oplus \langle \text{request}() \rangle . \mathbf{s}[\mathbf{b}][\mathbf{q}] \& \{ \text{send}(i) \} . C\langle \rangle \\ B\langle \rangle &= \mathbf{s}[\mathbf{q}][\mathbf{b}] \& \{ \text{add}(x) \} . \mathbf{s}[\mathbf{q}][\mathbf{b}] \& \{ \text{request}() \} . \mathbf{s}[\mathbf{b}][\mathbf{q}] \oplus \langle \text{send}(x) \rangle . B\langle \rangle \end{aligned}$$

Unfortunately, the system of processes above is not typable using standard multiparty session type systems because *role*  $\mathbf{q}$  is shared by P and C, thus violating linearity of channel  $\mathbf{s}[\mathbf{q}]$ . To solve this issue and still allow sharing and aliasing, in our work, instead of associating a channel  $c$  with a session type  $S$ , we separately associate  $c$  with a *tracked* type  $\text{tr}(\rho)$ , and  $S$  with *capability*  $\rho$ ,  $\{\rho \mapsto S\}$ . The capability can be passed between P and C as they take turns in using the channel, illustrated in Fig. 1 (b). As a first attempt, we now define the following global type, getting us closer to our framework.

$$G_1 = \mathbf{q} \rightarrow \mathbf{b} : \text{add}(\text{Int}). \mathbf{p} \rightarrow \mathbf{c} : \text{turn}(\text{tr}(\rho_{\mathbf{q}})). \mathbf{q} \rightarrow \mathbf{b} : \text{request}(). \\ \mathbf{b} \rightarrow \mathbf{q} : \text{send}(\text{Int}). \mathbf{c} \rightarrow \mathbf{p} : \text{turn}(\text{tr}(\rho_{\mathbf{q}})). G_1$$

However, a type such as  $\text{tr}(\rho_{\mathbf{q}})$  is usually too specific because it refers to the capability of a particular channel. It is preferable to be able to give definitions that abstract away from specific channels. We therefore introduce *existential types*, in the style of [36], which package a channel with its capability, in the form  $\exists[\rho] \{ \rho \mapsto S \} . \text{tr}(\rho)$ .

With the existential types in place, we can define our global type  $G$  in the following way. It now includes an extra initial message from P to C containing

$P ::= \mathbf{0} \mid P \mid Q \mid (\nu s)P$	inaction, parallel composition, restriction
$\mid c[\mathbf{p}] \oplus (l(v)).P \mid c[\mathbf{p}] \&_{i \in I} \{l_i(x_i).P_i\}$	select, branch
$\mid c[\mathbf{p}] \oplus (l(\text{pack}(\rho, \mathbf{s}[\mathbf{q}]))).P$	select pack
$\mid c[\mathbf{p}] \&_{i \in I} \{l_i(\text{pack}(\rho_i, \mathbf{s}_i[\mathbf{q}])).P_i\}$	branch pack
$\mid \text{def } D \text{ in } P \mid X\langle \tilde{x} \rangle$	recursion, process call
$D ::= X\langle \tilde{x} \rangle = P$	process declaration
$c ::= x \mid \mathbf{s}[\mathbf{p}]$	variable, channel with role $\mathbf{p}$
$v ::= c \mid \rho \mid \text{true} \mid \text{false} \mid 0 \mid 1 \mid \dots$	channel, capability, base value

Fig. 2. Multiparty session  $\pi$ -calculus

the channel used with the buffer. The session types  $S_{\mathbf{q}}$  and  $S'_{\mathbf{q}}$  are the same as before.

$$G = \mathbf{p} \rightarrow \mathbf{c} : \text{buffer}(\exists[\rho_{\mathbf{q}} \mid \{\rho_{\mathbf{q}} \mapsto S'_{\mathbf{q}}\}], \text{tr}(\rho_{\mathbf{q}})). \mu t. \mathbf{q} \rightarrow \mathbf{b} : \text{add}(\text{Int}). \mathbf{p} \rightarrow \mathbf{c} : \text{turn}(\{\rho_{\mathbf{q}} \mapsto S'_{\mathbf{q}}\}). \\ \mathbf{q} \rightarrow \mathbf{b} : \text{request}(). \mathbf{b} \rightarrow \mathbf{q} : \text{send}(\text{Int}). \mathbf{c} \rightarrow \mathbf{p} : \text{turn}(\{\rho_{\mathbf{q}} \mapsto S_{\mathbf{q}}\}). t$$

In § 4 we complete this example by showing the projections to a local type for each role, and the definitions of processes that implement each role.  $\square$

### Contributions of the paper

- (i) **MPST with capabilities**: we present a new version of MPST theory without linear typing for channels, but with linearly-typed capabilities. In § 2 we define a multiparty session  $\pi$ -calculus with capabilities, and its operational semantics, and in § 3 we define a MPST system for it.
- (ii) **Producer-Consumer Case Study**: in § 4 we present a detailed account of the producer-consumer case study, capturing the core of resource sharing and use of capabilities.
- (iii) **Type Safety**: in § 5 we state the type safety property, and outline its proof.

## 2 Multiparty Session $\pi$ -Calculus with Capabilities

Our  $\pi$ -calculus with multiparty session types is based on the language defined by Scalas *et al.* [28]. The syntax is defined in Fig. 2. We assume infinite sets of identifiers for variables ( $x$ ), sessions ( $\mathbf{s}$ ), capabilities ( $\rho$ ) and roles ( $\mathbf{p}$ ).

The calculus combines branch (resp., select) with input (resp., output), and a message  $l(v)$  consists of a label  $l$  and a payload  $v$ , which is a value. A message in session  $\mathbf{s}$  from role  $\mathbf{p}$  to role  $\mathbf{q}$  has the prefix  $\mathbf{s}[\mathbf{p}][\mathbf{q}]$ , where  $\mathbf{s}[\mathbf{p}]$  is represented by  $\mathbf{c}$  in the grammar. The select and branch operations come in two forms. The first form is standard, and the second form handles *packages*, which are the novel feature of our type system. A package consists of a capability  $\rho$  and a channel of type  $\text{tr}(\rho)$ . We will see in § 3 in the typing rules, the capability is existentially

$$\begin{aligned}
P \mid \mathbf{0} &\equiv P & P \mid Q &\equiv Q \mid P & (P \mid Q) \mid R &\equiv P \mid (Q \mid R) \\
(\nu s)\mathbf{0} &\equiv \mathbf{0} & (\nu s)(\nu s')P &\equiv (\nu s')(\nu s)P & (\nu s)P \mid Q &\equiv (\nu s)(P \mid Q) \text{ if } s \notin fc(Q) \\
\text{def } D \text{ in } \mathbf{0} &\equiv \mathbf{0} & \text{def } D \text{ in } (\nu s)P &\equiv (\nu s)(\text{def } D \text{ in } P) \text{ if } s \notin fc(P) \\
\text{def } D \text{ in } (P \mid Q) &\equiv (\text{def } D \text{ in } P) \mid Q \text{ if } dpv(D) \cap fpv(Q) = \emptyset \\
\text{def } D \text{ in } \text{def } D' \text{ in } P &\equiv \text{def } D' \text{ in } \text{def } D \text{ in } P \\
\text{if } (dpv(D) \cup fpv(D)) \cap dpv(D') &= (dpv(D') \cup fpv(D')) \cap dpv(D) = \emptyset
\end{aligned}$$

**Fig. 3.** Structural congruence (processes)

$$\begin{aligned}
&\frac{j \in I \text{ and } fv(v) = \emptyset}{\mathbf{s}[\mathbf{p}][\mathbf{q}] \&_{i \in I} \{l_i(x_i). P_i\} \mid \mathbf{s}[\mathbf{q}][\mathbf{p}] \oplus \langle l_j(v) \rangle . P \longrightarrow P_j \{v/x_j\} \mid P} \text{RCOM} \\
&\frac{j \in I}{\mathbf{s}[\mathbf{p}][\mathbf{q}] \&_{i \in I} \{l_i(\text{pack}(\rho_i, v_i)). P_i\} \mid \mathbf{s}[\mathbf{q}][\mathbf{p}] \oplus \langle l_j(\text{pack}(\rho, v)) \rangle . P \longrightarrow P_j \{v/v_i\} \mid P} \text{RCOMP} \\
&\frac{\tilde{x} = x_1, \dots, x_n \quad \tilde{v} = v_1, \dots, v_n \quad fv(\tilde{v}) = \emptyset}{\text{def } X \langle \tilde{x} \rangle = P \text{ in } (X \langle \tilde{x} \rangle \mid Q) \longrightarrow \text{def } X \langle \tilde{x} \rangle = P \text{ in } (P \{\tilde{v}/\tilde{x}\} \mid Q)} \text{RCALL} \\
&\frac{P \longrightarrow Q}{(\nu s)P \longrightarrow (\nu s)Q} \text{RRES} \quad \frac{P \longrightarrow Q}{P \mid R \longrightarrow Q \mid R} \text{RPAR} \quad \frac{P \longrightarrow Q}{\text{def } D \text{ in } P \longrightarrow \text{def } D \text{ in } Q} \text{RDEF}
\end{aligned}$$

**Fig. 4.** Reduction (processes)

quantified. This enables a channel to be delegated, with the information that it is linked to *some* capability, which will be transmitted in a second message.

As usual, we define structural congruence to compensate for the limitations of textual syntax. It is the smallest congruence satisfying the axioms in Fig. 3. The definition uses the concepts of *free channels* of a process,  $fc(P)$ ; *free process variables* of a process,  $fpv(P)$ ; and *defined process variables* of a process declaration,  $dpv(D)$ . We omit the definitions of these concepts, which are standard and can be found in [28].

We define a reduction-based operational semantics by the rules in Fig. 4. Rule RCOM is a standard communication between roles  $\mathbf{p}$  and  $\mathbf{q}$ . Rule RCOMP is communication of an existential package. Rule RCALL defines a standard approach to handling process definitions. The rest are standard contextual rules.

### 3 Multiparty Session Types with Capabilities

We now introduce a type system for the multiparty session  $\pi$ -calculus. The general methodology of multiparty session types is that system design begins with a *global type*, which specifies all of the communication among various *roles*. Given a global type  $G$  and a role  $\mathbf{p}$ , *projection* yields a *session type* or *local type*  $G \upharpoonright \mathbf{p}$  that describes all of the communication involving  $\mathbf{p}$ . This local type can be further projected for another role  $\mathbf{q}$ , to give a *partial session type* that describes communication between  $\mathbf{p}$  and  $\mathbf{q}$ .

$S ::=$		<i>local session type</i>
<b>end</b>		terminated session
$\mathbf{p} \oplus_{i \in I} !l_i(U_i).S_i$		selection towards role $p$
$\mathbf{p} \&_{i \in I} ?l_i(U_i).S_i$		branching from role $p$
$\mathbf{p} \oplus_{i \in I} !l_i(\exists[\rho_i \{\rho_i \mapsto U_i\}].\mathbf{tr}(\rho_i)).S_i$		pack selection towards role $p$
$\mathbf{p} \&_{i \in I} ?l_i(\exists[\rho_i \{\rho_i \mapsto U_i\}].\mathbf{tr}(\rho_i)).S_i$		pack branching from role $p$
$\mathbf{t}$		type variable
$\mu \mathbf{t}.S$		recursive session type
$G ::=$		<i>global type</i>
<b>end</b>		termination
$\mathbf{p} \rightarrow \mathbf{q} : \{l_i(U_i).G_i\}_{i \in I}$		interaction
$\mathbf{p} \rightarrow \mathbf{q} : \{l_i(\exists[\rho_i \{\rho_i \mapsto U_i\}].\mathbf{tr}(\rho_i)).G_i\}_{i \in I}$		pack interaction
$\mathbf{t}$		type variable
$\mu \mathbf{t}.G$		recursive type
$H ::=$		<i>partial session type</i>
<b>end</b>		terminated session
$\oplus_{i \in I} !l_i(U_i).H_i$		selection
$\&_{i \in I} ?l_i(U_i).H_i$		branching
$\oplus_{i \in I} !l_i(\exists[\rho_i \{\rho_i \mapsto U_i\}].\mathbf{tr}(\rho_i)).H_i$		pack selection
$\&_{i \in I} ?l_i(\exists[\rho_i \{\rho_i \mapsto U_i\}].\mathbf{tr}(\rho_i)).H_i$		pack branching
$\mathbf{t}$		type variable
$\mu \mathbf{t}.H$		recursive type
$C ::= \emptyset \mid C \otimes \{\rho \mapsto S\}$		<i>capabilities</i>
$B ::= \mathbf{Int} \mid \mathbf{Bool}$		<i>ground type</i>
$U ::=$		<i>payload type</i>
$B$		ground type
$\mathbf{tr}(\rho)$		tracked type
$\{\rho \mapsto S\}$		capability type
$S$ closed		session type
$\Gamma ::= \emptyset \mid \Gamma, x : U \mid \Gamma, \mathbf{s}[\mathbf{p}] : \mathbf{tr}(\rho)$		<i>environment</i>
$\Delta ::= \emptyset \mid \Delta, X : \tilde{U}$		<i>process names</i>

All branch and select types have the conditions  $I \neq \emptyset$  and  $U_i$  closed.

**Fig. 5.** Types, capabilities, environments

**Global types** Fig. 5. Each interaction has a source role  $\mathbf{p}$  and a target role  $\mathbf{q}$ . We combine branching and message transmission, so an interaction has a label  $l_i$ , a payload of type  $U_i$ , or of type  $\exists[\rho_i|\{\rho_i \mapsto U_i\}].\mathbf{tr}(\rho_i)$ , and a continuation type  $G_i$ . If there is only one branch then we usually abbreviate the syntax to  $\mathbf{p} \rightarrow \mathbf{q}; l(U)$ .  $G$ , respectively  $\mathbf{p} \rightarrow \mathbf{q}; l(\exists[\rho_i|\{\rho_i \mapsto U_i\}].\mathbf{tr}(\rho_i))$ .  $G$ . Recursive types are allowed, with the assumption that they are guarded. **Base types**  $B, B', \dots$  can be types like **Bool**, **Int**, etc. **Payload types**  $U, U_i, \dots$  are either base types, tracked types, capability types or *closed* session types.

**Local (session) types** Fig. 5. The single form of interaction from global types splits into *select* (internal choice) and *branch* (external choice). The *branching type*  $\mathbf{p} \&_{i \in I} ?l_i(U_i).S_i$  describes a channel that can receive a label  $l_i$  from role  $\mathbf{p}$  (for some  $i \in I$ , chosen by  $\mathbf{p}$ ), together with a *payload* of type  $U_i$ ; then, the channel must be used as the continuation type  $S_i$ . The *selection type*  $\mathbf{p} \oplus_{i \in I} !l_i(U_i).S_i$ , describes a channel that can choose a label  $l_i$  (for any  $i \in I$ ), and send it to  $\mathbf{p}$  together with a payload of type  $U_i$ ; then, the channel must be used as  $S_i$ . The types for *pack select* and *pack branch* act in a similar manner, and bind the capability  $\rho_i$  for the continuation type  $S_i$ . Session types also allow guarded recursion.

The relationship between global types and session types is formalised by the notion of projection.

**Definition 1.** The projection of  $G$  onto a role  $\mathbf{q}$ , written  $G \upharpoonright \mathbf{q}$ , is:

$$\begin{aligned} \mathbf{end} \upharpoonright \mathbf{q} &\triangleq \mathbf{end} & \mathbf{t} \upharpoonright \mathbf{q} &\triangleq \mathbf{t} & (\mu \mathbf{t}.G) \upharpoonright \mathbf{q} &\triangleq \begin{cases} \mu \mathbf{t}.(G \upharpoonright \mathbf{q}) & \text{if } G \upharpoonright \mathbf{q} \neq \mathbf{t}' \ (\forall \mathbf{t}') \\ \mathbf{end} & \text{otherwise} \end{cases} \\ (\mathbf{p} \rightarrow \mathbf{p}':\{l_i(U_i).G_i\}_{i \in I}) \upharpoonright \mathbf{q} &\triangleq \begin{cases} \mathbf{p}' \oplus_{i \in I} !l_i(U_i).(G_i \upharpoonright \mathbf{q}) & \text{if } \mathbf{q} = \mathbf{p}, \\ \mathbf{p} \&_{i \in I} ?l_i(U_i).(G_i \upharpoonright \mathbf{q}) & \text{if } \mathbf{q} = \mathbf{p}', \\ \prod_{i \in I} (G_i \upharpoonright \mathbf{q}) & \text{if } \mathbf{p} \neq \mathbf{q} \neq \mathbf{p}' \end{cases} \\ (\mathbf{p} \rightarrow \mathbf{p}':\{l_i(\exists[\rho_i|\{\rho_i \mapsto U_i\}].\mathbf{tr}(\rho_i)).G_i\}_{i \in I}) \upharpoonright \mathbf{q} &\triangleq \begin{cases} \mathbf{p}' \oplus_{i \in I} !l_i(\exists[\rho_i|\{\rho_i \mapsto U_i\}].\mathbf{tr}(\rho_i)).(G_i \upharpoonright \mathbf{q}) & \text{if } \mathbf{q} = \mathbf{p}, \\ \mathbf{p} \&_{i \in I} ?l_i(\exists[\rho_i|\{\rho_i \mapsto U_i\}].\mathbf{tr}(\rho_i)).(G_i \upharpoonright \mathbf{q}) & \text{if } \mathbf{q} = \mathbf{p}', \\ \prod_{i \in I} (G_i \upharpoonright \mathbf{q}) & \text{if } \mathbf{p} \neq \mathbf{q} \neq \mathbf{p}' \end{cases} \end{aligned}$$

Where the merge operator for session types,  $\sqcap$ , is defined by:

$$\begin{aligned} \mathbf{end} \sqcap \mathbf{end} &\triangleq \mathbf{end} & \mathbf{t} \sqcap \mathbf{t} &\triangleq \mathbf{t} & \mu \mathbf{t}.S \sqcap \mu \mathbf{t}.S' &\triangleq \mu \mathbf{t}.(S \sqcap S') \\ \mathbf{p} \&_{i \in I} ?l_i(U_i).S_i \sqcap \mathbf{p} \&_{j \in J} ?l_j(U_j).S'_j &\triangleq \\ &\mathbf{p} \&_{k \in I \cap J} ?l_k(U_k).(S_k \sqcap S'_k) \& \mathbf{p} \&_{j \in I \setminus J} ?l_j(U_j).S_i \& \mathbf{p} \&_{j \in J \setminus I} ?l_j(U_j).S'_j \\ \mathbf{p} \oplus_{i \in I} !l_i(U_i).S_i \sqcap \mathbf{p} \oplus_{i \in I} !l_i(U_i).S_i &\triangleq \mathbf{p} \oplus_{i \in I} !l_i(U_i).S_i \\ \mathbf{p} \&_{i \in I} ?l_i(\exists[\rho_i|\{\rho_i \mapsto U_i\}].\mathbf{tr}(\rho_i)).S_i \sqcap \mathbf{p} \&_{j \in J} ?l_j(\exists[\rho_j|\{\rho_j \mapsto U_j\}].\mathbf{tr}(\rho_j)).S'_j &\triangleq \\ \mathbf{p} \&_{k \in I \cap J} ?l_k(\exists[\rho_k|\{\rho_k \mapsto U_k\}].\mathbf{tr}(\rho_k)).(S_k \sqcap S'_k) \& \mathbf{p} \&_{j \in I \setminus J} ?l_j(\exists[\rho_i|\{\rho_i \mapsto U_i\}].\mathbf{tr}(\rho_i)).S_i \\ &\& \mathbf{p} \&_{j \in J \setminus I} ?l_j(\exists[\rho_j|\{\rho_j \mapsto U_j\}].\mathbf{tr}(\rho_j)).S'_j \\ \mathbf{p} \oplus_{i \in I} !l_i(\exists[\rho_i|\{\rho_i \mapsto U_i\}].\mathbf{tr}(\rho_i)).S_i \sqcap \mathbf{p} \oplus_{i \in I} !l_i(\exists[\rho_i|\{\rho_i \mapsto U_i\}].\mathbf{tr}(\rho_i)).S_i &\triangleq \\ &\mathbf{p} \oplus_{i \in I} !l_i(\exists[\rho_i|\{\rho_i \mapsto U_i\}].\mathbf{tr}(\rho_i)).S_i \end{aligned}$$

Projecting **end** or a type variable  $\mathbf{t}$  onto any role does not change it. Projecting a recursive type  $\mu \mathbf{t}.G$  onto  $\mathbf{q}$  means projecting  $G$  onto  $\mathbf{q}$ . However, if  $G$  does

not involve  $q$  then  $G \upharpoonright q$  is a type variable,  $t'$ , and it must be replaced by  $\text{end}$  to avoid introducing an unguarded recursive type. Projecting an interaction between  $p$  and  $p'$  onto either  $p$  or  $p'$  produces a select or a branch. Projecting onto a different role  $q$  ignores the interaction and combines the projections of the continuations using the merge operator.

The merge operator,  $\sqcap$ , introduced in [13,37], allows more global types to have defined projections, which in turn allows more processes to be typed. Different external choices from the same role  $p$  are integrated by merging the continuation types following a common message label, and including the branches with different labels. Merging for internal choices is undefined unless the interactions are identical. This excludes meaningless types that result when a sender  $p$  is unaware of which branch has been chosen by other roles in a previous interaction.

**Definition 2.** For a session type  $S$ ,  $\text{roles}(S)$  denotes the set of roles occurring in  $S$ . We write  $p \in S$  for  $p \in \text{roles}(S)$ , and  $p \in S \setminus q$  for  $p \in \text{roles}(S) \setminus \{q\}$ .

**Partial session types** Fig. 5 have the same cases as local types, without role annotations. Partial types have a notion of *duality* which exchanges branch and select but preserves payload types.

**Definition 3.**  $\overline{H}$  is the dual of  $H$ , defined by:

$$\begin{aligned} \overline{\oplus_{i \in I} !l_i(U_i).H_i} &\triangleq \&_{i \in I} ?l_i(U_i).\overline{H_i} & \quad \overline{\&_{i \in I} ?l_i(U_i).H_i} &\triangleq \oplus_{i \in I} !l_i(U_i).\overline{H_i} \\ \overline{\oplus_{i \in I} !l_i(\exists[\rho_i|\{\rho_i \mapsto U_i\}].\text{tr}(\rho_i)).H_i} &\triangleq \&_{i \in I} ?l_i(\exists[\rho_i|\{\rho_i \mapsto U_i\}].\text{tr}(\rho_i)).\overline{H_i} \\ \overline{\&_{i \in I} ?l_i(\exists[\rho_i|\{\rho_i \mapsto U_i\}].\text{tr}(\rho_i)).H_i} &\triangleq \oplus_{i \in I} !l_i(\exists[\rho_i|\{\rho_i \mapsto U_i\}].\text{tr}(\rho_i)).\overline{H_i} \\ \overline{\text{end}} &\triangleq \text{end} & \quad \overline{t} &\triangleq t & \quad \overline{\mu t.H} &\triangleq \mu t.\overline{H} \end{aligned}$$

Similarly to the projection of global types to local types, a local type can be projected onto a role  $q$  to give a partial type. This yields a partial type that only describes the communications in  $S$  that involve  $q$ . The definition follows the same principles as the previous definition (cf. Definition 1).

**Definition 4.**  $S \upharpoonright q$  is the partial projection of  $S$  onto  $q$ :

$$\begin{aligned} \text{end} \upharpoonright q &\triangleq \text{end} & \quad t \upharpoonright q &\triangleq t & \quad (\mu t.S) \upharpoonright q &\triangleq \begin{cases} \mu t.(S \upharpoonright q) & \text{if } S \upharpoonright q \neq t' (\forall t') \\ \text{end} & \text{otherwise} \end{cases} \\ (p \oplus_{i \in I} !l_i(U_i).S_i) \upharpoonright q &\triangleq \begin{cases} \oplus_{i \in I} !l_i(U_i).(S_i \upharpoonright q) & \text{if } q = p, \\ \prod_{i \in I} (S_i \upharpoonright q) & \text{if } p \neq q \end{cases} \\ (p \&_{i \in I} ?l_i(U_i).S_i) \upharpoonright q &\triangleq \begin{cases} \&_{i \in I} ?l_i(U_i).S_i \upharpoonright q & \text{if } q = p, \\ \prod_{i \in I} (S_i \upharpoonright q) & \text{if } p \neq q \end{cases} \\ (p \oplus_{i \in I} !l_i(\exists[\rho_i|\{\rho_i \mapsto U_i\}].\text{tr}(\rho_i)).S_i) \upharpoonright q &\triangleq \begin{cases} \oplus_{i \in I} !l_i(\exists[\rho_i|\{\rho_i \mapsto U_i\}].\text{tr}(\rho_i)).(S_i \upharpoonright q) & \text{if } q = p, \\ \prod_{i \in I} (S_i \upharpoonright q) & \text{if } p \neq q \end{cases} \\ (p \&_{i \in I} ?l_i(\exists[\rho_i|\{\rho_i \mapsto U_i\}].\text{tr}(\rho_i)).S_i) \upharpoonright q &\triangleq \begin{cases} \&_{i \in I} ?l_i(\exists[\rho_i|\{\rho_i \mapsto U_i\}].\text{tr}(\rho_i)).S_i \upharpoonright q & \text{if } q = p, \\ \prod_{i \in I} (S_i \upharpoonright q) & \text{if } p \neq q \end{cases} \end{aligned}$$



Where the merge operator for partial session types,  $\sqcap$ , is defined by:

$$\begin{aligned}
\text{end} \sqcap \text{end} &\triangleq \text{end} & \mathfrak{t} \sqcap \mathfrak{t} &\triangleq \mathfrak{t} & \mu t.H \sqcap \mu t.H' &\triangleq \mu t.(H \sqcap H') \\
&\&_{i \in I} ?l_i(U_i).H_i \sqcap \&_{i \in I} ?l_i(U_i).H'_i &\triangleq \&_{i \in I} ?l_i(U_i).(H_i \sqcap H'_i) \\
&\oplus_{i \in I} !l_i(U_i).H_i \sqcap \oplus_{j \in J} !l_j(U_j).H'_j &\triangleq \\
&\quad (\oplus_{k \in I \cap J} !l_k(U_k).(H_k \sqcap H'_k)) \oplus (\oplus_{i \in I \setminus J} !l_i(U_i).H_i) \oplus (\oplus_{j \in J \setminus I} !l_j(U_j).H'_j) \\
&\&_{i \in I} ?l_i(\exists[\rho_i|\{\rho_i \mapsto U_i\}].\text{tr}(\rho_i)).H_i \sqcap \&_{i \in I} ?l_i(\exists[\rho_i|\{\rho_i \mapsto U_i\}].\text{tr}(\rho_i)).H'_i &\triangleq \\
&\quad \&_{i \in I} ?l_i(\exists[\rho_i|\{\rho_i \mapsto U_i\}].\text{tr}(\rho_i)).(H_i \sqcap H'_i) \\
&\oplus_{i \in I} !l_i(\exists[\rho_i|\{\rho_i \mapsto U_i\}].\text{tr}(\rho_i)).H_i \sqcap \oplus_{j \in J} !l_j(\exists[\rho_j|\{\rho_j \mapsto U_j\}].\text{tr}(\rho_j)).H'_j &\triangleq \\
&\quad (\oplus_{k \in I \cap J} !l_k(\exists[\rho_k|\{\rho_k \mapsto U_k\}].\text{tr}(\rho_k)).(H_k \sqcap H'_k)) \oplus (\oplus_{i \in I \setminus J} !l_i(\exists[\rho_i|\{\rho_i \mapsto U_i\}].\text{tr}(\rho_i)).H_i) \\
&\quad \oplus (\oplus_{j \in J \setminus I} !l_j(\exists[\rho_j|\{\rho_j \mapsto U_j\}].\text{tr}(\rho_j)).H'_j)
\end{aligned}$$

Unlike session type merging,  $\sqcap$  can combine different *internal* choices, but *not* external choices because that could violate type safety. Different internal choices can depend on the outcome of previous interactions with other roles, since this dependency can be safely approximated as an internal choice. Different external choices, however cannot capture this dependency.

*Example 2 (Projections of Global and Local Types).* Consider the global type  $G$  of the producer-consumer example from the introduction.

$$\begin{aligned}
G = & \mathbf{p} \rightarrow \mathbf{c} : \text{buffer}(\exists[\rho_q|\{\rho_q \mapsto S'_q\}].\text{tr}(\rho_q)).\mu t.\mathbf{q} \rightarrow \mathbf{b} : \text{add}(\text{Int}).\mathbf{p} \rightarrow \mathbf{c} : \text{turn}(\{\rho_q \mapsto S'_q\}). \\
& \mathbf{q} \rightarrow \mathbf{b} : \text{request}(\text{Str}).\mathbf{b} \rightarrow \mathbf{q} : \text{send}(\text{Int}).\mathbf{c} \rightarrow \mathbf{p} : \text{turn}(\{\rho_q \mapsto S_q\}).\mathfrak{t}
\end{aligned}$$

It captures the interaction between the producer and consumer entities through roles  $\mathbf{p}$ ,  $\mathbf{c}$ , and between producer, consumer and buffer through roles  $\mathbf{q}$  (shared between producer and consumer) and  $\mathbf{b}$ . Projecting onto  $\mathbf{p}$  gives the session type

$$\begin{aligned}
S = G \upharpoonright_{\mathbf{p}} = & \mathbf{c} \oplus !\text{buffer}(\exists[\rho_q|\{\rho_q \mapsto S'_q\}].\text{tr}(\rho_q)).\mu t.\mathbf{c} \oplus !\text{turn}(\{\rho_q \mapsto S'_q\}). \\
& \mathbf{c} \& ?\text{turn}(\{\rho_q \mapsto S_q\}).\mathfrak{t}
\end{aligned}$$

and further projecting onto  $\mathbf{c}$  gives the partial session type:

$$H = S \upharpoonright_{\mathbf{c}} = \oplus !\text{buffer}(\exists[\rho_q|\{\rho_q \mapsto S'_q\}].\text{tr}(\rho_q)).!\mu t.\oplus !\text{turn}(\{\rho_q \mapsto S'_q\}).\& ?\text{turn}(\{\rho_q \mapsto S_q\}).\mathfrak{t}$$

**Definition 5 (Subtyping).** Subtyping on session types  $\leq_S$  is the largest relation such that (i) if  $S \leq_S S'$ , then  $\forall \mathbf{p} \in (\text{roles}(S) \cup \text{roles}(S')) S \upharpoonright_{\mathbf{p}} \leq_P S' \upharpoonright_{\mathbf{p}}$ , and (ii) is closed backwards under the coinductive rules in Fig. 6. Subtyping on partial session types  $\leq_P$  is defined coinductively by the rules in Fig. 7.

Intuitively, the *subtyping relation* says that a session type  $S$  is “smaller” than  $S'$  when  $S$  is “less demanding” than  $S'$  i.e., when  $S$  allows more internal choices, and imposes fewer external choices, than  $S'$ . Clause (i) links local and partial subtyping, and ensures that if two types are related, then their partial projections exist. This clause is used later in defining consistency in Definition 8. In the second clause (ii) rules SBR, SSEL define subtyping on branch/select types, and SBRP, SSELP define subtyping on branch pack/select pack types. SBR and SBRP are covariant in their continuation types as well as in the number of branches offered, whereas SSEL, and SSELP are contravariant in both. SB relates base types,

$$\begin{array}{c}
\frac{\forall i \in I \quad U_i \leq_S U'_i \quad S_i \leq_S S'_i \quad \text{SBR}}{\mathbf{p} \&_{i \in I} ?l_i(U_i).S_i \leq_S \mathbf{p} \&_{i \in I \cup J} ?l_i(U'_i).S'_i} \quad \frac{\forall i \in I \quad U'_i \leq_S U_i \quad S_i \leq_S S'_i \quad \text{SSEL}}{\mathbf{p} \oplus_{i \in I \cup J} !l_i(U_i).S_i \leq_S \mathbf{p} \oplus_{i \in I} !l_i(U'_i).S'_i} \\
\frac{\forall i \in I \quad U_i \leq_S U'_i \quad S_i \leq_S S'_i \quad \text{SBRP}}{\mathbf{p} \&_{i \in I} ?l_i(\exists[\rho_i | \{\rho_i \mapsto U_i\}].\text{tr}(\rho_i)).S_i \leq_S \mathbf{p} \&_{i \in I \cup J} ?l_i(\exists[\rho_i | \{\rho_i \mapsto U'_i\}].\text{tr}(\rho_i)).S'_i} \\
\frac{\forall i \in I \quad U'_i \leq_S U_i \quad S_i \leq_S S'_i \quad \text{SSEL}}{\mathbf{p} \oplus_{i \in I \cup J} !l_i(\exists[\rho_i | \{\rho_i \mapsto U_i\}].\text{tr}(\rho_i)).S_i \leq_S \mathbf{p} \oplus_{i \in I} !l_i(\exists[\rho_i | \{\rho_i \mapsto U'_i\}].\text{tr}(\rho_i)).S'_i} \\
\frac{B \leq_B B' \quad \text{SB} \quad \frac{\text{end} \leq_S \text{end} \quad \text{SEND}}{\mu \mathbf{t}.S \leq_S S'} \quad \frac{S \{\mu \mathbf{t}.S / \mathbf{t}\} \leq_S S' \quad \text{S}\mu\text{L}}{\mu \mathbf{t}.S \leq_S S'} \quad \frac{S \leq_S S' \quad \{\mu \mathbf{t}.S' / \mathbf{t}\} \quad \text{S}\mu\text{R}}{S \leq_S \mu \mathbf{t}.S'}}{\frac{B \leq_B B' \quad \text{SB} \quad \frac{\text{end} \leq_S \text{end} \quad \text{SEND}}{\mu \mathbf{t}.S \leq_S S'} \quad \frac{S \{\mu \mathbf{t}.S / \mathbf{t}\} \leq_S S' \quad \text{S}\mu\text{L}}{\mu \mathbf{t}.S \leq_S S'} \quad \frac{S \leq_S S' \quad \{\mu \mathbf{t}.S' / \mathbf{t}\} \quad \text{S}\mu\text{R}}{S \leq_S \mu \mathbf{t}.S'}}}
\end{array}$$

**Fig. 6.** Subtyping for local session types.

$$\begin{array}{c}
\frac{\forall i \in I \quad U_i \leq_S U'_i \quad H_i \leq_P H'_i \quad \text{SPARBR}}{\&_{i \in I} ?l_i(U_i).H_i \leq_P \&_{i \in I \cup J} ?l_i(U'_i).H'_i} \quad \frac{\forall i \in I \quad U'_i \leq_S U_i \quad H_i \leq_P H'_i \quad \text{SPARSEL}}{\oplus_{i \in I \cup J} !l_i(U_i).H_i \leq_P \oplus_{i \in I} !l_i(U'_i).H'_i} \\
\frac{\forall i \in I \quad U_i \leq_S U'_i \quad H_i \leq_P H'_i \quad \text{SPARBRP}}{\&_{i \in I} ?l_i(\exists[\rho_i | \{\rho_i \mapsto U_i\}].\text{tr}(\rho_i)).H_i \leq_P \&_{i \in I \cup J} ?l_i(\exists[\rho_i | \{\rho_i \mapsto U'_i\}].\text{tr}(\rho_i)).H'_i} \\
\frac{\forall i \in I \quad U'_i \leq_S U_i \quad H_i \leq_P H'_i \quad \text{SPARSELP}}{\oplus_{i \in I \cup J} !l_i(\exists[\rho_i | \{\rho_i \mapsto U_i\}].\text{tr}(\rho_i)).H_i \leq_P \oplus_{i \in I} !l_i(\exists[\rho_i | \{\rho_i \mapsto U'_i\}].\text{tr}(\rho_i)).H'_i} \\
\frac{\text{end} \leq_P \text{end} \quad \text{SPAREND} \quad \frac{H \{\mu \mathbf{t}.H / \mathbf{t}\} \leq_P H' \quad \text{SPAR}\mu\text{L}}{\mu \mathbf{t}.H \leq_P H'} \quad \frac{H \leq_P H' \quad \{\mu \mathbf{t}.H' / \mathbf{t}\} \quad \text{SPAR}\mu\text{R}}{H \leq_P \mu \mathbf{t}.H'}}{\frac{\text{end} \leq_P \text{end} \quad \text{SPAREND} \quad \frac{H \{\mu \mathbf{t}.H / \mathbf{t}\} \leq_P H' \quad \text{SPAR}\mu\text{L}}{\mu \mathbf{t}.H \leq_P H'} \quad \frac{H \leq_P H' \quad \{\mu \mathbf{t}.H' / \mathbf{t}\} \quad \text{SPAR}\mu\text{R}}{H \leq_P \mu \mathbf{t}.H'}}}
\end{array}$$

**Fig. 7.** Subtyping for partial session types.

if they are related by  $\leq_B$ .  $\text{SEND}$  relates terminated channel types.  $\text{S}\mu\text{L}$  and  $\text{S}\mu\text{R}$  are standard under coinduction [26, § 21], relating types up-to their unfolding.

**Capabilities** In our type system linearity is enforced via capabilities, rather than via environment splitting as in most session type systems. Each process has a capability set  $C$  associated with it, allowing it to communicate on the associated channels. The tracked type  $\text{tr}(\rho)$  is a singleton type associating a channel to capability  $\rho$  and to no other, which in turn maps to the channel's session type  $\{\rho \mapsto S\}$ . Hence two variables with the same capability  $\rho$  are aliases for the same channel. Individual capabilities are joined together using the  $\otimes$  operator:  $C = \{\rho_1 \mapsto S_1\} \otimes \dots \otimes \{\rho_n \mapsto S_n\}$ . The ordering is insignificant. The type system maintains the invariant that  $\rho_1, \dots, \rho_n$  are distinct.

**Definition 6 (Terminated capabilities).** A capability set  $C$  is terminated if for every  $\rho \in \text{dom}(C)$ ,  $C(\rho) = \text{end}$ .

**Definition 7 (Substitution of capabilities).**

$$\begin{aligned}
\{\rho \mapsto S\}[\rho' / \rho_2] &= \{\rho \mapsto S\} & \{\rho \mapsto S\}[\rho' / \rho] &= \{\rho' \mapsto S\} \\
\emptyset[\rho' / \rho] &= \emptyset & (C_1 \otimes C_2)[\rho' / \rho] &= C_1[\rho' / \rho] \otimes C_2[\rho' / \rho]
\end{aligned}$$

$$\begin{array}{c}
\text{TCAP} \quad \frac{}{\Gamma \vdash \rho : \{\rho \mapsto S\}; \{\rho \mapsto S\}} \quad \text{TVAL} \quad \frac{v \in B}{\Gamma \vdash v : B; \emptyset} \quad \text{TINACT} \quad \frac{C \text{ terminated}}{\Delta; \Gamma \vdash \mathbf{0}; C} \\
\text{TVAR} \quad \frac{c : \mathbf{tr}(\rho), \rho : \{\rho \mapsto S\} \in \Gamma}{\Gamma \vdash c : \mathbf{tr}(\rho); \emptyset} \\
\text{TPAR} \quad \frac{\Delta; \Gamma \vdash P; C_1 \quad \Delta; \Gamma \vdash Q; C_2}{\Delta; \Gamma \vdash P | Q; C_1 \otimes C_2} \quad \text{TSUB} \quad \frac{\Delta; \Gamma \vdash P; C \otimes \{\rho \mapsto U\} \quad U' \leq_S U}{\Delta; \Gamma \vdash P; C \otimes \{\rho \mapsto U'\}} \\
\text{TSEL} \quad \frac{\Gamma \vdash v : U; C \quad \Delta; \Gamma \vdash P; C' \otimes \{\rho \mapsto S_j\} \quad c : \mathbf{tr}(\rho), \rho : \{\rho \mapsto S_j\} \in \Gamma \quad j \in I}{\Delta; \Gamma \vdash c[\mathbf{p}] \oplus (l_j(v)).P; C \otimes C' \otimes \{\rho \mapsto \mathbf{p} \oplus_{i \in I} !l_i(U_i).S_i\}} \\
\text{TBR} \quad \frac{\Delta; \Gamma, x_i : U_i \vdash P_i; C \otimes C_i \otimes \{\rho \mapsto S_i\} \quad c : \mathbf{tr}(\rho), \rho : \{\rho \mapsto S_i\} \in \Gamma \quad \forall i \in I}{\Delta; \Gamma \vdash c[\mathbf{p}] \&_{i \in I} \{l_i(x_i).P_i\}; C \otimes \{\rho \mapsto \mathbf{p} \&_{i \in I} ?l_i(U_i).S_i\}} \\
\text{TSELP} \quad \frac{\Gamma \vdash v : \mathbf{tr}(\rho'); \emptyset \quad \Delta; \Gamma \vdash P; C \otimes \{\rho \mapsto S_j, \rho' \mapsto U\} \quad c : \mathbf{tr}(\rho), \rho : \{\rho \mapsto S_j\} \in \Gamma \quad j \in I}{\Delta; \Gamma \vdash c[\mathbf{p}] \oplus (l_j(\text{pack}(\rho', v))).P; C \otimes \{\rho \mapsto \mathbf{p} \oplus_{i \in I} !l_i(\exists[\rho' | \{\rho' \mapsto U\}].\mathbf{tr}(\rho')).S_i, \rho' \mapsto U\}} \\
\text{TBRP} \quad \frac{\Delta; \Gamma, \mathbf{v}_i : \mathbf{tr}(\rho_i), \rho_i : \{\rho_i \mapsto U_i\} \vdash P_i; C \otimes \{\rho \mapsto S_i\} \quad \forall i \in I \quad c : \mathbf{tr}(\rho), \rho : \{\rho \mapsto S_i\} \in \Gamma}{\Delta; \Gamma \vdash c[\mathbf{p}] \&_{i \in I} \{l_i(\text{pack}(\rho_i, \mathbf{v}_i)).P_i\}; C \otimes \{\rho \mapsto \mathbf{p} \&_{i \in I} ?l_i(\exists[\rho_i | \{\rho_i \mapsto U_i\}].\mathbf{tr}(\rho_i)).S_i\}} \\
\text{TRES} \quad \frac{\Delta; \Gamma, \Gamma' \vdash P; C \otimes C' \quad (\Gamma' = \{\mathbf{s}[\mathbf{p}] : \mathbf{tr}(\rho_p), \rho_p : \{\rho_p \mapsto S_p\}\}_{p \in I}, C' = \otimes_{p \in I} \{\rho_p \mapsto S_p\}) \text{ complete}}{\Delta; \Gamma \vdash (\nu s : \Gamma')P; C} \\
\text{TDEF} \quad \frac{\Delta, X : \tilde{U}; \tilde{x} : \tilde{U} \vdash P; \tilde{C} \quad \Delta, X : \tilde{U}; \Gamma \vdash Q; C}{\Delta; \Gamma \vdash \text{def } X \langle \tilde{x} : \tilde{U} \rangle = P; \tilde{C} \text{ in } Q; C} \quad \text{TCALL} \quad \frac{\forall i \in \{1..n\} \quad \Gamma \vdash v_i : U_i; C_i}{\Delta, X : U_1, \dots, U_n; \Gamma \vdash X \langle v_1, \dots, v_n \rangle; C_1 \otimes \dots \otimes C_n}
\end{array}$$

Fig. 8. Typing rules

There are two important concepts relating the environment  $\Gamma$  and the capability set  $C$ : *completeness* and *consistency*, used in our type system.

Completeness means that if a channel is in  $\Gamma$  and its capability is in  $C$ , then  $\Gamma$  also contains the other endpoints of the channel and  $C$  contains the corresponding capability. In this case, there is a self-contained collection of channels that can communicate. Consistency means that the opposite endpoints of every channel have dual partial types.

**Definition 8 (Completeness and consistency).**

$(\Gamma, C)$  is *complete* iff for all  $\mathbf{s}[\mathbf{p}] : \mathbf{tr}(\rho_p)$  with  $\rho_p : \{\rho_p \mapsto S_p\} \in \Gamma$  and  $\{\rho_p \mapsto S_p\} \in C$ ,  $\mathbf{q} \in S_p$  implies  $\mathbf{s}[\mathbf{q}] : \mathbf{tr}(\rho_q), \rho_q : \{\rho_q \mapsto S_q\} \in \Gamma$  and  $\{\rho_q \mapsto S_q\} \in C$ .

$(\Gamma, C)$  is *consistent* iff for all  $\mathbf{s}[\mathbf{p}] : \mathbf{tr}(\rho_p), \mathbf{s}[\mathbf{q}] : \mathbf{tr}(\rho_q), \rho_p : \{\rho_p \mapsto S_p\}, \rho_q : \{\rho_q \mapsto S_q\} \in \Gamma$  we have  $S_p \upharpoonright_{\mathbf{q}} \leq_P S_q \upharpoonright_{\mathbf{p}}$ .

**Definition 9.** *Typing judgements are inductively defined by the rules in Fig. 8, and have the form:  $\Gamma \vdash v : T; C$  for values, or  $\Delta; \Gamma \vdash P; C$  for processes (with  $(\Gamma, C)$  consistent, and  $\forall (c : \text{tr}(\rho) \in \Gamma; \{\rho \mapsto S\} \in C), S \upharpoonright_{\mathbf{p}}$  is defined  $\forall \mathbf{p} \in S$ ).*

$\Gamma$  is an environment of typed variables and channels together with their capability typing.  $\Delta$ , defined in Fig. 5 is an environment of typed process names, used in rules  $\text{TDEF}$  and  $\text{TCALL}$  for recursive process definitions and calls. If a channel  $\mathbf{s}[\mathbf{p}]$  is in  $\Gamma$ , with type  $\text{tr}(\rho)$ , then  $\Gamma$  also contains  $\rho : \{\rho \mapsto S\}$  for some session type  $S$ . The capability  $\rho$  might, or might not, be in  $C$ , to show whether or not the channel can be used. If  $\rho$  is in  $C$ , then it occurs with the same session type:  $\{\rho \mapsto S\}$ .

Rule  $\text{TCAP}$  takes the type for a capability  $\rho$  from the capability set.  $\text{TVAR}$  and  $\text{TVAL}$  are standard.  $\text{TINACT}$  has a standard condition that all session types have reached **end**, expressed as the capability set being terminated.  $\text{TPAR}$  combines the capability sets in a parallel composition.  $\text{TSUB}$  is a standard subsumption rule using  $\leq_s$  (Definition 5), the difference being the type in the capability set.  $\text{TSEL}$  (resp.  $\text{TBR}$ ) states that the selection (resp. branching) on channel  $\mathbf{c}[\mathbf{p}]$  is well typed if the capability associated with it is of compatible selection (resp. branching) type and the continuations  $P_i, \forall i \in I$  are well-typed with the continuation session types.  $\text{TSELP}$  is similar to  $\text{TSEL}$ , with the notable difference that an existential package is created for the channel being sent, containing the channel and its abstracted capability. Note that the actual capability to use the endpoint remains with process  $P$ .  $\text{TBRP}$  is similar to  $\text{TBR}$ , with the difference that it unpackages the channel received and binds its capability type in the continuation session type (used to identify the correct capability when received later).  $\text{TRER}$  requires the restricted environment  $\Gamma'$  and the associated capability set  $C'$  to be *complete* (Definition 8).  $\text{TDEF}$  takes account of capability sets as well as parameters, and  $\text{TCALL}$  similarly requires capability sets. The parameters of a defined process include any necessary capabilities, which then also appear in the corresponding  $C_i$ , because not all capabilities associated with the channel parameters need to be present when the call is made.

## 4 Case study: Producer-Consumer

We now expand on the producer-consumer scenario from §1 by discussing the process definitions and showing part of the typing derivation. To lighten the notation, we present a set of mutually recursive definitions, instead of using the formal syntax of `def ... in`.

Recall that the example consists of three processes: the producer, the consumer, and a one-place buffer (Fig. 1). The producer and the consumer communicate with the buffer on a single shared channel. Each of the two must wait to receive the *capability* to communicate on the channel before doing so.

The buffer  $\mathbf{B}$  is parameterised by channel  $\mathbf{x}$  and by the capability for it,  $\rho_{\mathbf{x}}$ , and alternately responds to **add** and **request** messages. At the end of the definition,  $\{\rho_{\mathbf{x}} \mapsto S_{\mathbf{b}}\}$  shows the held capability and its session type.

$\mathbf{B}(\mathbf{x} : \text{tr}(\rho_{\mathbf{x}}), \rho_{\mathbf{x}} : \{\rho_{\mathbf{x}} \mapsto S_{\mathbf{b}}\}) = \mathbf{x}[\mathbf{q}] \& \text{add}(i) . \mathbf{x}[\mathbf{q}] \& \text{request}(\mathbf{x}) . \mathbf{x}[\mathbf{p}] \oplus \text{send}(i) . \mathbf{B}(\mathbf{x}, \rho_{\mathbf{x}}); \{\rho_{\mathbf{x}} \mapsto S_{\mathbf{b}}\}$

The producer is represented by two process definitions: `Produce` and `P`. `Produce` is a recursive process with several parameters. Channels `x` and `y` are used to communicate with the consumer and the buffer, respectively. Their capabilities are  $\rho_x$  and  $\rho_y$ . Finally, `i` is the value to be sent to the buffer. The process sends a value to the buffer (`add(i)`), transfers the capability for the shared channel `y` (`turn(\rho_y)`) and receives it back from the consumer. Process `P` is the entry point for the producer. It has the same parameters as `Produce`, except for `i`. The only action of `P` is to send the consumer a shared reference to the channel used for communication with the buffer  $\text{---}x[c] \oplus \text{buffer}(\text{pack}(\rho_y, y[b]))$ .

$$\begin{aligned} \text{Produce}(x : \text{tr}(\rho_x), y : \text{tr}(\rho_y), i : \text{Int}, \rho_x : \{\rho_x \mapsto S'_p\}, \rho_y : \{\rho_y \mapsto S_q\}) &= y[b] \oplus \text{add}(i). \\ & x[c] \oplus \text{turn}(\rho_y). x[c] \& \text{turn}(\rho_y). \text{Produce}(x, y, i+1, \rho_x, \rho_y); \{\rho_x \mapsto S'_p\} \otimes \{\rho_y \mapsto S_q\} \\ P(x : \text{tr}(\rho_x), y : \text{tr}(\rho_y), \rho_x : \{\rho_x \mapsto S_p\}, \rho_y : \{\rho_y \mapsto S_q\}) &= \\ & x[c] \oplus \text{buffer}(\text{pack}(\rho_y, y[b])). \text{Produce}(x, y, 0, \rho_x, \rho_y); \{\rho_x \mapsto S_p\} \otimes \{\rho_y \mapsto S_q\} \end{aligned}$$

In a similar way, the consumer is represented by `Consume` and `C`. The parameters, however, are different. `C` has `x` and its capability  $\rho_x$ , for communication with the producer, but it does not have `y` or  $\rho_y$  for communication with the buffer. It receives `y` from the producer, as part of `pack(\rho_y, y[b])`, and `y` is passed as a parameter to `Consume`. The capability  $\rho_y$  is not a parameter of `Consume`, but it is received in a turn message from the producer.

$$\begin{aligned} \text{Consume}(x : \text{tr}(\rho_x), y : \text{tr}(\rho_y), \rho_x : \{\rho_x \mapsto S'_c\}) &= x[p] \& \text{turn}(\rho_y). y[b] \oplus \text{request}(r). \\ & y[b] \& \text{send}(i). x[p] \oplus \text{turn}(\rho_y). \text{Consume}(x, y, \rho_x); \{\rho_x \mapsto S'_c\} \\ C(x : \text{tr}(\rho_x), \rho_x : \{\rho_x \mapsto S_c\}) &= \\ & x[p] \& \text{buffer}(\text{pack}(\rho_y, y[b])). \text{Consume}(x, y, \rho_x); \{\rho_x \mapsto S_c\} \end{aligned}$$

The complete system consists of the producer, the consumer and the buffer in parallel, with sessions  $s_1$  (roles `p` and `c`) and  $s_2$  (roles `q` and `b`) scoped to construct a closed process.

$$(\nu s_1)((\nu s_2)(P\langle s_1[p], s_2[q], \rho_p, \rho_q \rangle \mid B\langle s_2[b], \rho_b \rangle) \mid C\langle s_1[c], \rho_c \rangle)$$

The session types involved in these processes are projections of the global type  $G$  (§3). They specify how each role is expected to use its channel endpoint. The roles are `b` for the buffer, `q` for the combined role of the producer and the consumer as they interact with the buffer, `p` for the producer, and `c` for the consumer.

$$\begin{aligned} S_b &= G \upharpoonright b = \mu t. q \& ? \text{add}(\text{Int}). q \& ? \text{request}(\text{Str}). q \oplus ! \text{send}(\text{Int}). t \\ S_q &= G \upharpoonright q = \mu t. b \oplus ! \text{add}(\text{Int}). b \oplus ! \text{request}(\text{Str}). b \& ? \text{send}(\text{Int}). t \\ S_p &= G \upharpoonright p = c \oplus ! \text{buffer}(\exists[\rho_q] \{\rho_q \mapsto S'_q\}). \text{tr}(\rho_q). \mu t. \\ & c \oplus ! \text{turn}(\{\rho_q \mapsto S'_q\}). c \& ? \text{turn}(\{\rho_q \mapsto S_q\}). t \\ S_c &= G \upharpoonright c = p \& ? \text{buffer}(\exists[\rho_q] \{\rho_q \mapsto S'_q\}). \text{tr}(\rho_q). \mu t. \\ & p \& ? \text{turn}(\{\rho_q \mapsto S'_q\}). p \oplus ! \text{turn}(\{\rho_q \mapsto S_q\}). t \end{aligned}$$

These types occur in the capabilities associated with each process. For example process  $P\langle s_1[p], s_2[q], \rho_p, \rho_q \rangle$  has  $\{\rho_q \mapsto S_q\} \otimes \{\rho_p \mapsto S_p\}$ , process  $B\langle s_2[b], \rho_b \rangle$  has  $\{\rho_b \mapsto S_b\}$ , and process  $C\langle s_1[c], \rho_c \rangle$  has  $\{\rho_c \mapsto S_c\}$ .

$$\begin{array}{c}
\frac{\Gamma \vdash \mathbf{x} : \mathbf{tr}(\rho_x), \mathbf{y} : \mathbf{tr}(\rho_y), i : \mathbf{Int}, \rho_x : \{\rho_x \mapsto S'_p\}, \rho_y : \{\rho_y \mapsto S_q\}; \{\rho_x \mapsto S'_p, \rho_y \mapsto S_q\}}{\Delta; \Gamma \vdash \mathbf{Produce}(x, y, i+1, \rho_x, \rho_y); \{\rho_x \mapsto S'_p, \rho_y \mapsto S_q\}} \text{TCALL} \\
\frac{\Delta; \Gamma \vdash \mathbf{x}[c] \& \{\mathbf{turn}(\rho_y).\mathbf{Produce}(x, y, i+1, \rho_x, \rho_y)\}; \{\rho_x \mapsto c \& ?\mathbf{turn}(\{\rho_q \mapsto S_q\}).S'_p\}}{\vdots} \text{TBR} \\
\vdots \\
\vdots \\
\frac{\Gamma \vdash \rho_q : \{\rho_q \mapsto S'_q\}; \{\rho_q \mapsto S'_q\} \quad \mathbf{x} : \mathbf{tr}(\rho_x), \rho_x : \{\rho_x \mapsto c \& ?\mathbf{turn}(\{\rho_q \mapsto S_q\}).S'_p\} \in \Gamma}{\Delta; \Gamma \vdash \mathbf{x}[c] \oplus \langle \mathbf{turn}(\rho_q) \rangle . \mathbf{x}[c] \& \{\mathbf{turn}(\rho_y).\mathbf{Produce}(x, y, i+1, \rho_x, \rho_y)\}; \{\rho_x \mapsto S'_p, \rho_y \mapsto S'_q\}} \text{TSEL} \\
\vdots \\
\vdots \\
\frac{i \in \mathbf{Int}}{\Gamma \vdash i : \mathbf{Int}; \emptyset} \text{TVAL} \quad \mathbf{y} : \mathbf{tr}(\rho_y), \rho_y : \{\rho_y \mapsto S'_q\} \in \Gamma}{\Delta; \Gamma \vdash \mathbf{y}[b] \oplus \langle \mathbf{add}(i) \rangle . \mathbf{x}[c] \oplus \langle \mathbf{turn}(\rho_q) \rangle . \mathbf{x}[c] \& \{\mathbf{turn}(\rho_q).\mathbf{Produce}(x, y, i+1, \rho_x, \rho_y)\}; \{\rho_x \mapsto S'_p, \rho_y \mapsto S'_q\}} \text{TSEL}
\end{array}$$

Fig. 9. Typing derivation for Produce.

$$\begin{array}{c}
\frac{\Gamma \vdash \mathbf{x} : \mathbf{tr}(\rho_x), \mathbf{y} : \mathbf{tr}(\rho_y), \rho_x : \{\rho_x \mapsto S'_p\}, \rho_y : \{\rho_y \mapsto S_q\}; \{\rho_x \mapsto S'_p, \rho_y \mapsto S_q\}}{\Delta; \Gamma \vdash \mathbf{Produce}(x, y, i, \rho_p, \rho_q); \{\rho_x \mapsto S'_p, \rho_y \mapsto S_q\}} \text{TCALL} \\
\vdots \\
\vdots \\
\frac{\mathbf{y} : \mathbf{tr}(\rho_y), \rho_y : \{\rho_y \mapsto S_q\}}{\Gamma \vdash \mathbf{y} : \mathbf{tr}(\rho_y); \emptyset} \text{TVAR} \quad \mathbf{x}, \rho_x : \{\rho_x \mapsto S'_p\} \in \Gamma}{\Delta; \Gamma \vdash \mathbf{x}[c] \oplus \langle \mathbf{buffer}(\mathbf{pack}(\rho_q, \mathbf{y}[b])) \rangle . \mathbf{Produce}(x, y, i, \rho_x, \rho_y); \{\rho_y \mapsto p \oplus !(\exists[\rho_y] \{\rho_y \mapsto S_q\}).\mathbf{tr}(\rho_y)).S'_p, \rho_y \mapsto S_q\}} \text{TSELP}
\end{array}$$

Fig. 10. Typing derivation for P.

To illustrate the typing rules, we show the typing derivation for the producer, i.e. processes `Produce` (Fig. 9) and `P` (Fig. 10). Full derivations for all of the processes are in the technical report. The derivations use the following definitions.

$$\begin{aligned}
S'_p &= \mu \mathbf{t} . c \oplus !\mathbf{turn}(\{\rho_q \mapsto S'_q\}).c \& ?\mathbf{turn}(\{\rho_q \mapsto S_q\}).t \\
S'_q &= \mathbf{b} \oplus !\mathbf{request}(\mathbf{Str}).\mathbf{b} \& ?\mathbf{send}(\mathbf{Int}).S_q \\
\Delta &= \mathbf{Produce} : (\mathbf{tr}(\rho_p), \mathbf{tr}(\rho_q), \mathbf{Int}, \{\rho_p \mapsto S'_p\}, \{\rho_q \mapsto S_q\}) \\
\Gamma &= \mathbf{x} : \mathbf{tr}(\rho_p), \mathbf{y} : \mathbf{tr}(\rho_q), i : \mathbf{Int}, \rho_p : \{\rho_p \mapsto S'_p\}, \rho_q : \{\rho_q \mapsto S_q\}
\end{aligned}$$

Scenarios with multiple producers/consumers can be represented in a similar way, the capabilities acting as a form of lock for the resource being shared. The full typing derivation for producer consumer case study can be found in the extended version of this paper [34].

## 5 Technical Results

Following standard practice in the MPST literature, we show type safety and hence communication safety by proving a subject reduction theorem (Theorem 1). In the usual way, session types evolve during reduction—in our system, this is seen in both the  $\Gamma$  environment and the capability set  $C$ .

**Definition 10 (Typing context reduction).** *The reduction  $(\Gamma; C) \longrightarrow (\Gamma'; C')$*

*is:*

$$\begin{aligned}
& (\mathbf{s}[\mathbf{p}]: \mathbf{tr}(\rho_{\mathbf{p}}), \mathbf{s}[\mathbf{q}]: \mathbf{tr}(\rho_{\mathbf{q}}), \rho_{\mathbf{p}}: \{\rho_{\mathbf{p}} \mapsto S_{\mathbf{p}}\}, \rho_{\mathbf{q}}: \{\rho_{\mathbf{q}} \mapsto S_{\mathbf{q}}\}; \{\rho_{\mathbf{p}} \mapsto S_{\mathbf{p}}, \rho_{\mathbf{q}} \mapsto S_{\mathbf{q}}\}) \longrightarrow \\
& (\mathbf{s}[\mathbf{p}]: \mathbf{tr}(\rho_{\mathbf{p}}), \mathbf{s}[\mathbf{q}]: \mathbf{tr}(\rho_{\mathbf{q}}), \rho_{\mathbf{p}}: \{\rho_{\mathbf{p}} \mapsto S_k\}, \rho_{\mathbf{q}}: \{\rho_{\mathbf{q}} \mapsto S'_k\}; \{\rho_{\mathbf{p}} \mapsto S_k, \rho_{\mathbf{q}} \mapsto S'_k\}) \\
& \quad \text{if } \begin{cases} \mathbf{unf}(S_{\mathbf{p}}) = \mathbf{q} \oplus_{i \in I} !l_i(U_i).S_i & k \in I \\ \mathbf{unf}(S_{\mathbf{q}}) = \mathbf{p} \&_{i \in I \cup J} ?l_i(U'_i).S'_i & U_k \leq_S U'_k \end{cases} \\
& \quad \text{or if } \begin{cases} \mathbf{unf}(S_{\mathbf{p}}) = \mathbf{q} \oplus_{i \in I} !l_i(\exists[\rho_i | \{\rho_i \mapsto U_i\}].\mathbf{tr}(\rho_i)).S_i & k \in I \\ \mathbf{unf}(S_{\mathbf{q}}) = \mathbf{p} \&_{i \in I \cup J} ?l_i(\exists[\rho_i | \{\rho_i \mapsto U'_i\}].\mathbf{tr}(\rho_i)).S'_i & U_k \leq_S U'_k \end{cases} \\
& (\Gamma, \mathbf{c}: \mathbf{tr}(\rho), \rho: \{\rho \mapsto U\}; C \otimes \{\rho \mapsto U\}) \longrightarrow (\Gamma', \mathbf{c}: \mathbf{tr}(\rho), \rho: \{\rho \mapsto U'\}; C' \otimes \{\rho \mapsto U'\}) \\
& \quad \text{if } (\Gamma; C) \longrightarrow (\Gamma'; C') \text{ and } U \leq_S U'
\end{aligned}$$

Following [28] our Definition 10 also accommodates subtyping ( $\leq_S$ ) and our iso-recursive type equivalence (hence, unfolds types explicitly).

**Theorem 1 (Subject reduction).** *If  $\Delta; \Gamma \vdash P; C$  and  $P \longrightarrow P'$ , then there exist  $\Gamma'$  and  $C'$  such that  $\Delta; \Gamma' \vdash P'; C'$  and  $(\Gamma; C) \longrightarrow^* (\Gamma'; C')$ .*

The proof is by induction on the derivation of  $P \longrightarrow P'$ , with an analysis of the derivation of  $\Delta; \Gamma \vdash P; C$ . A key case is  $\text{RRES}$ , which requires preservation of the condition in  $\text{TRRES}$  that  $(\Gamma, C)$  is consistent. This is because a communication reduction consumes matching prefixes from a pair of dual partial session types, which therefore remain dual. The full proof is in the extended version of this paper [34].

## 6 Related Work, Conclusion and Future Work

From the beginning of session types, channel endpoints were treated as linear resources so that each role in a protocol could be implemented by a unique agent. This approach is reinforced by several connections between session types and other linear type theories: the encodings of binary session types and multiparty session types into linear  $\pi$ -calculus types [12,28]; the Curry-Howard correspondence between binary session types and linear logic [6,35]; the connection between multiparty session types and linear logic [7,8].

Some session type systems generalise linearity. Vasconcelos [33] allows a session type to become non-linear, and sharable, when it reaches a state that is invariant with every subsequent message. Mostrous and Vasconcelos [24] define *affine* session types, in which each endpoint must be used at most once and can be discarded with an explicit operator. In Fowler *et al.*'s [15] implementation of session types for the Links web programming language, affine typing allows sessions to be cancelled when exceptions (including dropped connections) occur. Caires and Pérez [5] use monadic types to describe cancellation (i.e. affine sessions) and non-determinism. Pruiksma and Pfenning [27] use adjoint logic to describe session cancellation and other behaviours including multicast and replication.

Usually linearity spreads, because a data structure containing linear values must also be linear. In the standard  $\pi$ -calculus, exceptions to this nature of

linearity have been studied by Kobayashi in his work on deadlock-freedom Padovani [25] extends the linear  $\pi$ -calculus with composite regular types in such a way that data containing linear values can be shared among several processes. However, this sharing can occur only if there is no overlapping access to such values, which differs from our work where we have full sharing of values. On the other hand, we work directly with (multiparty) session types, whereas Padovani works with linear  $\pi$ -calculus and obtains his results via the encoding of session types into linear  $\pi$ -types [12].

Session types are related to the concept of *typestate* [30], especially in the work of Kouzapas *et al.* [21,22] which defines a typestate system for Java based on multiparty session types. Typestate systems require linear typing or some other form of alias control, to avoid conflicting state changes via multiple references. Approaches include the permission-based systems used in the Plural and Plaid languages [4,31] and the fine-grained approach of Militão *et al.* [23]. Crafa and Padovani [10] develop a “chemical” approach to concurrent typestate oriented programming, allowing objects to be accessed and modified concurrently by several processes, each potentially changing only part of their state. Our approach is partly inspired by Fähndrich and DeLine’s “adoption and focus” system [14], in which a shared stateful resource (in our case, a session channel) is separated from the linear key (capability, in our system) that enables it to be used. In this way the state changes of channels follow the standard session operations, channels can be shared (for example, stored in shared data structures), and access can be controlled by passing the capability around the system.

Balzer *et al.* [2,3] support sharing of binary session channels by allowing locks to be acquired and released at points that are explicitly specified in the session type. Our approach with multiparty sessions is not based on locks, so it doesn’t require runtime mechanisms for managing blocked processes and notifying them when locks are released.

We have presented a new system of multiparty session types with capabilities, which allows sharing of resources in a way that generalises the strictly linear or affine access control typical of session type systems. The key technical idea is to separate a channel from the capability of using the channel. This allows channels to be shared, while capabilities are linearly controlled. We use a form of existential typing to maintain the link between a channel and its capability, while both are transmitted in messages. We have proved communication safety, formulated as a subject reduction theorem (Theorem 1). An area of future work is to prove progress and deadlock-freedom properties along the lines of, for example, Coppo *et al.* [9]. Another possibility is to apply our techniques to functional languages with session types [17].

## References

1. Ancona, D., et al.: Behavioral types in programming languages. *Foundations and Trends in Programming Languages* **3**(2–3), 95–230 (2016). <https://doi.org/10.1561/25000000031>



2. Balzer, S., Pfenning, F.: Manifest sharing with session types. *PACMPL* **1**(ICFP), 37:1–37:29 (2017). <https://doi.org/10.1145/3110281>
3. Balzer, S., Toninho, B., Pfenning, F.: Manifest deadlock-freedom for shared session types. In: *ESOP. LNCS*, vol. 11423, pp. 611–639. Springer (2019). [https://doi.org/10.1007/978-3-030-17184-1\\_22](https://doi.org/10.1007/978-3-030-17184-1_22)
4. Bierhoff, K., Aldrich, J.: PLURAL: checking protocol compliance under aliasing. In: *ICSE Companion*. pp. 971–972. ACM Press (2008). <https://doi.org/http://doi.acm.org/10.1145/1370175.1370213>
5. Caires, L., Pérez, J.A.: Linearity, control effects, and behavioral types. In: *ESOP. LNCS*, vol. 10201, pp. 229–259. Springer (2017). [https://doi.org/10.1007/978-3-662-54434-1\\_9](https://doi.org/10.1007/978-3-662-54434-1_9)
6. Caires, L., Pfenning, F.: Session types as intuitionistic linear propositions. In: *CONCUR. LNCS*, vol. 6269, pp. 222–236. Springer (2010). [https://doi.org/10.1007/978-3-642-15375-4\\_16](https://doi.org/10.1007/978-3-642-15375-4_16)
7. Carbone, M., Lindley, S., Montesi, F., Schürmann, C., Wadler, P.: Coherence generalises duality: A logical explanation of multiparty session types. In: *CONCUR. LIPIcs*, vol. 59, pp. 33:1–33:15. Schloss Dagstuhl — Leibniz-Zentrum für Informatik (2016). <https://doi.org/10.4230/LIPIcs.CONCUR.2016.33>
8. Carbone, M., Montesi, F., Schürmann, C., Yoshida, N.: Multiparty session types as coherence proofs. In: *CONCUR. LIPIcs*, vol. 42. Schloss Dagstuhl — Leibniz-Zentrum für Informatik (2015). <https://doi.org/10.4230/LIPIcs.CONCUR.2015.412>
9. Coppo, M., Dezani-Ciancaglini, M., Yoshida, N., Padovani, L.: Global progress for dynamically interleaved multiparty sessions. *Mathematical Structures in Computer Science* **26**(2), 238–302 (2016). <https://doi.org/10.1017/S0960129514000188>
10. Crafa, S., Padovani, L.: The chemical approach to typestate-oriented programming. *ACM Transactions on Programming Languages and Systems* **39**(3), 13:1–13:45 (2017). <https://doi.org/10.1145/3064849>
11. Crary, K., Walker, D., Morrisett, G.: Typed memory management in a calculus of capabilities. In: *POPL*. pp. 262–275. ACM (1999). <https://doi.org/10.1145/292540.292564>
12. Dardha, O., Giachino, E., Sangiorgi, D.: Session types revisited. In: *PPDP. ACM* (2012). <https://doi.org/10.1145/2370776.2370794>
13. Deniélou, P., Yoshida, N., Bejleri, A., Hu, R.: Parameterised multiparty session types. *Logical Methods in Computer Science* **8**(4) (2012). [https://doi.org/10.2168/LMCS-8\(4:6\)2012](https://doi.org/10.2168/LMCS-8(4:6)2012)
14. Fähndrich, M., DeLine, R.: Adoption and focus: Practical linear types for imperative programming. In: *PLDI*. pp. 13–24. ACM (2002). <https://doi.org/10.1145/512529.512532>
15. Fowler, S., Lindley, S., Morris, J.G., Decova, S.: Exceptional asynchronous session types: session types without tiers. *PACMPL* **3**(POPL), 28:1–28:29 (2019). <https://doi.org/10.1145/3290341>
16. Gay, S.J., Ravara, A. (eds.): *Behavioural Types: From Theory to Tools*. River Publishers (2017). <https://doi.org/10.13052/rp-9788793519817>
17. Gay, S.J., Vasconcelos, V.T.: Linear type theory for asynchronous session types. *Journal of Functional Programming* **20**(1), 19–50 (2010). <https://doi.org/10.1017/S0956796809990268>
18. Honda, K., Yoshida, N., Carbone, M.: Multiparty asynchronous session types. In: *POPL*. pp. 273–284. ACM Press (2008). <https://doi.org/10.1145/1328438.1328472>
19. Honda, K., Vasconcelos, V.T., Kubo, M.: Language primitives and type discipline for structured communication-based programming. In: *ESOP. LNCS*, vol. 1381, pp. 122–138. Springer (1998). <https://doi.org/10.1007/BFb0053567>

20. Hüttel, H., et al.: Foundations of session types and behavioural contracts. *ACM Computing Surveys* **49**(1) (2016). <https://doi.org/10.1145/2873052>
21. Kouzapas, D., Dardha, O., Perera, R., Gay, S.J.: Typechecking protocols with Mungo and StMungo. In: *PPDP*. pp. 146–159. ACM (2016). <https://doi.org/10.1145/2967973.2968595>
22. Kouzapas, D., Dardha, O., Perera, R., Gay, S.J.: Typechecking protocols with Mungo and StMungo: a session type toolchain for Java. *Science of Computer Programming* **155**, 52–75 (2018). <https://doi.org/10.1016/j.scico.2017.10.006>
23. Militão, F., Aldrich, J., Caires, L.: Aliasing control with view-based tpestate. In: *FTFJP*. pp. 7:1–7:7. ACM (2010). <https://doi.org/10.1145/1924520.1924527>
24. Mostrous, D., Vasconcelos, V.T.: Affine sessions. *Logical Methods in Computer Science* **14**(4) (2018). [https://doi.org/10.23638/LMCS-14\(4:14\)2018](https://doi.org/10.23638/LMCS-14(4:14)2018)
25. Padovani, L.: Type reconstruction for the linear  $\pi$ -calculus with composite regular types. *Logical Methods in Computer Science* **11**(4) (2015). [https://doi.org/10.2168/LMCS-11\(4:13\)2015](https://doi.org/10.2168/LMCS-11(4:13)2015)
26. Pierce, B.C.: *Types and programming languages*. MIT Press (2002)
27. Pruiksmá, K., Pfenning, F.: A message-passing interpretation of adjoint logic. In: *PLACES*. *Electronic Proceedings in Theoretical Computer Science*, vol. 291, pp. 60–79. Open Publishing Association (2019). <https://doi.org/10.4204/EPTCS.291.6>
28. Scalas, A., Dardha, O., Hu, R., Yoshida, N.: A linear decomposition of multiparty sessions for safe distributed programming. In: *ECOOP*. *LIPIcs*, vol. 74, pp. 24:1–24:31. Schloss Dagstuhl — Leibniz-Zentrum für Informatik (2017). <https://doi.org/10.4230/LIPIcs.ECOOP.2017.24>
29. Scalas, A., Dardha, O., Hu, R., Yoshida, N.: A linear decomposition of multiparty sessions for safe distributed programming. Tech. Rep. 2, Imperial College London (2017), <https://www.doc.ic.ac.uk/research/technicalreports/2017/#2>
30. Strom, R.E., Yemini, S.: Tpestate: A programming language concept for enhancing software reliability. *IEEE Trans. Softw. Eng.* **12**(1), 157–171 (1986). <https://doi.org/10.1109/TSE.1986.6312929>
31. Sunshine, J., Naden, K., Stork, S., Aldrich, J., Tanter, É.: First-class state change in Plaid. In: *OOPSLA*. pp. 713–732. ACM (2011). <https://doi.org/10.1145/2048066.2048122>
32. Takeuchi, K., Honda, K., Kubo, M.: An interaction-based language and its typing system. In: *PARLE*. *Springer LNCS*, vol. 817, pp. 398–413 (1994)
33. Vasconcelos, V.T.: Fundamentals of session types. *Inf. Comput.* **217**, 52–70 (2012). <https://doi.org/10.1016/j.ic.2012.05.002>
34. Voinea, A.L., Dardha, O., Gay, S.J.: Resource sharing via capability-based multiparty session types. Tech. rep., School of Computing Science, University of Glasgow (2019), <http://www.dcs.gla.ac.uk/~ornela/publications/VDG19-Extended.pdf>
35. Wadler, P.: Propositions as sessions. In: *ICFP*. pp. 273–286. ACM (2012). <https://doi.org/10.1145/2364527.2364568>
36. Walker, D., Morrisett, J.G.: Alias types for recursive data structures. In: *TIC*. pp. 177–206. LNCS, Springer (2000)
37. Yoshida, N., Deniérou, P., Bejleri, A., Hu, R.: Parameterised multiparty session types. In: *FOSSACS* (2010). [https://doi.org/doi:10.1007/978-3-642-12032-9\\_10](https://doi.org/doi:10.1007/978-3-642-12032-9_10)

## A Producer Consumer Typing derivaton

We show the typing for the process definition of Produce:

$$S = \mu \mathbf{t}. \mathbf{b} \oplus ! \text{add}(\mathbf{Int}). \mathbf{c} \oplus ! \text{turn}(\{\rho_y \mapsto \bar{S}_b\}). \mathbf{c} \& ? \text{turn}(\{\rho_y \mapsto \bar{S}_b\}). t$$

$$\Delta = \text{Produce} : (\mathbf{tr}(\rho_p), \mathbf{tr}(\rho_y), \mathbf{Int}, \{\rho_p \mapsto S_p\}, \{\rho_y \mapsto S_q\})$$

$$\Gamma = \mathbf{x} : \mathbf{tr}(\rho_p), \mathbf{y} : \mathbf{tr}(\rho_y), i : \mathbf{Int}, \rho_p : \{\rho_p \mapsto S_p\}, \rho_y : \{\rho_y \mapsto S_q\}$$

$$\frac{\frac{\frac{\Gamma \vdash \mathbf{x} : \mathbf{tr}(\rho_x), \mathbf{y} : \mathbf{tr}(\rho_y), i : \mathbf{Int}, \rho_x : \{\rho_x \mapsto S'_p\}, \rho_y : \{\rho_y \mapsto S_q\}; \{\rho_x \mapsto S'_p, \rho_y \mapsto S_q\}}{\Delta; \Gamma \vdash \text{Produce}\langle \mathbf{x}, \mathbf{y}, i+1, \rho_x, \rho_y \rangle; \{\rho_x \mapsto S'_p, \rho_y \mapsto S_q\}} \text{TCALL}}{\Delta; \Gamma \vdash \mathbf{x}[c] \& \{\text{turn}(\rho_y). \text{Produce}\langle \mathbf{x}, \mathbf{y}, i+1, \rho_x, \rho_y \rangle\}; \{\rho_x \mapsto \mathbf{c} \& ? \text{turn}(\{\rho_y \mapsto S_q\}). S'_p\}} \text{TBR}}{\dots \text{TCAP}} \frac{\Gamma \vdash \rho_y : \{\rho_y \mapsto S'_q\}; \{\rho_y \mapsto S'_q\} \quad \mathbf{x} : \mathbf{tr}(\rho_x), \rho_x : \{\rho_x \mapsto \mathbf{c} \& ? \text{turn}(\{\rho_y \mapsto S_q\}). S'_p\} \in \Gamma}{\Delta; \Gamma \vdash \mathbf{x}[c] \oplus \langle \text{turn}(\rho_y) \rangle. \mathbf{x}[c] \& \{\text{turn}(\rho_y). \text{Produce}\langle \mathbf{x}, \mathbf{y}, i+1, \rho_x, \rho_y \rangle\}; \{\rho_x \mapsto S'_p, \rho_y \mapsto S'_q\}} \text{TSEL}}{\dots \text{TVAl}} \frac{i \in \mathbf{Int}}{\Gamma \vdash i : \mathbf{Int}; \emptyset} \frac{\mathbf{y} : \mathbf{tr}(\rho_y), \rho_y : \{\rho_y \mapsto S'_q\} \in \Gamma}{\Delta; \Gamma \vdash \mathbf{y}[b] \oplus \langle \text{add}(i) \rangle. \mathbf{x}[c] \oplus \langle \text{turn}(\rho_y) \rangle. \mathbf{x}[c] \& \{\text{turn}(\rho_y). \text{Produce}\langle \mathbf{x}, \mathbf{y}, i+1, \rho_x, \rho_y \rangle\}; \{\rho_x \mapsto S'_p, \rho_y \mapsto S_q\}} \text{TSEL}$$

We show the typing for the process P starting from the Produce process call:

$$\frac{\frac{\Gamma \vdash \mathbf{x} : \mathbf{tr}(\rho_x), \mathbf{y} : \mathbf{tr}(\rho_y), \rho_x : \{\rho_x \mapsto S'_p\}, \rho_y : \{\rho_y \mapsto S_q\}; \{\rho_x \mapsto S'_p, \rho_y \mapsto S_q\}}{\Delta; \Gamma \vdash \text{Produce}\langle \mathbf{x}, \mathbf{y}, i, \rho_p, \rho_y \rangle; \{\rho_x \mapsto S'_p, \rho_y \mapsto S_q\}} \text{TCALL}}{\dots \text{TVar}} \frac{\mathbf{y} : \mathbf{tr}(\rho_y), \rho_y : \{\rho_y \mapsto S_q\}}{\Gamma \vdash \mathbf{y} : \mathbf{tr}(\rho_y); \emptyset} \frac{\mathbf{x}, \rho_x : \{\rho_x \mapsto S_p\} \in \Gamma}{\Delta; \Gamma \vdash \mathbf{x}[c] \oplus \langle \text{buffer}(\text{pack}(\rho_y, \mathbf{y}[b])) \rangle. \text{Produce}\langle \mathbf{x}, \mathbf{y}, i, \rho_x, \rho_y \rangle; \{\rho_y \mapsto \mathbf{p} \oplus ! (\exists [\rho_y | \{\rho_y \mapsto S_q\}]. \mathbf{tr}(\rho_y)). S'_p, \rho_y \mapsto S_q\}} \text{TSELP}$$

Typing derivation for the consumer:

$$\Delta = \mathbf{C} : (\mathbf{tr}(\rho_x), \{\rho_x \mapsto S\}), \text{Consume} : (\mathbf{tr}(\rho_x), \mathbf{tr}(\rho_y), \{\rho_x \mapsto S\})$$

$$\Gamma = \mathbf{x} : \mathbf{tr}(\rho_x), \mathbf{y} : \mathbf{tr}(\rho_y), \rho_x : \{\rho_x \mapsto S\}$$

$$\Gamma' = \Gamma, \rho_y : \{\rho_y \mapsto S'_q\}$$

$$S = \mu \mathbf{t}. \mathbf{p} \& ? \text{turn}(\{\rho_y \mapsto S'_q\}). \mathbf{p} \oplus ! \text{turn}(\{\rho_y \mapsto S_q\}). t$$

We show the typing for the process definition of Consume:

$$\begin{array}{c}
\frac{\Gamma', i : \mathbf{Int} \vdash x : \mathbf{tr}(\rho_x), y : \mathbf{tr}(\rho_y), \rho_x : \{\rho_x \mapsto S_c\}; \{\rho_x \mapsto S_c\}}{\Delta; \Gamma', i : \mathbf{Int} \vdash \mathbf{Consume}\langle x, y, \rho_x \rangle; \{\rho_x \mapsto \mathbf{p} \oplus !\mathbf{turn}(\{\rho_y \mapsto S_q\}) \cdot S_c\}} \text{TCALL} \\
\frac{\overline{\Gamma', i : \mathbf{Int} \vdash \rho_y; \{\rho_y \mapsto S_q\}} \text{TCAP} \quad \mathbf{x} : \mathbf{tr}(\rho_x), \rho_x : \{\rho_x \mapsto S_c\} \in \Gamma' \quad \vdots}{\Delta; \Gamma', i : \mathbf{Int} \vdash \mathbf{x}[\mathbf{p}] \oplus \langle \mathbf{turn}(\rho_y) \rangle \cdot \mathbf{Consume}\langle x, y, \rho_x \rangle; \{\rho_x \mapsto \mathbf{p} \oplus !\mathbf{turn}(\{\rho_y \mapsto S_q\}) \cdot S_c, \rho_y \mapsto S_q\}} \text{TSEL} \\
\frac{\Delta; \Gamma' \vdash \mathbf{y}[\mathbf{q}] \& \langle \mathbf{send}(i) \rangle \cdot \mathbf{x}[\mathbf{p}] \oplus \langle \mathbf{turn}(\rho_y) \rangle \cdot \mathbf{Consume}\langle x, y, \rho_x \rangle; \{\rho_x \mapsto \mathbf{p} \oplus !\mathbf{turn}(\{\rho_y \mapsto S_q\}) \cdot S_c, \rho_y \mapsto \mathbf{b} \& ? \mathbf{send}(\mathbf{Int}) \cdot S_q\}}{\Delta; \Gamma' \vdash \mathbf{y}[\mathbf{q}] \& \langle \mathbf{send}(i) \rangle \cdot \mathbf{x}[\mathbf{p}] \oplus \langle \mathbf{turn}(\rho_y) \rangle \cdot \mathbf{Consume}\langle x, y, \rho_x \rangle; \{\rho_x \mapsto \mathbf{p} \oplus !\mathbf{turn}(\{\rho_y \mapsto S_q\}) \cdot S_c, \rho_y \mapsto \mathbf{b} \& ? \mathbf{send}(\mathbf{Int}) \cdot S_q\}} \text{TBR} \\
\frac{r \in \mathbf{Str} \quad \vdots}{\Gamma' \vdash r : \mathbf{Str}; \emptyset \text{ TVAL} \quad \mathbf{y}, \rho_y : \{\rho_y \mapsto S_q\} \in \Gamma' \quad \vdots} \\
\frac{\Delta; \Gamma' \vdash \mathbf{y}[\mathbf{b}] \oplus \langle \mathbf{request}(r) \rangle \cdot \mathbf{y}[\mathbf{b}] \& \langle \mathbf{send}(i) \rangle \cdot \mathbf{x}[\mathbf{p}] \oplus \langle \mathbf{turn}(\rho_y) \rangle \cdot \mathbf{Consume}\langle x, y, \rho_x \rangle; \{\rho_x \mapsto \mathbf{p} \oplus !\mathbf{turn}(\{\rho_y \mapsto S_q\}) \cdot S_c\} \otimes \{\rho_y \mapsto \mathbf{b} \oplus !\mathbf{request}(\mathbf{Str}) \cdot \mathbf{b} \& ? \mathbf{send}(\mathbf{Int}) \cdot S_q\}}{\Delta; \Gamma' \vdash \mathbf{y}[\mathbf{b}] \oplus \langle \mathbf{request}(r) \rangle \cdot \mathbf{y}[\mathbf{b}] \& \langle \mathbf{send}(i) \rangle \cdot \mathbf{x}[\mathbf{p}] \oplus \langle \mathbf{turn}(\rho_y) \rangle \cdot \mathbf{Consume}\langle x, y, \rho_x \rangle; \{\rho_x \mapsto \mathbf{p} \oplus !\mathbf{turn}(\{\rho_y \mapsto S_q\}) \cdot S_c, \rho_y \mapsto \mathbf{b} \& ? \mathbf{send}(\mathbf{Int}) \cdot S_q\}} \text{TSEL} \\
\frac{\Delta; \Gamma' \vdash \mathbf{x}[\mathbf{p}] \& \langle \mathbf{turn}(\rho_y) \rangle \cdot \mathbf{y}[\mathbf{b}] \oplus \langle \mathbf{request}(r) \rangle \cdot \mathbf{y}[\mathbf{b}] \& \langle \mathbf{send}(i) \rangle \cdot \mathbf{x}[\mathbf{p}] \oplus \langle \mathbf{turn}(\rho_y) \rangle \cdot \mathbf{Consume}\langle x, y, \rho_x \rangle; \{\rho_x \mapsto \mathbf{p} \& ? \mathbf{turn}(\{\rho_y \mapsto S_q'\}) \cdot \mathbf{p} \oplus !\mathbf{turn}(\{\rho_y \mapsto S_q\}) \cdot S\}}{\Delta; \Gamma' \vdash \mathbf{x}[\mathbf{p}] \& \langle \mathbf{turn}(\rho_y) \rangle \cdot \mathbf{y}[\mathbf{b}] \oplus \langle \mathbf{request}(r) \rangle \cdot \mathbf{y}[\mathbf{b}] \& \langle \mathbf{send}(i) \rangle \cdot \mathbf{x}[\mathbf{p}] \oplus \langle \mathbf{turn}(\rho_y) \rangle \cdot \mathbf{Consume}\langle x, y, \rho_x \rangle; \{\rho_x \mapsto \mathbf{p} \& ? \mathbf{turn}(\{\rho_y \mapsto S_q'\}) \cdot \mathbf{p} \oplus !\mathbf{turn}(\{\rho_y \mapsto S_q\}) \cdot S\}} \text{TBR}
\end{array}$$

We show the typing for the process definition of C starting with the typing for Consume:

$$\frac{\text{TCALL} \quad \Delta; \Gamma, \mathbf{y} : \mathbf{tr}(\rho_y), \rho_y : \{\rho_y \mapsto S_q'\} \vdash x : \mathbf{tr}(\rho_x), y : \mathbf{tr}(\rho_y), \rho_x : \{\rho_x \mapsto S_c'\}; \{\rho_x \mapsto S_c'\}}{\Delta; \Gamma, \mathbf{y} : \mathbf{tr}(\rho_y), \rho_y : \{\rho_y \mapsto S_q'\} \vdash \mathbf{Consume}\langle x, y, \rho_x \rangle; \{\rho_x \mapsto S_c'\} \quad \mathbf{x} : \mathbf{tr}(\rho_x), \rho_x : \{\rho_x \mapsto S_c'\} \in \Gamma} \text{TBRP} \\
\frac{\Delta; \Gamma \vdash \mathbf{x}[\mathbf{p}] \oplus \langle \mathbf{buffer}(\mathbf{pack}(\rho_y, \mathbf{y})) \rangle \cdot \mathbf{Consume}\langle x, y, \rho_x \rangle; \{\rho_x \mapsto \mathbf{c} \& ? l(\exists[\rho_y] \{\rho_y \mapsto S_q'\}) \cdot \mathbf{tr}(\rho_y) \cdot S_c'\}}{\Delta; \Gamma \vdash \mathbf{x}[\mathbf{p}] \oplus \langle \mathbf{buffer}(\mathbf{pack}(\rho_y, \mathbf{y})) \rangle \cdot \mathbf{Consume}\langle x, y, \rho_x \rangle; \{\rho_x \mapsto \mathbf{c} \& ? l(\exists[\rho_y] \{\rho_y \mapsto S_q'\}) \cdot \mathbf{tr}(\rho_y) \cdot S_c'\}}$$

Typing derivation for the buffer process  $\mathbf{B}\langle \mathbf{x}, \rho_x \rangle$ :

$$\frac{\frac{\mathbf{x} : \mathbf{tr}(\rho_x), \{\rho_x \mapsto S_b\} \in \Gamma, i : \mathbf{Int}, r : \mathbf{Str}}{\Gamma, i : \mathbf{Int}, r : \mathbf{Str} \vdash \mathbf{x} : \mathbf{tr}(\rho_x); \{\rho_x \mapsto S_b\}} \text{TVAR}}{\Delta; \Gamma, \mathbf{x} : \mathbf{tr}(\rho_x), i : \mathbf{Int}, r : \mathbf{Str} \vdash \mathbf{B}\langle \mathbf{x} \rangle; \{\rho_x \mapsto S_b\}} \text{TCALL} \\
\frac{\vdots \quad \overline{\Gamma, i : \mathbf{Int}, r : \mathbf{Str} \vdash i; \emptyset} \text{TVAL} \quad x \in \Gamma, \mathbf{x} : \mathbf{tr}(\rho_x), i : \mathbf{Int}, r : \mathbf{Str}}{\Delta; \Gamma, \mathbf{x} : \mathbf{tr}(\rho_x), i : \mathbf{Int}, r : \mathbf{Str} \vdash \mathbf{x}[\mathbf{p}] \oplus \langle \mathbf{send}(i) \rangle \cdot \mathbf{B}\langle \mathbf{x}, \rho_x \rangle; \{\rho_x \mapsto \mathbf{q} \oplus !\mathbf{send}(\mathbf{Int}) \cdot S_b\}} \text{TSEL} \\
\frac{\vdots \quad \mathbf{x} : \mathbf{tr}(\rho_x), \rho_x : \{\rho_x \mapsto \mathbf{q} \oplus !\mathbf{send}(\mathbf{Int}) \cdot S_b\} \in \Gamma}{\Delta; \Gamma, i : \mathbf{Int} \vdash \mathbf{x}[\mathbf{q}] \& \langle \mathbf{request}(r) \rangle \cdot \mathbf{x}[\mathbf{p}] \oplus \langle \mathbf{send}(i) \rangle \cdot \mathbf{B}\langle \mathbf{x}, \rho_x \rangle; \{\rho_x \mapsto \mathbf{q} \& ? \mathbf{request}(\mathbf{Str}) \cdot \mathbf{q} \oplus !\mathbf{send}(\mathbf{Int}) \cdot S_b\}} \text{TBR} \\
\frac{\vdots \quad \mathbf{x} : \mathbf{tr}(\rho_x), \{\rho_x \mapsto \mathbf{q} \& ? \mathbf{request}(\mathbf{Str}) \cdot \mathbf{q} \oplus !\mathbf{send}(\mathbf{Int}) \cdot S_b\} \in \Gamma}{\Delta; \Gamma \vdash \mathbf{x}[\mathbf{q}] \& \langle \mathbf{add}(i) \rangle \cdot \mathbf{x}[\mathbf{q}] \& \langle \mathbf{request}(r) \rangle \cdot \mathbf{x}[\mathbf{p}] \oplus \langle \mathbf{send}(i) \rangle \cdot \mathbf{B}\langle \mathbf{x}, \rho_x \rangle; \{\rho_x \mapsto \mathbf{q} \& ? \mathbf{add}(\mathbf{Int}) \cdot \mathbf{q} \& ? \mathbf{request}(\mathbf{Str}) \cdot \mathbf{q} \oplus !\mathbf{send}(\mathbf{Int}) \cdot S_b\}} \text{TBR}$$

## B Proofs

**Proposition 1.**  $\mathbf{unf}(\overline{H}) = \overline{\mathbf{unf}(H)}$

*Proof.* By induction on the unfolding of  $H$ . [29]

**Proposition 2.** For all session types  $S$  and roles  $\mathbf{p}$ ,  $\mathbf{unf}(S) \upharpoonright \mathbf{p} = \mathbf{unf}(S \upharpoonright \mathbf{p})$ .

*Proof.* By induction on the unfolding of  $S$ . [29]

**Proposition 3.** *If  $(\Gamma, C) \longrightarrow^* (\Gamma', C')$  then  $\text{dom}(\Gamma) = \text{dom}(\Gamma')$  and  $\text{dom}(C) = \text{dom}(C')$ .*

*Proof.* We first verify the following, by induction on the size of  $\text{dom}(\Gamma)$ :  $(\Gamma, C) \longrightarrow^* (\Gamma', C')$  implies  $\text{dom}(\Gamma) = \text{dom}(\Gamma')$  and  $\text{dom}(C) = \text{dom}(C')$ .

Then, we can prove the main statement, by induction on the length of the sequence of reductions in  $(\Gamma, C) \longrightarrow^* (\Gamma', C')$ . The base case is trivial, with 0 reductions, and  $(\Gamma, C) = (\Gamma', C')$ , while in the inductive case, we apply the induction hypothesis.

**Corollary 1.** *If  $(\Gamma_1, \Gamma_2; C_1 \otimes C_2)$  is consistent and  $C_2 \leq_S C'_2$ , then  $(\Gamma_1, \Gamma_2; C_1 \otimes C'_2)$  is consistent.*

**Lemma 1.** *If  $(\Gamma; C) \longrightarrow (\Gamma'; C')$  and  $(\Gamma; C)$  is consistent (resp. complete), then so is  $(\Gamma'; C')$ .*

*Proof.* By induction on  $(\Gamma; C) \longrightarrow (\Gamma'; C')$ , as per Definition 10.

**Corollary 2.** *If  $(\Gamma_1, \Gamma_2; C_1 \otimes C_2)$  is consistent and  $(\Gamma_1; C_1) \longrightarrow^* (\Gamma'_1; C'_1)$ , then  $(\Gamma'_1, \Gamma_2; C'_1 \otimes C_2)$  is consistent.*

*Proof.* Assume all the hypotheses, and let  $n$  be the length of the sequence of reductions in  $(\Gamma_1; C_1) \longrightarrow^* (\Gamma'_1; C'_1)$ . In the base case,  $n = 0$ , the thesis holds trivially. In the inductive case  $n = n' + 1$ , we have:

$$(\Gamma_1, C_1) \longrightarrow \dots \longrightarrow (\Gamma_1^*, C_1^*) \longrightarrow (\Gamma'_1, C'_1)$$

and by the induction hypothesis,  $(\Gamma_1^*, \Gamma_2; C_1^* \otimes C_2)$  is consistent. This implies that  $(\Gamma'_1, \Gamma_2; C'_1 \otimes C_2)$  is consistent: we prove such a fact with a further induction on the size of  $(\Gamma_2; C_2)$ . In the base case  $(\Gamma_2; C_2) = (\emptyset; \emptyset)$  we conclude immediately by Lemma 1. In the inductive case we have  $(\Gamma_2; C_2) = (\Gamma_0, c : \text{tr}(\rho), \rho : \{\rho \mapsto U\}; C_0 \otimes \{\rho \mapsto U\})$ ; by applying the induction hypothesis we get that  $(\Gamma'_1, \Gamma_0; C'_1 \otimes C_0)$  is consistent. We examine the shape of the additional entry  $(c : \text{tr}(\rho), \rho : \{\rho \mapsto U\}; \{\rho \mapsto U\})$  and its consistency w.r.t.  $(\Gamma'_1, \Gamma_0; C'_1 \otimes C_0)$ , similarly to the inductive case in the proof of Lemma 1. In all cases, we conclude that  $(\Gamma'_1, \Gamma_2; C'_1 \otimes C_2)$  is consistent.

**Proposition 4 (Weakening).** *For any multiparty session process  $P$  with  $\Delta; \Gamma \vdash P; C$ :*

1. *if  $\Delta$  and  $\Delta'$  are disjoint, then  $\Delta, \Delta'; \Gamma \vdash P; C$ .*
2. *if  $\Gamma$  and  $\Gamma'$  are disjoint, then  $\Delta; \Gamma, \Gamma' \vdash P; C$ .*

*Proof.* By induction on typing derivations, with a case analysis on the last rule applied.

**Proposition 5 (Strengthening).** *For any multiparty session process  $P$ :*

1. *if  $\Delta, \Delta'; \Gamma \vdash P; C$  and  $\Delta' \notin \text{fpv}(P)$  then  $\Delta; \Gamma \vdash P; C$ .*
2. *if  $\Delta; \Gamma, \Gamma' \vdash P; C$  and  $\Gamma' \notin \text{fv}(P)$  then  $\Delta; \Gamma \vdash P; C$ .*

*Proof.* By induction on typing derivations, with a case analysis on the last rule applied.

**Proposition 6.** *If  $\Delta; \Gamma, \rho : \{\rho \mapsto S\} \vdash P; C$  and  $\rho \notin C$  and  $\nexists c : \text{tr}(\rho) \notin \Gamma$  then  $\Delta; \Gamma \vdash P; C$ .*

*Proof.* By induction on typing derivations, with a case analysis on the last rule applied.

**Proposition 7.** *If  $\Delta; \Gamma \vdash P; C$  and there exists  $C'$  such that  $C'$  terminated and  $C$  and  $C'$  are disjoint then  $\Delta; \Gamma \vdash P; C \otimes C'$ .*

*Proof.* By induction on typing derivations, with a case analysis on the last rule applied.

**Proposition 8.** *For all multiparty session processes  $P, P'$  if  $\Delta; \Gamma \vdash P; C$  and  $P \equiv P'$ , then  $\Delta; \Gamma \vdash P'; C$ .*

*Proof.* The proof proceeds by induction on the structural congruence  $\equiv$ .

–  $P | \mathbf{0} \equiv P$  Left to right we have  $\Delta; \Gamma \vdash P | \mathbf{0}; C$  and  $P | \mathbf{0} \equiv P$ .

$$\frac{\Delta; \Gamma \vdash P; C_1 \quad \frac{C_2 \text{ terminated}}{\Delta; \Gamma \vdash \mathbf{0}; C_2} \text{ T}_{\text{INACT}}}{\Delta; \Gamma \vdash P | \mathbf{0}; C = C_1 \otimes C_2} \text{ T}_{\text{PAR}}$$

Since  $C_2$  terminated and  $C_2$  and  $C_1$  are disjoint then by Proposition 7  $\Delta; \Gamma \vdash P; C_1 \otimes C_2$ .

Right to left we have  $\Delta; \Gamma \vdash P; C$  and  $P | \mathbf{0} \equiv P$ . From  $\text{T}_{\text{INACT}}$  we know:  $\Delta; \Gamma \vdash \mathbf{0}; \emptyset$ .

$$\frac{\Delta; \Gamma \vdash P; C \quad \Delta; \Gamma \vdash \mathbf{0}; \emptyset}{\Delta; \Gamma \vdash P | \mathbf{0}; C} \text{ T}_{\text{PAR}}$$

–  $P | Q \equiv Q | P$  Left to right we have:  $\Delta; \Gamma \vdash P | Q; C_1 \otimes C_2$  and  $P | Q \equiv Q | P$ .

$$\frac{\Delta; \Gamma \vdash P; C_1 \quad \Delta; \Gamma \vdash Q; C_2}{\Delta; \Gamma \vdash P | Q; C_1 \otimes C_2} \text{ T}_{\text{PAR}}$$

By applying  $\text{T}_{\text{PAR}}$  to the two premises we get:

$$\frac{\Delta; \Gamma \vdash Q; C_2 \quad \Delta; \Gamma \vdash P; C_1}{\Delta; \Gamma \vdash Q | P; C_2 \otimes C_1} \text{ T}_{\text{PAR}}$$

$C_1 \otimes C_2 = C_2 \otimes C_1$ .

Right to left we have  $\Delta; \Gamma \vdash Q | P; C_2 \otimes C_1$  and  $P | Q \equiv Q | P$ .

$$\frac{\Delta; \Gamma \vdash Q; C_2 \quad \Delta; \Gamma \vdash P; C_1}{\Delta; \Gamma \vdash Q | P; C_2 \otimes C_1} \text{ T}_{\text{PAR}}$$

By applying  $\text{T}_{\text{PAR}}$  to the two premises we get:

$$\frac{\Delta; \Gamma \vdash P; C_1 \quad \Delta; \Gamma \vdash Q; C_2}{\Delta; \Gamma \vdash P | Q; C_1 \otimes C_2} \text{ T}_{\text{PAR}}$$

$C_2 \otimes C_1 = C_1 \otimes C_2$ .

–  $(P | Q) | R \equiv P(Q | R)$  Left to right we have:  $\Delta; \Gamma \vdash (P | Q) | R; (C_1 \otimes C_2) \otimes C_3$  and  $(P | Q) | R \equiv P(Q | R)$ .

$$\frac{\frac{\Delta; \Gamma \vdash P; C_1 \quad \Delta; \Gamma \vdash Q; C_2}{\Delta; \Gamma \vdash P | Q; C_1 \otimes C_2} \text{ T}_{\text{PAR}} \quad \Delta; \Gamma \vdash R; C_3}{\Delta; \Gamma \vdash (P | Q) | R; (C_1 \otimes C_2) \otimes C_3} \text{ T}_{\text{PAR}}$$

By applying  $\text{T}_{\text{PAR}}$  to the three premises we get:

$$\frac{\Delta; \Gamma \vdash P; C_1 \quad \frac{\Delta; \Gamma \vdash Q; C_2 \quad \Delta; \Gamma \vdash R; C_3}{\Delta; \Gamma \vdash Q | R; C_2 \otimes C_3} \text{ T}_{\text{PAR}}}{\Delta; \Gamma \vdash P(Q | R); C_1 \otimes (C_2 \otimes C_3)} \text{ T}_{\text{PAR}}$$

$(C_1 \otimes C_2) \otimes C_3 = C_1 \otimes (C_2 \otimes C_3)$ .

Right to left we have  $\Delta; \Gamma \vdash P(Q | R); C_1 \otimes (C_2 \otimes C_3)$ .

$$\frac{\Delta; \Gamma \vdash P; C_1 \quad \frac{\Delta; \Gamma \vdash Q; C_2 \quad \Delta; \Gamma \vdash R; C_3}{\Delta; \Gamma \vdash Q | R; C_2 \otimes C_3} \text{ T}_{\text{PAR}}}{\Delta; \Gamma \vdash P(Q | R); C_1 \otimes (C_2 \otimes C_3)} \text{ T}_{\text{PAR}}$$

By applying  $\text{T}_{\text{PAR}}$  to the three premises we get:

$$\frac{\frac{\Delta; \Gamma \vdash P; C_1 \quad \Delta; \Gamma \vdash Q; C_2}{\Delta; \Gamma \vdash P | Q; C_1 \otimes C_2} \text{TPAR} \quad \Delta; \Gamma \vdash R; C_3}{\Delta; \Gamma \vdash (P | Q) | R; (C_1 \otimes C_2) \otimes C_3} \text{TPAR}$$

$$C_1 \otimes (C_2 \otimes C_3) = (C_1 \otimes C_2) \otimes C_3.$$

- $(\nu s)\mathbf{0} \equiv \mathbf{0}$  Left to right we have:  $\Delta; \Gamma \vdash (\nu s)\mathbf{0}; C$  and  $(\nu s)\mathbf{0} \equiv \mathbf{0}$ . By inversion on  $\text{TRES}$  and  $\text{TINACT}$  we obtain  $C$  terminated.

From  $\text{TINACT}$  we have  $\Delta; \Gamma \vdash \mathbf{0}; C$ .

Right to left we have  $\Delta; \Gamma \vdash \mathbf{0}; C$  and  $(\nu s)\mathbf{0} \equiv \mathbf{0}$ . From  $\text{TINACT}$  we have  $C$  terminated.

$$\frac{\frac{C \otimes C' \text{ terminated}}{\Delta; \Gamma, \Gamma' \vdash \mathbf{0}; C \otimes C'} \text{TINACT} \quad (\Gamma' = \{\mathbf{s}[p] : \mathbf{tr}(\rho_p), \rho_p : \{\rho_p \mapsto S_p\}\}_{p \in I}, C' = \otimes_{p \in I} \{\rho_p \mapsto S_p\})}{\Delta; \Gamma \vdash (\nu s : \Gamma')\mathbf{0}; C} \text{TRES}$$

- $(\nu s)(\nu s')P \equiv (\nu s')(\nu s)P$  Left to right: We construct the derivation for  $(\nu s)(\nu s')P$ .

$$\frac{\text{TRES} \quad \frac{\Delta; \Gamma, \Gamma', \Gamma'' \vdash P; C \otimes C' \otimes C''}{\Gamma'' = \{\mathbf{s}'[p'_i] : \mathbf{tr}(\rho'_i), \rho_{p'} : \{\rho_{p'} \mapsto S_{p'}\}\}_{i \in I}, C'' = \otimes_{p' \in I} \{\rho_{p'} \mapsto S_{p'}\}} \text{TRES} \quad \Delta; \Gamma, \Gamma' \vdash (\nu s' : \Gamma'')P; C \otimes C'}{\vdots} \quad \frac{(\Gamma' = \{\mathbf{s}[p] : \mathbf{tr}(\rho_p), \rho_p : \{\rho_p \mapsto S_p\}\}_{p \in I}, C' = \otimes_{p \in I} \{\rho_p \mapsto S_p\})}{\Delta; \Gamma \vdash (\nu s : \Gamma')(\nu s' : \Gamma'')P; C} \text{TRES}$$

By rearranging:

$$\frac{\text{TRES} \quad \frac{\Delta; \Gamma, \Gamma', \Gamma'' \vdash P; C \otimes C' \otimes C''}{(\Gamma' = \{\mathbf{s}[p] : \mathbf{tr}(\rho_p), \rho_p : \{\rho_p \mapsto S_p\}\}_{p \in I}, C' = \otimes_{p \in I} \{\rho_p \mapsto S_p\})} \text{TRES} \quad \Delta; \Gamma, \Gamma'' \vdash (\nu s : \Gamma')P; C \otimes C''}{\vdots} \quad \frac{\Gamma'' = \{\mathbf{s}'[p'_i] : \mathbf{tr}(\rho'_i), \rho_{p'} : \{\rho_{p'} \mapsto S_{p'}\}\}_{i \in I}, C'' = \otimes_{p' \in I} \{\rho_{p'} \mapsto S_{p'}\}}{\Delta; \Gamma \vdash (\nu s' : \Gamma'')(\nu s : \Gamma')P; C} \text{TRES}$$

Right to left:

$$\frac{\text{TRES} \quad \frac{\Delta; \Gamma, \Gamma', \Gamma'' \vdash P; C \otimes C' \otimes C''}{(\Gamma' = \{\mathbf{s}[p] : \mathbf{tr}(\rho_p), \rho_p : \{\rho_p \mapsto S_p\}\}_{p \in I}, C' = \otimes_{p \in I} \{\rho_p \mapsto S_p\})} \text{TRES} \quad \Delta; \Gamma, \Gamma'' \vdash (\nu s : \Gamma')P; C \otimes C''}{\vdots} \quad \frac{\Gamma'' = \{\mathbf{s}'[p'_i] : \mathbf{tr}(\rho'_{p'_i}), \rho_{p'} : \{\rho_{p'} \mapsto S_{p'}\}\}_{p' \in I}, C'' = \otimes_{p' \in I} \{\rho_{p'} \mapsto S_{p'}\}}{\Delta; \Gamma \vdash (\nu s' : \Gamma'')(\nu s : \Gamma')P; C} \text{TRES}$$

Right to left:

$$\begin{array}{c}
\text{TRES} \\
\frac{\Delta; \Gamma, \Gamma', \Gamma'' \vdash P; C \otimes C' \otimes C''}{(\Gamma' = \{\mathbf{s}[p] : \mathbf{tr}(\rho_p), \rho_p : \{\rho_p \mapsto S_p\}\}_{p \in I}, C' = \otimes_{p \in I} \{\rho_p \mapsto S_p\})} \\
\frac{\Delta; \Gamma, \Gamma'' \vdash (\nu s : \Gamma')P; C \otimes C''}{\vdots} \\
\frac{\Gamma'' = \{\mathbf{s}'[p'] : \mathbf{tr}(\rho'_{p'}), \rho_{p'} : \{\rho_{p'} \mapsto S_{p'}\}\}_{p' \in I}, C'' = \otimes_{p' \in I} \{\rho_{p'} \mapsto S_{p'}\}}{\Delta; \Gamma \vdash (\nu s' : \Gamma'')(\nu s : \Gamma')P; C} \text{TRES}
\end{array}$$

–  $(\nu s)P \mid Q \equiv (\nu s)(P \mid Q)$  if  $s \notin \text{fc}(Q)$  Left to right:

$$\frac{\frac{\Delta; \Gamma, \Gamma' \vdash P; C_1 \otimes C'}{(\Gamma' = \{\mathbf{s}[p] : \mathbf{tr}(\rho_p), \rho_p : \{\rho_p \mapsto S_p\}\}_{p \in I}, C' = \otimes_{p \in I} \{\rho_p \mapsto S_p\})} \text{TRES} \quad \Delta; \Gamma \vdash Q; C_2}{\Delta; \Gamma \vdash (\nu s : \Gamma')P \mid Q; C_1 \otimes C_2} \text{TPAR}$$

By Proposition 4  $\Delta; \Gamma \vdash Q; C_2$  with  $\Gamma'$  we obtain  $\Delta; \Gamma, \Gamma' \vdash Q; C_2$ .

$$\frac{\frac{\Delta; \Gamma, \Gamma' \vdash P; C_1 \otimes C' \quad \Delta; \Gamma, \Gamma' \vdash Q; C_2}{\Delta; \Gamma, \Gamma' \vdash P \mid Q; C_1 \otimes C_2 \otimes C'} \text{TPAR} \quad \vdots}{(\Gamma' = \{\mathbf{s}[p] : \mathbf{tr}(\rho_p), \rho_p : \{\rho_p \mapsto S_p\}\}_{p \in I}, C' = \otimes_{p \in I} \{\rho_p \mapsto S_p\})} \text{TRES} \\
\Delta; \Gamma \vdash (\nu s : \Gamma')(P \mid Q); C_1 \otimes C_2$$

–  $\text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } \mathbf{0} \equiv \mathbf{0}$  Left to right: From the induction hypothesis we have  $\Delta; \Gamma \vdash \text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } \mathbf{0}; C$ .

$$\frac{\frac{\Delta, X : \tilde{U}; \tilde{x} : \tilde{U} \vdash Q_X; \tilde{C} \quad \frac{\text{TINACT} \quad C \text{ terminated}}{\Delta, X : \tilde{U}; \Gamma \vdash \mathbf{0}; C}}{\Delta; \Gamma \vdash \text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } \mathbf{0}; C} \text{TDEF}$$

From  $\text{TINACT}$ :  $\Delta; \Gamma \vdash \mathbf{0}; C'$  and  $C'$  terminated. Since both  $C$  and  $C'$  are terminated then  $C = C'$ .

Right to left: From the induction hypothesis we have  $\Delta; \Gamma \vdash \mathbf{0}; C$ . From  $\text{TINACT}$  we obtain  $C$  terminated. We construct the derivation for process:  $\text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } \mathbf{0}$ .

$$\frac{\frac{\Delta, X : \tilde{U}; \tilde{x} : \tilde{U} \vdash Q_X; \tilde{C} \quad \frac{\text{TINACT} \quad C' \text{ terminated}}{\Delta, X : \tilde{U}; \Gamma \vdash \mathbf{0}; C'}}{\Delta; \Gamma \vdash \text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } \mathbf{0}; C'} \text{TDEF}$$

Since both  $C$  and  $C'$  are terminated then  $C = C'$ .

–  $\text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } (\nu s)P \equiv (\nu s)(\text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } P)$   $s \notin \text{fc}(Q)$



Left to right: From the induction hypothesis:  $\Delta; \Gamma \vdash \text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } (\nu s : \Gamma') P; C$ . We construct the derivation for the process:

$$\frac{\Delta, X : \tilde{U}; \tilde{x} : \tilde{U} \vdash Q_X; \tilde{C} \quad \frac{\Delta, X : \tilde{U}; \Gamma, \Gamma' \vdash P; C \otimes C' \quad (\Gamma' = \{\mathbf{s}[p] : \mathbf{tr}(\rho_p), \rho_p : \{\rho_p \mapsto S_p\}\}_{p \in I}, C' = \otimes_{p \in I} \{\rho_p \mapsto S_p\})}{\Delta, X : \tilde{U}; \Gamma \vdash (\nu s : \Gamma') P; C} \text{TRRES}}{\Delta; \Gamma \vdash \text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } (\nu s : \Gamma') P; C} \text{TDEF}$$

By rearranging the premises:

$$\frac{\frac{\Delta, X : \tilde{U}; \Gamma, \Gamma' \vdash P; C \otimes C' \quad \Delta, X : \tilde{U}; \tilde{x} : \tilde{U} \vdash Q_X; \tilde{C}}{\Delta; \Gamma, \Gamma' \vdash \text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } P; C \otimes C'} \text{TDEF} \quad \vdots}{\frac{(\Gamma' = \{\mathbf{s}[p] : \mathbf{tr}(\rho_p), \rho_p : \{\rho_p \mapsto S_p\}\}_{p \in I}, C' = \otimes_{p \in I} \{\rho_p \mapsto S_p\})}{\Delta; \Gamma \vdash (\nu s : \Gamma') \text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } P; C} \text{TRRES}}{\Delta; \Gamma \vdash (\nu s : \Gamma') \text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } P; C} \text{TRES}$$

Right to left:

$$\frac{\frac{\Delta, X : \tilde{U}; \Gamma, \Gamma' \vdash P; C \otimes C' \quad \Delta, X : \tilde{U}; \tilde{x} : \tilde{U} \vdash Q_X; \tilde{C}}{\Delta; \Gamma, \Gamma' \vdash \text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } P; C \otimes C'} \text{TDEF} \quad \vdots}{\frac{(\Gamma' = \{\mathbf{s}[p] : \mathbf{tr}(\rho_p), \rho_p : \{\rho_p \mapsto S_p\}\}_{p \in I}, C' = \otimes_{p \in I} \{\rho_p \mapsto S_p\})}{\Delta; \Gamma \vdash (\nu s : \Gamma') \text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } P; C} \text{TRRES}}{\Delta; \Gamma \vdash (\nu s : \Gamma') \text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } P; C} \text{TRES}$$

By rearranging the premises:

$$\frac{\Delta, X : \tilde{U}; \tilde{x} : \tilde{U} \vdash Q_X; \tilde{C} \quad \frac{\Delta, X : \tilde{U}; \Gamma, \Gamma' \vdash P; C \otimes C' \quad (\Gamma' = \{\mathbf{s}[p] : \mathbf{tr}(\rho_p), \rho_p : \{\rho_p \mapsto S_p\}\}_{p \in I}, C' = \otimes_{p \in I} \{\rho_p \mapsto S_p\})}{\Delta, X : \tilde{U}; \Gamma \vdash (\nu s : \Gamma') P; C} \text{TRRES}}{\Delta; \Gamma \vdash \text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } (\nu s : \Gamma') P; C} \text{TDEF}$$

–  $\text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } P \mid Q \equiv (\text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } P) \mid Q$  Left to right:

From the induction hypothesis:  $\Delta; \Gamma \vdash \text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } P \mid Q; C$ . We construct the derivation for the process:

$$\frac{\Delta, X : \tilde{U}; \tilde{x} : \tilde{U} \vdash Q_X; \tilde{C} \quad \frac{\Delta, X : \tilde{U}; \Gamma \vdash P; C_1 \quad \Delta, X : \tilde{U}; \Gamma \vdash Q; C_2}{\Delta, X : \tilde{U}; \Gamma \vdash P \mid Q; C = C_1 \otimes C_2} \text{TPAR}}{\Delta; \Gamma \vdash \text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } P \mid Q; C} \text{TDEF}$$

By rearranging the premises:

$$\frac{\frac{\Delta, X : \tilde{U}; \tilde{x} : \tilde{U} \vdash Q_X; \tilde{C} \quad \Delta, X : \tilde{U}; \Gamma \vdash P; C_1}{\Delta, X : \tilde{U}; \Gamma \vdash \text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } P; C_1} \text{TDEF} \quad \Delta, X : \tilde{U}; \Gamma \vdash Q; C_2}{\Delta; \Gamma \vdash (\text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } P) \mid Q; C} \text{TPAR}$$

Right to left:

From the induction hypothesis:  $\Delta; \Gamma \vdash (\text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } P) \mid Q; \mathbf{C}$ . We construct the derivation for the process:

$$\frac{\frac{\Delta, X : \tilde{U}; \tilde{x} : \tilde{U} \vdash Q_X; \tilde{\mathbf{C}} \quad \Delta, X : \tilde{U}; \Gamma \vdash P; \mathbf{C}_1}{\Delta, X : \tilde{U}; \Gamma \vdash \text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } P; \mathbf{C}_1} \text{TDEF} \quad \Delta, X : \tilde{U}; \Gamma \vdash Q; \mathbf{C}_2}{\Delta; \Gamma \vdash (\text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } P) \mid Q; \mathbf{C}} \text{TPAR}$$

By rearranging the premises:

$$\frac{\Delta, X : \tilde{U}; \tilde{x} : \tilde{U} \vdash Q_X; \tilde{\mathbf{C}} \quad \frac{\Delta, X : \tilde{U}; \Gamma \vdash P; \mathbf{C}_1 \quad \Delta, X : \tilde{U}; \Gamma \vdash Q; \mathbf{C}_2}{\Delta, X : \tilde{U}; \Gamma \vdash P \mid Q; \mathbf{C} = \mathbf{C}_1 \otimes \mathbf{C}_2} \text{TPAR}}{\Delta; \Gamma \vdash \text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } P \mid Q; \mathbf{C}} \text{TDEF}$$

- $\text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } \text{def } Y \langle \tilde{y} : \tilde{U} \rangle = Q_Y \text{ in } P \equiv \text{def } Y \langle \tilde{y} : \tilde{U} \rangle = Q_Y \text{ in } \text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } P$   
 Left to right: From the induction hypothesis:  $\Delta; \Gamma \vdash \text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } \text{def } Y \langle \tilde{y} : \tilde{U} \rangle = Q_Y \text{ in } P; \mathbf{C}$ .  
 We provide the derivaton for this process:

$$\frac{\Delta, X : \tilde{U}; \tilde{x} : \tilde{U} \vdash Q_X; \tilde{\mathbf{C}} \quad \frac{\Delta, X : \tilde{U}, Y : \tilde{U}; \tilde{y} : \tilde{U} \vdash Q_Y; \tilde{\mathbf{C}}' \quad \Delta, X : \tilde{U}, Y : \tilde{U}; \Gamma \vdash P; \mathbf{C}}{\Delta, X : \tilde{U}; \Gamma \vdash \text{def } Y \langle \tilde{y} : \tilde{U} \rangle = Q_Y \text{ in } P; \mathbf{C}} \text{TDEF}}{\Delta; \Gamma \vdash \text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } \text{def } Y \langle \tilde{y} : \tilde{U} \rangle = Q_Y \text{ in } P; \mathbf{C}} \text{TDEF}$$

By Proposition 5  $\Delta, X : \tilde{U}, Y : \tilde{U}; \tilde{y} : \tilde{U} \vdash Q_Y; \tilde{\mathbf{C}}'$  we obtain:  $\Delta, Y : \tilde{U}; \tilde{y} : \tilde{U} \vdash Q_Y; \tilde{\mathbf{C}}'$ .

By rearranging the premises:

$$\frac{\frac{\text{TDEF} \quad \Delta, X : \tilde{U}; \tilde{x} : \tilde{U} \vdash Q_X; \tilde{\mathbf{C}} \quad \Delta, X : \tilde{U}, Y : \tilde{U}; \Gamma \vdash P; \mathbf{C}}{\Delta, Y : \tilde{U}; \Gamma \vdash \text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } P; \mathbf{C}} \quad \Delta, Y : \tilde{U}; \tilde{y} : \tilde{U} \vdash Q_Y; \tilde{\mathbf{C}}'}{\Delta; \Gamma \vdash \text{def } Y \langle \tilde{y} : \tilde{U} \rangle = Q_Y \text{ in } \text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } P; \mathbf{C}} \text{TDEF}$$

Right to left: From the induction hypothesis:  $\Delta; \Gamma \vdash \text{def } Y \langle \tilde{y} : \tilde{U} \rangle = Q_Y \text{ in } \text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } P; \mathbf{C}$ .  
 We provide the derivation for this process:

$$\frac{\frac{\text{TDEF} \quad \Delta, Y : \tilde{U}, X : \tilde{U}; \tilde{x} : \tilde{U} \vdash Q_X; \tilde{\mathbf{C}} \quad \Delta, X : \tilde{U}, Y : \tilde{U}; \Gamma \vdash P; \mathbf{C}}{\Delta, Y : \tilde{U}; \Gamma \vdash \text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } P; \mathbf{C}} \quad \Delta, Y : \tilde{U}; \tilde{y} : \tilde{U} \vdash Q_Y; \tilde{\mathbf{C}}'}{\Delta; \Gamma \vdash \text{def } Y \langle \tilde{y} : \tilde{U} \rangle = Q_Y \text{ in } \text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } P; \mathbf{C}} \text{TDEF}$$

By Proposition 5  $\Delta, Y : \tilde{U}, X : \tilde{U}; \tilde{x} : \tilde{U} \vdash Q_X; \tilde{\mathbf{C}}$  we obtain:  $\Delta, X : \tilde{U}; \tilde{x} : \tilde{U} \vdash Q_X; \tilde{\mathbf{C}}$ .

By rearranging the premises:

$$\frac{\Delta, X : \tilde{U}; \tilde{x} : \tilde{U} \vdash Q_X; \tilde{\mathbf{C}} \quad \frac{\text{TDEF} \quad \Delta, Y : \tilde{U}; \tilde{y} : \tilde{U} \vdash Q_Y; \tilde{\mathbf{C}}' \quad \Delta, X : \tilde{U}, Y : \tilde{U}; \Gamma \vdash P; \mathbf{C}}{\Delta, X : \tilde{U}; \Gamma \vdash \text{def } Y \langle \tilde{y} : \tilde{U} \rangle = Q_Y \text{ in } P; \mathbf{C}} \text{TDEF}}{\Delta; \Gamma \vdash \text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } \text{def } Y \langle \tilde{y} : \tilde{U} \rangle = Q_Y \text{ in } P; \mathbf{C}} \text{TDEF}$$

**Definition 11 (Substitution of Capabilities).** *Substitution of capabilities is defined as:*

$$\begin{aligned} \{\rho \mapsto S\}[\rho'/\rho_2] &= \{\rho \mapsto S\} & \{\rho \mapsto S\}[\rho'/\rho] &= \{\rho' \mapsto S\} \\ \emptyset[\rho'/\rho] &= \emptyset & (C_1 \otimes C_2)[\rho'/\rho] &= C_1[\rho'/\rho] \otimes C_2[\rho'/\rho] \end{aligned}$$

**Lemma 2 (Substitution).**

1. If  $\Delta; \Gamma, x : U \vdash P; C$ , and  $\Gamma' \vdash v : U; \emptyset$ , then  $\Delta; \Gamma, \Gamma' \vdash P\{v/x\}; C$ .
2. If  $\Delta; \Gamma, \rho : \{\rho \mapsto S\} \vdash P; C \otimes \{\rho \mapsto S\}$ ,  $\Gamma' \vdash \rho' : \{\rho' \mapsto S\}; \{\rho' \mapsto S\}$  and  $(\Gamma, \Gamma'; C \otimes \{\rho' \mapsto S\})$  consistent, then  $\Delta; \Gamma, \Gamma' \vdash P\{\rho'/\rho\}; C \otimes \{\rho' \mapsto S\}$ .
3. If  $\Delta; \Gamma, c : \mathbf{tr}(\rho), \rho : \{\rho \mapsto S\} \vdash P; C$ , and  $c' : \mathbf{tr}(\rho'), \rho' : \{\rho' \mapsto S\} \in \Gamma'; \{\rho' \mapsto S\}$  and  $(\Gamma, \Gamma'; C)$  consistent, then  $\Delta; \Gamma, \Gamma' \vdash P\{\rho'/\rho\}; C$ .

**Definition 12.** For all pairs of multiparty session typing contexts and capability collections  $(\Gamma; C)$ ,  $(\Gamma'; C')$ , the relation  $C \leq_S C'$  holds iff  $\text{dom}(\Gamma) = \text{dom}(\Gamma')$ ,  $\text{dom}(C) = \text{dom}(C')$  and  $\forall c : \mathbf{tr}(\rho), \rho : \{\rho \mapsto U\} \in \text{dom}(\Gamma)$  then  $C(\rho) \leq_S C'(\rho)$ . The following rule is defined, corresponding to 0 or more consecutive applications of  $\text{TMSUB}$ :

$$\frac{\text{TMSUB} \quad \Delta; \Gamma \vdash P; C \quad C' \leq_S C}{\Delta; \Gamma \vdash P; C'}$$

**Proposition 9.** If  $\Delta; \Gamma \vdash P \mid Q; C$  then there exist  $C_1, C_2, C'_1, C'_2$  such that  $C = C_1 \otimes C_2$ ,  $C_1 \leq_S C'_1$ ,  $C_2 \leq_S C'_2$ ,  $\Delta; \Gamma \vdash P; C'_1$ ,  $\Delta; \Gamma \vdash Q; C'_2$ . Moreover:

$$\begin{aligned} & \frac{\frac{\text{TMSUB} \quad \Delta; \Gamma \vdash P; C'_1 \quad C_1 \leq_S C'_1}{\Delta; \Gamma \vdash P; C_1} \quad \frac{\text{TMSUB} \quad \Delta; \Gamma \vdash Q; C'_2 \quad C_2 \leq_S C'_2}{\Delta; \Gamma \vdash Q; C_2}}{\Delta; \Gamma \vdash P \mid Q; C_1 \otimes C_2} \text{TPAR} \\ & \text{iff} \frac{\frac{\Delta; \Gamma \vdash P; C'_1 \quad \Delta; \Gamma \vdash Q; C'_2}{\Delta; \Gamma \vdash P \mid Q; C'_1 \otimes C'_2} \text{TPAR} \quad C_1 \otimes C_2 \leq_S C'_1 \otimes C'_2}{\Delta; \Gamma \vdash P \mid Q; C_1 \otimes C_2} \text{TMSUB} \\ & \text{iff} \frac{\frac{\Delta; \Gamma \vdash P; C'_1}{\Delta; \Gamma \vdash P; C_1} \text{TMSUB} \quad \frac{\Delta; \Gamma \vdash Q; C'_2 \quad C_2 \leq_S C'_2}{\Delta; \Gamma \vdash Q; C_2} \text{TMSUB}}{\Delta; \Gamma \vdash P \mid Q; C'_1 \otimes C'_2} \text{TPAR} \quad C_1 \otimes C_2 \leq_S C'_1 \otimes C'_2}{\Delta; \Gamma \vdash P \mid Q; C_1 \otimes C_2} \text{TMSUB} \\ & \text{iff} \frac{\frac{\Delta; \Gamma \vdash P; C'_1 \quad C_1 \leq_S C'_1}{\Delta; \Gamma \vdash P; C_1} \text{TMSUB} \quad \Delta; \Gamma \vdash Q; C'_2}{\Delta; \Gamma \vdash P \mid Q; C_1 \otimes C'_2} \text{TPAR} \quad C_1 \otimes C_2 \leq_S C_1 \otimes C'_2}{\Delta; \Gamma \vdash P \mid Q; C_1 \otimes C_2} \text{TMSUB} \end{aligned}$$

*Proof.* The first part of the statement is proven by inversion of  $\text{TPAR}$ , by Definition 12 and adding a possibly vacuous instance of  $\text{TMSUB}$ , as in the last case in the statement after “moreover”. The “iff”

relations among the typing derivations are straightforward: the hypotheses of one derivation imply all the others, and if one hypothesis is falsified, none of the derivations hold.

**Proposition 10.**  $\Delta; \Gamma_1 \vdash (\nu s : \Gamma_2)P; C_1$  then there exist  $\Gamma'_1, \Gamma'_2, C'_1, C'_2$  such that  $(\Gamma_1; C_1) \leq_s (\Gamma'_1; C'_1)$ ,  $(\Gamma_2; C_2) \leq_s (\Gamma'_2; C'_2)$  and  $\Delta; \Gamma_1, \Gamma_2 \vdash P; C'_1 \otimes C'_2$ . Moreover:

$$\frac{\frac{\Delta; \Gamma_1, \Gamma_2 \vdash P; C'_1 \otimes C'_2}{C_1 \otimes C_2 \leq_s C'_1 \otimes C'_2} \text{TMSUB} \quad \frac{\Delta; \Gamma_1, \Gamma_2 \vdash P; C'_1 \otimes C'_2}{C_2 \leq_s C'_2} \text{TMSUB}}{\Delta; \Gamma_1, \Gamma_2 \vdash P; C_1 \otimes C_2} \text{TMSUB} \quad \frac{\Delta; \Gamma_1, \Gamma_2 \vdash P; C'_1 \otimes C'_2}{\Delta; \Gamma_1 \vdash (\nu s : \Gamma_2)P; C'_1} \text{TRRES}}{\Delta; \Gamma_1 \vdash (\nu s : \Gamma_2)P; C_1} \text{TRRES} \quad \text{iff} \quad \frac{\Delta; \Gamma_1, \Gamma_2 \vdash P; C'_1 \otimes C'_2}{\Delta; \Gamma_1 \vdash (\nu s : \Gamma_2)P; C_1} \text{TRRES} \quad \frac{C_1 \leq_s C'_1}{\Delta; \Gamma_1 \vdash (\nu s : \Gamma_2)P; C_1} \text{TMSUB}$$

**Proposition 11 (Subtyping normalisation).** If  $\Delta; \Gamma \vdash P; C$  then there exists a derivation that proves the judgement by only applying rule TMSUB on the conclusions of TBR, TSEL, TBRP, TSELP, and TCALL.

*Proof (Theorem 1).* By induction on the derivation of the reduction  $P \rightarrow P'$ :

- **case RCom** We have:  $P = \mathbf{s}[p][q] \&_{i \in I} \{l_i(x_i). Q_i\} \mid \mathbf{s}[q][p] \oplus \langle l_j(v) \rangle . Q \rightarrow Q_j \{v/x_j\} \mid Q = P'$ , where if  $j \in I$  and  $fv(v) = \emptyset$ , and  $C = C_1 \otimes \{\rho_p \mapsto p \&_{i \in I} ?l_i(U_i).S_i\} \otimes C_2 \otimes \{\rho_q \mapsto q \oplus_{j \in I} !l_j(U).S\}$ . We distinguish two cases based on whether the payload communicated has a capability attached or not.

**In the first case**, the payload has no capability attached. We provide the derivation for  $P$ , allowing (possibly vacuous) instances of TMSUB as per Proposition 11:

$$\frac{\frac{\text{TBR} \quad \frac{\Delta; \Gamma, x_i : U'_i \vdash Q_i; C_1^\circ \otimes \{\rho_p \mapsto S'_i\} \quad \mathbf{s}[p] : \mathbf{tr}(\rho_p), \rho_p : \{\rho_p \mapsto S'_i\} \in \Gamma}{\Delta; \Gamma \vdash \mathbf{s}[p][q] \&_{i \in I} \{l_i(x_i). Q_i\}; C_1^\circ \otimes \{\rho_p \mapsto p \&_{i \in I} ?l_i(U'_i).S'_i\}} \quad C_1 \leq_s C'_1}{\Delta; \Gamma \vdash \mathbf{s}[p][q] \&_{i \in I} \{l_i(x_i). Q_i\}; C_1 \otimes \{\rho_p \mapsto p \&_{i \in I} ?l_i(U_i).S_i\}} \text{TMSUB}}{\vdots} \quad \frac{\frac{v \in U'}{\Gamma \vdash v : U'; \emptyset} \text{TVAL} \quad \frac{\mathbf{s}[q] : \mathbf{tr}(\rho_q), \rho_q : \{\rho_q \mapsto S'\} \in \Gamma \quad \Delta; \Gamma \vdash Q; C_2^\circ \otimes \{\rho_q \mapsto S'\}}{\Delta; \Gamma \vdash \mathbf{s}[q][p] \oplus \langle l_j(v) \rangle . Q; C_2^\circ \otimes \{\rho_q \mapsto q \oplus_{j \in I} !l_j(U').S'\}} \text{TSEL}}{\vdots} \quad \frac{\vdots}{\Delta; \Gamma \vdash \mathbf{s}[q][p] \oplus \langle l_j(v) \rangle . Q; C_2} \quad C_2 \leq_s C'_2 \text{TMSUB}}{\Delta; \Gamma \vdash \mathbf{s}[p][q] \&_{i \in I} \{l_i(x_i). Q_i\} \mid \mathbf{s}[q][p] \oplus \langle l_j(v) \rangle . Q; C} \text{TPAR}$$

$$\begin{aligned} C &= C_1 \otimes C_2 \\ C_1 &= C_1^\circ \otimes \{\rho_p \mapsto S_p\} \text{ where } S_p = p \&_{i \in I} ?l_i(U_i).S_i \\ C_2 &= C_2^\circ \otimes \{\rho_q \mapsto S_q\} \text{ where } S_q = q \oplus_{j \in I} !l_j(U).S \\ C'_1 &= C_1'^\circ \otimes \{\rho_p \mapsto S'_p\} \text{ where } S'_p = p \&_{i \in I} ?l_i(U'_i).S'_i \\ C'_2 &= C_2'^\circ \otimes \{\rho_q \mapsto S'_q\} \text{ where } S'_q = q \oplus_{j \in I} !l_j(U').S' \end{aligned}$$

From the consistency of  $(\Gamma; C) = (\Gamma; C_1 \otimes C_2)$ , and since  $C_1 \leq_s C'_1$  and  $C_2 \leq_s C'_2$  we also have:  $U' \leq_s U'_i$ .

Before proceeding, we prove  $(\Gamma; C) \longrightarrow (\Gamma; C')$ , and therefore,  $(\Gamma; C) \longrightarrow^* (\Gamma; C')$ :

We observe that:

$$(\mathfrak{s}[\mathbf{p}] : \mathbf{tr}(\rho_{\mathbf{p}}), \mathfrak{s}[\mathbf{q}] : \mathbf{tr}(\rho_{\mathbf{q}}); \{\rho_{\mathbf{p}} \mapsto S_{\mathbf{p}}, \rho_{\mathbf{q}} \mapsto S_{\mathbf{q}}\}) \longrightarrow (\mathfrak{s}[\mathbf{p}] : \mathbf{tr}(\rho_{\mathbf{p}}), \mathfrak{s}[\mathbf{q}] : \mathbf{tr}(\rho_{\mathbf{q}}); \{\rho_{\mathbf{p}} \mapsto S'_j, \rho_{\mathbf{q}} \mapsto S'\})$$

since  $(\Gamma; C)$  is consistent by hypothesis, and therefore  $\mathbf{unf}(S_{\mathbf{p}} \upharpoonright \mathbf{q})$  and  $\mathbf{unf}(S_{\mathbf{q}} \upharpoonright \mathbf{p})$  have at least  $l_j$  in common, with compatible payload types as per Definition 10.

Then we can prove the following statement:

$$(\Gamma; C_1 \otimes C_2 \otimes \{\rho_{\mathbf{p}} \mapsto S_{\mathbf{p}}, \rho_{\mathbf{q}} \mapsto S_{\mathbf{q}}\}) \longrightarrow (\Gamma; C'_1 \otimes C'_2 \otimes \{\rho_{\mathbf{p}} \mapsto S'_j, \rho_{\mathbf{q}} \mapsto S'\})$$

by induction on the size of  $C_1 \otimes C_2$ . The base case is given above, while for the inductive case we apply the induction hypothesis use the subtyping relations between the capability sets to conclude by the inductive rule of Definition 10.

We can now continue proving the main statement, observing:

$$\begin{array}{ll} (\Gamma; C') \text{ is consistent} & \text{by Lemma 1} \\ \Delta; \Gamma, x_j : U'_j \vdash Q_i; C'_1{}^\circ \otimes \{\rho_{\mathbf{p}} \mapsto S'_j\} \ (j \in I) & \text{from the premise of TBR} \\ \Delta; \Gamma, x_j : U'_j \vdash Q_j; C'_1{}^\circ \otimes \{\rho_{\mathbf{p}} \mapsto S'_j\} & \text{from the premise of TSub} \\ \Gamma \vdash v : U' & \text{from the premise of TSEL} \\ (\Gamma, C'_1{}^\circ \otimes \{\rho_{\mathbf{p}} \mapsto S'_j\}) \text{ is consistent} & \text{from the above} \\ \Delta; \Gamma \vdash Q_j \{v/x_j\}; C'_1{}^\circ \otimes \{\rho_{\mathbf{p}} \mapsto S'_j\} & \text{from the above and Lemma 2} \end{array}$$

Therefore we conclude by:

$$\frac{\Delta; \Gamma \vdash Q_j \{v/x_j\}; C'_1{}^\circ \otimes \{\rho_{\mathbf{p}} \mapsto S'_j\} \quad \Delta; \Gamma \vdash Q; C'_2{}^\circ \otimes \{\rho_{\mathbf{q}} \mapsto S'\}}{\Delta; \Gamma \vdash Q_j \{v/x_j\} \mid Q; C'} \text{TPAR}$$

**Second case case**, the payload has a capability attached, which means that the payload in itself must be a capability.

By inversion of TPAR and TBR/TSEL, allowing (possibly vacuous) instances of TMSUB as per Proposition 11, there exist  $C_1, C_2$  such that  $C = C_1 \otimes C_2$ , and  $C'_1, C'_2$  such that:

$$\begin{array}{c} \text{TBR} \\ \frac{\Delta; \Gamma, \rho_i : \{\rho_i \mapsto U'_i\} \vdash Q_i; C'_1{}^\circ \otimes \{\rho_{\mathbf{p}} \mapsto S'_i, \rho_i \mapsto U'_i\} \quad \mathfrak{s}[\mathbf{p}] : \mathbf{tr}(\rho_{\mathbf{p}}), \rho_{\mathbf{p}} : \{\rho_{\mathbf{p}} \mapsto S'_i\} \in \Gamma}{\Delta; \Gamma \vdash \mathfrak{s}[\mathbf{p}][\mathbf{q}] \&_{i \in I} \{l_i(\rho_i). Q_i\}; C'_1{}^\circ \otimes \{\rho_{\mathbf{p}} \mapsto \mathbf{p} \&_{i \in I} l_i(\{\rho_i \mapsto U'_i\}). S'_i\}} \quad C_1 \leq_s C'_1}{\Delta; \Gamma \vdash \mathfrak{s}[\mathbf{p}][\mathbf{q}] \&_{i \in I} \{l_i(\rho_i). Q_i\}; C_1} \text{TMSUB} \\ \vdots \\ \text{TCAP} \\ \frac{\mathfrak{s}[\mathbf{q}] : \mathbf{tr}(\rho_{\mathbf{q}}), \rho_{\mathbf{q}} : \{\rho_{\mathbf{q}} \mapsto S'\} \in \Gamma \quad \Delta; \Gamma \vdash Q; C'_2{}^\circ \otimes \{\rho_{\mathbf{q}} \mapsto S'\} \quad \Gamma \vdash \rho : \{\rho \mapsto U'\}; \{\rho \mapsto U'\}}{\Delta; \Gamma \vdash \mathfrak{s}[\mathbf{q}][\mathbf{p}] \oplus \langle l_j(v) \rangle . Q; C'_2{}^\circ \otimes \{\rho_{\mathbf{q}} \mapsto \mathbf{q} \oplus_{j \in I} l_j(\{\rho \mapsto U'\}). S'\} \otimes \{\rho \mapsto U'\}} \text{TSEL} \\ \vdots \\ \text{TMSUB} \\ \frac{\Delta; \Gamma \vdash \mathfrak{s}[\mathbf{q}][\mathbf{p}] \oplus \langle l_j(v) \rangle . Q; C_2}{\Delta; \Gamma \vdash \mathfrak{s}[\mathbf{q}][\mathbf{p}] \oplus \langle l_j(v) \rangle . Q; C_2} \text{TMSUB} \\ \text{TPAR} \\ \frac{\Delta; \Gamma \vdash \mathfrak{s}[\mathbf{p}][\mathbf{q}] \&_{i \in I} \{l_i(\rho_i). Q_i\} \mid \mathfrak{s}[\mathbf{q}][\mathbf{p}] \oplus \langle l_j(v) \rangle . Q; C_2}{\Delta; \Gamma \vdash \mathfrak{s}[\mathbf{p}][\mathbf{q}] \&_{i \in I} \{l_i(\rho_i). Q_i\} \mid \mathfrak{s}[\mathbf{q}][\mathbf{p}] \oplus \langle l_j(v) \rangle . Q; C} \text{TPAR} \end{array}$$

$$\begin{aligned}
C &= C_1 \otimes C_2 \\
C_1 &= C_1^\circ \otimes \{\rho_p \mapsto S_p\} \text{ where } S_p = \mathbf{p} \&_{i \in I} ?l_i(U_i).S_i \\
C_2 &= C_2^\circ \otimes \{\rho_q \mapsto S_q\} \otimes \{\rho \mapsto U\} \text{ where } S_q = \mathbf{q} \oplus_{j \in I} !l_j(U).S \\
C'_1 &= C_1^\circ \otimes \{\rho_p \mapsto S'_p\} \text{ where } S'_p = \mathbf{p} \&_{i \in I} ?l_i(U'_i).S'_i \\
C'_2 &= C_2^\circ \otimes \{\rho_q \mapsto S'_q\} \otimes \{\rho \mapsto U'\} \text{ where } S'_q = \mathbf{q} \oplus_{j \in I} !l_j(U').S'
\end{aligned}$$

From the consistency of  $(\Gamma; C) = (\Gamma; C_1 \otimes C_2)$ , and since  $C_1 \leq_S C'_1$  and  $C_2 \leq_S C'_2$  we also have:  $U' \leq_S U'_i$ .

Before proceeding, we prove  $(\Gamma; C) \longrightarrow (\Gamma; C')$ , and therefore,  $(\Gamma; C) \longrightarrow^* (\Gamma; C')$ :

We observe that:

$$(\mathbf{s}[\mathbf{p}] : \mathbf{tr}(\rho_p), \mathbf{s}[\mathbf{q}] : \mathbf{tr}(\rho_q); \{\rho_p \mapsto S_p, \rho_q \mapsto S_q\}) \longrightarrow (\mathbf{s}[\mathbf{p}] : \mathbf{tr}(\rho_p), \mathbf{s}[\mathbf{q}] : \mathbf{tr}(\rho_q); \{\rho_p \mapsto S'_p, \rho_q \mapsto S'_q\})$$

since  $(\Gamma; C)$  is consistent by hypothesis, and therefore  $\mathbf{unf}(S_p \upharpoonright \mathbf{q})$  and  $\mathbf{unf}(S_q \upharpoonright \mathbf{p})$  have at least  $l_j$  in common, with compatible payload types as per Definition 10.

Then we can prove the following statement:

$$(\Gamma; C_1^\circ \otimes C_2^\circ \otimes \{\rho_p \mapsto S_p, \rho_q \mapsto S_q, \rho \mapsto U\}) \longrightarrow (\Gamma; C_1^\circ \otimes C_2^\circ \otimes \{\rho_p \mapsto S'_p, \rho_q \mapsto S'_q, \rho \mapsto U'\})$$

by induction on the size of  $C_1 \otimes C_2$ . The base case is given above, while for the inductive case we apply the induction hypothesis use the subtyping relations between the capability sets to conclude by the inductive rule of Definition 10.

We can now continue proving the main statement, observing:

$$\begin{array}{ll}
(\Gamma; C') \text{ is consistent} & \text{by Lemma 1} \\
\Delta; \Gamma, \rho_j : \{\rho_j \mapsto U'_j\} \vdash Q_j; C_1^\circ \otimes \{\rho_p \mapsto S'_p, \rho_j \mapsto U'_j\} \ (j \in I) & \text{from the premise of TBR} \\
\Delta; \Gamma, \rho_j : \{\rho_j \mapsto U'_j\} \vdash Q_j; C_1^\circ \otimes \{\rho_p \mapsto S'_p, \rho_j \mapsto U'_j\} \ (j \in I) & \text{from the premise of TSub} \\
\Gamma \vdash \rho : \{\rho \mapsto U'\}; \{\rho \mapsto U'\} & \text{from the premise of TSEL} \\
(\Gamma; C_1^\circ \otimes \{\rho_p \mapsto S'_p, \rho \mapsto U'\}) \text{ is consistent} & \text{from the above and Corollary 2} \\
\Delta; \Gamma \vdash Q_j \{v/\rho_j\}; C_1^\circ \otimes \{\rho_p \mapsto S'_p, \rho \mapsto U'\} & \text{from the above and Lemma 2}
\end{array}$$

Therefore we conclude by:

$$\frac{\Delta; \Gamma \vdash Q_j \{v/\rho_j\}; C_1^\circ \otimes \{\rho_p \mapsto S'_p, \rho \mapsto U'\} \quad \Delta; \Gamma \vdash Q; C_2^\circ \otimes \{\rho_q \mapsto S'_q\}}{\Delta; \Gamma \vdash Q_j \{v/x_j\} \mid Q; C'} \text{TPAR}$$

– **case RComP**

We have:  $P = \mathbf{s}[\mathbf{p}][\mathbf{q}] \&_{i \in I} ?l_i(\mathbf{pack}(\rho_i, \mathbf{v}_i)).Q_i \mid \mathbf{s}[\mathbf{q}][\mathbf{p}] \oplus (l_j(\mathbf{pack}(\rho, \mathbf{v}))).Q \longrightarrow Q_j \{v/v_j\} \mid Q = P'$ , where: if  $j \in I$  and  $fv(v) = \emptyset$ .

$$\begin{array}{c}
\text{TBRP} \\
\frac{\Delta; \Gamma, v_i : \mathbf{tr}(\rho_i), \rho_i : \{\rho_i \mapsto U'_i\} \vdash Q_i; C_1^{\circ} \otimes \{\rho_p \mapsto S'_i\} \quad \mathbf{s}[p] \in \Gamma}{\Delta; \Gamma \vdash \mathbf{s}[p][q] \&_{i \in I} ?l_i(\mathbf{pack}(\rho_i, v_i)).Q_i; C_1^{\circ} \otimes \{\rho_p \mapsto S_p\}} \quad C_1 \leq_S C_1' \\
\hline
\Delta; \Gamma \vdash \mathbf{s}[p][q] \&_{i \in I} ?l_i(\mathbf{pack}(\rho_i, v_i)).Q_i; C_1 \\
\vdots \\
\frac{v : \mathbf{tr}(\rho), \rho : \{\rho \mapsto U\} \in \Gamma}{\Gamma \vdash v : \mathbf{tr}(\rho); \emptyset} \text{TVAR} \\
\vdots \\
\frac{\mathbf{s}[q] : \mathbf{tr}(\rho_q) \in \Gamma \quad \Delta; \Gamma \vdash Q; C_2^{\circ} \otimes \{\rho_q \mapsto S'\} \otimes \{\rho \mapsto U'\} \quad j \in I}{\Delta; \Gamma \vdash \mathbf{s}[q][p] \oplus (l_j(\mathbf{pack}(\rho, v))).Q; C_2^{\circ} \otimes \{\rho_q \mapsto S_q\} \otimes \{\rho \mapsto U'\}} \text{TSELP} \\
\vdots \\
\frac{\Delta; \Gamma \vdash \mathbf{s}[q][p] \oplus (l_j(\mathbf{pack}(\rho, v))).Q; C_2}{\Delta; \Gamma \vdash \mathbf{s}[q][p] \oplus (l_j(\mathbf{pack}(\rho, v))).Q; C_2} \text{TMSUB} \\
\hline
\Delta; \Gamma \vdash \mathbf{s}[p][q] \&_{i \in I} ?l_i(\mathbf{pack}(\rho_i, v_i)).Q_i \mid \mathbf{s}[q][p] \oplus (l_j(\mathbf{pack}(\rho, v))).Q; C_1 \otimes C_2 \quad \text{TTPAR}
\end{array}$$

$$C = C_1 \otimes C_2$$

$$C_1 = C_1^{\circ} \otimes \{\rho_p \mapsto S_p\} \text{ where } S_p = \mathbf{p} \&_{i \in I} ?l_i(\exists[\rho_i | \{\rho_i \mapsto U_i\}]. \mathbf{tr}(\rho_i)).S_i$$

$$C_2 = C_2^{\circ} \otimes \{\rho \mapsto U\} \otimes \{\rho_q \mapsto S_q\} \text{ where } S_q = \mathbf{q} \oplus_{j \in I} !l_j(\exists[\rho | \{\rho \mapsto U\}]. \mathbf{tr}(\rho)).S$$

$$C_1' = C_1^{\circ} \otimes \{\rho_p \mapsto S'_p\} \text{ where } S'_p = \mathbf{p} \&_{i \in I} ?l_i(U'_i).S'_i$$

$$C_2' = C_2^{\circ} \otimes \{\rho \mapsto U'\} \otimes \{\rho_q \mapsto S'_q\} \text{ where } S'_q = \mathbf{q} \oplus_{j \in I} !l_j(\exists[\rho | \{\rho \mapsto U'\}]. \mathbf{tr}(\rho)).S'$$

From the consistency of  $(\Gamma; C) = (\Gamma; C_1 \otimes C_2)$ , and since  $C_1 \leq_S C_1'$  and  $C_2 \leq_S C_2'$  we also have:  $U \leq_S U'_j$ .

Before proceeding, we prove  $(\Gamma; C) \longrightarrow (\Gamma; C')$ , and therefore,  $(\Gamma; C) \longrightarrow^* (\Gamma; C')$ :

We observe that:

$$(\mathbf{s}[p] : \mathbf{tr}(\rho_p), \mathbf{s}[q] : \mathbf{tr}(\rho_q); \{\rho_p \mapsto S_p, \rho_q \mapsto S_q\}) \longrightarrow (\mathbf{s}[p] : \mathbf{tr}(\rho_p), \mathbf{s}[q] : \mathbf{tr}(\rho_q); \{\rho_p \mapsto S'_p, \rho_q \mapsto S'_q\})$$

since  $(\Gamma; C)$  is consistent by hypothesis, and therefore  $\mathbf{unf}(S_p \upharpoonright \mathbf{q})$  and  $\mathbf{unf}(S_q \upharpoonright \mathbf{p})$  have at least  $l_j$  in common, with compatible payload types as per Definition 10.

Then we can prove the following statement:

$$(\Gamma; C_1^{\circ} \otimes C_2^{\circ} \otimes \{\rho_p \mapsto S_p, \rho_q \mapsto S_q, \rho \mapsto U\}) \longrightarrow (\Gamma; C_1^{\circ} \otimes C_2^{\circ} \otimes \{\rho_p \mapsto S'_p, \rho_q \mapsto S'_q, \rho \mapsto U\})$$

by induction on the size of  $C_1 \otimes C_2$ . The base case is given above, while for the inductive case we apply the induction hypothesis use the subtyping relations between the capability sets to conclude by the inductive rule of Definition 10.

We can now continue proving the main statement, observing:

$$\begin{array}{ll}
(\Gamma; C') \text{ is consistent} & \text{by Lemma 1} \\
\Delta; \Gamma, v_j : \mathbf{tr}(\rho_j), \rho_j : \{\rho_j \mapsto U'_j\} \vdash Q_j; C_1^{\circ} \otimes \{\rho_p \mapsto S'_j\} \quad (j \in I) & \text{from the premise of TBR} \\
\Gamma \vdash v : \mathbf{tr}(\rho); \emptyset & \text{from the premise of TSEL} \\
(\Gamma, C_1^{\circ} \otimes \{\rho_p \mapsto S'_j\}) \text{ is consistent} & \text{from the above and Corollary 2} \\
\Delta; \Gamma \vdash Q_j \{v/v_j\}; C_1^{\circ} \otimes \{\rho_p \mapsto S'_j\} & \text{from the above and Lemma 2}
\end{array}$$

Therefore we conclude by:

$$\frac{\Delta; \Gamma \vdash Q_j\{v/v_j\}; C_1^{\circ} \otimes \{\rho_p \mapsto S'_j\} \quad \Delta; \Gamma \vdash Q; C_2^{\circ} \otimes \{\rho_q \mapsto S'\} \otimes \{\rho \mapsto U'\}}{\Delta; \Gamma \vdash Q_j\{v/v_j\} \mid Q; C'} \text{TPAR}$$

– **case RCall**

We have:  $P = \text{def } X\langle \tilde{x} \rangle = Q_X \text{ in } (X\langle \tilde{v} \rangle \mid Q) \longrightarrow \text{def } X\langle \tilde{x} \rangle = Q_X \text{ in } (Q_X\{\tilde{v}/\tilde{x}\} \mid Q) = P'$ .

$$\frac{\frac{\frac{\forall i \in \{1..n\} \quad \Gamma \vdash v_i : U_i; C'_i}{\Delta, X : \tilde{U}; \Gamma \vdash X\langle \tilde{v} \rangle; C'_X = C'_1 \otimes \dots \otimes C'_n} \text{TCALL} \quad C_X \leq_s C'_X}{\Delta, X : \tilde{U}; \Gamma \vdash X\langle \tilde{v} \rangle; C_X} \text{TMSUB} \quad \Delta, X : \tilde{U}; \Gamma \vdash Q; C_Q}{\Delta, X : \tilde{U}; \Gamma \vdash (X\langle \tilde{v} \rangle \mid Q); C} \text{TPAR}}{\Delta, X : \tilde{U}; \tilde{x} : \tilde{U} \vdash Q_X; \tilde{C}} \text{TDEF} \quad \vdots$$

$$\frac{\Delta, X : \tilde{U}; \tilde{x} : \tilde{U} \vdash Q_X; \tilde{C}}{\Delta; \Gamma \vdash \text{def } X\langle \tilde{x} \rangle = Q_X \text{ in } (X\langle \tilde{v} \rangle \mid Q); C} \text{TDEF}$$

Observe that from  $\Delta, X : \tilde{U}; \tilde{x} : \tilde{U} \vdash Q_X; \tilde{C}$ , by applying Lemma 2  $n$  times (each time obtaining a consistent context) we obtain  $\Delta, X : \tilde{U}; \Gamma \vdash Q_X\{\tilde{v}/\tilde{x}\}; C'_X$ . By applying TMSUB we obtain  $\Delta, X : \tilde{U}; \Gamma \vdash Q_X\{\tilde{v}/\tilde{x}\}; C_X$ .

$$\frac{\Delta, X : \tilde{U}; \tilde{x} : \tilde{U} \vdash Q_X; \tilde{C} \quad \frac{\Delta, X : \tilde{U}; \Gamma \vdash Q_X\{\tilde{v}/\tilde{x}\}; C_X \quad \Delta, X : \tilde{U}; \Gamma \vdash Q; C_Q}{\Delta, X : \tilde{U}; \Gamma \vdash Q_X\{\tilde{v}/\tilde{x}\} \mid Q; C} \text{TPAR}}{\Delta; \Gamma \vdash \text{def } X\langle \tilde{x} \rangle = Q_X \text{ in } (Q_X\{\tilde{v}/\tilde{x}\} \mid Q); C} \text{TDEF}$$

– **case RRes**

We have  $P = (\nu s : \Gamma')Q \longrightarrow (\nu s)R = P'$ , with  $Q \longrightarrow R$  (from the rule premise).

$$\frac{\text{TRES} \quad \Delta; \Gamma, \Gamma' \vdash Q; C \otimes C_1 \quad (\Gamma' = \{\mathbf{s}[p] : \mathbf{tr}(\rho_p), \rho_p : \{\rho_p \mapsto S_p\}\}_{p \in I}, C_1 = \otimes_{p \in I} \{\rho_p \mapsto S_p\})}{\Delta; \Gamma \vdash (\nu s : \Gamma')Q; C}$$

By the induction hypothesis,  $\Delta; \Gamma, \Gamma' \vdash R; C_2$  and  $(\Gamma, \Gamma', C \otimes C_1) \longrightarrow^* (\Gamma, \Gamma', C_2)$ .

By Proposition 3 we know that  $\text{dom}(C_2) = \text{dom}(C \otimes C_1) = \text{dom}(C \otimes_{p \in I} \{\rho_p \mapsto S_p\})$ .

So we can rewrite  $C_2$  as  $C' \otimes C'_1$ , where  $\text{dom}(C') = \text{dom}(C)$ ,  $\text{dom}(C'_1) = \text{dom}(C_1)$ , and  $C'_1 = \otimes_{p \in I} \{\rho_p \mapsto S'_p\}$ .

The reduction  $(\Gamma, \Gamma', C \otimes C_1) \longrightarrow^* (\Gamma, \Gamma', C_2)$  then becomes:  $(\Gamma, \Gamma', C \otimes C_1) \longrightarrow^* (\Gamma, \Gamma', C' \otimes C'_1)$ .

By Definition 10  $(\Gamma, \Gamma', C' \otimes C'_1)$  is consistent, and therefore by Corollary 2  $(\Gamma', C')$  is consistent.

Hence:

$$\frac{\text{TRES} \quad \Delta; \Gamma, \Gamma' \vdash R; C' \otimes C'_1 \quad (\Gamma' = \{\mathbf{s}[p] : \mathbf{tr}(\rho_p), \rho_p : \{\rho_p \mapsto S_p\}\}_{p \in I}, C'_1 = \otimes_{p \in I} \{\rho_p \mapsto S'_p\})}{\Delta; \Gamma \vdash (\nu s : \Gamma')R; C'}$$



– **case RPar**

We have  $P = Q \mid R \longrightarrow Q' \mid R = P'$ , with  $Q \longrightarrow Q'$  from the rule premise.

$$\text{T}_{\text{PAR}} \frac{\Delta; \Gamma \vdash Q; C_1 \quad \Delta; \Gamma \vdash R; C_2}{\Delta; \Gamma \vdash Q \mid R; C = C_1 \otimes C_2}$$

By the induction hypothesis  $\Delta; \Gamma \vdash Q'; C_3$ , and  $(\Gamma, C_1) \longrightarrow^* (\Gamma, C_3)$ .

$$\text{T}_{\text{PAR}} \frac{\Delta; \Gamma \vdash Q'; C_3 \quad \Delta; \Gamma \vdash R; C_2}{\Delta; \Gamma \vdash Q' \mid R; C_3 \otimes C_2 = C'}$$

By Corollary 2  $(\Gamma, C_1 \otimes C_2) \longrightarrow^* (\Gamma, C_3 \otimes C_2)$ , which is to say  $(\Gamma, C) \longrightarrow^* (\Gamma, C')$  as required.

– **case RDef** We have  $P = \text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } Q \longrightarrow \text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } Q' = P'$  from the rule premise.

$$\frac{\Delta, X : \tilde{U}; \tilde{x} : \tilde{U} \vdash Q_X; \tilde{C} \quad \Delta, X : \tilde{U}; \Gamma \vdash Q; C}{\Delta; \Gamma \vdash \text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } Q; C} \text{T}_{\text{DEF}}$$

By the induction hypothesis,  $\Delta, X : \tilde{U}; \Gamma \vdash Q'; C'$  and  $(\Gamma, C) \longrightarrow^* (\Gamma, C')$ , and we conclude by:

$$\frac{\Delta, X : \tilde{U}; \tilde{x} : \tilde{U} \vdash Q_X; \tilde{C} \quad \Delta, X : \tilde{U}; \Gamma \vdash Q'; C'}{\Delta; \Gamma \vdash \text{def } X \langle \tilde{x} : \tilde{U} \rangle = Q_X \text{ in } Q'; C'} \text{T}_{\text{DEF}}$$

– **case RCong**

We have  $P \equiv Q$ ,  $P' \equiv Q'$ , and  $Q \longrightarrow Q'$  from the rule premise. By Proposition 8  $\Delta; \Gamma \vdash Q; C$ . By the induction hypothesis  $\Delta; \Gamma \vdash Q'; C'$  and  $(\Gamma, C) \longrightarrow^* (\Gamma, C')$ . By Proposition 8 we conclude  $\Delta; \Gamma \vdash P'; C'$ .