Globally Governed Session Semantics

Dimitrios Kouzapas and Nobuko Yoshida
Imperial College London

Abstract. This paper proposes a new bisimulation theory based on multiparty session types where a choreography specification governs the behaviour of session typed processes and their observer. The bisimulation is defined with the observer cooperating with the observed process in order to form complete global session scenarios and usable for proving correctness of optimisations for globally coordinating threads and processes. The induced bisimulation is strictly more fine-grained than the standard session bisimulation. The difference between the governed and standard bisimulations only appears when more than two interleaved multiparty sessions exist. This distinct feature enables to reason real scenarios in the large-scale distributed system where multiple choreographic sessions need to be interleaved. The compositionality of the governed bisimilarity is proved through the soundness and completeness with respect to the governed reduction-based congruence. Finally its usage is demonstrated by a thread transformation governed under multiple sessions in a real usecase in the large-scale cyberinfrustracture.

1 Introduction

Modern society increasingly depends on distributed software infrastructures such as the backend of popular Web portals, global E-science cyberinfrastructure, e-healthcare and e-governments. An application in these environments is typically organised into many components which communicate through message passing. Thus an application is naturally designed as a collection of interaction scenarios, or *multiparty sessions*, each following an interaction pattern, or *choreographic protocol*. The theories of multiparty session types [12] capture these two natural abstraction units, representing the situation where two or more multiparty sessions (choreographies) can interleave for a single point application, with each message clearly identifiable as belonging to a specific session.

This paper introduces a new behavioural theory which can reason about distributed processes globally controlled by multiple choreographic sessions. Typed behavioural theory has been one of the central topics of the study of the π-calculus throughout its history, for example, in order to reason about various encodings into the typed π-calculi [18, 20]. Our theory treats the mutual effects of multiple choreographic sessions which are shared among distributed participants as their common knowledges or agreements, reflecting the origin of choreographic frameworks [4]. These features distinct our theory from any type-based bisimulations in the literature and make the theory applicable to real choreographic usecase from a large-scale distributed system. Since our bisimulation is based on the regulation of conversational behaviours of distributed components by global specifications, we call our bisimulation *globally governed bisimulation*.

To illustrate the key idea, we first explain the mechanisms of multiparty session types [12]. Let us consider a simple protocol where participant 1 sends a message of type `bool` to participant 2. To develop the code for this protocol, we start by specifying the *global type* [12] as $G_1 = 1 \to 2 \colon \langle \texttt{bool} \rangle ; \texttt{end}$ where $\to$ signifies the flow of communication and `end` denotes protocol termination. With agreement on G_1 as a specification for participant 1 and participant 2, each program can be implemented separately. Then for type-checking, G_1 is *projected* into local session types: one local session type from 1's point of view,

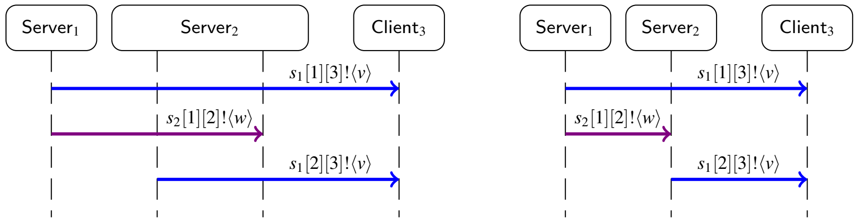
Server$_1$
Server$_2$
Client$_3$
$s_1[1][3]!\langle v\rangle$
$s_2[1][2]!\langle w\rangle$
$s_1[2][3]!\langle v\rangle$
Server$_1$
Server$_2$
Client$_3$
$s_1[1][3]!\langle v\rangle$
$s_2[1][2]!\langle w\rangle$
$s_1[2][3]!\langle v\rangle$

Fig. 1. Resource Managment Example: (a) before optimisation; (b) after optimisation

$[2]!\langle \texttt{bool}\rangle$ (output to 2 with bool-type), and another from 2's point of view, $[1]?\langle\texttt{bool}\rangle$ (input from 1 with bool-type), against which both processes are checked to be correct.

Now we explain how our new theory can reason about an optimisation of choreography interactions (a simplified usecase (UC.R2.13 "Acquire Data From Instrument") from [16]). Consider the two global types between three participants $(1,2,3)$:

$$G_a = 1 \to 3 : \langle ser\rangle.2 \to 3 : \langle ser\rangle.\texttt{end}, \quad G_b = 1 \to 2 : \langle sig\rangle.\texttt{end}$$

and a scenario in Figure 1(a) where Client3 (participant 3) uses two services, the first from Server1 (participant 1) and Server2 (participant 2), and Server1 sends an internal signal to Server2. The three parties belonging to these protocols are implemented as:

$$P_1 = a[1](x).b[1](y).x[3]!\langle v\rangle;y[2]!\langle w\rangle;\mathbf{0} \quad P_2 = a[2](x).\overline{b}[2](y).(y[1]?(z);\mathbf{0} \mid x[3]!\langle v\rangle;\mathbf{0})$$
$$P_3 = \overline{a}[3](x).x[1]?(z);x[2]?(y);\mathbf{0}$$

where session name a establishes the session corresponding to G_a. Client3 (P_3) initiates a session involving three processes as the third participant by $\overline{a}[3](x)$: Service1 (P_1) and Service2 (P_2) participate to the session $a[1](x)$ and $a[2](x)$, respectively. Similarly the session corresponding to G_b is established between Service1 and Service2.

Since from Client3, the internal signal is invisible, we optimise Server2 to a single thread to avoid an unnecessary thread creation as $R_2 = a[2](x).\overline{b}[2](y).y[1]?(z);x[3]!\langle v\rangle;\mathbf{0}$ in Figure 1(b). Note that both P_2 and R_2 are typable under G_a and G_b. Obviously, in the untyped setting, $P_1 \mid P_2$ and $P_1 \mid R_2$ are *not* bisimilar since in P_2, the output action $x[3]!\langle v\rangle$ can be observed before the input action $y[1]?(z)$ happens. However, with the global constraints given by G_a and G_b, a service provided by Server2 is only available to Client3 after Server1 sends a signal to Server2, i.e. action $x[3]!\langle v\rangle$ can only happen after action $y[1]?(z)$ in P_2. Hence $P_1 \mid P_2$ and $P_1 \mid R_2$ are not distinguishable by Client3 and the thread optimisation of R_2 is correct.

On the other hand, if we change the global type G_a as:

$$G'_a = 2 \to 3 : \langle ser\rangle.1 \to 3 : \langle ser\rangle.\texttt{end}$$

then R_2 can perform both the output to Client3 and the input from Server1 concurrently since G'_a states that Client3 can receive the message from Server2 first. Hence $P_1 \mid P_2$ and $P_1 \mid R_2$ are no longer equivalent.

The key point to make this difference possible is to observe the behaviour of processes together with the information provided by the global types. The global types can define additional knowledge about how the observer (the client in the above example) will collaborate with the observed processes so that different global types (i.e. global witnesses) can induce the different equivalences.

Contributions This paper introduces two kinds of typed bisimulations based on multiparty session types. The first bisimulation is solely based on local (endpoint) types defined without global information, hence it resembles the standard linearity-based bisimulation.

$P ::= \overline{u}[\mathtt{p}](x).P$	Request	$\mid$	$\mathtt{if}\ e\ \mathtt{then}\ P\ \mathtt{else}\ Q$	Conditional
$\mid\ u[\mathtt{p}](x).P$	Accept	$\mid$	$P \mid Q$	Parallel
$\mid\ c[\mathtt{p}]!\langle e\rangle;P$	Sending	$\mid$	$\mathbf{0}$	Inaction
$\mid\ c[\mathtt{p}]?(x);P$	Receiving	$\mid$	$(\nu\ n)P$	Hiding
$\mid\ c[\mathtt{p}] \oplus l;P$	Selection	$\mid$	$\mu X.P$	Recursion
$\mid\ c[\mathtt{p}]\&\{l_i : P_i\}_{i\in I}$	Branching	$\mid$	X	Variable
$u ::= x \mid a$	Identifier		$c ::= s[\mathtt{p}] \mid x$	Session
$n ::= s \mid a$	Name		$v ::= a \mid \mathtt{tt} \mid \mathtt{ff} \mid s[\mathtt{p}]$	Value
$e ::= v \mid x \mid e\ \mathtt{and}\ e' \mid e = e' \mid \ldots$	Expression			

Fig. 2. Syntax for synchronous multiparty session calculus

The second one is a *globally governed session bisimilarity* which uses multiparty session types as information for a global witness. We prove that each coincides with a corresponding standard contextual equivalence [11] (Theorems 3.1 and 4.1). The governed bisimulation gives more fine-grained equivalences than the locally typed bisimulation. We identify the condition when the two semantics exactly coincide (Theorem 4.2). Interestingly our theorem (Theorem 4.3) shows this difference appears only when processes are running under more than two interleaved global types. This feature makes the theory applicable to real situation where multiple choreographies are used in a single, large application. We demonstrate the use of governed bisimulation through the running example, which is applicable to a thread optimisation of a real usecase from a large scale distributed system [16]. The appendix includes auxiliary definitions, the full proofs and a full derivation of a usecase from [16].

2 Synchronous Multiparty Sessions

This section defines a synchronous version of the multiparty session types. The syntax and typing follows [3] except we eliminate queues for asynchronous communication. We chose synchrony since it allows the simplest formulations for demonstrating the essential concepts of governed bisimulations. The extension to asynchrony is given in [7].

Syntax Figure 2 defines the syntax for synchronous multiparty session calculus. Note the expression includes name matching ($n = n$). We call $\mathtt{p}, \mathtt{p}', \mathtt{q}, \ldots$ (range over the natural numbers) the *participants*. For the primitives for session initiation, $\overline{u}[\mathtt{p}](x).P$ initiates a new session through an identifier u (which represents a shared interaction point) with the other multiple participants, each of shape $u[\mathtt{p}](x).Q_{\mathtt{q}}$ where $1 \leq \mathtt{q} \leq \mathtt{p} - 1$. The (bound) variable x is the channel used to do the communications. Session communications (communications that take place inside an established session) are performed using the next two pairs: the sending and receiving of a value and the selection and branching (where the former chooses one of the branches offered by the latter). Process $c[\mathtt{p}]!\langle e\rangle;P$ sends a value to $\mathtt{p}$; accordingly, process $c[\mathtt{p}]?(x);P$ denotes the intention of receiving a value from the participant $\mathtt{p}$. The same holds for selection/branching. Process $\mathbf{0}$ is the inactive process. Other processes are standard. We say that a process is closed if it does not contain free variables. $\mathtt{fn}(P)/\mathtt{bn}(P)$ and $\mathtt{fv}(P)/\mathtt{bv}(P)$ denote a set of free/bound names and free/bound variables, respectively. We use the standard structure rules (denoted by $\equiv$) including $\mu X.P \equiv P\{\mu X.P/X\}$.

$$a[1](x).P_1 \mid \dots \mid \overline{a}[n](x).P_n \longrightarrow (\nu\, s)(P_1\{s[1]/x\} \mid \dots \mid P_n\{s[n]/x\}) \qquad \text{[Link]}$$

$$s[\mathtt{p}][\mathtt{q}]!\langle e\rangle;P \mid s[\mathtt{q}][\mathtt{p}]?(x);Q \longrightarrow P \mid Q\{v/x\} \quad (e\downarrow v) \qquad \text{[Comm]}$$

$$s[\mathtt{p}][\mathtt{q}]\oplus l_k;P \mid s[\mathtt{q}][\mathtt{p}]\&\{l_i : P_i\}_{i\in I} \longrightarrow P \mid P_k \quad k\in I \qquad \text{[Label]}$$

$$\mathtt{if}\ e\ \mathtt{then}\ P\ \mathtt{else}\ Q \longrightarrow P \quad (e\downarrow \mathtt{tt}) \qquad \mathtt{if}\ e\ \mathtt{then}\ P\ \mathtt{else}\ Q \longrightarrow Q \quad (e\downarrow \mathtt{ff}) \quad \text{[If]}$$

$$\frac{P\longrightarrow P'}{(\nu\, n)P\longrightarrow(\nu\, n)P'}\ \text{[Res]} \qquad \frac{P\longrightarrow P'}{P\mid Q\longrightarrow P'\mid Q}\ \text{[Par]} \qquad \frac{P\equiv P'\longrightarrow Q'\equiv Q}{P\longrightarrow Q}\ \text{[Str]}$$

Fig. 3. Operational semantics for synchronous multiparty session calculus

Operational semantics Operational semantics of the calculus are defined in Figure 3. Rule [Link] defines synchronous session initiation. All session roles must be present to synchronously reduce each role $\mathtt{p}$ on a fresh session name $s[\mathtt{p}]$. Rules [Comm] is for sending a value to the corresponding receiving process where $e\downarrow v$ means expression e evaluates to value v. The interaction between selection and branching is defined via rule [Label]. Other rules are standard. We write $\twoheadrightarrow$ for $(\longrightarrow\cup\equiv)^*$.

Global types, ranged over by $G, G', \dots$ describe the whole conversation scenario of a multiparty session as a type signature. Its grammar is given in Figure 4. The global type $\mathtt{p}\to\mathtt{q} : \langle U\rangle.G'$ says that participant $\mathtt{p}$ sends a message of type U to the participant $\mathtt{q}$ and then interactions described in G' take place. *Exchange types* $U, U', \dots$ consist of *sorts* types $S, S', \dots$ for values (either base types or global types), and *local session* types $T, T', \dots$ for channels (defined in the next paragraph). Type $\mathtt{p}\to\mathtt{q} : \{l_i : G_i\}_{i\in I}$ says participant $\mathtt{p}$ sends one of the labels l_i to $\mathtt{q}$. If l_j is sent, interactions described in G_j take place. In both cases we assume $\mathtt{p}\neq\mathtt{q}$. Type $\mu\mathtt{t}.G$ is a recursive type, assuming type variables $(\mathtt{t}, \mathtt{t}', \dots)$ are guarded in the standard way, i.e., type variables only appear under some prefix. We take an *equi-recursive* view of recursive types, not distinguishing between $\mu\mathtt{t}.G$ and its unfolding $G\{\mu\mathtt{t}.G/\mathtt{t}\}$.We assume that G in the grammar of sorts is closed, i.e., without free type variables. Type $\mathtt{end}$ represents the termination of the session.

Local types are defined in Figure 4 and correspond to the communication actions, representing sessions from the view-points of single participants. The *send type* $[\mathtt{p}]!\langle U\rangle;T$ expresses the sending to $\mathtt{p}$ of a value of type U, followed by the communications of T. The *selection type* $[\mathtt{p}]\oplus\{l_i : T_i\}_{i\in I}$ represents the transmission to $\mathtt{p}$ of a label l_i chosen in the set $\{l_i \mid i\in I\}$ followed by the communications described by T_i. The *receive* and *branching* are dual. Other types are the same as global types.

The relation between global and local types is formalised by the standard projection function [12]. For example, $(\mathtt{p}'\to\mathtt{q} : \langle U\rangle.G)\lceil\mathtt{p}$ is defined as: $[\mathtt{q}]!\langle U\rangle;(G\lceil\mathtt{p})$ if $\mathtt{p}=\mathtt{p}'$, $[\mathtt{p}']?(U);(G\lceil\mathtt{p})$ if $\mathtt{p}=\mathtt{q}$ and $G\lceil\mathtt{p}$ otherwise. Then the *projection set* of $s : G$ is defined as $\mathtt{proj}(s : G) = \{s[\mathtt{p}] : G\lceil\mathtt{p} \mid \mathtt{p}\in\mathtt{roles}(G)\}$ where $\mathtt{roles}(G)$ denotes the set of the roles appearing in G.

Typing system The typing judgements for expressions and processes are of the shapes:

$$\Gamma\vdash e : S \quad \text{and} \quad \Gamma\vdash P\triangleright\Delta$$

where Γ is the standard environment which associates variables to sort types, shared names to global types and process variables to session environments; and Δ is the session environment which associates channels to session types. Formally we define: $\Gamma ::= \emptyset \mid \Gamma\cdot u : S \mid \Gamma\cdot X : \Delta$ and $\Delta ::= \emptyset \mid \Delta\cdot s[\mathtt{p}] : T$, assuming we can write

Global	G	$::=$	$\mathtt{p}\to\mathtt{q}:\langle U\rangle.G'$	exchange	Local T	$::=$	$[\mathtt{p}]!\langle U\rangle;T$	send
		$\mid$	$\mathtt{p}\to\mathtt{q}:\{l_i:G_i\}_{i\in I}$	branching		$\mid$	$[\mathtt{p}]?(U);T$	receive
		$\mid$	$\mu\mathtt{t}.G$	recursion		$\mid$	$[\mathtt{p}]\oplus\{l_i:T_i\}_{i\in I}$	selection
		$\mid$	$\mathtt{t}$	variable		$\mid$	$[\mathtt{p}]\&\{l_i:T_i\}_{i\in I}$	branching
		$\mid$	$\mathtt{end}$	end		$\mid$	$\mu\mathtt{t}.T$	recursion
Exchange	U	$::=$	$S \mid T$			$\mid$	$\mathtt{t}$	variable
Sort	S	$::=$	$\mathtt{bool} \mid \langle G\rangle$			$\mid$	$\mathtt{end}$	end

Fig. 4. Global and local types

$\Gamma\cdot u:S$ if $u\notin\mathtt{dom}(\Gamma)$. We extend this to a concatenation for typing environments as $\Delta\cdot\Delta'=\Delta\cup\Delta'$. Typing Δ is *coherent with respect to session s* (notation $\mathtt{co}(\Delta(s))$) if for all $s[\mathtt{p}]:T_{\mathtt{p}},s[\mathtt{q}]:T_{\mathtt{q}}\in\Delta$, $T_{\mathtt{p}}$ and $T_{\mathtt{q}}$ are dual each other (it is given by exchanging ! by ? and $\oplus$ by & [10]). A typing Δ is *coherent* (notation $\mathtt{co}(\Delta)$) if it is coherent with respect to all s in its domain. We say that the typing judgement $\Gamma\vdash P\triangleright\Delta$ is *coherent* if $\mathtt{co}(\Delta)$.

The typing rules are essentially identical to the communication typing system for programs in [3] (since we do not require queues). We leave the rules in Figure 8 in Appendix A. The rest of the paper can be read without knowing the typing system.

Type soundness Next we define the reduction semantics for local types. Since session environments represent the forthcoming communications, by reducing processes session environments can change. This can be formalised as in [3, 12] by introducing the notion of reduction of session environments, whose rules are:

1. $\{s[\mathtt{p}]:[\mathtt{q}]!\langle U\rangle;T\cdot s[\mathtt{q}]:[\mathtt{p}]?(U);T'\}\longrightarrow\{s[\mathtt{p}]:T\cdot s[\mathtt{q}]:T'\}$.
2. $\{s[\mathtt{p}]:[\mathtt{q}]\oplus\{l_i:T_i\}_{i\in I}\cdot s[\mathtt{q}]:[\mathtt{p}]\&\{l_j:T'_j\}_{j\in J}\}\longrightarrow\{s[\mathtt{p}]:T_k\cdot s[\mathtt{q}]:T'_k\}\ I\subseteq J,k\in I$.
3. $\Delta\cup\Delta'\longrightarrow\Delta\cup\Delta''$ if $\Delta'\longrightarrow\Delta''$.

We write $\twoheadrightarrow=\longrightarrow^*$. Note that $\Delta\twoheadrightarrow\Delta'$ is non-deterministic (i.e. not always confluent) by the second rule. Then the typing system satisfies the subject reduction theorem [3] such that: if $\Gamma\vdash P\triangleright\Delta$ is coherent and $P\twoheadrightarrow P'$ then $\Gamma\vdash P'\triangleright\Delta'$ is coherent with $\Delta\twoheadrightarrow\Delta'$.

3 Synchronous Multiparty Session Semantics

This section presents a typed behavioural theory for the synchronous multiparty sessions. The typed bisimulation is defined with the labelled transition system (LTS) between a tuple of the environments (Γ,Δ), which controls behaviours of untyped processes. The constraint given by the environment LTSs, which accurately captures interactions in the presence of multiparty sessions, is at the heart of our typed semantics. The next section extends to more fine-grained LTSs with the additional information of a global witness.

Labels We use the following labels $(\ell,\ell',\ldots)$:

$$\begin{array}{lll}\ell & ::= & \overline{a}[A](s) \mid a[A](s) \mid s[\mathtt{p}][\mathtt{q}]!\langle v\rangle \mid s[\mathtt{p}][\mathtt{q}]!(a)\\ & \mid & s[\mathtt{p}][\mathtt{q}]!(s'[\mathtt{p}']) \mid s[\mathtt{p}][\mathtt{q}]?\langle v\rangle \mid s[\mathtt{p}][\mathtt{q}]\oplus l \mid s[\mathtt{p}][\mathtt{q}]\&l \mid \tau\end{array}$$

A role set A is a set of multiparty session types roles. Labels $\overline{a}[A](s)$ and $a[A](s)$ define the accept and request of a fresh session s by roles in set A respectively. Actions on session channels are denoted with labels $s[\mathtt{p}][\mathtt{q}]!\langle v\rangle$ and $s[\mathtt{p}][\mathtt{q}]?\langle v\rangle$ for output and input of value v from $\mathtt{p}$ to $\mathtt{q}$ on session s. Bound output values can be shared channels or session roles (delegation). $s[\mathtt{p}][\mathtt{q}]\oplus l$ and $s[\mathtt{p}][\mathtt{q}]\&l$ define the selection and branching respectively. Label τ is the standard hidden transition.

Dual label definition is used to define the parallel rule in the label transition system:

$$
\begin{array}{llll}
\langle\text{Req}\rangle & \overline{a}[\mathtt{p}](x).P \xrightarrow{\overline{a}[\{\mathtt{p}\}](s)} P\{s[\mathtt{p}]/x\} & \langle\text{Acc}\rangle & a[\mathtt{p}](x).P \xrightarrow{a[\{\mathtt{p}\}](s)} P\{s[\mathtt{p}]/x\} \\
\langle\text{Send}\rangle & s[\mathtt{p}][\mathtt{q}]!\langle e\rangle;P \xrightarrow{s[\mathtt{p}][\mathtt{q}]!\langle v\rangle} P \quad (e\downarrow v) & \langle\text{Rcv}\rangle & s[\mathtt{p}][\mathtt{q}]?(x);P \xrightarrow{s[\mathtt{p}][\mathtt{q}]?\langle v\rangle} P\{v/x\} \\
\langle\text{Sel}\rangle & s[\mathtt{p}][\mathtt{q}]\oplus l;P \xrightarrow{s[\mathtt{p}][\mathtt{q}]\oplus l} P & \langle\text{Bra}\rangle & s[\mathtt{p}][\mathtt{q}]\&\{l_i:P_i\}_{i\in I} \xrightarrow{s[\mathtt{p}][\mathtt{q}]\&l_k} P_k
\end{array}
$$

$$
\langle\text{Tau}\rangle\ \frac{P\xrightarrow{\ell}P' \quad Q\xrightarrow{\ell'}Q' \quad \ell\asymp\ell'}{P\mid Q\xrightarrow{\tau}(\nu\ \mathtt{bn}(\ell)\cap\mathtt{bn}(\ell'))(P'\mid Q')}
\qquad
\langle\text{Par}\rangle\ \frac{P\xrightarrow{\ell}P' \quad \mathtt{bn}(\ell)\cap\mathtt{fn}(Q)=\emptyset}{P\mid Q\xrightarrow{\ell}P'\mid Q}
$$

$$
\langle\text{Res}\rangle\ \frac{P\xrightarrow{\ell}P' \quad n\notin\mathtt{fn}(\ell)}{(\nu\ n)P\xrightarrow{\ell}(\nu\ n)P'}
\quad
\langle\text{OpenS}\rangle\ \frac{P\xrightarrow{s[\mathtt{p}][\mathtt{q}]!\langle s'[\mathtt{p}']\rangle}P'}{(\nu\ s')P\xrightarrow{s[\mathtt{p}][\mathtt{q}]!(s'[\mathtt{p}'])}P'}
\quad
\langle\text{OpenN}\rangle\ \frac{P\xrightarrow{s[\mathtt{p}][\mathtt{q}]!\langle a\rangle}P'}{(\nu\ a)P\xrightarrow{s[\mathtt{p}][\mathtt{q}]!(a)}P'}
$$

$$
\langle\text{Alpha}\rangle\ \frac{P\equiv_\alpha P' \quad P'\xrightarrow{\ell}Q'}{P\xrightarrow{\ell}Q}
\qquad
\langle\text{AcPar}\rangle\ \frac{P_1\xrightarrow{a[A](s)}P_1' \quad P_2\xrightarrow{a[A'](s)}P_2' \quad A\cap A'=\emptyset}{P_1\mid P_2\xrightarrow{a[A\cup A'](s)}P_1'\mid P_2'}
$$

$$
\langle\text{ReqPar}\rangle\ \frac{P_1\xrightarrow{a[A](s)}P_1' \quad P_2\xrightarrow{\overline{a}[A'](s)}P_2' \quad A\cap A'=\emptyset,\ A\cup A'\text{ not complete w.r.t }\max(A')}{P_1\mid P_2\xrightarrow{\overline{a}[A\cup A'](s)}P_1'\mid P_2'}
$$

$$
\langle\text{TauS}\rangle\ \frac{P_1\xrightarrow{a[A](s)}P_1' \quad P_2\xrightarrow{\overline{a}[A'](s)}P_2' \quad A\cap A'=\emptyset,\ A\cup A'\text{ complete w.r.t }\max(A')}{P_1\mid P_2\xrightarrow{\tau}(\nu\ s)(P_1'\mid P_2')}
$$

We omit the synmetric case of $\langle\text{Par}\rangle$ and conditonals.

Fig. 5. Labelled transition system for processes

$$s[\mathtt{p}][\mathtt{q}]!\langle v\rangle\asymp s[\mathtt{q}][\mathtt{p}]?\langle v\rangle \quad s[\mathtt{p}][\mathtt{q}]!(v)\asymp s[\mathtt{q}][\mathtt{p}]?\langle v\rangle \quad s[\mathtt{p}][\mathtt{q}]\oplus l\asymp s[\mathtt{q}][\mathtt{p}]\&l$$

Dual labels are input and output (resp. selection and branching) on the same session channel and on complementary roles. For example, in $s[\mathtt{p}][\mathtt{q}]!\langle v\rangle$ and $s[\mathtt{q}][\mathtt{p}]?\langle v\rangle$, role p sends to q and role q receives from p. Another important definition for the session initiation is the notion of the complete role set. We say the role set A is *complete with respect to n* if $n=\max(A)$ and $A=\{1,2,\ldots,n\}$. The complete role set means that all global protocol participants are present in the set. For example, $\{1,3,4\}$ is not complete, but $\{1,2,3,4\}$ is. We use $\mathtt{fn}(\ell)$ and $\mathtt{bn}(\ell)$ to denote a set of free and bound names in ℓ and set $\mathsf{n}(\ell)=\mathtt{bn}(\ell)\cup\mathtt{fn}(\ell)$.

Labelled transition system for processes Figure 5 gives the untyped labelled transition system. Rules $\langle\text{Req}\rangle$ and $\langle\text{Acc}\rangle$ define the accept and request actions for a fresh session s on role $\{\mathtt{p}\}$. Rules $\langle\text{Send}\rangle$ and $\langle\text{Rcv}\rangle$ give the send and receive respectively for value v from role p to role q in session s. Rules $\langle\text{Sel}\rangle$ and $\langle\text{Bra}\rangle$ define selecting and branching labels.

The last three rules are for collecting and synchronising the multiparty participants together. Rule $\langle\text{AccPar}\rangle$ accumulates the accept participants and records them into role set A. Rule $\langle\text{ReqPar}\rangle$ accumulates the accept participants and the request participant into role set A. Note that the request action role set always includes the maximum role number among the participants. Finally, rule $\langle\text{TauS}\rangle$ checks that a role set is complete, thus a new session can be created under the τ-action (synchronisation). Other rules are standard. See Example 3.1. We write $\Longrightarrow$ for the reflexive and transitive closure of $\longrightarrow$, $\xRightarrow{\ell}$ for the transitions $\Longrightarrow\xrightarrow{\ell}\Longrightarrow$ and $\xRightarrow{\hat{\ell}}$ for $\xRightarrow{\ell}$ if $\ell\neq\tau$ otherwise $\Longrightarrow$.

Typed labelled transition relation We define the typed LTS on the basis of the untyped one. This is realised by introducing the definition of an environment labelled transition system, defined in Figure 6. $(\Gamma,\Delta)\xrightarrow{\ell}(\Gamma',\Delta')$ means that an environment (Γ,Δ) allows an action to take place, and the resulting environment is (Γ',Δ').

$$
\begin{array}{rrcl}
\Gamma(a) = \langle G\rangle, s \text{ fresh implies} & (\Gamma,\Delta) & \xrightarrow{a[A](s)} & (\Gamma, \Delta\cdot\{s[i] : G\lceil i\}_{i\in A}) \\
\Gamma(a) = \langle G\rangle, s \text{ fresh implies} & (\Gamma,\Delta) & \xrightarrow{\overline{a}[A](s)} & (\Gamma, \Delta\cdot\{s[i] : G\lceil i\}_{i\in A}) \\
\Gamma \vdash v : U, s[\mathtt{q}] \notin \mathtt{dom}(\Delta) \text{ implies} & (\Gamma, \Delta\cdot s[\mathtt{p}] : [\mathtt{q}]!\langle U\rangle; T) & \xrightarrow{s[\mathtt{p}][\mathtt{q}]!\langle v\rangle} & (\Gamma, \Delta\cdot s[\mathtt{p}] : T) \\
s[\mathtt{q}] \notin \mathtt{dom}(\Delta), a \notin \mathtt{dom}(\Gamma) \text{ implies} & (\Gamma, \Delta\cdot s[\mathtt{p}] : [\mathtt{q}]!\langle U\rangle; T) & \xrightarrow{s[\mathtt{p}][\mathtt{q}]!(a)} & (\Gamma\cdot a : U, \Delta\cdot s[\mathtt{p}] : T) \\
\Gamma \vdash v : U, s[\mathtt{q}] \notin \mathtt{dom}(\Delta) \text{ implies} & (\Gamma, \Delta\cdot s[\mathtt{p}] : [\mathtt{q}]?(U); T) & \xrightarrow{s[\mathtt{p}][\mathtt{q}]?\langle v\rangle} & (\Gamma, \Delta\cdot s[\mathtt{p}] : T) \\
a \notin \mathtt{dom}(\Gamma), s[\mathtt{q}] \notin \mathtt{dom}(\Delta) \text{ implies} & (\Gamma, \Delta\cdot s[\mathtt{p}] : [\mathtt{q}]?(U); T) & \xrightarrow{s[\mathtt{p}][\mathtt{q}]?\langle a\rangle} & (\Gamma\cdot a : U, \Delta\cdot s[\mathtt{p}] : T) \\
s[\mathtt{q}] \notin \mathtt{dom}(\Delta) \text{ implies} & (\Gamma, \Delta\cdot s'[\mathtt{p}'] : T'\cdot s[\mathtt{p}] : [\mathtt{q}]!\langle T'\rangle; T) & \xrightarrow{s[\mathtt{p}][\mathtt{q}]!\langle s'[\mathtt{p}']\rangle} & (\Gamma, \Delta\cdot s[\mathtt{p}] : T) \\
s[\mathtt{q}] \notin \mathtt{dom}(\Delta) \text{ implies} & (\Gamma, \Delta\cdot s[\mathtt{p}] : [\mathtt{q}]!\langle T'\rangle; T) & \xrightarrow{s[\mathtt{p}][\mathtt{q}]!(s'[\mathtt{p}'])} & (\Gamma, \Delta\cdot s[\mathtt{p}] : T\cdot\{s'[\mathtt{p}_i] : T_i\}) \\
s[\mathtt{q}], s'[\mathtt{p}'] \notin \mathtt{dom}(\Delta) \text{ implies} & (\Gamma, \Delta\cdot s[\mathtt{p}] : [\mathtt{q}]?(T'); T) & \xrightarrow{s[\mathtt{p}][\mathtt{q}]?\langle s'[\mathtt{p}']\rangle} & (\Gamma, \Delta\cdot s'[\mathtt{p}'] : T'\cdot s[\mathtt{p}] : T) \\
s[\mathtt{q}] \notin \mathtt{dom}(\Delta) \text{ implies} & (\Gamma, \Delta\cdot s[\mathtt{p}] : [\mathtt{q}]\oplus\{l_i : T_i\}_{i\in I}) & \xrightarrow{s[\mathtt{p}][\mathtt{q}]\oplus l_k} & (\Gamma, \Delta\cdot s[\mathtt{p}] : T_k) \\
s[\mathtt{q}] \notin \mathtt{dom}(\Delta) \text{ implies} & (\Gamma, \Delta\cdot s[\mathtt{p}] : [\mathtt{q}]\&\{l_i : T_i\}_{i\in I}) & \xrightarrow{s[\mathtt{p}][\mathtt{q}]\& l_k} & (\Gamma, \Delta\cdot s[\mathtt{p}] : T_k) \\
\Delta \longrightarrow \Delta' \quad \text{or} \quad \Delta = \Delta' \text{ implies} & (\Gamma,\Delta) & \xrightarrow{\tau} & (\Gamma, \Delta')
\end{array}
$$

Fig. 6. Labelled Transition Relation for Environments

The intuition for this definition is that observables on session channels occur when the corresponding endpoint is not present in the linear typing environment Δ, and the type of an action's object respects the environment (Γ,Δ). In the case when new names are created or received, the environment (Γ,Δ) is extended.

The first rule says that reception of a message via a is possible when a's type $\langle G\rangle$ is recorded into Γ and the resulting session environment records projected types from G ($\{s[i] : G\lceil i\}_{i\in A}$). The second rule is for the send of a message via a and it is dual to the first rule. The next four rules are free value output, bound name output, free value input and name input. Rest of rules are free session output, bound session output, and session input as well as selection and branching rules. The bound session output records a set of session types $s'[\mathtt{p}_i]$ at opened session s'. The final rule ($\ell = \tau$) follows the reduction rules for linear session environment defined in § 2 ($\Delta = \Delta'$ is the case for the reduction at hidden sessions). Note that if Δ already contains destination ($s[\mathtt{q}]$), the environment cannot perform the visible action, but only the final τ-action.

The typed LTS requires that a process can perform an untyped action ℓ and that its typing environment (Γ,Δ) can match the action ℓ.

Definition 3.1 (Typed transition). *Typed transition* relation is defined as $\Gamma_1 \vdash P_1 \triangleright \Delta_1 \xrightarrow{\ell} \Gamma_2 \vdash P_2 \triangleright \Delta_2$ if (1) $P_1 \xrightarrow{\ell} P_2$ and (2) $(\Gamma_1,\Delta_1) \xrightarrow{\ell} (\Gamma_2,\Delta_2)$ with $\Gamma_i \vdash P_i \triangleright \Delta_i$.

Synchronous multiparty behavioural theory We first define a relation $\mathscr{R}$ as *typed relation* if it relates two closed, coherent typed terms $\Gamma \vdash P_1 \triangleright \Delta_1 \mathscr{R}\ \Gamma \vdash P_2 \triangleright \Delta_2$. We often write $\Gamma \vdash P_1 \triangleright \Delta_1 \mathscr{R}\ P_2 \triangleright \Delta_2$.

Next we define the *barb* [1]: we write $\Gamma \vdash P \triangleright \Delta \downarrow_{s[\mathtt{p}][\mathtt{q}]}$ if $P \equiv (\nu\ \tilde{a}\tilde{s})(s[\mathtt{p}][\mathtt{q}]!\langle v\rangle; R \mid Q)$ with $s \notin \tilde{s}$ and $s[\mathtt{q}] \notin \mathtt{dom}(\Delta)$; and $\Gamma \vdash P \triangleright \Delta \downarrow_a$ if $P \equiv (\nu\ \tilde{a}\tilde{s})(\overline{a}[n](s).R \mid Q)$ with $a \notin \tilde{a}$. Then we write m for either a or $s[\mathtt{p}][\mathtt{q}]$. We define $\Gamma \vdash P \triangleright \Delta \Downarrow_m$ if there exists Q such that $P \twoheadrightarrow Q$ and $\Gamma \vdash Q \triangleright \Delta' \downarrow_m$.

We write $\Delta_1 \rightleftharpoons \Delta_2$ if there exists Δ such that $\Delta_1 \twoheadrightarrow \Delta$ and $\Delta_2 \twoheadrightarrow \Delta$. We now define the contextual congruence based on the barb and [11].

Definition 3.2 (Reduction congruence). A typed relation $\mathscr{R}$ is *reduction congruence* if it satisfies the following conditions for each $\Gamma \vdash P_1 \triangleright \Delta_1 \mathscr{R}\ P_2 \triangleright \Delta_2$ with $\Delta_1 \rightleftharpoons \Delta_2$.

1. $\Gamma \vdash P_1 \triangleright \Delta_1 \Downarrow_m$ iff $\Gamma \vdash P_2 \triangleright \Delta_2 \Downarrow_m$
2. Whenever $\Gamma \vdash P_1 \triangleright \Delta_1 \mathscr{R} P_2 \triangleright \Delta_2$ holds, $P_1 \twoheadrightarrow P_1'$ implies $P_2 \twoheadrightarrow P_2'$ such that $\Gamma \vdash P_1' \triangleright \Delta_1' \mathscr{R} P_2' \triangleright \Delta_2'$ holds with $\Delta_1' \rightleftharpoons \Delta_2'$.
3. For all closed context C, such that $\Gamma \vdash C[P_1'] \triangleright \Delta_1'$ and $\Gamma \vdash C[P_2'] \triangleright \Delta_2'$ where $\Delta_1' \rightleftharpoons \Delta_2'$, $\Gamma \vdash C[P_1] \triangleright \Delta_1' \mathscr{R} \Gamma \vdash C[P_2] \triangleright \Delta_2'$.

The union of all reduction congruence relations is denoted as $\cong^s$.

Definition 3.3 (Synchronous multiparty session bisimulation). A typed relation $\mathscr{R}$ over closed processes is a (weak) *synchronous multiparty session bisimulation* or often a *synchronous bisimulation* if, whenever $\Gamma \vdash P_1 \triangleright \Delta_1 \mathscr{R} P_2 \triangleright \Delta_2$, it holds:

1. $\Gamma \vdash P_1 \triangleright \Delta_1 \xrightarrow{\ell} \Gamma' \vdash P_1' \triangleright \Delta_1'$ implies $\Gamma \vdash P_2 \triangleright \Delta_2 \overset{\hat{\ell}}{\Longrightarrow} \Gamma' \vdash P_2' \triangleright \Delta_2'$ such that $\Gamma' \vdash P_1' \triangleright \Delta_1' \mathscr{R} P_2' \triangleright \Delta_2'$.
2. The symmetric case.

The maximum bisimulation exists which we call *synchronous bisimilarity*, denoted by $\approx^s$. We sometimes leave environments implicit, writing e.g. $P \approx^s Q$. We also write $\approx$ for untyped synchronous bisimilarity which is defined by the untyped LTS in Figure 5 but without the environment LTS in Figure 6.

Lemma 3.1. *If $\Gamma \vdash P_1 \triangleright \Delta_1 \approx^s P_2 \triangleright \Delta_2$ then $\Delta_1 \rightleftharpoons \Delta_2$.*

Proof. The proof uses the co-induction method and can be found in Appendix C.2. □

Theorem 3.1 (Soundness and completeness). $\cong^s = \approx^s$.

Proof. The proof is a simplification of the proof of Theorem 4.1 in Appendix C.7. □

Example 3.1 (Synchronous multiparty bisimulation). We use the running example from § 1. First we explain the LTS for session initialisation from Figure 5. By $\langle \text{Acc} \rangle$ and $\langle \text{Req} \rangle$,

$P_1 \xrightarrow{a[\{1\}](s_1)} P_1' = b[1](y).s_1[1][3]!\langle v \rangle; y[2]!\langle w \rangle; \mathbf{0}$
$P_2 \xrightarrow{a[\{2\}](s_1)} P_2' = \overline{b}[2](y).(y[1]?(z);\mathbf{0} \mid s_1[2][3]!\langle v \rangle;\mathbf{0}) \quad P_3 \xrightarrow{\overline{a}[\{3\}](s_1)} P_3' = s_1[3][1]?(z);s_1[3][2]?(y);\mathbf{0}$
with

$\Gamma \vdash P_1' \triangleright s_1[1] : [3]!\langle U \rangle;\texttt{end}, \quad \Gamma \vdash P_2' \triangleright s_1[2] : [3]!\langle U \rangle;\texttt{end}, \quad \Gamma \vdash P_3' \triangleright s_1[3] : [1]?(U);[2]?(U);\texttt{end}$

By $\langle \text{AccPar} \rangle$, we have $P_1 \mid P_2 \xrightarrow{a[\{1,2\}](s_1)} P_1' \mid P_2'$. We have another possible initialisation: $P_1 \mid P_3 \xrightarrow{\overline{a}[\{1,3\}](s_1)} P_1' \mid P_3'$. From both of them, if we compose another process, the set $\{1,2,3\}$ becomes complete so that by synchronisation $\langle \text{TauS} \rangle$,

$$\Gamma \vdash P_1 \mid P_2 \mid P_3 \triangleright \emptyset \xrightarrow{\tau} (\nu\, s_1)(P_1' \mid P_2' \mid P_3') \triangleright \emptyset$$

Further we have:

$$\Gamma \vdash P_1' \mid P_2' \triangleright \emptyset \xrightarrow{\tau}$$
$$(\nu\, s_2)(s_1[1][3]!\langle v \rangle; s_2[1][2]!\langle w \rangle;\mathbf{0} \mid s_2[2][1]?(z);\mathbf{0} \mid s_1[2][3]!\langle v \rangle;\mathbf{0}) = Q_1 \triangleright \Delta$$

with $\Delta_0 = s_1[1] : [3]!\langle U \rangle;\texttt{end} \cdot s_1[2] : [3]!\langle U \rangle;\texttt{end}$. Then

$$\Gamma \vdash Q_1 \mid P_3' \triangleright \Delta_0 \cdot s_1[3] : [1]?(U);[2]?(U);\texttt{end} \approx^s \mathbf{0} \triangleright \emptyset$$

since $(\Gamma, \Delta) \not\xrightarrow{\ell}$ for any $\ell \neq \tau$ (note the condition of Line 3 in Figure 6). However by the untyped synchronous bisimulation, $Q_1 \mid P_3' \not\approx \mathbf{0}$ since, e.g. $Q_1 \mid P_3' \xrightarrow{s_1[1][3]!\langle v \rangle}$.

4 Globally Governed Behavioural Theory

We introduce the semantics for globally governed behavioural theory. In the previous section, the local typing (Δ) constrains the untyped LTS to give rise to a local typed LTS. In a multiparty distributed environment, communications follow the global protocol, which controls both an observed process and its observer. The local typing is not sufficient to maintain the consistency of transitions of a process with respect to a global protocol. In this section we refine the environment LTS with a *global environment* E to give a more fine-grained control over the LTS of the processes.

Global environments and configurations We define a *global environment* $(E, E', ...)$ as a mapping from session names to global types.

$$E \ ::= \ E \cdot s : G \ \mid \ \emptyset$$

The projection definition is extended to include E as $\mathtt{proj}(E) = \bigcup_{s:G \in E} \mathtt{proj}(s : G)$.

We define a labelled reduction relation over global environments which corresponds to $\Delta \longrightarrow \Delta'$ defined in § 2. We use the labels $\lambda \in \{s : \mathtt{p} \to \mathtt{q} : U, s : \mathtt{p} \to \mathtt{q} : l\}$ to annotate reductions over global environments. We define $\mathtt{out}(\lambda)$ and $\mathtt{inp}(\lambda)$ as $\mathtt{out}(s : \mathtt{p} \to \mathtt{q} : U) = \mathtt{out}(s : \mathtt{p} \to \mathtt{q} : l) = \mathtt{p}$ and as $\mathtt{inp}(s : \mathtt{p} \to \mathtt{q} : U) = \mathtt{inp}(s : \mathtt{p} \to \mathtt{q} : l) = \mathtt{q}$ and $\mathtt{p} \in \ell$ if $\mathtt{p} \in \mathtt{out}(\ell) \cup \mathtt{inp}(\ell)$. We often omit the label λ by writing $\longrightarrow$ for $\xrightarrow{\lambda}$ and $\longrightarrow^*$ for $(\xrightarrow{\lambda})^*$. The first rule is the axiom for the input and output interaction between two parties; the second rule is for the choice; the third and forth rules formulate the case that the action λ can be performed under $\mathtt{p} \to \mathtt{q}$ if $\mathtt{p}$ and $\mathtt{q}$ are not related to the participants in λ; and the fifth rule is a congruent rule.

$$\{s : \mathtt{p} \to \mathtt{q} : \langle U \rangle.G\} \xrightarrow{s:\mathtt{p}\to\mathtt{q}:U} \{s : G\} \qquad \{s : \mathtt{p} \to \mathtt{q} : \{l_i : G_i\}_{i \in I}\} \xrightarrow{s:\mathtt{p}\to\mathtt{q}:l_k} \{s : G_k\}$$

$$\frac{\{s : G\} \xrightarrow{\lambda} \{s : G'\} \quad \mathtt{p},\mathtt{q} \notin \lambda}{\{s : \mathtt{p} \to \mathtt{q} : \langle U \rangle.G\} \xrightarrow{\lambda} \{s : \mathtt{p} \to \mathtt{q} : \langle U \rangle.G'\}}$$

$$\frac{\{s : G_i\} \xrightarrow{\lambda} \{s : G_i'\} \quad i \in I, \quad \mathtt{p},\mathtt{q} \notin \lambda}{\{s : \mathtt{p} \to \mathtt{q} : \{l_i : G_i\}_{i \in I}\} \xrightarrow{\lambda} \{s : \mathtt{p} \to \mathtt{q} : \{l_i : G_i'\}_{i \in I}\}} \qquad \frac{E \xrightarrow{\lambda} E'}{E \cdot E_0 \xrightarrow{\lambda} E' \cdot E_0}$$

As a simple example of the above LTS, consider $s : \mathtt{p} \to \mathtt{q} : \langle U_1 \rangle.\mathtt{p}' \to \mathtt{q}' : \{l_1 : \mathtt{end}, l_2 : \mathtt{p}' \to \mathtt{q}' : \langle U_2 \rangle.\mathtt{end}\}$. Since $\mathtt{p}, \mathtt{q}, \mathtt{p}', \mathtt{q}'$ are pairwise distinct, we can apply the second and third rules to obtain:

$$s : \mathtt{p} \to \mathtt{q} : \langle U_1 \rangle.\mathtt{p}' \to \mathtt{q}' : \{l_1 : \mathtt{end}, l_2 : \mathtt{p}' \to \mathtt{q}' : \langle U_2 \rangle.\mathtt{end}\} \xrightarrow{s:\mathtt{p}'\to\mathtt{q}':l_1} s : \mathtt{p} \to \mathtt{q} : \langle U_1 \rangle.\mathtt{end}$$

Next we introduce the *governance judgement* which controls the behaviour of processes by the global environment.

Definition 4.1 (Governance judgement). *Let $\Gamma \vdash P \triangleright \Delta$ be coherent. We write $E, \Gamma \vdash P \triangleright \Delta$ if $\exists E' \cdot E \longrightarrow^* E'$ and $\Delta \subseteq \mathtt{proj}(E')$.*

The global environment E records the knowledge of both the environment (Δ) of the observed process P and the environment of its *observer*. The side conditions ensure that E is coherent with Δ: there exist E' reduced from E whose projection should cover the environment of P (since E should include the observer's information together with the observed process information recorded into Δ).

Next we define the LTS for well-formed environment configurations.

$$[\mathrm{Acc}]\,\frac{\Gamma \vdash a : \langle G\rangle \quad (\Gamma,\Delta_1) \xrightarrow{a[A](s)} (\Gamma,\Delta_2)}{(E,\Gamma,\Delta_1) \xrightarrow{a[A](s)} (E\cdot s : G,\Gamma,\Delta_2)} \qquad [\mathrm{Req}]\,\frac{\Gamma \vdash a : \langle G\rangle \quad (\Gamma,\Delta_1) \xrightarrow{\overline{a}[A](s)} (\Gamma,\Delta_2)}{(E,\Gamma,\Delta_1) \xrightarrow{\overline{a}[A](s)} (E\cdot s : G,\Gamma,\Delta_2)}$$

$$[\mathrm{Out}]\,\frac{\Gamma \vdash v : U \quad (\Gamma,\Delta_1) \xrightarrow{s[\mathtt{p}][\mathtt{q}]!\langle v\rangle} (\Gamma,\Delta_2) \quad E_1 \xrightarrow{s:\mathtt{p}\to\mathtt{q}:U} E_2}{(E_1,\Gamma,\Delta_1) \xrightarrow{s[\mathtt{p}][\mathtt{q}]!\langle v\rangle} (E_2,\Gamma,\Delta_2)} \qquad [\mathrm{In}]\,\frac{(\Gamma,\Delta_1) \xrightarrow{s[\mathtt{p}][\mathtt{q}]?\langle v\rangle} (\Gamma\cdot v : U,\Delta_2) \quad E_1 \xrightarrow{s:\mathtt{q}\to\mathtt{p}:U} E_2}{(E_1,\Gamma,\Delta_1) \xrightarrow{s[\mathtt{p}][\mathtt{q}]?\langle v\rangle} (E_2,\Gamma\cdot v : U,\Delta_2)}$$

$$[\mathrm{ResN}]\,\frac{\begin{array}{c}(\Gamma,\Delta_1) \xrightarrow{s[\mathtt{p}][\mathtt{q}]!(a)} (\Gamma\cdot a : \langle G\rangle,\Delta_2)\\ E_1 \xrightarrow{s:\mathtt{q}\to\mathtt{p}:\langle G\rangle} E_2\end{array}}{(E_1,\Gamma,\Delta_1) \xrightarrow{s[\mathtt{p}][\mathtt{q}]!(a)} (E_2,\Gamma\cdot a : \langle G\rangle,\Delta_2)} \qquad [\mathrm{ResS}]\,\frac{\begin{array}{c}(\Gamma,\Delta_1) \xrightarrow{s[\mathtt{p}][\mathtt{q}]!(s'[\mathtt{p}'])} (\Gamma,\Delta_2\cdot\{s'[\mathtt{p}_i] : T_i\})\\ E_1 \xrightarrow{s:\mathtt{q}\to\mathtt{p}:T} E_2 \quad \cdot\forall i.G\lceil \mathtt{p}_i = T_i\end{array}}{(E_1,\Gamma,\Delta_1) \xrightarrow{s[\mathtt{p}][\mathtt{q}]!(s'[\mathtt{p}'])} (E_2\cdot s' : G,\Gamma,\Delta_2\cdot\{s'[\mathtt{p}_i] : T_i\})}$$

$$[\mathrm{Sel}]\,\frac{(\Gamma,\Delta_1) \xrightarrow{s[\mathtt{p}][\mathtt{q}]\oplus l} (\Gamma,\Delta_2) \quad E_1 \xrightarrow{s:\mathtt{p}\to\mathtt{q}:l} E_2}{(E_1,\Gamma,\Delta_1) \xrightarrow{s[\mathtt{p}][\mathtt{q}]\oplus l} (E_2,\Gamma,\Delta_2)} \qquad [\mathrm{Bra}]\,\frac{(\Gamma,\Delta_1) \xrightarrow{s[\mathtt{p}][\mathtt{q}]\& l} (\Gamma,\Delta_2) \quad E_1 \xrightarrow{s:\mathtt{q}\to\mathtt{p}:l} E_2}{(E_1,\Gamma,\Delta_1) \xrightarrow{s[\mathtt{p}][\mathtt{q}]\& l} (E_2,\Gamma,\Delta_2)}$$

$$[\mathrm{Tau}]\,\frac{(\Delta_1 = \Delta_2,\ E_1 = E_2)\vee(\Delta_1 \xrightarrow{\lambda} \Delta_2,\ E_1 \xrightarrow{\lambda} E_2)}{(E_1,\Gamma,\Delta_1) \xrightarrow{\tau} (E_2,\Gamma,\Delta_2)} \qquad [\mathrm{Inv}]\,\frac{E_1 \longrightarrow^* E_1' \quad (E_1',\Gamma_1,\Delta_1) \xrightarrow{\ell} (E_2,\Gamma_2,\Delta_2)}{(E_1,\Gamma_1,\Delta_1) \xrightarrow{\ell} (E_2,\Gamma_2,\Delta_2)}$$

Fig. 7. The LTS for the environment configuations

Definition 4.2 (Environment configuration). *We write* (E,Γ,Δ) *if* $\exists E'\cdot E \longrightarrow^* E'$ *and* $\Delta \subseteq \mathtt{proj}(E')$*.*

Figure 7 defines a LTS over environment configurations that refines the LTS over environments (i.e $(\Gamma,\Delta) \xrightarrow{\ell} (\Gamma',\Delta')$) in § 3.

Each rule requires a corresponding environment transition (Figure 6 in § 3) and a corresponding labelled global environment transition in order to control a transition following the global protocol. [Acc] is the rule for accepting a session initialisation so that it creates a new mapping $s : G$ which matches Γ in a governed environment E. [Req] is the rule for requesting a new session and it is dual to [Acc].

The next seven rules are the transition relations on session channels and we assume the condition $\mathtt{proj}(E_1) \supseteq \Delta$ to ensure the base action of the environment matches one in a global environment. [Out] is a rule for the output where the type of the value and the action of (Γ,Δ) meets those in E. [In] is a rule for the input and dual to [Out]. [ResN] is a scope opening rule for a name so that the environment can perform the corresponding type $\langle G\rangle$ of a. [ResS] is a scope opening rule for a session channel which creates a set of mappings for the opened session channel s' corresponding to the LTS of the environment. [Sel] and [Bra] are the rules for selection and branching, which is similar to [Out] and [In]. In [Tau] rule, we refined the reduction relation on Δ in § 2 as follows:

1. $\{s[\mathtt{p}] : [\mathtt{q}]!\langle U\rangle;T \cdot s[\mathtt{q}] : [\mathtt{p}]?(U);T'\} \xrightarrow{s:\mathtt{p}\to\mathtt{q}:U} \{s[\mathtt{p}] : T \cdot s[\mathtt{q}] : T'\}$.
2. $\{s[\mathtt{p}] : [\mathtt{q}]\oplus\{l_i : T_i\}_{i\in I} \cdot s[\mathtt{q}] : [\mathtt{p}]\&\{l_j : T_j'\}_{j\in J}\} \xrightarrow{s:\mathtt{p}\to\mathtt{q}:l_k} \{s[\mathtt{p}] : T_k \cdot s[\mathtt{q}] : T_k'\}\ I \subseteq J, k \in I$.
3. $\Delta \cup \Delta' \xrightarrow{\lambda} \Delta \cup \Delta''$ if $\Delta' \xrightarrow{\lambda} \Delta''$.

[Inv] is the key rule: the global environment E_1 reduces to E_1' to perform the observer's actions, hence the observed process can perform the action w.r.t. E_1'. Hereafter we write $\longrightarrow$ for $\xrightarrow{\tau}$.

Example 4.1 (LTS for environment configuration). Let $E = s : \mathtt{p} \to \mathtt{q} : \langle U\rangle.\mathtt{p} \to \mathtt{q} : \langle U\rangle.G$, $\Gamma = v : U$ and $\Delta = s[\mathtt{p}] : [\mathtt{q}]!\langle U\rangle;T_{\mathtt{p}}$ with $G\lceil \mathtt{p} = T_{\mathtt{p}}$, $G\lceil \mathtt{q} = T_{\mathtt{q}}$ and $\mathtt{roles}(G) = \{\mathtt{p},\mathtt{q}\}$.

Then (E,Γ,Δ) is an environment configuration since if $E \longrightarrow E'$ then $\mathtt{proj}(E') \supset \Delta$ because $E \xrightarrow{s:\mathtt{p}\to\mathtt{q}:U} s:\mathtt{p}\to\mathtt{q}:\langle U\rangle.G$, $\mathtt{proj}(s:\mathtt{p}\to\mathtt{q}:\langle U\rangle.G) = s[\mathtt{p}]:[\mathtt{q}]!\langle U\rangle;T_\mathtt{p}\cdot s[\mathtt{q}]:[\mathtt{p}]?(U);T_\mathtt{q}$ and $\mathtt{proj}(s:\mathtt{p}\to\mathtt{q}:\langle U\rangle.G) \supset \Delta$. Then we can apply $[\mathrm{Out}]$ to $s:\mathtt{p}\to\mathtt{q}:\langle U\rangle.G \xrightarrow{s:\mathtt{p}\to\mathtt{q}:U} s:G$ and $(\Gamma, s[\mathtt{p}]:[\mathtt{q}]!\langle U\rangle;T_\mathtt{p}) \xrightarrow{s[\mathtt{p}][\mathtt{q}]!\langle v\rangle} (\Gamma, s[\mathtt{p}]:T_\mathtt{p})$ to obtain $(s:\mathtt{p}\to\mathtt{q}:\langle U\rangle.G,\Gamma,\Delta) \xrightarrow{s[\mathtt{p}][\mathtt{q}]!\langle v\rangle} (s:G,\Gamma,s[\mathtt{p}]:T_\mathtt{p})$. By this and $E \longrightarrow s:\mathtt{p}\to\mathtt{q}:\langle U\rangle.G$, using $[\mathrm{Inv}]$, we can obtain $(E,\Gamma,\Delta) \xrightarrow{s[\mathtt{p}][\mathtt{q}]!\langle v\rangle} (s:G,\Gamma,s[\mathtt{p}]:T_\mathtt{p})$, as required.

Governed reduction-closed congruency To define the reduction-closed congruency, we first refine the barb, which is controlled by the global witness where observables of a configuration are defined with the global environment of the observer.

$$\begin{array}{rl}
(E,\Gamma,\Delta\cdot s[\mathtt{p}]:[\mathtt{q}]!\langle U\rangle;T) \downarrow_{s[\mathtt{p}][\mathtt{q}]} & \text{if } s[\mathtt{q}] \notin \mathtt{dom}(\Delta), \exists E'\cdot E \longrightarrow^* E' \xrightarrow{s:\mathtt{p}\to\mathtt{q}:U}, \Delta \subseteq \mathtt{proj}(E') \\
(E,\Gamma,\Delta\cdot s[\mathtt{p}]:[\mathtt{q}]\oplus\{l_i:T_i\}_{i\in I}) \downarrow_{s[\mathtt{p}][\mathtt{q}]} & \text{if } s[\mathtt{q}] \notin \mathtt{dom}(\Delta), \exists E'\cdot E \longrightarrow^* E' \xrightarrow{s:\mathtt{p}\to\mathtt{q}:l_k}, k\in I, \Delta \subseteq \mathtt{proj}(E'), \\
(E,\Gamma,\Delta) \downarrow_a & \text{if } a \in \mathtt{dom}(\Gamma)
\end{array}$$

We write $(\Gamma,\Delta,E) \Downarrow_m$ if $(\Gamma,\Delta,E) \longrightarrow^* (\Gamma,\Delta',E')$ and $(\Gamma,\Delta',E') \downarrow_m$.

Let us write $T_1 \sqsubseteq T_2$ if the syntax tree of T_2 includes T_1. For example, $[\mathtt{q}]?(U');T \sqsubseteq [\mathtt{p}]!\langle U\rangle;[\mathtt{q}]?(U');T$. Then we define: $E_1 \sqcup E_2 = \{E_i(s) \mid E_j(s) \sqsubseteq E_i(s), i,j\in\{1,2\}, i\neq j\} \cup E_1 \setminus \mathtt{dom}(E_2) \cup E_2 \setminus \mathtt{dom}(E_1)$. As an example of $E_1 \sqcup E_2$, let us define:

$$E_1 = s_1:\mathtt{p}\to\mathtt{q}:\langle U_1\rangle.\mathtt{p}'\to\mathtt{q}':\langle U_2\rangle.\mathtt{p}\to\mathtt{q}:\langle U_3\rangle.\mathtt{end}\cdot s_2:\mathtt{p}\to\mathtt{q}:\langle W_2\rangle.\mathtt{end}$$
$$E_2 = s_1:\mathtt{p}\to\mathtt{q}:\langle U_3\rangle.\mathtt{end}\cdot s_2:\mathtt{p}'\to\mathtt{q}':\langle W_1\rangle.\mathtt{p}\to\mathtt{q}:\langle W_2\rangle.\mathtt{end}$$

Then $E_1 \sqcup E_2 = \mathtt{p}\to\mathtt{q}:\langle U_1\rangle.\mathtt{p}'\to\mathtt{q}':\langle U_2\rangle.\mathtt{p}\to\mathtt{q}:\langle U_3\rangle.\mathtt{end}\cdot s_2:\mathtt{p}'\to\mathtt{q}':\langle W_1\rangle.\mathtt{p}\to\mathtt{q}:\langle W_2\rangle.\mathtt{end}$.

The behavioural relation with respects to a global whiteness is defined below.

Definition 4.3 (Configuration relation). The relation $\mathscr{R}$ is a *configuration relation* between two configurations $E_1,\Gamma \vdash P_1 \triangleright \Delta_1$ and $E_2,\Gamma \vdash P_2 \triangleright \Delta_2$, written $E_1 \sqcup E_2,\Gamma \vdash P \triangleright \Delta_1 \mathrel{\mathscr{R}} P_2 \triangleright \Delta_2$ if $E_1 \sqcup E_2$ is defined.

Proposition 4.1 (Decidability). *(1) Given E_1 and E_2, a problem whether $E_1 \sqcup E_2$ is defined or not is decidable and if it is defined, the calculation of $E_1 \sqcup E_2$ terminates; and (2) Given E, a set $\{E' \mid E \longrightarrow^* E'\}$ is finite.*

For the proof, see Appendix C.5.

Definition 4.4 (Global configuration transition). We write $E_1,\Gamma \vdash P_1 \triangleright \Delta_1 \xrightarrow{\ell} E_2,\Gamma' \vdash P_2 \triangleright \Delta_2$ if $E_1,\Gamma \vdash P_1 \triangleright \Delta_1$, $P_1 \xrightarrow{\ell} P_2$ and $(E_1,\Gamma,\Delta_1) \xrightarrow{\ell} (E_2,\Gamma',\Delta_2)$.

Below states that the configuration LTS preserves the well-formedness.

Proposition 4.2. *(1) $(E_1,\Gamma,\Delta_1) \xrightarrow{\ell} (E_2,\Gamma_2,\Delta_2)$ implies that (E_2,Γ_2,Δ_2) is an environment configuration; and (2) If $\Gamma \vdash P \triangleright \Delta$ and $P \longrightarrow P'$ with $\mathtt{co}(\Delta)$, then $E,\Gamma \vdash P \triangleright \Delta \longrightarrow E,\Gamma \vdash P' \triangleright \Delta'$ and $\mathtt{co}(\Delta')$.*

Proof. The proof for Part 1 can be found in Appendix C.4. Part 2 is verified by simple transitions using $[\mathrm{Tau}]$ in Figure 7. $\mathtt{co}(\Delta')$ is derived by Theorem A.1. □

The definition of the reduction congruence for governance follows. Below we define $E,\Gamma \vdash P \triangleright \Delta \Downarrow_n$ if $P \Downarrow_m$ and $(E,\Gamma,\Delta) \Downarrow_m$.

Definition 4.5 (Governed reduction congruence). A configuration relation $\mathscr{R}$ is *governed reduction congruence* if $E,\Gamma \vdash P_1 \triangleright \Delta_1 \mathscr{R} P_2 \triangleright \Delta_2$ then

1. $E,\Gamma \vdash P_1 \triangleright \Delta_1 \Downarrow_n$ if and only if $E,\Gamma \vdash P_2 \triangleright \Delta_2 \Downarrow_n$
2. $P_1 \twoheadrightarrow P_1'$ if and only if $P_2 \twoheadrightarrow P_2'$ and $E,\Gamma \vdash P_1' \triangleright \Delta_1' \mathscr{R} P_2' \triangleright \Delta_2'$
3. For all closed context C, such that $E,\Gamma \vdash C[P_1] \triangleright \Delta_1'$ and $E,\Gamma \vdash C[P_2] \triangleright \Delta_2'$ then $E,\Gamma \vdash C[P_1] \triangleright \Delta_1' \mathscr{R} C[P_2] \triangleright \Delta_2'$.

The union of all governed reduction congruence relations is denoted as $\cong^s_g$.

Globally governed bisimulation and its properties This subsection introduces the globally governed bisimulation relation definition and studies its main properties.

Definition 4.6 (Globally governed bisimulation). A configuration relation $\mathscr{R}$ is a *globally governed weak bisimulation* (or governed bisimulation) if whenever $E,\Gamma \vdash P_1 \triangleright \Delta_1 \mathscr{R} P_2 \triangleright \Delta_2$, it holds:

1. $E,\Gamma \vdash P_1 \triangleright \Delta_1 \xrightarrow{\ell} E_1',\Gamma' \vdash P_1' \triangleright \Delta_1'$ implies $E,\Gamma \vdash P_2 \triangleright \Delta_2 \xRightarrow{\hat{\ell}} E_2',\Gamma' \vdash P_2' \triangleright \Delta_2'$ such that $E_1' \sqcup E_2',\Gamma' \vdash P_1' \triangleright \Delta_1' \mathscr{R} P_2' \triangleright \Delta_2'$.
2. The symmetric case.

The maximum bisimulation exists which we call *governed bisimilarity*, denoted by $\approx^s_g$. We sometimes leave environments implicit, writing e.g. $P \approx^s_g Q$.

Lemma 4.1. *(1) $\approx^s_g$ is congruent; and (2) $\cong^s_g \subseteq \approx^s_g$*

Proof. The proof of (1) is by a case analysis on the context structure. The interesting case is the parallel composition, which uses Proposition 4.2. See Appendix C.6. The proof of (2) follows the facts that bisimulation has a stratifying definition (the proof method uses the technique from [1]) and that the external actions can always be tested (the technique from [8]). The proof can be found in Appendix C.7. □

Theorem 4.1 (Sound and completeness). $\approx^s_g = \cong^s_g$.

The relationship between $\approx^s$ and $\approx^s_g$ is given as follows. See Appendix C.8 for the proof.

Theorem 4.2. *If for all E, $E,\Gamma \vdash P_1 \triangleright \Delta_1 \approx^s_g P_2 \triangleright \Delta_2$ then $\Gamma \vdash P_1 \triangleright \Delta_1 \approx^s \Gamma \vdash P_2 \triangleright \Delta_2$. Also if $\Gamma \vdash P_1 \triangleright \Delta_1 \approx^s \Gamma \vdash P_2 \triangleright \Delta_2$, then for all E, $E,\Gamma \vdash P_1 \triangleright \Delta_1 \approx^s_g P_2 \triangleright \Delta_2$.*

To justify the above theorem, consider the following processes:

$$\begin{aligned} P_1 &= s_1[1][3]!\langle v\rangle; s_2[1][2]!\langle w\rangle;\mathbf{0} \mid s_1[2][3]!\langle v\rangle; s_2[2][1]?(x); s_2[2][3]!\langle x\rangle;\mathbf{0} \\ P_2 &= s_1[1][3]!\langle v\rangle;\mathbf{0} \mid s_2[1][2]!\langle w\rangle;\mathbf{0} \mid s_1[2][3]!\langle v\rangle; s_2[2][1]?(x); s_2[2][3]!\langle x\rangle;\mathbf{0} \end{aligned}$$

then we have $P_1 \approx^s P_2$. By the above theorem, we expect that for all E, we have $E,\Gamma \vdash P_1 \triangleright \Delta_1$ and $E,\Gamma \vdash P_2 \triangleright \Delta_2$ then $E \vdash P_1 \approx^s_g P_2$. This is in fact true because the possible E that can type P_1 and P_2 are:

$$\begin{aligned} E_1 &= s_1 : 1 \to 3 : \langle U\rangle.2 \to 3 : \langle U\rangle.\mathtt{end} \cdot s_2 : 1 \to 2 : \langle W\rangle.2 \to 3 : \langle W\rangle.\mathtt{end} \\ E_2 &= s_1 : 2 \to 3 : \langle U\rangle.1 \to 3 : \langle U\rangle.\mathtt{end} \cdot s_2 : 1 \to 2 : \langle W\rangle.2 \to 3 : \langle W\rangle.\mathtt{end} \end{aligned}$$

Note that all E that are instances up-to weakening (see Lemma C.2) are E_1 and E_2.

To clarify the difference between $\approx^s$ and $\approx^s_g$, we introduce the notion of a *simple multiparty process* defined in [12]. A simple process contains only a single session so that it satisfies the progress property as proved in [12]. Formally a process P is *simple* when it is typable with a type derivation where the session typing in the premise and the conclusion of each prefix rule is restricted to at most a single session (i.e. any $\Gamma \vdash P \triangleright \Delta$ which appears in a derivation, Δ contains at most one session channel in its domain, see [12]). Since there is no interleaving of sessions in simple processes, the difference between $\approx^s$ and $\approx^s_g$ disappears.

Theorem 4.3 (Coincidence). *Assume P_1 and P_2 are simple. If $\exists E \cdot E, \Gamma \vdash P_1 \triangleright \Delta_1 \approx^s_g P_2 \triangleright \Delta_2$ then $\Gamma \vdash P_1 \triangleright \Delta_1 \approx^s P_2 \triangleright \Delta_2$.*

Proof. The proof follows the fact that if P is simple and $\Gamma \vdash P \triangleright \Delta \xrightarrow{\ell} P' \triangleright \Delta'$ then $\exists E \cdot E, \Gamma \vdash P \triangleright \Delta \xrightarrow{\ell} P' \triangleright \Delta'$ to continue that if P_1, P_2 are simple and $\exists E \cdot E, \Gamma \vdash P_1 \triangleright \Delta_1 \approx^s_g P_2 \triangleright \Delta_2$ then $\forall E, E, \Gamma \vdash P_1 \triangleright \Delta_1 \approx^s_g P_2 \triangleright \Delta_2$. The result then comes by applying Lemma 4.2. The details of the proof are in the Appendix C.9. $\square$

To justify the above theorem, consider: $P_1 = s[1][2]?(x); s[1][3]!\langle x\rangle; \mathbf{0} \mid s[2][1]!\langle v\rangle; \mathbf{0}$ and $P_2 = s[1][3]!\langle v\rangle; \mathbf{0}$. It holds that for $E = s : 2 \to 1 : \langle U\rangle.1 \to 3 : \langle U\rangle.\mathtt{end}$ then $E \vdash P_1 \approx^s_g P_2$. We can easily reason $P_1 \approx^s P_2$.

Example 4.2 (Governed bisimulation). Recall the example from § 1 and Example 3.1. Q_1 is the process corresponding to Example 3.1, while Q_2 has a parallel thread instead of the sequential composition (this corresponds to $P_1 \mid R_2$ in § 1).

$$\begin{aligned} Q_1 &= s_1[1][3]!\langle v\rangle; s_2[1][2]!\langle w\rangle; \mathbf{0} \mid s_2[2][1]?(x); \mathbf{0} \mid s_1[2][3]!\langle v\rangle; \mathbf{0} \\ Q_2 &= s_1[1][3]!\langle v\rangle; s_2[1][2]!\langle w\rangle; \mathbf{0} \mid s_2[2][1]?(x); s_1[2][3]!\langle v\rangle; \mathbf{0} \end{aligned}$$

Assume: $\Gamma = v : S \cdot w : S$
$\Delta = s_1[1] : [3]!\langle S\rangle; \mathtt{end} \cdot s_1[2] : [3]!\langle S\rangle; \mathtt{end} \cdot s_2[1] : [2]!\langle S\rangle; \mathtt{end} \cdot s_2[2] : [1]?(S); \mathtt{end}$

Then we have $\Gamma \vdash Q_1 \triangleright \Delta$ and $\Gamma \vdash Q_2 \triangleright \Delta$. Now assume the two global witnesses as:

$$\begin{aligned} E_1 &= s_1 : 1 \to 3 : \langle S\rangle.2 \to 3 : \langle S\rangle.\mathtt{end} \cdot s_2 : 1 \to 2 : \langle S\rangle.\mathtt{end} \\ E_2 &= s_1 : 2 \to 3 : \langle S\rangle.1 \to 3 : \langle S\rangle.\mathtt{end} \cdot s_2 : 1 \to 2 : \langle S\rangle.\mathtt{end} \end{aligned}$$

Then the projection of E_1 and E_2 are given as:

$$\begin{aligned} \mathtt{proj}(E_1) &= s_1[1] : [3]!\langle S\rangle; \mathtt{end} \cdot s_1[2] : [3]!\langle S\rangle; \mathtt{end} \cdot s_1[3] : [1]?(S); [2]?(S); \mathtt{end} \\ &\quad s_2[1] : [2]!\langle S\rangle; \mathtt{end} \cdot s_2[2] : [1]?(S); \mathtt{end} \\ \mathtt{proj}(E_2) &= s_1[1] : [3]!\langle S\rangle; \mathtt{end} \cdot s_1[2] : [3]!\langle S\rangle; \mathtt{end} \cdot s_1[3] : [2]?(S); [1]?(S); \mathtt{end} \cdot \\ &\quad s_2[1] : [2]!\langle S\rangle; \mathtt{end} \cdot s_2[2] : [1]?(S); \mathtt{end} \end{aligned}$$

with $\Delta \subset \mathtt{proj}(E_1)$ and $\Delta \subset \mathtt{proj}(E_2)$. The reader should note that the difference between E_1 and E_2 is the type of the participant 3 at s_1.

By definition, we can write: $E_i, \Gamma \vdash Q_1 \triangleright \Delta$ and $E_i, \Gamma \vdash Q_2 \triangleright \Delta$ for $i = 1, 2$. Both processes are well-formed global configurations under both witnesses. Now we can observe $\Gamma \vdash Q_1 \triangleright \Delta \xrightarrow{s[2][3]!\langle v\rangle} \Gamma \vdash Q_1' \triangleright \Delta'$ but $\Gamma \vdash Q_2 \triangleright \Delta \overset{s[2][3]!\langle v\rangle}{\not\longrightarrow}$. Hence $\Gamma \vdash Q_1 \triangleright \Delta \not\approx^s Q_2 \triangleright \Delta$. By the same argument, we have: $E_2, \Gamma \vdash Q_1 \triangleright \Delta \not\approx^s_g Q_2 \triangleright \Delta$. On the other hand, since E_1 *forces* to wait the action $s[2][3]!\langle v\rangle$, $E_1, \Gamma \vdash Q_1 \triangleright \Delta \overset{s[2][3]!\langle v\rangle}{\not\longrightarrow}$. Hence Q_1 and Q_2 are bisimilar under E_1, i.e. $E_1, \Gamma \vdash Q_1 \triangleright \Delta \approx^s_g Q_2 \triangleright \Delta$. This concludes the optimisation is correct.

The above example for the thread transformation is the *minimum* to demonstrate a difference between $\approx^s_g$ and $\approx^s$. This discipline can be applied to general situations where multiple agents need to interact following a global specification. We tested the real world usecase UC.R2.13 "Acquire Data From Instrument" from the Ocean Observatories Initiative (OOI) [16] Use Case library (Release 2). In this usecase, a user program (`U`) is connected to the Integrated Observatory Network (ION), which provides the infrastructure between users and remote sensing instruments. The user requests, via an ION agent service (`A`), the acquisition of data from an instrument (`I`). In the implementation, the ION agent (`A`) is realised by two sub ION agents (`A1` and `A2`) which internally interact and synchronise together. We are able to reason that the behaviour of `A1` and `A2` is equated by `A` by $\approx^s_g$ applying the thread transformation technique in Example 4.2. See Appendix D.

5 Related and Future Work

As a typed foundation for structured communications programming, session types [10, 19] have been studied over the last decade for a wide range of process calculi and programming languages. Recently several works developed multiparty session types and their extensions. While typed behavioural equivalences are one of the central topics of the π-calculus, surprisingly the typed behavioural semantics based on session types have been less explored, and the existing ones only focus on binary (two-party) sessions. Our work [15] develops an *asynchronous binary* session typed behavioural theory with event operations. An LTS is defined on session type process judgements and ensures session typed properties, such as linearity in the presence of asynchronous queues. The work [17] proves the proof conversions induced by Linear Logic interpretation coincide with an observational equivalence over a strict subset of the binary synchronous session processes. The main focus of our paper is *multiparty* session types and governed bisimulation, whose definitions and properties crucially depend on information of global types. In the first author's PhD thesis [14], we studied governed bisimulations can be systematically developed under various semantics including three kinds of asynchronous semantics by modularly changing the LTS for processes, environments and global types. For governed bisimulations, we can reuse all of the definitions among four semantics by only changing the conditions of the LTS of global types to suit each semantics. Another recent work [5] gives an a fully abstract encoding of a *binary* synchronous session typed calculus into a linearly typed π-calculus [2]. We believe the same encoding method is smoothly applicable to $\approx^s$ since it is defined solely based on the projected types (i.e. local types). However a governed bisimulation requires a global witness, hence the additional global information would be required for full abstraction.

The constructions of our work are hinted by [9] which studies typed behavioural semantics for the π-calculus with IO-subtyping where a LTS for pairs of typing environments and processes is used for defining typed testing equivalences and barbed congruence. On the other hand, in [9], the type environment indexing the observational equivalence resembles more a dictator where the refinement can be obtained by the fact that the observer has only partial knowledge on the typings, than a coordinator like our approach. Several papers have developed bisimulations for the higher-order π-calculus or its variants using the information of the environments. Among them, a recent paper [13] uses a pair of a process and an observer knowledge set for the LTS. The knowledge set contains a mapping from first order values to the higher-order processes, which allows a tractable higher-order behavioural theory using the first-order LTS.

We record a choreographic type as the witness in the environment to obtain fine-grained bisimulations of multiparty processes. The highlight of our bisimulation construction is an effective use of the semantics of global types for LTSs of processes (cf. [Inv] in Figure 7 and Definition 4.4). Global types can give a guidance how to coordinate parallel threads giving explicit protocols, hence it is applicable to a semantic-preserving optimisation (cf. Example 4.2 and Appendix D). While it is known that it is undecidable to check $P \approx Q$ in the full π-calculus, it is an interesting future topic to investigate automated bisimulation-checking techniques for the governed bisimulations for some subset of multiparty session processes.

References

1. R. M. Amadio, I. Castellani, and D. Sangiorgi. On bisimulations for the asynchronous pi-calculus. *TCS*, 195(2):291–324, 1998.
2. M. Berger, K. Honda, and N. Yoshida. Sequentiality and the π-calculus. In *Proc. TLCA'01*, volume 2044 of *LNCS*, pages 29–45, 2001.
3. L. Bettini et al. Global progress in dynamically interleaved multiparty sessions. In *CONCUR*, volume 5201 of *LNCS*, pages 418–433. Springer, 2008.
4. W3C Web Services Choreography. `http://www.w3.org/2002/ws/chor/`.
5. R. Demangeon and K. Honda. Full abstraction in a subtyped pi-calculus with linear types. In *CONCUR*, volume 6901 of *LNCS*, pages 280–296. Springer, 2011.
6. P.-M. Deniélou and N. Yoshida. Multiparty session types meet communicating automata. In *ESOP*, volume 7211 of *LNCS*, pages 194–213. Springer, 2012.
7. On-line Appendix of this paper. `http://www.doc.ic.ac.uk/~yoshida/governed`.
8. M. Hennessy. *A Distributed Pi-Calculus*. CUP, 2007.
9. M. Hennessy and J. Rathke. Typed behavioural equivalences for processes in the presence of subtyping. *Mathematical Structures in Computer Science*, 14(5):651–684, 2004.
10. K. Honda, V. T. Vasconcelos, and M. Kubo. Language primitives and type disciplines for structured communication-based programming. In *ESOP'98*, volume 1381 of *LNCS*, pages 22–138. Springer, 1998.
11. K. Honda and N. Yoshida. On reduction-based process semantics. *TCS*, 151(2):437–486, 1995.
12. K. Honda, N. Yoshida, and M. Carbone. Multiparty Asynchronous Session Types. In *POPL'08*, pages 273–284. ACM, 2008.
13. V. Koutavas and M. Hennessy. A testing theory for a higher-order cryptographic language. In *ESOP*, volume 6602 of *LNCS*, pages 358–377, 2011.
14. D. Kouzapas. *A study of bisimulation theory for session types*. PhD thesis, Department of Computing, Imperial College London, May 2013.
15. D. Kouzapas, N. Yoshida, and K. Honda. On asynchronous session semantics. In *FMOODS/-FORTE*, volume 6722 of *Lecture Notes in Computer Science*, pages 228–243, 2011.
16. Ocean Observatories Initiative (OOI). `http://www.oceanobservatories.org/`.
17. J. A. Pérez, L. Caires, F. Pfenning, and B. Toninho. Linear logical relations for session-based concurrency. In *ESOP*, volume 7211 of *LNCS*, pages 539–558. Springer, 2012.
18. B. Pierce and D. Sangiorgi. Typing and subtyping for mobile processes. *MSCS*, 6(5):409–454, 1996.
19. K. Takeuchi, K. Honda, and M. Kubo. An Interaction-based Language and its Typing System. In *PARLE'94*, volume 817 of *LNCS*, pages 398–413, 1994.
20. N. Yoshida. Graph types for monadic mobile processes. In *FSTTCS*, volume 1180 of *LNCS*, pages 371–386. Springer, 1996.
21. N. Yoshida and V. T. Vasconcelos. Language primitives and type discipline for structured communication-based programming revisited: Two systems for higher-order session communication. *Electr. Notes Theor. Comput. Sci.*, 171(4):73–93, 2007.

A Appendix for Typing Rules

A.1 Two projections

The relation between global and local types is formalised by the standard projection function [12].

Definition A.1 (Global projection and projection set). The projection of a global type G onto a participant $\mathtt{p}$ is defined by induction on G:

$$\mathtt{p}' \to \mathtt{q} : \langle U \rangle.G\lceil\mathtt{p} = \begin{cases} [\mathtt{q}]!\langle U\rangle;G\lceil\mathtt{p} & \mathtt{p}=\mathtt{p}' \\ [\mathtt{p}']?(U);G\lceil\mathtt{p} & \mathtt{p}=\mathtt{q} \\ G\lceil\mathtt{p} & \text{otherwise} \end{cases} \qquad \mathtt{p}' \to \mathtt{q} : \{l_i : G_i\}_{i\in I}\lceil\mathtt{p} = \begin{cases} [\mathtt{q}]\oplus\{l_i : G_i\lceil\mathtt{p}\}_{i\in I} & \mathtt{p}=\mathtt{p}' \\ [\mathtt{p}']\&\{l_i : G_i\lceil\mathtt{p}\}_{i\in I} & \mathtt{p}=\mathtt{q} \\ G_1\lceil\mathtt{p} & \text{if } \forall j\in I.\ G_1\lceil\mathtt{p} = G_j\lceil\mathtt{p} \end{cases}$$

$$(\mu\mathtt{t}.G)\lceil\mathtt{p} = \begin{cases} \mu\mathtt{t}.(G\lceil\mathtt{p}) & \mathtt{p}\in G \\ \mathtt{end} & \text{otherwise} \end{cases} \qquad \mathtt{t}\lceil\mathtt{p} = \mathtt{t} \quad \mathtt{end}\lceil\mathtt{p} = \mathtt{end}$$

Then the *projection set* of $s : G$ is defined as $\mathtt{proj}(s : G) = \{s[\mathtt{p}] : G\lceil\mathtt{p} \mid \mathtt{p}\in\mathtt{roles}(G)\}$ where $\mathtt{roles}(G)$ denotes the set of the roles appearing in G.

We also need the following projection from a local type T to produce binary session types for defining the equivalence relations later.

Definition A.2 (Local projection). The projection of a local type T onto a participant $\mathtt{p}$ is defined by induction on T:

$$[\mathtt{p}]!\langle U\rangle;T\lceil\mathtt{q} = \begin{cases} !\langle U\rangle;T\lceil\mathtt{q} & \mathtt{q}=\mathtt{p} \\ T\lceil\mathtt{q} & \text{otherwise} \end{cases} \qquad [\mathtt{p}]?(U);T\lceil\mathtt{q} = \begin{cases} ?(U);T\lceil\mathtt{q} & \mathtt{q}=\mathtt{p} \\ T\lceil\mathtt{q} & \text{otherwise} \end{cases}$$

$$[\mathtt{p}]\oplus\{l_i : T_i\}_{i\in I}\lceil\mathtt{q} = \begin{cases} \oplus\{l_i : T_i\lceil\mathtt{q}\}_{i\in I} & \mathtt{q}=\mathtt{p} \\ T_1\lceil\mathtt{q} & \text{if } \forall i\in I.T_i\lceil\mathtt{q} = T_1\lceil\mathtt{q} \end{cases}$$

$$[\mathtt{p}]\&\{l_i : T_i\}_{i\in I}\lceil\mathtt{q} = \begin{cases} \&\{l_i : T_i\lceil\mathtt{q}\}_{i\in I} & \mathtt{q}=\mathtt{p} \\ T_1\lceil\mathtt{q} & \text{if } \forall i\in I.T_i\lceil\mathtt{q} = T_1\lceil\mathtt{q} \end{cases}$$

The rest is similar as Definition A.1.

The duality over the projected types are defined as: $\mathtt{end} = \overline{\mathtt{end}}$, $\mathtt{t} = \bar{\mathtt{t}}$, $\overline{\mu\mathtt{t}.T} = \mu\mathtt{t}.\overline{T}$, $\overline{!\langle U\rangle;T} = ?(U);\overline{T}$, $\overline{?(U);T} = !\langle U\rangle;\overline{T}$, $\overline{\oplus\{l_i : T_i\}_{i\in I}} = \&\{l_i : \overline{T_i}\}_{i\in I}$ and $\overline{\&\{l_i : T_i\}_{i\in I}} = \oplus\{l_i : \overline{T_i}\}_{i\in I}$. We note that if $\mathtt{p},\mathtt{q}\in\mathtt{roles}(G)$ then $(G\lceil\mathtt{p})\lceil\mathtt{q} = \overline{(G\lceil\mathtt{q})\lceil\mathtt{p}}$.

A.2 Typing system and its properties

The typing judgements for expressions and processes are of the shapes:

$$\Gamma \vdash e : S \quad \text{and} \quad \Gamma \vdash P \triangleright \Delta$$

where Γ is the standard environment which associates variables to sort types, shared names to global types and process variables to session environments; and Δ is the session environment which associates channels to session types. Formally we define:

$$\Gamma \ ::= \ \emptyset \mid \Gamma\cdot u : S \mid \Gamma\cdot X : \Delta \quad \text{and} \quad \Delta \ ::= \ \emptyset \mid \Delta\cdot s[\mathtt{p}] : T$$

assuming we can write $\Gamma\cdot u : S$ if $u \notin \mathtt{dom}(\Gamma)$. We extend this to a concatenation for typing environments as $\Delta\cdot\Delta' = \Delta\cup\Delta'$. We define coherency of session environments as follows:

Definition A.3 (Coherency). Typing Δ is *coherent with respect to session s* (notation $\mathtt{co}(\Delta(s))$) if $\forall s[\mathtt{p}] : T_{\mathtt{p}}, s[\mathtt{q}] : T_{\mathtt{q}} \in \Delta$ with $\mathtt{p} \neq \mathtt{q}$ then $T_{\mathtt{p}}\lceil \mathtt{q} = \overline{T_{\mathtt{q}}\lceil \mathtt{p}}$. A typing Δ is *coherent* (notation $\mathtt{co}(\Delta)$) if it is coherent with respect to all s in its domain. We say that the typing judgement $\Gamma \vdash P \triangleright \Delta$ is *coherent* if $\mathtt{co}(\Delta)$.

The typing rules are essentially identical to the communication typing system for programs in [3] (since we do not require queues).

We say a typing Δ is *fully coherent* (notation $\mathtt{fco}(\Delta)$) if it is coherent and if $s[\mathtt{p}] : T_{\mathtt{p}} \in \Delta$ then for all $\mathtt{q} \in \mathtt{roles}(T_{\mathtt{p}})$, $s[\mathtt{q}] : T_{\mathtt{q}} \in \Delta$.

$$\Gamma \cdot u : S \vdash u : S \; [\text{Name}] \quad \Gamma \vdash \mathtt{tt}, \mathtt{ff} : \mathtt{bool} \; [\text{Bool}] \quad \frac{\Gamma \vdash e_i : \mathtt{bool}}{\Gamma \vdash e_1 \; \mathtt{and} \; e_2 : \mathtt{bool}} \; [\text{And}]$$

$$\frac{\Gamma \vdash a : \langle G \rangle \quad \Gamma \vdash P \triangleright \Delta \cdot x[\mathtt{p}] : G\lceil \mathtt{p} \quad \max(\mathtt{roles}(G)) = \mathtt{p}}{\Gamma \vdash \overline{a}[\mathtt{p}](x).P \triangleright \Delta} \; [\text{MReq}] \qquad \frac{\Gamma \vdash a : \langle G \rangle \quad \Gamma \vdash P \triangleright \Delta \cdot x[\mathtt{p}] : G\lceil \mathtt{p}}{\Gamma \vdash a[\mathtt{p}](x).P \triangleright \Delta} \; [\text{MAcc}]$$

$$\frac{\Gamma \vdash e : S \quad \Gamma \vdash P \triangleright \Delta \cdot c : T}{\Gamma \vdash c[\mathtt{q}]!\langle e \rangle; P \triangleright \Delta \cdot c : [\mathtt{q}]!\langle S \rangle; T} \; [\text{Send}] \qquad \frac{\Gamma \cdot x : S \vdash P \triangleright \Delta \cdot c : T}{\Gamma \vdash c[\mathtt{q}]?(x); P \triangleright \Delta \cdot c : [\mathtt{q}]?(S); T} \; [\text{Recv}]$$

$$\frac{\Gamma \vdash P \triangleright \Delta \cdot c : T}{\Gamma \vdash c[\mathtt{q}]!\langle c' \rangle; P \triangleright \Delta \cdot c : [\mathtt{q}]!\langle T' \rangle; T \cdot c' : T'} \; [\text{Deleg}] \qquad \frac{\Gamma \vdash P \triangleright \Delta \cdot c : T \cdot x : T'}{\Gamma \vdash c[\mathtt{q}]?(x); P \triangleright \Delta \cdot c : [\mathtt{q}]?(T'); T} \; [\text{SRecv}]$$

$$\frac{\Gamma \vdash P \triangleright \Delta \cdot c : T}{\Gamma \vdash c[\mathtt{q}] \oplus l_i; P \triangleright \Delta \cdot c : [\mathtt{q}] \oplus \{l_i : T_i\}_{i \in I}} \; [\text{Sel}] \qquad \frac{\Gamma \vdash P_i \triangleright \Delta \cdot c : T_i \quad \forall\, i \in I}{\Gamma \vdash c[\mathtt{q}]\&\{l_i : P_i\}_{i \in I} \triangleright \Delta \cdot c : [\mathtt{q}]\&\{l_i : T_i\}_{i \in I}} \; [\text{Bra}]$$

$$\frac{\Gamma \vdash P_1 \triangleright \Delta_1 \quad \Gamma \vdash P_2 \triangleright \Delta_2 \quad \Delta_1 \cap \Delta_2 = \emptyset}{\Gamma \vdash P_1 \mid P_2 \triangleright \Delta_1 \cdot \Delta_2} \; [\text{Conc}] \qquad \frac{\Gamma \vdash e : \mathtt{bool} \quad \Gamma \vdash P \triangleright \Delta \quad \Gamma \vdash Q \triangleright \Delta}{\Gamma \vdash \mathtt{if}\; e \;\mathtt{then}\; P \;\mathtt{else}\; Q \triangleright \Delta} \; [\text{If}]$$

$$\frac{\Delta \, \mathtt{end} \text{ only}}{\Gamma \vdash \mathbf{0} \triangleright \Delta} \; [\text{Inact}] \qquad \frac{\Gamma \cdot a : \langle G \rangle \vdash P \triangleright \Delta}{\Gamma \vdash (\nu\, a)P \triangleright \Delta} \; [\text{NRes}]$$

$$\frac{\mathtt{fco}(\{s[1] : T_1 \ldots s[n] : T_n\}) \quad \Gamma \vdash P \triangleright \Delta \cdot s[1] : T_1 \ldots s[n] : T_n}{\Gamma \vdash (\nu\, s)P \triangleright \Delta} \; [\text{SRes}] \qquad \Gamma \cdot X : \Delta \vdash X \triangleright \Delta \; [\text{Var}] \quad \frac{\Gamma \cdot X : \Delta \vdash P \triangleright \Delta}{\Gamma \vdash \mu X.P \triangleright \Delta} \; [\text{Rec}]$$

Fig. 8. Typing System for Synchronous Multiparty Session Calculus

Figure 8 defines the typing system. Rule [Name] types a shared name or shared variable to type S. Boolean $\mathtt{tt}, \mathtt{ff}$ are typed with the $\mathtt{bool}$ type via rule [Bool]. Logical expressions are also typed with the $\mathtt{bool}$ type via rule [And], etc. Rules [MReq] and [MAcc] check that the local type of a session role agrees with the global type of the initiating shared name. Rules [Send] and [Recv] prefix the local type with send and receive local types respectively, after checking the type environment for the sending value type (receiving variable type resp.). Delegation is typed under rules [Deleg] and [Srecv] where we check type consistency of the delegating/receiving session role. Rules [Sel] and [Bra] type select and branch processes respectively. A select process uses the select local type. A branching process checks that all continuing process have a consistent typing environments. [Conc] types a parallel composition of processes by checking the disjointness of their typing environments. Conditional is typed with [If], where we check the expression e to be of `bool` type and the branching processes to have the same typing environment. Rule [Nres] defines the typing for shared name restriction. Rule [Sres] uses the full coherency property to restrict a session name. Recursive rules [Var] and [Rec] are standard. Finally the inactive process $\mathbf{0}$ is typed with the complete typing environment, where every session role is mapped to the inactive local type `end`. The following theorem is proved in [3].

Theorem A.1 (Subject reduction). *If $\Gamma \vdash P \triangleright \Delta$ is coherent and $P \longrightarrow\!\!\!\!\rightarrow P'$ then $\Gamma \vdash P' \triangleright \Delta'$ is coherent with $\Delta \longrightarrow\!\!\!\!\rightarrow \Delta'$.*

B Appendix for Sections 2 and 2

We list the omitted definitions from Section 2 and

$$P \equiv P \mid \mathbf{0} \quad P \mid Q \equiv Q \mid P \quad (P \mid Q) \mid R \equiv P \mid (Q \mid R) \quad P \equiv_\alpha P \quad \mu X.P \equiv P\{\mu X.P/X\}$$
$$(\nu\, n)(\nu\, n')P \equiv (\nu\, n')(\nu\, n)P \quad (\nu\, n)(\nu\, n')P \equiv (\nu\, nn')P \quad (\nu\, n)\mathbf{0} \equiv \mathbf{0}$$
$$(\nu\, n)(P) \mid Q \equiv (\nu\, n)(P \mid Q) \quad n \notin \mathtt{fn}(Q)$$

Fig. 9. Structural Congruence for Synchronous Multiparty Session Calculus

The structural congruence rules are defined in figure 9.

We define the roles occurring in a global type and the roles occurring in a local type.

Definition B.1 (Roles).

- *We define* $\mathtt{roles}(G)$ *as the set of roles in protocol* G*. Note that for all* $u : G \in \Gamma$*,* $\mathtt{roles}(G) = \{1, 2, ..., n\}$ *for some* n*.*
- *We define* $\mathtt{roles}(T)$ *on local types as:*

$$\mathtt{roles}(\mathtt{end}) = \emptyset \quad \mathtt{roles}(\mathrm{t}) = \emptyset \quad \mathtt{roles}(\mu \mathrm{t}.T) = \mathtt{roles}(T)$$

$$\mathtt{roles}([\mathrm{p}]!\langle U\rangle;T) = \{\mathrm{p}\} \cup \mathtt{roles}(T) \qquad \mathtt{roles}([\mathrm{p}]?(U);T) = \{\mathrm{p}\} \cup \mathtt{roles}(T)$$
$$\mathtt{roles}([\mathrm{p}] \oplus \{l_i : T_i\}_{i\in I}) = \{\mathrm{p}\} \cup \mathtt{roles}(T) \quad \mathtt{roles}([\mathrm{p}]\&\{l_i : T_i\}_{i\in I}) = \{\mathrm{p}\} \cup \mathtt{roles}(T)$$

C Proofs for Bisimulation Properties

C.1 Parallel Observer Property

Lemma C.1. *If $\Gamma \vdash P_1 \triangleright \Delta_1, \Gamma \vdash P_2 \triangleright \Delta_2$ and $E, \Gamma \vdash P_1 \mid P_2 \triangleright \Delta$ then*

1. *$\Delta = \Delta_1 \cup \Delta_2$, $\Delta_1 \cap \Delta_2 = \emptyset$*
2. *$E, \Gamma \vdash P_1 \triangleright \Delta_1$ and $E, \Gamma \vdash P_2 \triangleright \Delta_2$*

Proof. Part 1 is obtain from typing rule [Conc]. Part 2 is immediate from part 1, since $\Delta \subseteq \Delta_1$ (resp. $\Delta \subseteq \Delta_2$). □

C.2 Proof for Lemma 3.1

Proof. We use the coinduction method which is implied by the bisimilarity definition.

Assume that for $\Gamma \vdash P_1 \triangleright \Delta_1 \approx^s P_2 \triangleright \Delta_2$, we have $\Delta_1 \rightleftharpoons \Delta_2$. Then by the definition of $\rightleftharpoons$, there exists Δ such that

$$\Delta_1 \longrightarrow^* \Delta \text{ and } \Delta_2 \longrightarrow^* \Delta \tag{1}$$

Now assume that $\Gamma \vdash P_1 \triangleright \Delta_1 \xrightarrow{\ell} P_1' \triangleright \Delta_1'$ then, $\Gamma \vdash P_2 \triangleright \Delta_2 \overset{\ell}{\Longrightarrow} P_2' \triangleright \Delta_2'$ and by the typed transition definition we get $(\Gamma, \Delta_1) \xrightarrow{\ell} (\Gamma, \Delta_1')$, $(\Gamma, \Delta_2) \overset{\ell}{\Longrightarrow} (\Gamma, \Delta_2')$. We need to show that $\Delta_1' \rightleftharpoons \Delta_2'$.

We prove by a case analysis on the transition $\xrightarrow{\ell}$ on (Γ, Δ_1) and (Γ, Δ_2).

- **Case $\ell = \tau$:** We use the fact that $\xrightarrow{\tau}$ with $\equiv$ coincides with $\longrightarrow$. Then by Theorem A.1, we obtain if $\Gamma \vdash P_1 \triangleright \Delta_1$ and $P_1 \longrightarrow P_1'$ then $\Gamma \vdash P_1' \triangleright \Delta_1'$ and $\Delta_1 \longrightarrow \Delta_1'$ or $\Delta_1 = \Delta_1'$.
  For the reversed direction, if $\Gamma \vdash P_2 \triangleright \Delta_2$ and $P_2 \twoheadrightarrow P_2'$ then $\Gamma \vdash P_2' \triangleright \Delta_2'$ and $\Delta_2 \longrightarrow^* \Delta_2'$. From the hypothesis on $\Gamma \vdash P_1' \triangleright \Delta_1'$ and $\Gamma \vdash P_2' \triangleright \Delta_2'$, we obtain there exists Δ such that $\Delta_1' \longrightarrow^* \Delta$ and $\Delta_2' \longrightarrow^* \Delta$, as required.

  Case $\ell = a[\mathtt{p}](s)$ or $\ell = \overline{a}[\mathtt{p}](s)$: Then

  $$(\Gamma, \Delta_1) \xrightarrow{\ell} (\Gamma, \Delta_1 \cdot s[\mathtt{p}] : T_{\mathtt{p}} \cdot \ldots \cdot s[\mathtt{q}] : T_{\mathtt{q}})$$

  and

  $$(\Gamma, \Delta_2) \Longrightarrow \xrightarrow{\ell} \Longrightarrow (\Gamma, \Delta_2'' \cdot s[\mathtt{p}] : T_{\mathtt{p}} \cdot \ldots \cdot s[\mathtt{q}] : T_{\mathtt{q}})$$

  We set

  $$\Delta' = \Delta \cdot s[\mathtt{p}] : T_{\mathtt{p}} \cdot \ldots \cdot s[\mathtt{q}] : T_{\mathtt{q}}$$

  to obtain $\Delta_1' \longrightarrow^* \Delta'$ and $\Delta_2' \longrightarrow^* \Delta'$, by the coinduction hypothesis (1).

- **Case $\ell = s[\mathtt{p}][\mathtt{q}]!\langle v \rangle$:**
  We know from the definition of environment transition, that $s[\mathtt{q}] \notin \mathtt{dom}(\Delta_1)$ and $s[\mathtt{q}] \notin \mathtt{dom}(\Delta_2)$, thus $s[\mathtt{q}] \notin \mathtt{dom}(\Delta)$ We set

  $$\Delta_1 = s[\mathtt{p}] : [\mathtt{q}]!\langle v \rangle; T \cdot \Delta_1''$$

  and

  $$\Delta_2 = s[\mathtt{p}] : [\mathtt{q}]!\langle v \rangle; T \cdot \Delta_2''$$

  so

  $$\Delta = s[\mathtt{p}] : [\mathtt{q}]!\langle v \rangle; T \cdot \Delta''$$

  by (1). We set $\Delta' = s[\mathtt{p}] : T \cdot \Delta''$ to obtain $\Delta_1' \longrightarrow^* \Delta'$ and $\Delta_2' \longrightarrow^* \Delta'$.

– **Case** $\ell = s[\mathtt{p}][\mathtt{q}]!(s'[\mathtt{p}'])$**:**
We know from the definition of environment transition, that $s[\mathtt{q}] \notin \mathtt{dom}(\Delta_1)$ and $s[\mathtt{q}] \notin \mathtt{dom}(\Delta_2)$, thus $s[\mathtt{q}] \notin \mathtt{dom}(\Delta)$. We set

$$\Delta_1 = s[\mathtt{p}] : [\mathtt{q}]!\langle T' \rangle; T \cdot \Delta_1''$$

and

$$\Delta_2 = s[\mathtt{p}] : [\mathtt{q}]!\langle T' \rangle; T \cdot \Delta_2''$$

so

$$\Delta = s[\mathtt{p}] : [\mathtt{q}]!\langle v \rangle; T \cdot \Delta''$$

by (1). We set $\Delta' = s[\mathtt{p}] : T \cdot \Delta'' \cdot \{s[\mathtt{p}_i] : T_i\}$ to obtain $\Delta_1' \longrightarrow^* \Delta'$ and $\Delta_2' \longrightarrow^* \Delta'$.

– The remaining cases on session channel actions are similar.

□

C.3 Weakening - Strengthening

The following lemmas are essential for invariant properties.

Lemma C.2 (Weakening).

1. If $E, \Gamma \vdash P \triangleright \Delta$ then
  – $E \cdot s : G, \Gamma \vdash P \triangleright \Delta$.
  – $E = E' \cdot s : G$ *and* $\exists G' \cdot \{s : G'\} \twoheadrightarrow \{s : G\}$ *then* $E' \cdot s : G', \Gamma \vdash P \triangleright \Delta$.

2. If $(E, \Gamma, \Delta) \xrightarrow{\ell} (E, \Gamma', \Delta')$ then
  – $(E \cdot s : G, \Gamma, \Delta) \xrightarrow{\ell} (E \cdot s : G, \Gamma', \Delta')$
  – *If* $E = E' \cdot s : G$ *and* $\{s : G'\} \twoheadrightarrow \{s : G\}$ *then* $(E' \cdot s : G', \Gamma, \Delta) \xrightarrow{\ell} (E' \cdot s : G', \Gamma', \Delta')$

3. If $E, \Gamma \vdash P_1 \triangleright \Delta_2 \approx_g P_2 \triangleright \Delta_2$
  – $E \cdot s : G, \Gamma \vdash P_1 \triangleright \Delta_2 \approx_g P_2 \triangleright \Delta_2$
  – *If* $E = E' \cdot s : G$ *and* $\{s : G'\} \twoheadrightarrow\subseteq \{s : G\}$ *then* $E' \cdot s : G', \Gamma \vdash P_1 \triangleright \Delta_2 \approx_g P_2 \triangleright \Delta_2$

Proof. We only show Part 1. Other parts are similar.

– From the governance judgement definition we have that $E \longrightarrow^* E_1$ and $\mathtt{proj}(E_1) \supseteq \Delta$.
Let $E \cdot s : G \longrightarrow E_1 \cdot s : G$. Then $\mathtt{proj}(E_1 \cdot s : G) = \mathtt{proj}(E_1) \cup \mathtt{proj}(s : G) \supseteq \mathtt{proj}(E_1) \supseteq \Delta$.
– From the governance judgement definition we have that $E \cdot s : G \longrightarrow^* E_1 \cdot s : G_1$ and $\mathtt{proj}(E_1 \cdot s : G_1) \supseteq \Delta$.
Let $E \cdot s : G' \longrightarrow^* E_1 \cdot s : G' \longrightarrow^* E_1 \cdot S : G_1$. Then the result is immediate.

□

Lemma C.3 (Strengthening).

1. If $E \cdot s : G, \Gamma \vdash P \triangleright \Delta, E_1 \cdot s : G_1$ and
  – *If* $s \notin \mathtt{fn}(P)$ *then* $E, \Gamma \vdash P \triangleright \Delta$
  – *If* $\exists G', \{s : G\} \twoheadrightarrow \{s : G'\} \twoheadrightarrow \{s : G_1\}$ *then* $E' \cdot s : G', \Gamma \vdash P \triangleright \Delta$

2. If $(E \cdot s : G, \Gamma, \Delta) \xrightarrow{\ell} (E' \cdot s : G, \Gamma', \Delta')$ then

– $(E,\Gamma,\Delta) \xrightarrow{\ell} (E',\Gamma',\Delta')$
– *If* $\exists G', \{s:G\} \twoheadrightarrow \{s:G'\} \twoheadrightarrow \{s:G_1\}\ S\ (E\cdot s:G',\Gamma,\Delta) \xrightarrow{\ell} (E'\cdot s:G',\Gamma',\Delta')$

3. *If* $E\cdot s:G,\Gamma \vdash P_1 \triangleright \Delta_2, E_1 \approx_g P_2 \triangleright \Delta_2, E_2$
   – *If* $s \notin \mathtt{fn}(P)$ *then* $E,\Gamma \vdash P_1 \triangleright \Delta_2 \approx_g P_2 \triangleright \Delta_2$
   – *If* $\exists G', \{s:G\} \twoheadrightarrow \{s:G'\} \twoheadrightarrow \{s:G_1\}\ E\cdot s:G',\Gamma \vdash P_1 \triangleright \Delta_2 \approx_g P_2 \triangleright \Delta_2$

Proof. We prove for part 1. Other parts are similar.

– From the governance judgement definition we have that $E\cdot s:G \longrightarrow^* E_1\cdot s:G_1$ and $\mathtt{proj}(E_1\cdot s:G_1) = \mathtt{proj}(E_1)\cup\mathtt{proj}(s:G_1) \supseteq \Delta$. Since $s\notin\mathtt{fn}(P)$ then $s\notin\mathtt{dom}(\Delta)$, then $\mathtt{proj}(s:G_1)\cap\Delta=\emptyset$. So $\mathtt{proj}(E_1)\supseteq\Delta$ and $E\longrightarrow^* E_1$.
– The result is immediate from the definition of governance judgement.

□

C.4 Configuration Transition Properties

Lemma C.4.

– *If* $E \xrightarrow{s:\mathtt{p}\to\mathtt{q}:U} E'$ *then* $\{s[\mathtt{p}]:[\mathtt{q}]!\langle U\rangle;T_{\mathtt{p}}, s[\mathtt{q}]:[\mathtt{p}]?(U);T_{\mathtt{q}}\} \subseteq \mathtt{proj}(E)$ *and* $\{s[\mathtt{p}]:T_{\mathtt{p}}, s[\mathtt{q}]:T_{\mathtt{q}}\} \subseteq \mathtt{proj}(E')$.
– *If* $E \xrightarrow{s:\mathtt{p}\to\mathtt{q}:l} E'$ *then* $\{s[\mathtt{p}]:[\mathtt{q}]\oplus\{l_i:T_{i\mathtt{p}}\}, s[\mathtt{q}]:[\mathtt{p}]\&\{l_i:T_{i\mathtt{q}}\}\} \subseteq \mathtt{proj}(E)$ *and* $\{s[\mathtt{p}]:T_{k\mathtt{p}}, s[\mathtt{q}]:T_{k\mathtt{q}}\} \subseteq \mathtt{proj}(E')$

Proof. Part 1: We apply induction on the definition structure of $s:\mathtt{p}\to\mathtt{q}:U$. The base case

$$\{s:\mathtt{p}\to\mathtt{q}:\langle U\rangle.G\} \xrightarrow{s:\mathtt{p}\to\mathtt{q}:U} \{s:G\}$$

is easy since

$$\{s[\mathtt{p}]:(\mathtt{p}\to\mathtt{q}:\langle U\rangle.G)\lceil\mathtt{p}, s[\mathtt{q}]:(\mathtt{p}\to\mathtt{q}:\langle U\rangle.G)\lceil\mathtt{q}\} =$$
$$\{s[\mathtt{p}]:[\mathtt{q}]!\langle U\rangle;T_{\mathtt{p}}, s[\mathtt{q}]:[\mathtt{p}]?(U);T_{\mathtt{q}}\} \subseteq \mathtt{proj}(s:\mathtt{p}\to\mathtt{q}:\langle U\rangle.G)$$

and

$$\{s[\mathtt{p}]:G\lceil\mathtt{p}, s[\mathtt{q}]:G\lceil\mathtt{q}\} = \{s[\mathtt{p}]:T_{\mathtt{p}}, s[\mathtt{q}]:T_{\mathtt{q}}\} \subseteq \mathtt{proj}(s:G)$$

The main induction rule concludes that:

$$\{s:\mathtt{p}'\to\mathtt{q}':\langle U\rangle.G\} \xrightarrow{s:\mathtt{p}\to\mathtt{q}:U} \{s:G'\}$$

if $\mathtt{p}\neq\mathtt{p}'$ and $\mathtt{q}\neq\mathtt{q}'$ and $\{s:G\} \xrightarrow{s:\mathtt{p}\to\mathtt{q}:U} \{s:G'\}$. From the induction hypothesis we know that:

$$\{s[\mathtt{p}]:[\mathtt{q}]!\langle U\rangle;T_{\mathtt{p}}, s[\mathtt{q}]:[\mathtt{p}]?(U);T_{\mathtt{q}}\} \subseteq \mathtt{proj}(s:G)$$
$$\{s[\mathtt{p}]:T_{\mathtt{p}}, s[\mathtt{q}]:T_{\mathtt{q}}\} \subseteq \mathtt{proj}(s:G')$$

to conclude that:

$$\{s[\mathtt{p}]:(\mathtt{p}'\to\mathtt{q}':\langle U\rangle.G)\lceil\mathtt{p}, s[\mathtt{q}]:(\mathtt{p}'\to\mathtt{q}':\langle U\rangle.G)\lceil\mathtt{q}\} =$$
$$\{s[\mathtt{p}]:G\lceil\mathtt{p}, s[\mathtt{q}]:G\lceil\mathtt{q}\} =$$
$$\{s[\mathtt{p}]:[\mathtt{q}]!\langle U\rangle;T_{\mathtt{p}}, s[\mathtt{q}]:[\mathtt{p}]?(U);T_{\mathtt{q}}\} \subseteq \mathtt{proj}(s:G)$$

and

$$\{s[\mathtt{p}] : (\mathtt{p}' \to \mathtt{q}' : \langle U \rangle.G')\lceil\mathtt{p}, s[\mathtt{q}] : (\mathtt{p}' \to \mathtt{q}' : \langle U \rangle.G')\lceil\mathtt{q}\} = \\ \{s[\mathtt{p}] : G'\lceil\mathtt{p}, s[\mathtt{q}] : G'\lceil\mathtt{q}\} = \\ \{s[\mathtt{p}] : T_\mathtt{p}, s[\mathtt{q}] : T_\mathtt{q}\} \subseteq \mathtt{proj}(s : G)$$

as required.

Part 2: Similar. □

Proof for Proposition 4.2

Proof. **(1)** We apply induction on the definition structure of $\xrightarrow{\ell}$.

Basic Step:

Case: $\ell = \overline{a}[s](A)$.
From rule [Acc] we get

$$(E_1, \Gamma_1, \Delta_1) \xrightarrow{\ell} (E_1 \cdot s : G, \Gamma_1, \Delta_1 \cdot \{s[\mathtt{p}_i] : s\lceil\mathtt{p}_i\}_{\mathtt{p}_i \in A})$$

From the environment configuration definition we get that

$$\exists E_1' \cdot E_1 \longrightarrow^* E_1', \quad \mathtt{proj}(E_1') \supseteq \Delta_1$$

We also get that $\mathtt{proj}(s : G) \supseteq \{s[\mathtt{p}_i] : s\lceil\mathtt{p}_i\}_{i \in A}$. So we can safely conclude that

$$E_1 \cdot s : G \longrightarrow^* E_1' \cdot s : G, \mathtt{proj}(E_1 \cdot s : G) \supseteq \Delta_1 \cdot \{s[\mathtt{p}_i] : s\lceil\mathtt{p}_i\}_{\mathtt{p}_i \in A}$$

Case: $\ell = \overline{a}[s](A)$. Similar as above.

Case: $\ell = s[\mathtt{p}][\mathtt{q}]!\langle v \rangle$.
From rule [Out] we get

$$\begin{array}{rcl} (E_1, \Gamma, \Delta \cdot s[\mathtt{p}] : [\mathtt{q}]!\langle U \rangle; T) & \xrightarrow{\ell} & (E_2, \Gamma, \Delta \cdot s[\mathtt{p}] : T) \quad (2) \\ \mathtt{proj}(E_1) & \supseteq & \Delta \cdot s[\mathtt{p}] : [\mathtt{q}]!\langle U \rangle; T \quad (3) \\ E_1 & \xrightarrow{s:\mathtt{p}\to\mathtt{q}:U} & E_2 \quad (4) \end{array}$$

From 3, we obtain $\mathtt{proj}(E_1) \supseteq \Delta \cdot \{s[\mathtt{p}] : [\mathtt{q}]!\langle U \rangle; T \cdot s[\mathtt{q}] : [\mathtt{p}]?(U); T'\}$ and from 4 and Lemma C.4, we obtain that $\mathtt{proj}(E_2) \supseteq \Delta \cdot \{s[\mathtt{p}] : T \cdot s[\mathtt{q}] : T'\}$.
Case: $\ell = s[\mathtt{p}][\mathtt{q}]!(s'[\mathtt{p}'])$.

$$\begin{array}{rcl} (E_1, \Gamma, \Delta \cdot s[\mathtt{p}] : [\mathtt{q}]!\langle T\mathtt{p}' \rangle; T) & \xrightarrow{\ell} & (E_2 \cdot s : G, \Gamma, \Delta \cdot s[\mathtt{p}] : T \cdot \{s[\mathtt{p}_i] : s\lceil\mathtt{p}_i\}) \quad (5) \\ \mathtt{proj}(E_1) & \supseteq & \Delta \cdot s[\mathtt{p}] : [\mathtt{q}]!\langle T_\mathtt{p}' \rangle; T \quad (6) \\ E_1 & \xrightarrow{s:\mathtt{p}\to\mathtt{q}:T_\mathtt{p}'} & E_2 \quad (7) \\ \mathtt{proj}(s : G) & \supseteq & \{s[\mathtt{p}_i] : s\lceil\mathtt{p}_i\} \quad (8) \end{array}$$

From 6 we get $\mathtt{proj}(E_1) \supseteq \Delta \cdot \{s[\mathtt{p}] : [\mathtt{q}]!\langle U \rangle; T \cdot s[\mathtt{q}] : [\mathtt{p}]?(U); T'\}$ and from 7 and lemma C.4 we get that $\mathtt{proj}(E_2) \supseteq \Delta \cdot \{s[\mathtt{p}] : T \cdot s[\mathtt{q}] : T'\} \supset \Delta \cdot s[\mathtt{p}] : T$. From 8 we get that $\mathtt{proj}(E_2 \cdot s : G) \supseteq \Delta \cdot s[\mathtt{p}] : T \cdot \{s[\mathtt{p}_i] : s\lceil\mathtt{p}_i\}$ as required.

The rest of the base cases are similar.
Inductive Step:
The inductive rule for environment configuration is [Inv]. Let $(E_1, \Gamma_1, \Delta_1) \xrightarrow{\ell} (E_2, \Gamma_2, \Delta_2)$. From rule [Inv] we get:

$$E_1 \longrightarrow^* E_1' \tag{9}$$

$$(E_1', \Gamma_1, \Delta_1) \xrightarrow{\ell} (E_2, \Gamma_2, \Delta_2) \tag{10}$$

From the inductive hypothesis we know that for 10 $\exists E_3 \cdot E_2 \longrightarrow^* E_3$ and $\Delta_2 \subseteq \mathtt{proj}(E_3)$. The result is then trivial from 9. □

Lemma C.5.

1. *If* $(E, \Gamma, \Delta_1) \xrightarrow{\ell} (E', \Gamma', \Delta_2)$ *then* $(\Gamma, \Delta_1) \xrightarrow{\ell} (\Gamma', \Delta_2)$
2. *If* $(E, \Gamma, \Delta_1) \xrightarrow{\ell} (E', \Gamma', \Delta_1')$ *and* $\Delta_1 \rightleftharpoons \Delta_2$ *then* $(E, \Gamma, \Delta_2) \xRightarrow{\ell} (E', \Gamma', \Delta_2')$
3. *If* $(\Gamma, \Delta_1) \xrightarrow{\ell} (\Gamma', \Delta_2)$ *then there exists E such that* $(E, \Gamma, \Delta) \xrightarrow{\ell} (E', \Gamma', \Delta_2)$
4. *If* $(E, \Gamma, \Delta \cdot s[\mathtt{p}] : T_\mathtt{p}) \xrightarrow{\ell} (E', \Gamma, \Delta' \cdot s[\mathtt{p}] : T_\mathtt{p})$ *then* $(E, \Gamma, \Delta) \xrightarrow{\ell} (E', \Gamma, \Delta')$
5. *If* $(E, \Gamma, \Delta_1) \xrightarrow{\ell} (E', \Gamma, \Delta_2)$ *then* $(E, \Gamma, \Delta_1 \cdot \Delta) \xrightarrow{\ell}_s (E', \Gamma, \Delta_2 \cdot \Delta)$
   provided that if $(E, \Gamma, \Delta) \xrightarrow{\ell'} (E, \Gamma, \Delta')$ *then* $\ell \not\asymp \ell'$

Proof. Part 1:
The proof for part 1 is easy to be implied by a case analysis on the configuration transition definition with respect to environment transition definition.
Part 2:
By the case analysis on ℓ.
Case $\ell = \tau$**:** The result is trivial.
Case $\ell = \overline{a}[\mathtt{p}](s)$ **or** $\ell = a[\mathtt{p}](s)$**:** The result comes from a simple transition.
Case $\ell = s[\mathtt{p}][\mathtt{q}]!\langle v \rangle$**:** $\Delta_1 \rightleftharpoons \Delta_2$ implies $\Delta_1 \longrightarrow^* \Delta$ and $\Delta_2 \longrightarrow^* \Delta$ for some Δ and $\Delta = \Delta' \cdot s[\mathtt{p}] : [\mathtt{q}]!\langle U \rangle; T$.
$(E, \Gamma, \Delta_2) \Longrightarrow (E, \Gamma, \Delta) \xrightarrow{\ell}$ as required.
Case $\ell = s[\mathtt{p}][\mathtt{q}]!(s'[\mathtt{p}'])$**:** $\Delta_1 \rightleftharpoons \Delta_2$ implies $\Delta_1 \longrightarrow^* \Delta$ and $\Delta_2 \longrightarrow^* \Delta$ for some Δ and $\Delta = \Delta' \cdot s[\mathtt{p}] : [\mathtt{q}]!\langle T' \rangle; T$.
$(E, \Gamma, \Delta_2) \Longrightarrow (E, \Gamma, \Delta) \xrightarrow{\ell}$ as required.
The remaining cases are similar.
Part 3:
We do a case analysis on ℓ.
Cases $\ell = \tau, \ell = \overline{a}[\mathtt{p}](s), \ell = a[\mathtt{p}](s)$**:** The result holds for any E.
Case $\ell = s[\mathtt{p}][\mathtt{q}]!\langle v \rangle$: $\Delta_1 = \Delta_1' \cdot \Delta_1''$ with $\Delta_1'' = s[\mathtt{p}] : [\mathtt{q}]!\langle U \rangle; T_\mathtt{p} \cdot \ldots \cdot s[\mathtt{r}] : T_\mathtt{r}$ Choose $E = E' \cdot s : G$ with $\Delta_1'' \subseteq \mathtt{proj}(s : G)$ and $s[\mathtt{q}] : [\mathtt{p}]?(U); T_\mathtt{q} \in \mathtt{proj}(s : G)$ and $\Delta_1 \subseteq \mathtt{proj}(E)$
By the definition of configuration transition relation, we obtain $(E, \Gamma, \Delta) \xrightarrow{\ell} (E, \Gamma', \Delta_2)$, as required.

Remaining cases are similar.
Part 4:

$(E,\Gamma,\Delta \cdot s[\mathtt{p}] : T_{\mathtt{p}}) \xrightarrow{\ell} (E',\Gamma,\Delta' \cdot s[\mathtt{p}] : T_{\mathtt{p}})$ implies that $s[\mathtt{p}] \notin \mathtt{subj}(\ell)$. The result then follows from the definition of configuration transition.

Part 5:

Case $\ell = \tau, \ell = \overline{a}[\mathtt{p}](s), \ell = a[\mathtt{p}](s)$**:** The result holds by definition of the configuration transition.

Case $\ell = s[\mathtt{p}][\mathtt{q}]!\langle U\rangle$**:** we have that $\Delta_1 = \Delta_1' \cdot s[\mathtt{p}] : [\mathtt{q}]!\langle U\rangle;T$ and $E \xrightarrow{s:\mathtt{p}\to\mathtt{q}:U} E'$. $s[\mathtt{q}] \in \Delta$, then by definition of weak configuration pair we have $\Delta = \Delta'' \cdot s[\mathtt{q}] : \mathtt{q}[U][T]?()$; and $(E,\Gamma,\Delta) \xrightarrow{s[\mathtt{q}][\mathtt{p}]?\langle U\rangle}$. But this contradicts with the assumption $\ell \not\asymp \ell'$, so $s[\mathtt{q}] \notin \Delta$. By the definition of configuration pair transition we get that $(E,\Gamma,\Delta_1 \cdot \Delta) \xrightarrow{s[\mathtt{p}][\mathtt{q}]!\langle U\rangle} (E,\Gamma,\Delta_2 \cdot \Delta)$. Remaining cases are similar.

□

C.5 Proof of Proposition 4.1

(1) since $T_1 \sqsubseteq T_2$ is a syntactic tree inclusion, it is reducible to a problem to check the isomorphism between two types. This problem is decidable [21]. *(2)* the global LTS has one-to-one correspondence with the LTS of global automata in [6] whose reachability set is finite. □

C.6 Proof for Lemma 4.1

Proof. Since we are dealing with closed processes, the interesting case is parallel composition. We need to show that if $E,\Gamma \vdash P \triangleright \Delta_1 \approx_g Q \triangleright \Delta_2$ then for all R such that $E,\Gamma \vdash P \mid R \triangleright \Delta_3, E,\Gamma \vdash Q \mid R \triangleright \Delta_4$ then $E,\Gamma \vdash P \mid R \triangleright \Delta_3 \approx_g Q \mid R \triangleright \Delta_4$.

Let

$$\begin{aligned} S = \{(E,\Gamma \vdash P \mid R \triangleright \Delta_3,\ E,\Gamma \vdash Q \mid R \triangleright \Delta_4) \mid \\ E,\Gamma \vdash P \triangleright \Delta_1 \approx_g Q \triangleright \Delta_2, \\ \forall R \cdot E,\Gamma \vdash P \mid R \triangleright \Delta_3, E,\Gamma \vdash Q \mid R \triangleright \Delta_4\} \end{aligned}$$

Before we proceed to a case analysis, we extract general results. Let $\Gamma \vdash P \triangleright \Delta_1, \Gamma \vdash Q \triangleright \Delta_2, \Gamma \vdash R \triangleright \Delta_5, \Gamma \vdash P \mid R \triangleright \Delta_3, \Gamma \vdash Q \mid R \triangleright \Delta_4$ then from typing rule [Conc] we get

$$\Delta_3 = \Delta_1 \cup \Delta_5 \quad (11)$$

$$\Delta_4 = \Delta_2 \cup \Delta_5 \quad (12)$$

$$\Delta_1 \cap \Delta_5 = \emptyset \quad (13)$$

$$\Delta_2 \cap \Delta_5 = \emptyset \quad (14)$$

We prove that S is a bisimulation. There are three cases:

Case: $E,\Gamma \vdash P \mid R \triangleright \Delta_3 \xrightarrow{\ell} E',\Gamma \vdash P' \mid R \triangleright \Delta_3'$

From typed transition definition we have that:

$$P \mid R \xrightarrow{\ell} P' \mid R \quad (15)$$

$$(E,\Gamma,\Delta_3) \xrightarrow{\ell} (E',\Gamma,\Delta_3') \quad (16)$$

Transition (15) and rule $\langle\text{Par}\rangle$ (LTS in Figure 5) imply:

$$P \xrightarrow{\ell} P' \tag{17}$$

From (11), transition (16) can be written as $(E,\Gamma,\Delta_1 \cup \Delta_5) \xrightarrow{\ell} (E',\Gamma,\Delta_1' \cup \Delta_5)$, to conclude from Lemma C.5 part 4, that:

$$(E,\Gamma,\Delta_1) \xrightarrow{\ell} (E',\Gamma,\Delta_1') \tag{18}$$

$$\texttt{subj}(\ell) \ \notin \ \texttt{dom}(\Delta_5) \tag{19}$$

Transitions 17 and 18 imply $E,\Gamma \vdash P \triangleright \Delta_1 \xrightarrow{\ell} E',\Gamma \vdash P' \triangleright \Delta_1'$. From the definition of set S we get that $E,\Gamma \vdash Q \triangleright \Delta_2 \overset{\ell}{\Longrightarrow} E',\Gamma \vdash Q' \triangleright \Delta_2'$.
From the typed transition definition we have that:

$$Q \overset{\ell}{\Longrightarrow} Q' \tag{20}$$

$$(E,\Gamma,\Delta_2) \overset{\ell}{\Longrightarrow} (E',\Gamma,\Delta_2') \tag{21}$$

From 19 and part 5 of Lemma C.5 we can write: $(E,\Gamma,\Delta_2 \cup \Delta_5) \overset{\ell}{\Longrightarrow} (E',\Gamma,\Delta_2' \cup \Delta_5)$, to imply from 20 that $E,\Gamma \vdash P \mid R \triangleright \Delta_4 \overset{\ell}{\Longrightarrow} E',\Gamma \vdash P' \mid R \triangleright \Delta_4'$ as required.
Case: 2

$$E,\Gamma \vdash P \mid R \triangleright \Delta_3 \xrightarrow{\tau} E' \vdash P' \mid R' \triangleright \Delta_3'$$

From the typed transition definition we have that:

$$P \mid R \xrightarrow{\tau} P' \mid R' \tag{22}$$

$$(E,\Gamma,\Delta_3) \xrightarrow{\tau} (E,\Gamma,\Delta_3') \tag{23}$$

From 22 and rule $\langle\text{Tau}\rangle$ we get

$$P \xrightarrow{\ell} P' \tag{24}$$

$$R \xrightarrow{\ell'} R' \tag{25}$$

From 11 transition 23 can be written $(E,\Gamma,\Delta_1 \cup \Delta_5) \xrightarrow{\tau} (E,\Gamma,\Delta_1' \cup \Delta_5')$, to conclude that

$$(E,\Gamma,\Delta_1) \xrightarrow{\ell} (E,\Gamma,\Delta_1') \tag{26}$$

$$(E,\Gamma,\Delta_5) \xrightarrow{\ell'} (E,\Gamma,\Delta_5') \tag{27}$$

From 24 and 26 we conclude that $E,\Gamma \vdash P \triangleright \Delta_1 \xrightarrow{\ell} E,\Gamma \vdash P' \triangleright \Delta_1'$ and from 25 and 27 $E,\Gamma \vdash R \triangleright \Delta_5 \xrightarrow{\ell} E,\Gamma \vdash R' \triangleright \Delta_5'$.
From the definition of set S we get that $E,\Gamma \vdash Q \triangleright \Delta_2 \overset{\ell}{\Longrightarrow} E,\Gamma \vdash Q' \triangleright \Delta_2'$, implies

$$Q \overset{\ell}{\Longrightarrow} Q' \tag{28}$$

$$(E,\Gamma,\Delta_2) \overset{\ell}{\Longrightarrow} (E,\Gamma,\Delta_2') \tag{29}$$

From 25 we get that $Q \mid R \overset{\tau}{\Longrightarrow} Q' \mid R'$ and $(E,\Gamma,\Delta_2 \cup \Delta_5) \overset{\tau}{\Longrightarrow} (E,\Gamma,\Delta_2' \cup \Delta_5')$, implies

$$E,\Gamma \vdash Q \mid R \triangleright \Delta_4 \overset{\tau}{\Longrightarrow} E' \vdash Q' \mid R' \triangleright \Delta_4'$$

Case: 3

$$E,\Gamma \vdash P \mid R \triangleright \Delta_3 \overset{\ell}{\longrightarrow} E' \vdash P \mid R' \triangleright \Delta_3'$$

□

C.7 Proof for Lemma 4.1

Proof. We take into advantage the fact that bisimulation has a stratifying definition.

- $\approx_{g_0}$ is the union of all configuration relations, $E,\Gamma \vdash P \triangleright \Delta_1 \; R \; Q \triangleright \Delta_2$.
- $E,\Gamma \vdash P \triangleright \Delta_1 \approx_{g_n} Q \triangleright \Delta_2$ if
  - $E,\Gamma \vdash P \triangleright \Delta_1 \overset{\ell}{\longrightarrow} E',\Gamma \vdash P' \triangleright \Delta_1'$ then $E,\Gamma \vdash Q \triangleright \Delta_2 \overset{\ell}{\Longrightarrow} E',\Gamma \vdash Q \triangleright \Delta_2'$ and $E',\Gamma \vdash P' \triangleright \Delta_1' \approx_{g_{n-1}} Q' \triangleright \Delta_2'$
  - The symmetric case.
- $\approx_{g_n}^{\omega} = \bigcap_{0 \leq i \leq n} \approx_{g_i}$

  From coinduction theory, we know that $(\bigcap_{\forall n} \approx_{g_n}) = \approx_g$.
  To this purpose we define a set of tests $T\langle N, \vec{\ell_n}\rangle$ to inductively show that:

$$\begin{array}{ll} \text{If} & E,\Gamma \vdash P_1 \triangleright \Delta_1 \cong_g P_2 \triangleright \Delta_2 \text{ implies} \\ & E,\Gamma \vdash P_1 \mid T\langle N,\vec{\ell_n}\rangle \triangleright \Delta_1 \cong_g P_2 \mid T\langle N,\vec{\ell_n}\rangle \triangleright \Delta_2 \text{ implies} \\ \forall n, & E,\Gamma \vdash P_1 \triangleright \Delta_1 \approx_{g_n} P_2 \triangleright \Delta_2 \text{ implies} \\ & E,\Gamma \vdash P_1 \triangleright \Delta_1 \approx_g P_2 \triangleright \Delta_2 \end{array}$$

We give the definition for $T\langle N,\vec{\ell_n}\rangle$:
$T\langle N, succ, \vec{\ell_n}\rangle = Q\langle N,n,\vec{\ell_i}\rangle \mid \ldots \mid Q\langle N,n,\vec{\ell_i}\rangle$
where

1. $i \in I$
2. $\bigcup_{i\in I} \vec{\ell_i} = \vec{\ell_n}$
3. $n \; ::= \; s[\mathrm{p}] \;\mid\; a.$
4. $N \; ::= \; \emptyset \;\mid\; N \cdot s[\mathrm{p}] \;\mid\; N \cdot a$ is a set of names for testing the receiving objects.

to define

- $Q\langle N,a,a[A](s)\cdot\vec{\ell_n}\rangle = \overline{a}[n](x).Q\langle N,s[n],\vec{\ell_i}\rangle \mid \ldots \mid a[\mathrm{p}](x).Q\langle N,s[\mathrm{p}],\vec{\ell_i}\rangle, i \in I.$
- $Q\langle N,s[\mathrm{q}],s[\mathrm{p}][\mathrm{q}]?\langle v\rangle\cdot\vec{\ell_n}\rangle = s[\mathrm{q}][\mathrm{p}]!\langle v\rangle; Q\langle N,s[\mathrm{q}],\vec{\ell_n}\rangle.$
- $Q\langle N,s[\mathrm{q}],s[\mathrm{p}][\mathrm{q}]\&l\cdot\vec{\ell_n}\rangle = s[\mathrm{q}][\mathrm{p}] \oplus l; Q\langle N,s[\mathrm{q}],\vec{\ell_n}\rangle.$
- $Q\langle N,a,\overline{a}[A](s)\cdot\vec{\ell_n}\rangle = a[q](x).Q\langle N,s[q],\vec{\ell_i}\rangle \mid \ldots \mid a[\mathrm{p}](x).Q\langle N,s[\mathrm{p}],\vec{\ell_i}\rangle, i \in I.$

- $Q\langle N, s[\mathrm{q}], s[\mathrm{p}][\mathrm{q}]!\langle v\rangle \cdot \vec{\ell_n}\rangle$
  $= s[\mathrm{q}][\mathrm{p}]?(x); \mathtt{if}\ x \in N\ \mathtt{then}\ Q\langle N, s[\mathrm{q}], \vec{\ell_n}\rangle\ \mathtt{else}\ (\nu\ b)(b[1](x).Q\langle N, s[\mathrm{q}], \vec{\ell_n}\rangle)$.
- $Q\langle N, s[\mathrm{q}], s[\mathrm{p}][\mathrm{q}]!\langle s'[\mathrm{p}']\rangle \cdot \vec{\ell_n}\rangle$
  $= s[\mathrm{q}][\mathrm{p}]?(x); \mathtt{if}\ x \in N\ \mathtt{then}\ Q\langle N, s[\mathrm{q}], \vec{\ell_n}\rangle\ \mathtt{else}\ (\nu\ b)(b[1](x).Q\langle N, s[\mathrm{q}], \vec{\ell_n}\rangle)$.
- $Q\langle N, s[\mathrm{q}], s[\mathrm{p}][\mathrm{q}] \oplus l_k \cdot \vec{\ell_n}\rangle$
  $= s[\mathrm{q}][\mathrm{p}]\&\{l_k : Q\langle N, s[\mathrm{q}], \vec{\ell_n}\rangle,\ l_i : (\nu\ b)(b[1](x).Q\langle N, s[\mathrm{q}], \vec{\ell_n}\rangle)\}$.
- $Q\langle N, n, \emptyset\rangle = R$.

where $R = (\nu\ b)(b[1](x).R')$ or $R = \mathbf{0}$. R completes the session type on session channel n and is used to keep processes typed.

From the definition of $T\langle N, \vec{\ell_n}\rangle$ we can show that $\forall T\langle N, \ell \cdot \vec{\ell_n}\rangle, T\langle N, \ell \cdot \vec{\ell_n}\rangle \overset{\ell'}{\Longrightarrow} T'\langle N, \vec{\ell_n}\rangle, \ell \asymp \ell'$.

We prove the required result inductively:

$E, \Gamma \vdash P_1 \triangleright \Delta_3 \cong_g P_2 \triangleright \Delta_4$ implies
$\forall \ell \cdot \vec{\ell_n}$ choose $T\langle N, \ell \cdot \vec{\ell_n}\rangle, E, \Gamma \vdash P_1 \mid T\langle N, \ell \cdot \vec{\ell_n}\rangle \triangleright \Delta_1 \cong_g P_2 \mid T\langle N, \ell \cdot \vec{\ell_n}\rangle \triangleright \Delta_2$ implies
$E, \Gamma \vdash P_1 \mid T\langle N, \ell \cdot \vec{\ell_n}\rangle \triangleright \Delta_1 \twoheadrightarrow P_1' \mid T\langle N, \vec{\ell_n}\rangle \triangleright \Delta_1'$,
$E, \Gamma \vdash P_2 \mid T\langle N, \vec{\ell_n}\rangle \triangleright \Delta_2 \twoheadrightarrow P_2' \mid T\langle N, \vec{\ell_n}\rangle \triangleright \Delta_2'$ then by induction hypothesis
$P_1' \approx_{g_n} P_2'$ implies
$\forall n, E, \Gamma \vdash P_1 \triangleright \Delta_1 \approx_{g_n} P_2 \triangleright \Delta_2$ implies
$E, \Gamma \vdash P_1 \triangleright \Delta_1 \approx_g P_2 \triangleright \Delta_2$

We need to show that if

$$E, \Gamma \vdash P_1 \mid T\langle N, \ell \cdot \vec{\ell_n}\rangle \triangleright \Delta_1 \cong_g P_2 \mid T\langle N, \ell \cdot \vec{\ell_n}\rangle \triangleright \Delta_2$$

then

$$E, \Gamma \vdash P_1 \mid T\langle N, \ell \cdot \vec{\ell_n}\rangle \triangleright \Delta_1 \twoheadrightarrow P_1' \mid T\langle N, \vec{\ell_n}\rangle \triangleright \Delta_1', E, \Gamma \vdash P_2 \mid T\langle N, \vec{\ell_n}\rangle \triangleright \Delta_2 \twoheadrightarrow P_2' \mid T\langle N, \vec{\ell_n}\rangle \triangleright \Delta_2'$$

We perform a case analysis on $E, \Gamma \vdash P_1 \triangleright \Delta_3 \xrightarrow{\ell} P_1 \triangleright \Delta_3'$:

- $E, \Gamma \vdash P_1 \triangleright \Delta_3 \xrightarrow{s[\mathrm{p}][\mathrm{q}]?\langle v\rangle} P_1 \triangleright \Delta_3'$ implies, $E, \Gamma \vdash P_1 \mid T\langle N, s[\mathrm{p}][\mathrm{q}]?\langle v\rangle \cdot \vec{\ell_n}\rangle \triangleright \Delta_1 = E, \Gamma \vdash P_1 \mid Q\langle N, s[\mathrm{p}], s[\mathrm{p}][\mathrm{q}]?\langle v\rangle \cdot \vec{\ell_i}\rangle \mid \dots \mid Q\langle N, n, \vec{\ell_i}\rangle \triangleright \Delta_1 \longrightarrow P_1' \mid Q\langle N, s[\mathrm{p}], \vec{\ell_i}\rangle \mid \dots \mid Q\langle N, n, \vec{\ell_i}\rangle \triangleright \Delta_1$.

  $E, \Gamma \vdash P_2 \mid T\langle N, s[\mathrm{p}][\mathrm{q}]?\langle v\rangle \cdot \vec{\ell_n}\rangle \triangleright \Delta_2$ needs to match the reduction, $E, \Gamma \vdash P_2 \mid T\langle N, s[\mathrm{p}][\mathrm{q}]?\langle v\rangle \cdot \vec{\ell_n}\rangle \triangleright \Delta_2 \twoheadrightarrow E, \Gamma \vdash P_2''' \mid T\langle N, s[\mathrm{p}][\mathrm{q}]?\langle v\rangle \cdot \vec{\ell_n}\rangle \triangleright \Delta_2''' \longrightarrow E, \Gamma \vdash P_2'' \mid T'\langle N, \vec{\ell_n}\rangle \triangleright \Delta_2'' \to \to E, \Gamma \vdash P_2' \mid T'\langle N, \vec{\ell_n}\rangle \triangleright \Delta_2'$
- $E, \Gamma \vdash P_1 \triangleright \Delta_3 \xrightarrow{a[A](s)} P_1 \vdash \Delta_3' \triangleright$ implies, $E, \Gamma \vdash P_1 \mid T\langle N, a[A](s) \cdot \vec{\ell_n}\rangle \triangleright \Delta_1 = E, \Gamma \vdash P_1 \mid Q\langle N, a, a[A](s) \cdot \vec{\ell_i}\rangle \mid \dots \mid Q\langle N, n, \vec{\ell_i}\rangle \triangleright \Delta_1 \longrightarrow E, \Gamma \vdash P_1' \mid Q\langle N, a, \vec{\ell_i}\rangle \mid \dots \mid Q\langle N, n, \vec{\ell_i}\rangle \triangleright \Delta_1$.

  $E, \Gamma \vdash P_2 \mid T\langle N, a[A](s) \cdot \vec{\ell_n}\rangle \triangleright \Delta_2$ needs to match the reduction $E, \Gamma \vdash P_2 \mid T\langle N, a[A](s) \cdot \vec{\ell_n}\rangle \triangleright \Delta_2 \twoheadrightarrow E, \Gamma \vdash P_2''' \mid T\langle N, a[A](s) \cdot \vec{\ell_n}\rangle \triangleright \Delta_2''' \longrightarrow E, \Gamma \vdash P_2'' \mid T'\langle N, \vec{\ell_n}\rangle \triangleright \Delta_2'' \twoheadrightarrow E, \Gamma \vdash P_2' \mid T'\langle N, \vec{\ell_n}\rangle \triangleright \Delta_2'$

– $E,\Gamma \vdash P_1 \triangleright \Delta_3 \xrightarrow{s[\mathrm{p}][\mathrm{q}]!\langle v\rangle} P_1 \vdash \Delta_3' \triangleright$ implies, $E,\Gamma \vdash P_1 \mid T\langle N, s[\mathrm{p}][\mathrm{q}]!\langle v\rangle \cdot \vec{\ell_n}\rangle \triangleright \Delta_1 = E,\Gamma \vdash P_1 \mid Q\langle N, s[\mathrm{p}], s[p][q]!\langle v\rangle \cdot \vec{\ell_i}\rangle \mid \ldots \mid Q\langle N, n, \vec{\ell_i}\rangle \triangleright \Delta_1 \twoheadrightarrow E,\Gamma \vdash P_1' \mid Q\langle N, s[\mathrm{p}], \vec{\ell_i}\rangle \mid \ldots \mid Q\langle N, n, \vec{\ell_i}\rangle \triangleright \Delta_1$.

$E,\Gamma \vdash P_2 \mid T\langle N, s[\mathrm{p}][\mathrm{q}]!\langle v\rangle \cdot \vec{\ell_n}\rangle \triangleright \Delta_2$ needs to match the reduction, $E,\Gamma \vdash P_2 \mid T\langle N, s[\mathrm{p}][\mathrm{q}]!\langle v\rangle \cdot \vec{\ell_n}\rangle \triangleright \Delta_2 \twoheadrightarrow E,\Gamma \vdash P_2''' \mid T\langle N, s[\mathrm{p}][\mathrm{q}]!\langle v\rangle \cdot \vec{\ell_n}\rangle \triangleright \Delta_2''' \twoheadrightarrow E,\Gamma \vdash P_2'' \mid T'\langle N, \vec{\ell_n}\rangle \triangleright \Delta_2'' \twoheadrightarrow E,\Gamma \vdash P_2' \mid T'\langle N, \vec{\ell_n}\rangle \triangleright \Delta_2'$

□

C.8 Proof for Lemma 4.2

Proof. We prove direction if $\forall E, E,\Gamma \vdash P_1 \triangleright \Delta_1 \approx_g P_2 \triangleright \Delta_2$ then $\Gamma \vdash P_1 \triangleright \Delta_1 \approx^s \Gamma \vdash P_2 \triangleright \Delta_2$. If $\Gamma \vdash P_1 \triangleright \Delta_1 \xrightarrow{\ell} P_1' \triangleright \Delta_1'$ then $P_1 \xrightarrow{\ell} P_1'$ and $(\Gamma,\Delta_1) \xrightarrow{\ell} (\Gamma',\Delta_1')$.

From part 3 of Lemma C.5 we choose E such that $(E,\Gamma,\Delta_1) \xrightarrow{\ell} (E',\Gamma',\Delta_1')$. Since $\forall E, E,\Gamma \vdash P_1 \triangleright \Delta_1 \approx_g P_2 \triangleright \Delta_2$ it can now be implied that, $E,\Gamma \vdash P_1 \triangleright \Delta_1 \xrightarrow{\ell} E',\Gamma \vdash P_1' \triangleright \Delta_1'$ implies, $E,\Gamma \vdash P_2 \triangleright \Delta_2 \stackrel{\ell}{\Longrightarrow} E',\Gamma \vdash P_2' \triangleright \Delta_2'$ implies, $P_2 \stackrel{\ell}{\Longrightarrow} P_2'$ and $(E,\Gamma,\Delta_2) \stackrel{\ell}{\Longrightarrow} (E',\Gamma',\Delta_2')$.
From part 1 of Lemma C.5 we get $(\Gamma,\Delta_2) \stackrel{\ell}{\Longrightarrow} (\Gamma',\Delta_2')$ implies $\Gamma \vdash P_2 \triangleright \Delta_2 \stackrel{\ell}{\Longrightarrow} P_2' \triangleright \Delta_2'$ as required.

We prove direction if $\Gamma \vdash P_1 \triangleright \Delta_1 \approx^s \Gamma \vdash P_2 \triangleright \Delta_2$ then $\forall E, E,\Gamma \vdash P_1 \triangleright \Delta_1 \approx_g P_2 \triangleright \Delta_2$. Let $E,\Gamma \vdash P_1 \triangleright \Delta_1 \xrightarrow{\ell} P_1' \triangleright \Delta_1'$ then

$$P_1 \xrightarrow{\ell} P_1' \tag{30}$$
$$(E,\Gamma,\Delta_1) \xrightarrow{\ell} (E',\Gamma',\Delta_1') \tag{31}$$

If $\Gamma \vdash P_1 \triangleright \Delta_1 \xrightarrow{\ell} P_1' \triangleright \Delta_1'$ then $P_1 \xrightarrow{\ell} P_1', (\Gamma,\Delta_1) \xrightarrow{\ell} (\Gamma',\Delta_1'), \Gamma \vdash P_2 \triangleright \Delta_2 \xrightarrow{\ell} P_2' \triangleright \Delta_2'$
From the last implication we get

$$P_2 \stackrel{\ell}{\Longrightarrow} P_2' \tag{32}$$
$$(\Gamma,\Delta_2) \stackrel{\ell}{\Longrightarrow} (\Gamma',\Delta_2') \tag{33}$$
$$\Delta_1 \rightleftharpoons \Delta_2 \tag{34}$$

We apply part 2 of Lemma C.5 to 31 and 34 to get $(E,\Gamma,\Delta_2) \stackrel{\ell}{\Longrightarrow} (E',\Gamma',\Delta_2')$. From the last result and 32 we get $E,\Gamma \vdash P_2 \triangleright \Delta_2 \stackrel{\ell}{\Longrightarrow} E',\Gamma \vdash P_2' \triangleright \Delta_2'$.

C.9 Proof for Theorem 4.3

Proof. We follow the requirement of part 3 of Lemma C.5 to show that if P is simple and $\Gamma \vdash P \triangleright \Delta \xrightarrow{\ell} \Gamma \vdash P' \triangleright \Delta'$ then $\exists E \cdot E,\Gamma \vdash P \triangleright \Delta \xrightarrow{\ell} E',\Gamma \vdash P' \triangleright \Delta'$.

From that point on we apply part 2 of Lemma C.5 to get that if P_1, P_2 are simple and $\exists E \cdot E,\Gamma \vdash P_1 \triangleright \Delta_1 \approx_g P_2 \triangleright \Delta_2$ then $\forall E, E,\Gamma \vdash P_1 \triangleright \Delta_1 \approx_g P_2 \triangleright \Delta_2$. By applying Lemma 4.2 we are done. □

D Usecase: UC.R2.13 “Acquire Data From Instrument” from the Ocean Observatories Initiative (OOI) [16]

The governance bisimulation can be used in numerous ways: it can be applied to the optimisation and verification of distributed systems, and the correctness of service communication. In this section, we present a usecase based on the real world usecase UC.R2.13 “Acquire Data From Instrument” from the Ocean Observatories Initiative (OOI) [16], where we intent to show the optimisation and verification of network services.

In this usecase we assume a user program (U) which is connected to the Integrated Observatory Network (ION). The ION provides the interface between users and remote sensing instruments. The user requests, via the ION agent services (A), the acquisition of processed data from an instrument (I). More specifically the user requests from the ION two different formats of the instrument data. In the above usecase we distinguish two points of communication coordination: i) an internal ION multiparty communication and ii) an external communication between ION instruments and agents and the user. In other words it is natural to require the initiation of two multiparty session types to coordinate the services and clients involved in the usecase.

The behaviour of the multiparty session connection between the User (U) and ION is dependent on the implementation and the synchronisation of the internal ION session.

Next we present three possible implementation scenarios and compare their behaviour with respect to the user program. Depending on the ION requirements we can chose the best implementation with the correct behaviour.

D.1 Usecase Scenario 1

In the first scenario the user program (U) wants to acquire the first format of data from the instrument (I) and at the same time acquire the second format of the data from an agent service (A). The communication between the agent (A) and the instrument happens internally in the ION on a separate private session.

- A new session connection s_1 is established between (U), (I) and (A).
- A new session connection s_2 is established between (A) and (I).
- (I) sends raw data through s_2 to (A).
- (A) sends processed data (format 1) through s_1 to (U).
- (A) sends acknowledgement through s_2 to (I).
- (I) sends processed data (format 2) through s_1 to (U).

The above scenario is implemented as follows:

$$I_0 \mid A \mid U$$

where

$$\begin{aligned}
I_0 &= a[\mathtt{i0}](s_1).\overline{b}[\mathtt{i0}](s_2).s_2[\mathtt{i0}][\mathtt{a_1}]!\langle \mathtt{rd}\rangle;s_2[\mathtt{i0}][\mathtt{a_1}]?(x);s_1[\mathtt{i0}][\mathtt{u}]!\langle \mathtt{pd}\rangle;\mathbf{0}\\
A &= a[\mathtt{a_1}](s_1).b[\mathtt{a_1}](s_2).s_2[\mathtt{a_1}][\mathtt{i0}]?(x);s_1[\mathtt{a_1}][\mathtt{u}]!\langle \mathtt{pd}\rangle;s_2[\mathtt{a_1}][\mathtt{i0}]!\langle \mathtt{ack}\rangle;\mathbf{0}\\
U &= \overline{a}[\mathtt{u}](s_1).s_1[\mathtt{u}][\mathtt{a_1}]?(x);s_1[\mathtt{u}][\mathtt{i0}]?(y);\mathbf{0}
\end{aligned}$$

and $\mathtt{i}$ is the instrument role, $\mathtt{a_1}$ is the agent role and $\mathtt{u}$ is the user role.

D.2 Usecase scenario 2

Use case scenario 1 implementation requires from the instrument program to process raw data in a particular format (format 2) before sending them to the user program. In a more modular and fine-grain implementation, the instrument program should only send raw data to the ION interface for processing and forwarding to the user. A separate session between the instrument and the ION interface and a separate session between the ION interface and the user make a distinction into different logical and processing levels.

To capture the above implementation we assume a scenario with the user program ($\mathtt{U}$), the instrument ($\mathtt{I}$) and agents ($\mathtt{A}_1$) and ($\mathtt{A}_2$):

- A new session connection s_1 is established between ($\mathtt{U}$), ($\mathtt{A}_1$) and ($\mathtt{A}_2$).
- A new session connection s_2 is established between ($\mathtt{A}_1$, $\mathtt{A}_2$) and ($\mathtt{I}$).
- ($\mathtt{I}$) sends raw data through s_2 to ($\mathtt{A}_1$).
- ($\mathtt{A}_1$) sends processed data (format 1) through s_1 to ($\mathtt{U}$).
- ($\mathtt{A}_1$) sends acknowledgement through s_2 to ($\mathtt{I}$).
- ($\mathtt{I}$) sends raw data through s_2 to ($\mathtt{A}_2$).
- ($\mathtt{A}_2$) sends processed data (format 2) through s_1 to ($\mathtt{U}$).
- ($\mathtt{A}_2$) sends acknowledgement through s_2 to ($\mathtt{I}$).

The above scenario is implemented as follows:

$$I_1 \mid A_1 \mid A_2 \mid U$$

where

$$\begin{aligned}
I_1 &= \overline{b}[\mathtt{i}](s_2).s_2[\mathtt{i}][\mathtt{a}_1]!\langle\mathtt{rd}\rangle;s_2[\mathtt{i}][\mathtt{a}_1]?(x);s_2[\mathtt{i}][\mathtt{a}_2]!\langle\mathtt{rd}\rangle;s_2[\mathtt{i}][\mathtt{a}_1]?(x);\mathbf{0}\\
A_1 &= a[\mathtt{a}_1](s_1).b[\mathtt{a}_1](s_2).s_2[\mathtt{a}_1][\mathtt{i}]?(x);s_1[\mathtt{a}_1][\mathtt{u}]!\langle\mathtt{pd}\rangle;s_2[\mathtt{a}_1][\mathtt{i}]!\langle\mathtt{ack}\rangle;\mathbf{0}\\
A_2 &= a[\mathtt{a}_2](s_1).b[\mathtt{a}_2](s_2).s_2[\mathtt{a}_2][\mathtt{i}]?(x);s_1[\mathtt{a}_2][\mathtt{u}]!\langle\mathtt{pd}\rangle;s_2[\mathtt{a}_2][\mathtt{i}]!\langle\mathtt{ack}\rangle;\mathbf{0}\\
U &= \overline{a}[\mathtt{u}](s_1).s_1[\mathtt{u}][\mathtt{a}_1]?(x);s_1[\mathtt{u}][\mathtt{a}_2]?(y);\mathbf{0}
\end{aligned}$$

and $\mathtt{i}$ is the instrument role, $\mathtt{a}_1$ and $\mathtt{a}_2$ are the agent roles and $\mathtt{u}$ is the user role. Furthermore for session s_1 we have that role $\mathtt{i0}$ (from scenario 1) $= \mathtt{a}_2$, since we want to maintain the session s_1 as it is defined in the scenario 1.

D.3 Usecase scenario 3

A step further is to enhance the performance of usecase scenario 2 if the instrument ($\mathtt{I}$) code in usecase scenario 2 can have a different implementation, where raw data are sent to both agents ($\mathtt{A}_1$, $\mathtt{A}_2$) before any acknowledgement is received. ION agents can process data in parallel resulting in an optimised implementation.

- A new session connection s_1 is established between ($\mathtt{U}$), ($\mathtt{A}_1$) and ($\mathtt{A}_2$).
- A new session connection s_2 is established between ($\mathtt{A}_1$, $\mathtt{A}_2$) and ($\mathtt{I}$).
- ($\mathtt{I}$) sends raw data through s_2 to ($\mathtt{A}_1$).
- ($\mathtt{I}$) sends raw data through s_2 to ($\mathtt{A}_2$).
- ($\mathtt{A}_1$) sends processed data (format 1) through s_1 to ($\mathtt{U}$).
- ($\mathtt{A}_1$) sends acknowledgement through s_2 to ($\mathtt{I}$).

- $(\mathtt{A}_2)$ sends processed data (format 2) through s_1 to $(\mathtt{U})$.
- $(\mathtt{A}_2)$ sends acknowledgement through s_2 to $(\mathtt{I})$.
- A new session connection s_1 is established between $(\mathtt{U})$, $(\mathtt{A}_1)$ and $(\mathtt{A}_2)$.

The process is now refined as

$$I_2 \mid A_1 \mid A_2 \mid U$$

where

$$I_2 = \overline{b}[\mathtt{i}](s_2).s_2[\mathtt{i}][\mathtt{a}_1]!\langle\mathtt{rd}\rangle;s_2[\mathtt{i}][\mathtt{a}_2]!\langle\mathtt{rd}\rangle;s_2[\mathtt{i}][\mathtt{a}_1]?(x);s_2[\mathtt{i}][\mathtt{a}_1]?(x);\mathbf{0}$$

and $\mathtt{i}$ implements the instrument role, $\mathtt{a}_1$ and $\mathtt{a}_2$ are the agent roles and $\mathtt{u}$ is the user role.

D.4 Bisimulations

The main concern of the three scenarios is to implement the Integrated Ocean Network interface respecting the multiparty communication protocols.

Having the user process as the observer we can see that typed processes:

$$\Gamma \vdash I_0 \mid A \triangleright \Delta_0$$
$$\Gamma \vdash I_1 \mid A_1 \mid A_2 \triangleright \Delta_1$$

are bisimilar (using $\approx^s$) since in both process we observe the following labelled transitions (recall that $\mathtt{i0} = \mathtt{a}_2$) :

$$\Gamma \vdash I_0 \mid A \triangleright \Delta_0 \xrightarrow{\tau} \xrightarrow{a[s](\mathtt{a}_1,\mathtt{i0})} \xrightarrow{s_1[\mathtt{a}_1][\mathtt{u}]!\langle\mathtt{pd}\rangle} \xrightarrow{s_1[\mathtt{i0}][\mathtt{u}]!\langle\mathtt{pd}\rangle}$$

and

$$\Gamma \vdash I_1 \mid A_1 \mid A_2 \triangleright \Delta_1 \xrightarrow{\tau} \xrightarrow{a[s](\mathtt{a}_1,\mathtt{a}_2)} \xrightarrow{s_1[\mathtt{a}_1][\mathtt{u}]!\langle\mathtt{pd}\rangle} \xrightarrow{s_1[\mathtt{a}_2][\mathtt{u}]!\langle\mathtt{pd}\rangle}$$

The two implementations (scenario 1 and scenario 2) are completely interchangeable with respect to $\approx^s$.

If we proceed with the case of the scenario 3 we can see that typed process $\Gamma \vdash I_2 \mid A_1 \mid A_2 \triangleright \Delta_2$ cannot be simulated (using $\approx^s$) by scenarios 1 and 2, since we can observe the execution:

$$\Gamma \vdash I_1 \mid A_1 \mid A_2 \triangleright \Delta_1 \xrightarrow{\tau} \xrightarrow{a[s](\mathtt{a}_1,\mathtt{a}_2)} \xrightarrow{s_1[\mathtt{a}_2][\mathtt{u}]!\langle\mathtt{pd}\rangle}$$

By changing the communication ordering in the ION private session s_2 we changed the communication behaviour on the external session channel s_1. Nevertheless, the communication behaviour remains the same if we take into account the global multiparty protocol of s_1 and the way it governs the behaviour of the three usecase scenarios.

Hence we use $\approx^s_g$. The definition of the global environment is as follows:

$$E = s_1 : \mathtt{a}_1 \to \mathtt{u} : \langle\mathtt{PD}\rangle.\mathtt{a}_2 \to \mathtt{u} : \langle\mathtt{PD}\rangle.$$

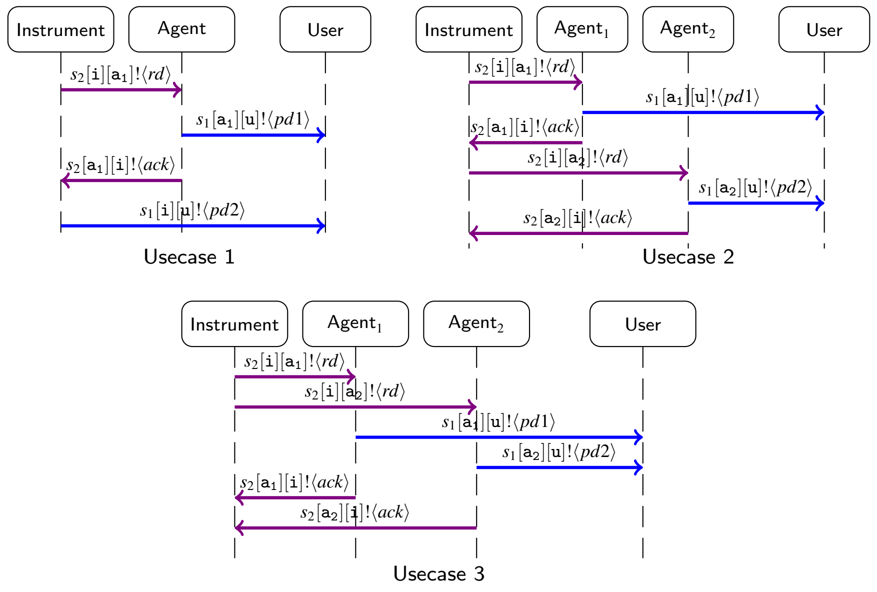
Instrument
Agent
User
$s_2[\mathtt{i}][\mathtt{a}_1]!\langle rd\rangle$
$s_1[\mathtt{a}_1][\mathtt{u}]!\langle pd1\rangle$
$s_2[\mathtt{a}_1][\mathtt{i}]!\langle ack\rangle$
$s_1[\mathtt{i}][\mathtt{u}]!\langle pd2\rangle$
Usecase 1
Instrument
Agent$_1$
Agent$_2$
User
$s_2[\mathtt{i}][\mathtt{a}_1]!\langle rd\rangle$
$s_1[\mathtt{a}_1][\mathtt{u}]!\langle pd1\rangle$
$s_2[\mathtt{a}_1][\mathtt{i}]!\langle ack\rangle$
$s_2[\mathtt{i}][\mathtt{a}_2]!\langle rd\rangle$
$s_1[\mathtt{a}_2][\mathtt{u}]!\langle pd2\rangle$
$s_2[\mathtt{a}_2][\mathtt{i}]!\langle ack\rangle$
Usecase 2
Instrument
Agent$_1$
Agent$_2$
User
$s_2[\mathtt{i}][\mathtt{a}_1]!\langle rd\rangle$
$s_2[\mathtt{i}][\mathtt{a}_2]!\langle rd\rangle$
$s_1[\mathtt{a}_1][\mathtt{u}]!\langle pd1\rangle$
$s_1[\mathtt{a}_2][\mathtt{u}]!\langle pd2\rangle$
$s_2[\mathtt{a}_1][\mathtt{i}]!\langle ack\rangle$
$s_2[\mathtt{a}_2][\mathtt{i}]!\langle ack\rangle$
Usecase 3

Fig. 10. Three usecases from UC.R2.13 "Acquire Data From Instrument" in [16]

The global protocol governs processes $I_1 \mid A_1 \mid A_2$ (similarly $I_0 \mid A$) and $I_2 \mid A_1 \mid A_2$ to always observe action $\xrightarrow{s_1[\mathtt{a}_2][\mathtt{u}]!\langle \mathtt{pd}\rangle}$ after action $\xrightarrow{s_1[\mathtt{a}_1][\mathtt{u}]!\langle \mathtt{pd}\rangle}$ for both processes.

Also note that the global protocol for s_2 is not present in the global environment, because s_2 is restricted. The specification and implementation of session s_2 are abstracted from the behaviour of session s_1.

E Concluding remarks

The bisimulation techniques developed in this paper present interests in both the theoretical and the applied aspects. We developed semantics for typed environments and use them to define labelled transition semantics for typed processes. We show that session type bisimulations can be defined, either by taking only the local session information of each process into account ($\approx^s$) or by taking the global session protocols into account ($\approx^s_g$). We show that the corresponding bisimulations are reduction-closed, barb preserving congruences. Theorem 4.2 shows the relation between the two typed bisimulation approaches: if two terms are equivalent by the governed bisimulation $\approx^s_g$ under all governed environments, then they are also bisimilar by $\approx^s$.

Our bisimulation techniques can also be used for proving correctness of the global optimisations and verifications of systems. Usually systems based on services are implemented using different levels of abstractions, and thus use a set of multiparty protocols, one for each level of abstraction. A possible change on the implementation of a service level may lead to the change of the entire system behaviour (see Appendix D for a detailed example). Our techniques are used to reason about the correctness of the optimisation in such systems since the governed bisimulation can take the global overview of the systems into account.