Formally Verified Liveness with Synchronous Multiparty Session Types in Rocq

Anonymous author
Anonymous affiliation

Anonymous author
Anonymous affiliation

Abstract

Multiparty session types (MPST) offer a framework for the description of communication-based protocols involving multiple participants. In the *top-down* approach to MPST, the communication pattern of the session is described using a *global type*. Then the global type is *projected* on to a *local type* for each participant, and the individual processes making up the session are type-checked against these projections. Typed sessions possess certain desirable properties such as *safety*, *deadlock-freedom* and *liveness* (also called *lock-freedom*).

In this work, we present the first mechanised proof of liveness for synchronous multiparty session types in the Rocq Proof Assistant. Building on recent work, we represent global and local types as coinductive trees using the paco library. We use a coinductively defined *subtyping* relation on local types together with another coinductively defined *plain-merge* projection relation relating local and global types . We then *associate* collections of local types, or *local type contexts*, with global types using this projection and subtyping relations, and prove an *operational correspondence* between a local type context and its associated global type. We then utilize this association relation to prove the safety and liveness of associated local type contexts and, consequently, the multiparty sessions typed by these contexts.

Besides clarifying the often informal proofs of liveness found in the MPST literature, our Rocq mechanisation also enables the certification of lock-freedom properties of communication protocols. Our contribution amounts to around 12K lines of Rocq code.

2012 ACM Subject Classification Replace ccsdesc macro with valid one

Keywords and phrases Dummy keyword

Digital Object Identifier 10.4230/LIPIcs.CVIT.2016.23

Acknowledgements Anonymous acknowledgements

1 Introduction

Multiparty session types [19] provide a type discipline for the correct-by-construction specification of message-passing protocols. Desirable protocol properties guaranteed by session types include *safety* (the labels and types of senders' payloads cohere with the capabilities of the receivers), *deadlock-freedom* (also called *progress* or *non-stuck property* [14]) (it is possible for the session to progress so long as it has at least one active participant), and *liveness* (also called *lock-freedom* [41] or *starvation-freedom* [8]) (if a process is waiting to send and receive then a communication involving it eventually happens).

There exists two common methodologies for multiparty session types. In the *bottom-up* approach, the individual processes making up the session are typed using a collection of *participants* and *local types*, that is, a *local type context*, and the properties of the session is examined by model-checking this local type context. Contrastingly, in the *top-down* approach sessions are typed by a *global type* that is related to the processes using endpoint *projections* and *subtyping*. The structure of the global type ensures that the desired properties are satisfied by the session. These two approaches have their advantages and disadvantages:

$$\begin{tikzcd}
\mathsf{G} \arrow[rr, dotted, "\rightarrow"] \arrow[d, dotted, "\upharpoonright"] \arrow[dr, "\sqsubseteq"] & & \mathsf{G}' \arrow[d, "\sqsubseteq"] \\
\mathsf{T} \arrow[r] \arrow[d, dotted, "\vdash_{\mathsf{P}}"] & \{(p_i, T_i) \mid i \in I\} = \Gamma \arrow[r, "\rightarrow"] \arrow[d, "\vdash_{\mathcal{M}}"] & \Gamma' \arrow[d, "\vdash_{M}"] \\
\mathsf{P} \arrow[r] & \prod_i \mathsf{p}_i \triangleleft \mathsf{P}_i = \mathcal{M} \arrow[r, "\rightarrow"] & \mathcal{M}'
\end{tikzcd}$$

Figure 1 Design overview. The dotted lines correspond to relations inherited from [14] while the solid lines denote relations that are new, or substantially rewritten, in this paper.

the bottom-up approach is generally able to type more sessions, while type-checking and type-inferring in the top-down approach tend to be more efficient than model-checking the bottom-up system [40].

In this work, we present the Rocq [4] formalisation of a synchronous MPST that that ensures the aforementioned properties for typed sessions. Our type system uses an *association* relation ($\sqsubseteq$) [44, 32] defined using (coinductive plain) projection [38] and subtyping, in order to relate local type contexts and global types. This association relation ensures *operational correspondence* between the labelled transition system (LTS) semantics we define for local type contexts and global types. We then type ($\vdash_{\mathcal{M}}$) sessions using local type contexts that are associated with global types, which ensure that the local type context, and hence the session, is well-behaved in some sense. Whenever an associated local type context Γ types a session $\mathcal{M}$, our type system guarantees the following properties:

1. **Subject Reduction** (Theorem 6.2): If $\mathcal{M}$ can progress into $\mathcal{M}'$, then Γ can progress into Γ' such that Γ' types $\mathcal{M}'$.
2. **Session Fidelity** (Theorem 6.5): If Γ can progress into Γ', then $\mathcal{M}$ can progress into $\mathcal{M}'$ such that $\mathcal{M}'$ is typable by Γ'.
3. **Safety** (Theorem 6.7): If $\mathcal{M}$ can progress into $\mathcal{M}'$ by one or more communications, participant p in $\mathcal{M}'$ sends to participant q and q receives from p, then the labels of p and q cohere.
4. **Deadlock-Freedom** (Theorem 6.4): Either every participant in $\mathcal{M}$ has terminated, or $\mathcal{M}$ can progress.
5. **Liveness** (Theorem 6.11): If participant p attemps to communicate with participant q in $\mathcal{M}$, then $\mathcal{M}$ can progress (in possibly multiple steps) into a session $\mathcal{M}'$ where that communication has occured.

To our knowledge, this work presents the first mechanisation of liveness for multiparty session types in a proof assistant.

Our Rocq implementation builds upon the recent formalisation of subject reduction for MPST by Ekici et. al. [14], which itself is based on [17]. The methodology in [14] takes an equirecursive approach where an inductive syntactic global or local type is identified with the coinductive tree obtained by fully unfolding the recursion. It then defines a coinductive projection relation between global and local type trees, the LTS semantics for global type trees, and typing rules for the session calculus outlined in [17]. We extensively use these definitions and the lemmas concerning them, but we still depart from and extend [14] in numerous ways by introducing local typing contexts, their correspondence with global types and a new typing relation. Our addition to the code amounts to around 12K lines of Rocq code.

As with [14], our implementation heavily uses the parameterized coinduction technique of the paco [20] library. Namely, our liveness property is defined using possibly infinite *execution traces* which we represent as coinductive streams. The relevant predicates on these traces, such as fairness, are then defined using linear temporal logic (LTL)[33]. The LTL modalities eventually ($\diamond$) and always ($\Box$) can be expressed as least and greatest fixpoints respectively using expansion laws. This allows us to represent the properties that use these modalities as inductive and coinductive predicates in Rocq. This approach, together with the proof techniques provided by paco, results in compositional and clear proofs.

Outline. In Section 2 we define our session calculus and its LTS semantics. In Section 3 we introduce local and global type trees. In Section 4 we give LTS semantics to local type contexts and global types, and detail the association relation between them. In Section 5 we define safety and liveness for local type contexts, and prove that they hold for contexts associated with a global type tree. In Section 6 we give the typing rules for our session calculus, and prove the desired properties of these typable sessions.

2 The Session Calculus

We introduce the simple synchronous session calculus that our type system will be used on.

2.1 Processes and Sessions

▶ **Definition 2.1** (Expressions and Processes). *We define processes as follows:*

$$\mathsf{P} ::= \mathsf{p}!\ell(\mathsf{e}).\mathsf{P} \;\mid\; \sum_{i\in I} \mathsf{p}?\ell_i(x_i).\mathsf{P}_i \;\mid\; \text{if e then P else P} \;\mid\; \mu \boldsymbol{X}.\mathsf{P} \;\mid\; \boldsymbol{X} \;\mid\; \boldsymbol{0}$$

where e *is an expression that can be a variable, a value such as* **true**, 0 *or* -3, *or a term built from expressions by applying the operators* **succ**, **neg**, $\neg$, *non-deterministic choice* $\oplus$ *and* $>$.

$\mathsf{p}!\ell(\mathsf{e}).\mathsf{P}$ is a process that sends the value of expression e with label ℓ to participant p, and continues with process P. $\sum_{i\in I} \mathsf{p}?\ell_i(x_i).\mathsf{P}_i$ is a process that may receive a value from p with any label ℓ_i where $i \in I$, binding the result to x_i and continuing with P_i, depending on which ℓ_i the value was received from. $\mathbf{X}$ is a recursion variable, $\mu\mathbf{X}.\mathsf{P}$ is a recursive process, if e then P else P is a conditional and $\mathbf{0}$ is a terminated process.

Processes can be composed in parallel into sessions.

▶ **Definition 2.2** (Multiparty Sessions). *Multiparty sessions are defined as follows.*

$$\mathcal{M} \;::=\; \mathsf{p} \triangleleft \mathsf{P} \quad\mid\quad (\mathcal{M} \mid \mathcal{M}) \quad\mid\quad \mathcal{O}$$

$\mathsf{p} \triangleleft \mathsf{P}$ denotes that participant p is running the process P, $\mid$ indicates parallel compositon. We write $\prod_{i\in I} \mathsf{p}_i \triangleleft \mathsf{P}_i$ to denote the session formed by p_i running P_i in parallel for all $i \in I$. $\mathcal{O}$ is an empty session with no participants, that is, the unit of parallel composition. In Rocq processes and sessions are defined with the inductive types `process` and `session`.

```
Inductive process : Type ≜
  | p_send : part → label → expr → process →
      process
  | p_recv : part → list(option process) → process
  | p_ite : expr → process → process → process
  | p_rec : process → process
  | p_var : nat → process
  | p_inact : process.
```

```
Inductive session: Type ≜
  | s_ind : part   → process → session
  | s_par : session → session → session
  | s_zero : session.
Notation "p '←−' P"  ≜  (s_ind p P) (at level 50, no
    associativity).
Notation "s1 '|||' s2" ≜  (s_par s1 s2) (at level 50, no
    associativity).
```

2.2 Structural Congruence and Operational Semantics

We define a structural congruence relation $\equiv$ on sessions which expresses the commutativity, associativity and unit of the parallel composition operator.

$$\frac{}{\mathsf{p} \triangleleft \mathsf{P} \mid \mathsf{q} \triangleleft \mathsf{Q} \equiv \mathsf{q} \triangleleft \mathsf{Q} \mid \mathsf{p} \triangleleft \mathsf{P}}\ [\textsc{sc-sym}] \qquad \frac{}{(\mathsf{p} \triangleleft \mathsf{P} \mid \mathsf{q} \triangleleft \mathsf{Q}) \mid \mathsf{r} \triangleleft \mathsf{R} \equiv \mathsf{p} \triangleleft \mathsf{P} \mid (\mathsf{q} \triangleleft \mathsf{Q} \mid \mathsf{r} \triangleleft \mathsf{R})}\ [\textsc{sc-assoc}]$$

$$\frac{}{\mathsf{p} \triangleleft \mathsf{P} \mid \mathcal{O} \equiv \mathsf{p} \triangleleft \mathsf{P}}\ [\textsc{sc-o}]$$

Table 1 Structural Congruence over Sessions

We now give the operational semantics for sessions by the means of a labelled transition system. We use labelled *reactive* semantics [41, 6] which doesn't contain explicit silent τ actions for internal reductions (that is, evaluation of if expressions and unfolding of recursion) while still considering β reductions up to those internal reductions by using an unfolding relation. This stands in contrast to the more standard semantics used in [14, 17, 41]. For the advantages of our approach see Remark 6.3.

In reactive semantics silent transitions are captured by an *unfolding* relation ($\Rrightarrow$), and β reductions are defined up to this unfolding (Table 2).

$$[\textsc{Unf-struct}]\ \frac{\mathcal{M} \equiv \mathcal{N}}{\mathcal{M} \Rrightarrow \mathcal{N}} \qquad [\textsc{Unf-rec}]\ \mathsf{p} \triangleleft \mu\mathbf{X}.\mathsf{P} \mid \mathcal{N} \ \Rrightarrow \mathsf{p} \triangleleft \mathsf{P}[\mu\mathbf{X}.\mathsf{P}/\mathbf{X}] \mid \mathcal{N} \qquad [\textsc{Unf-condt}]\ \frac{e \downarrow \mathsf{true}}{\mathsf{p} \triangleleft \ \mathsf{if}\ e\ \mathsf{then}\ \mathsf{P}\ \mathsf{else}\ \mathsf{Q} \mid \mathcal{N} \ \Rrightarrow \ \mathsf{p} \triangleleft \mathsf{P} \mid \mathcal{N}}$$

$$[\textsc{Unf-condf}]\ \frac{e \downarrow \mathsf{false}}{\mathsf{p} \triangleleft \ \mathsf{if}\ e\ \mathsf{then}\ \mathsf{P}\ \mathsf{else}\ \mathsf{Q} \mid \mathcal{N} \ \Rrightarrow \ \mathsf{p} \triangleleft \mathsf{Q} \mid \mathcal{N}} \qquad [\textsc{Unf-trans}]\ \frac{\mathcal{M} \Rrightarrow \mathcal{M}' \quad \mathcal{M}' \Rrightarrow \mathcal{N}}{\mathcal{M} \Rrightarrow \mathcal{N}}$$

Table 2 Unfolding of Sessions

$\mathcal{M} \Rrightarrow \mathcal{N}$ means that $\mathcal{M}$ can transition to $\mathcal{N}$ through some internal actions, that is, a reduction that doesn't involve a communication. We say that $\mathcal{M}$ *unfolds* to $\mathcal{N}$. In Rocq it's captured by the predicate `unfoldP : session → session → Prop`.

$$[\textsc{R-comm}]\ \frac{j \in I \quad e \downarrow v}{\mathsf{p} \triangleleft \sum_{i \in I} \mathsf{q}?\ell_i(x_i).\mathsf{P}_i \mid \mathsf{q} \triangleleft \mathsf{p}!\ell_j(\mathsf{e}).\mathsf{Q} \mid \mathcal{N} \xrightarrow{(\mathsf{p},\mathsf{q})\ell_j} \mathsf{p} \triangleleft \mathsf{P}_j[v/x_j] \mid \mathsf{q} \triangleleft \mathsf{Q} \mid \mathcal{N}}$$

$$[\textsc{R-unfold}]\ \frac{\mathcal{M} \Rrightarrow \mathcal{M}' \quad \mathcal{M}' \xrightarrow{\lambda} \mathcal{N}' \quad \mathcal{N}' \Rrightarrow \mathcal{N}}{\mathcal{M} \xrightarrow{\lambda} \mathcal{N}}$$

Table 3 Reactive Semantics of Sessions

Table 3 illustrates the rules for communicating transitons. [R-comm] captures communications between processes, and [R-unfold] lets us consider reductions up to unfoldings.

In Rocq, `betaP_lbl M lambda M'` denotes $\mathcal{M} \xrightarrow{\lambda} \mathcal{M}'$. We write $\mathcal{M} \to \mathcal{M}'$ if $\mathcal{M} \xrightarrow{\lambda} \mathcal{M}'$ for some λ, which is written `betaP M M'` in Rocq. We write $\to^*$ to denote the reflexive transitive closure of $\to$, which is called `betaRtc` in Rocq.

3 The Type System

We briefly recap the core definitions of local and global type trees, subtyping and projection from [17]. We take an equirecursive approach and work directly on the possibly infinite local and global type trees obtained by unfolding the recursion in guarded syntactic types, details of this approach can be found in [14] and hence are omitted here.

3.1 Local Type Trees

We start by defining the sorts that will be used to type expressions, and local types that will be used to type single processes.

▶ **Definition 3.1** (Sorts). *Sorts are defined as follows:*

$$S ::= \quad \texttt{int} \mid \texttt{bool} \mid \texttt{nat}$$

```
Inductive sort: Type ≜
  | sbool: sort
  | sint : sort
  | snat : sort.
```

▶ **Definition 3.2.** *Local type trees are defined coinductively with the following syntax:*

$$\begin{aligned} \mathsf{T} ::= \quad & \mathsf{end} \\ \mid \quad & \mathsf{p}\&\{\ell_i(S_i).\mathsf{T}_i\}_{i\in I} \\ \mid \quad & \mathsf{p}\oplus\{\ell_i(S_i).\mathsf{T}_i\}_{i\in I} \end{aligned}$$

```
CoInductive ltt: Type ≜
 | ltt_end : ltt
 | ltt_recv: part → list (option(sort*ltt)) → ltt
 | ltt_send: part → list (option(sort*ltt)) → ltt.
```

In the above definition, `end` represents a role that has finished communicating. $\mathsf{p}\oplus\{\ell_i(S_i).\mathbb{T}_i\}_{i\in I}$ denotes a role that may, from any $i \in I$, receive a value of sort S_i with message label ℓ_i and continue with $\mathbb{T}_i$. Similarly, $\mathsf{p}\&\{\ell_i(S_i).\mathbb{T}_i\}_{i\in I}$ represents a role that may choose to send a value of sort S_i with message label ℓ_i and continue with $\mathbb{T}_i$ for any $i \in I$.

In Rocq we represent the continuations using a `list` of `option` types. In a continuation `gcs : list (option(sort*ltt))`, index `k` (using zero-indexing) being equal to `Some (s_k, T_k)` means that $\ell_k(S_k).\mathsf{T}_k$ is available in the continuation. Similarly index `k` being equal to `None` or being out of bounds of the list means that the message label ℓ_k is not present in the continuation.

▶ Remark 3.3. Note that Rocq allows us to create types such as `ltt_send q []` which don't correspond to well-formed local types as the continuation is empty. In our implementation we define a predicate `wfltt : ltt → Prop` capturing that all the continuations in the local type tree are non-empty. Henceforth we assume that all local types we mention satisfy this property.

3.2 Subtyping

We define the subsorting relation on sorts and the subtyping relation on local type trees.

▶ **Definition 3.4** (Subsorting and Subtyping). *Subsorting* $\leq$ *is the least reflexive binary relation that satisfies* `nat` $\leq$ `int`. *Subtyping* $\leqslant$ *is the largest relation between local type trees* *coinductively defined by the following rules:*

$$\frac{}{\mathsf{end} \leqslant \mathsf{end}}\ [\textsc{sub-end}] \qquad \frac{\forall i \in I: \quad S_i' \leq S_i \quad \mathsf{T}_i \leqslant \mathsf{T}_i'}{\mathsf{p}\&\{\ell_i(S_i).\mathsf{T}_i\}_{i\in I\cup J} \leqslant \mathsf{p}\&\{\ell_i(S_i').\mathsf{T}_i'\}_{i\in I}}\ [\textsc{sub-in}]$$

$$\frac{\forall i \in I: \quad S_i \leq S_i' \quad \mathsf{T}_i \leqslant \mathsf{T}_i'}{\mathsf{p}\oplus\{\ell_i(S_i).\mathsf{T}_i\}_{i\in I} \leqslant \mathsf{p}\oplus\{\ell_i(S_i').\mathsf{T}_i'\}_{i\in I\cup J}}\ [\textsc{sub-out}]$$

Intutively, $\mathsf{T}_1 \leqslant \mathsf{T}_2$ means that a role of type T_1 can be supplied anywhere a role of type T_2 is needed. [sub-in] captures the fact that we can supply a role that is able to receive more labels than specified, and [sub-out] captures that we can supply a role that has fewer labels available to send. Note the contraviance of the sorts in [sub-in], if the supertype demands the ability to receive an `nat` then the subtype can receive `nat` or `int`.

In Rocq, the subtyping relation `subtypeC : ltt → ltt → Prop` is expressed as a greatest fixpoint using the `Paco` library [20], for details of we refer to [17].

3.3 Global Types and Type Trees

While local types specify the behaviour of one role in a protocol, global types give a bird's eye view of the whole protocol.

▶ **Definition 3.5** (Global type). *We define global types inductively as follows:*

$$\mathbb{G} ::= \quad \mathsf{end} \ \mid\ \mathsf{p} \to \mathsf{q} : \{\ell_i(S_i).\mathbb{G}_i\}_{i\in I} \ \mid\ \boldsymbol{t} \ \mid\ \mu\boldsymbol{t}.\mathbb{G}$$

We further inductively define the function $\mathtt{pt}(\mathbb{G})$ *that denotes the participants of type* $\mathbb{G}$*:*

$$\mathtt{pt}(\mathsf{end}) = \mathtt{pt}(\boldsymbol{t}) = \emptyset$$

$$\mathtt{pt}(\mathsf{p} \to \mathsf{q} : \{\ell_i(S_i).\mathbb{G}_i\}_{i\in I}) = \{\mathsf{p},\mathsf{q}\} \cup \bigcup_{i\in I} \mathtt{pt}(\mathbb{G}_i)$$

$$\mathtt{pt}(\mu\boldsymbol{T}.\mathbb{G}) = \mathtt{pt}(\mathbb{G})$$

end denotes a protocol that has ended, $\mathsf{p} \to \mathsf{q} : \{\ell_i(S_i).\mathbb{G}_i\}_{i\in I}$ denotes a protocol where for any $i \in I$, participant p may send a value of sort S_i to another participant q via message label ℓ_i, after which the protocol continues as $\mathbb{G}_i$.

As in the case of local types, we adopt an equirecursive approach and work exclusively on possibly infinite global type trees.

▶ **Definition 3.6** (Global type trees). *We define global type trees coinductively as follows:*

$$\mathsf{G} ::= \quad \mathsf{end} \ \mid\ \mathsf{p} \to \mathsf{q} : \{\ell_i(S_i).\mathsf{G}_i\}_{i\in I}$$

```
CoInductive gtt: Type ≜
| gtt_end    : gtt
| gtt_send   : part → part → list (option (sort*gtt)) →
    gtt.
```

We extend the function `pt` onto trees by defining $\mathtt{pt}(\mathsf{G}) = \mathtt{pt}(\mathbb{G})$ where the global type $\mathbb{G}$ corresponds to the global type tree G. Technical details of this definition such as well-definedness can be found in [14, 17].

In Rocq `pt` is captured with the predicate `isgPartsC : part → gtt → Prop`, where `isgPartsC p G` denotes $\mathsf{p} \in \mathtt{pt}(\mathsf{G})$.

3.4 Projection

We now define coinductive projections with plain merging (see [40] for a survey of other notions of merge).

▶ **Definition 3.7** (Projection). *The projection of a global type tree onto a participant* r *is the largest relation* $\upharpoonright_{\mathsf{r}}$ *between global type trees and local type trees such that, whenever* $\mathsf{G} \upharpoonright_{\mathsf{r}} \mathsf{T}$*:*

- $\mathsf{r} \notin \mathsf{pt}\{\mathsf{G}\}$ *implies* $\mathsf{T} = \mathsf{end}$*;* [Proj-End]
- $\mathsf{G} = \mathsf{p} \to \mathsf{r} : \{\ell_i(S_i).\mathsf{G}_i\}_{i \in I}$ *implies* $\mathsf{T} = \mathsf{p}\&\{\ell_i(S_i).\mathsf{T}_i\}_{i \in I}$ *and* $\forall i \in I, \mathsf{G} \upharpoonright_{\mathsf{r}} \mathsf{T}_i$ [Proj-In]
- $\mathsf{G} = \mathsf{r} \to \mathsf{q} : \{\ell_i(S_i).\mathsf{G}_i\}_{i \in I}$ *implies* $\mathsf{T} = \mathsf{q}\oplus\{\ell_i(S_i).\mathsf{T}_i\}_{i \in I}$ *and* $\forall i \in I, \mathsf{G} \upharpoonright_{\mathsf{r}} \mathsf{T}_i$ [Proj-Out]
- $\mathsf{G} = \mathsf{p} \to \mathsf{q} : \{\ell_i(S_i).\mathsf{G}_i\}_{i \in I}$ *and* $\mathsf{r} \notin \{\mathsf{p}, \mathsf{q}\}$ *implies that there are* $\mathsf{T}_i, i \in I$ *such that* $\mathsf{T} = \bigsqcap_{i \in I} \mathsf{T}_i$ *and* $\forall i \in I, \mathsf{G} \upharpoonright_{\mathsf{r}} \mathsf{T}_i$ [Proj-Cont]

where $\bigsqcap$ *is the plain merging operator, defined as*

$$\mathsf{T}_1 \bigsqcap \mathsf{T}_2 = \begin{cases} \mathsf{T}_1 & \text{if } \mathsf{T}_1 = \mathsf{T}_2 \\ \text{undefined} & \text{otherwise} \end{cases}$$

Informally, the projection of a global type tree G onto a participant r extracts a specification for participant r from the protocol whose bird's-eye view is given by G. [Proj-End] expresses that if r is not a participant of G then r does nothing in the protocol. [Proj-In] and [Proj-Out] handle the cases where r is involved in a communication in the root of G. [Proj-Cont] says that, if r is not involved in the root communication of G, then the only way it knows its role in the protocol is if there is a role for it that works no matter what choices p and q make in their communication. This "works no matter the choices of the other participants" property is captured by the merge operations.

In Rocq, projection is defined as a `Paco` greatest fixpoint as the relation `projectionC : gtt → part → ltt → Prop`.

We further have the following fact about projections that lets us regard it as a partial function:

▶ **Lemma 3.8** ([14]). *If* `projectionC G p T` *and* `projectionC G p T'` *then* `T = T'`.

We write $\mathsf{G} \upharpoonright \mathsf{r} = \mathsf{T}$ when $\mathsf{G} \upharpoonright_{\mathsf{r}} \mathsf{T}$. Furthermore we will be frequently be making assertions about subtypes of projections of a global type e.g. $\mathsf{T} \leqslant \mathsf{G} \upharpoonright \mathsf{r}$. In our Rocq implementation we define the predicate `issubProj : ltt → gtt → part → Prop` as a shorthand for this.

3.5 Balancedness, Global Tree Contexts and Grafting

We introduce an important constraint on the types of global type trees we will consider, balancedness.

▶ **Definition 3.9** (Balanced Global Type Trees). *A global tree* G *is balanced if for any subtree* G' *of* G*, there exists* k *such that for all* $\mathsf{p} \in \mathsf{pt}(\mathsf{G}')$*,* p *occurs on every path from the root of* G' *of length at least* k*.*

We omit the technical details of this definition and the Rocq implementation, they can be found in [17] and [14].

Intutively, balancedness is a regularity condition that imposes a notion of *liveness* on the protocol described by the global type tree. Indeed, our liveness results in Section 6 hold only for balanced global types. Another reason for formulating balancedness is that it allows us to use the "grafting" technique, turning proofs by coinduction on infinite trees to proofs by induction on finite global type tree contexts.

▶ **Definition 3.10** (Global Type Tree Context). *Global type tree contexts are defined inductively with the following syntax:*

$$\mathcal{G} ::= \quad \mathsf{p} \to \mathsf{q} : \{\ell_i(S_i).\mathcal{G}_i\}_{i \in I} \;\;\big|\;\; [\;]_i$$

```
Inductive gtth: Type ≜
  | gtth_hol    : fin → gtth
  | gtth_send   : part → part → list (option (sort *
      gtth)) → gtth.
```

We additionally define `pt` *and* `ishParts` *on contexts analogously to* `pt` *and* `isgPartsC` *on trees.*

A global type tree context can be thought of as the finite prefix of a global type tree, where holes $[\;]_i$ indicate the cutoff points. Global type tree contexts are related to global type trees with the grafting operation.

▶ **Definition 3.11** (Grafting). *Given a global type tree context $\mathcal{G}$ whose holes are in the indexing set I and a set of global types $\{\mathsf{G}_i\}_{i \in I}$, the grafting $\mathcal{G}[\mathsf{G}_i]_{i \in I}$ denotes the global type tree obtained by substituting $[\;]_i$ with G_i in $\mathcal{G}$.*

In Rocq the indexed set $\{\mathsf{G}_i\}_{i \in I}$ is represented using a `list (option gtt)`*. Grafting is expressed with the inductive relation* `typ_gtth : list (option gtt) → gtth → gtt → Prop`*.* `typ_gtth gs gcx gt` *means that the grafting of the set of global type trees* `gs` *onto the context* `gcx` *results in the tree* `gt`*.*

Furthermore, we have the following lemma that relates global type tree contexts to balanced global type trees.

▶ **Lemma 3.12** (Proper Grafting Lemma, [14]). *If* `G` *is a balanced global type tree and* `isgPartsC p G`*, then there is a global type tree context* `Gctx` *and an option list of global type trees* `gs` *such that* `typ_gtth gs Gctx G`*,* `~ ishParts p Gctx` *and every* `Some` *element of* `gs` *is of shape* `gtt_end`*,* `gtt_send p q` *or* `gtt_send q p`*.*

3.12 enables us to represent a coinductive global type tree featuring participant `p` as the grafting of a context that doesn't contain `p` with a list of trees that are all of a certain structure. If `typ_gtth gs Gctx G`, `~ ishParts p Gctx` and every `Some` element of `gs` is of shape `gtt_end`, `gtt_send p q` or `gtt_send q p`, then we call the pair `gs` and `Gctx` as the `p`-grafting of `G`, expressed in Rocq as `typ_p_gtth gs Gctx p G`. When we don't care about the contents of `gs` we may just say that `G` is `p`-grafted by `Gctx`.

▶ Remark 3.13. From now on, all the global type trees we will be referring to are assumed to be balanced. When talking about the Rocq implementation, any `G : gtt` we mention is assumed to satisfy the predicate `wfgC G`, expressing that `G` corresponds to some global type and that `G` is balanced. Furthermore, we will often require that a global type is projectable onto all its participants. This is captured by the predicate `projectableA G = ∀ p, ∃ T, projectionC G p T`. As with `wfgC`, we will be assuming that all types we mention are projectable.

4 Semantics of Types

In this section we introduce local type contexts, and define Labelled Transition System semantics on these constructs.

4.1 Typing Contexts

We start by defining typing contexts as finite mappings of participants to local type trees.

▶ **Definition 4.1** (Typing Contexts).

$$\Gamma \ ::= \ \emptyset \ \mid \ \Gamma, \mathsf{p} : \mathsf{T}$$

```
Module M ≜ MMaps.RBT.Make(Nat).

Module MF ≜ MMaps.Facts.Properties Nat M.

Definition tctx: Type ≜ M.t ltt.
```

Intuitively, $\mathsf{p} : \mathsf{T}$ means that participant p is associated with a process that has the type tree T. We write $\mathrm{dom}(\Gamma)$ to denote the set of participants occuring in Γ. We write $\Gamma(\mathsf{p})$ for the type of p in Γ. We define the composition Γ_1, Γ_2 iff $\mathrm{dom}(\Gamma_1) \cap \mathrm{dom}(\Gamma_2) = \emptyset$.

In the Rocq implementation we implement local typing contexts as finite maps of participants, which are represented as natural numbers, and local type trees. We use the red-black tree based finite map implementation of the MMaps library [27].

▶ Remark 4.2. From now on, we assume the all the types in the local type contexts always have non-empty continuations. In Rocq terms, if `T` is in context `gamma` then `wfltt T` holds. This is expressed by the predicate `wfltt: tctx → Prop`.

4.2 Local Type Context Reductions

We now give LTS semantics to local typing contexts, for which we first define the transition labels.

▶ **Definition 4.3** (Transition labels). *A transition label α has the following form:*

$$\begin{array}{lll} \alpha ::= & \mathsf{p} : \mathsf{q} \& \ell(S) & (\mathsf{p} \textit{ receives a value of sort } S \textit{ from } \mathsf{q} \textit{ with message label } \ell) \\ & \mid \ \mathsf{p} : \mathsf{q} \oplus \ell(S) & (\mathsf{p} \textit{ sends a value of sort } S \textit{ to } \mathsf{q} \textit{ with message label } \ell\ ) \\ & \mid \ (\mathsf{p}, \mathsf{q})\ell & (\textit{A synchronized communication from } \mathsf{p} \textit{ to } \mathsf{q} \textit{ occurs via message label } \ell) \end{array}$$

In Rocq they are defined as follows:

```
Notation opt_lbl ≜ nat.
Inductive label: Type ≜
  | lrecv: part → part → option sort → opt_lbl → label
  | lsend: part → part → option sort → opt_lbl → label
  | lcomm: part → part → opt_lbl → label.
```

Next we define labelled transitions for local type contexts.

▶ **Definition 4.4** (Typing context reductions). *The typing context transition $\xrightarrow{\alpha}$ is defined inductively by the following rules:*

$$\frac{k \in I}{\mathsf{p} : \mathsf{q} \& \{\ell_i(S_i).\mathsf{T}_i\}_{i \in I} \xrightarrow{\mathsf{p}:\mathsf{q}\&\ell_k(S_k)} \mathsf{p} : \mathsf{T}_k} \ [\Gamma\text{-}\&]$$

$$\frac{k \in I}{\mathsf{p} : \mathsf{q} \oplus \{\ell_i(S_i).\mathsf{T}_i\}_{i \in I} \xrightarrow{\mathsf{p}:\mathsf{q}\oplus\ell_k(S_k)} \mathsf{p} : \mathsf{T}_k} \ [\Gamma\text{-}\oplus] \qquad \frac{\Gamma \xrightarrow{\alpha} \Gamma'}{\Gamma, \mathsf{p} : \mathsf{T} \xrightarrow{\alpha} \Gamma', \mathsf{p} : \mathsf{T}} \ [\Gamma\text{-},]$$

$$\frac{\Gamma_1 \xrightarrow{\mathsf{p}:\mathsf{q}\oplus\ell(S)} \Gamma_1' \qquad \Gamma_2 \xrightarrow{\mathsf{q}:\mathsf{p}\&\ell(S')} \Gamma_2' \qquad S \leq S'}{\Gamma_1, \Gamma_2 \xrightarrow{(\mathsf{p},\mathsf{q})\ell} \Gamma_1', \Gamma_2'} \ [\Gamma\text{-}\oplus\&]$$

We write $\Gamma \xrightarrow{\alpha}$ *if there exists* Γ' *such that* $\Gamma \xrightarrow{a} \Gamma'$*. We define a reduction* $\Gamma \to \Gamma'$ *that holds iff* $\Gamma \xrightarrow{(\mathsf{p},\mathsf{q})\ell} \Gamma'$ *for some* p, q, ℓ*. We write* $\Gamma \to$ *iff* $\Gamma \to \Gamma'$ *for some* Γ'*. We write* $\to^*$ *for the reflexive transitive closure of* $\to$*.*

[Γ-$\oplus$] and [Γ-&], express a single participant sending or receiving. [Γ-$\oplus$&] expresses a synchronized communication where one participant sends while another receives, and they both progress with their continuation. [Γ-,] shows how to extend a context.

In Rocq typing context reductions are defined the following way:

```
Inductive tctxR: tctx → label → tctx → Prop ≜
  | Rsend: ∀ p q xs n s T,
           p ≠ q →
           onth n xs = Some (s, T) →
           tctxR (M.add p (ltt_send q xs) M.empty) (lsend p q (Some s) n) (M.add p T M.empty)
  | Rrecv: ...
  | Rcomm: ∀ p q g1 g1' g2 g2' s s' n (H1: MF.Disjoint g1 g2) (H2: MF.Disjoint g1' g2'),
           p ≠ q →
           tctxR g1 (lsend p q (Some s) n) g1'  →
           tctxR g2 (lrecv q p (Some s') n) g2' →
           subsort s s' →
           tctxR (disj_merge g1 g2 H1) (lcomm p q n) (disj_merge g1' g2' H2)
  | RvarI: ∀ g l g' p T,
           tctxR g l g' →
           M.mem p g = false →
           tctxR (M.add p T g) l (M.add p T g')
  | Rstruct: ∀ g1 g1' g2 g2' l, tctxR g1' l g2' →
    M.Equal g1 g1' →
    M.Equal g2 g2' →
    tctxR g1 l g2.
```

`Rsend`, `Rrecv` and `RvarI` are straightforward translations of [Γ - &], [Γ - $\oplus$] and [Γ -,]. `Rcomm` captures [$\Gamma - \oplus$&] using the `disj_merge` function we defined for the compositions, and requires a proof that the contexts given are disjoint to be applied. `RStruct` captures the indistinguishability of local contexts under the `M.Equal` predicate from the MMaps library. We give an example to illustrate typing context reductions.

▶ **Example 4.5.** Let

$$\mathsf{T}_{\mathsf{p}} = \mathsf{q}\oplus\{\ell_0(\mathtt{int}).\mathsf{T}_{\mathsf{p}}\ ,\ \ell_1(\mathtt{int}).\mathsf{end}\}$$
$$\mathsf{T}_{\mathsf{q}} = \mathsf{p}\&\{\ell_0(\mathtt{int}).\mathsf{T}_{\mathsf{q}}\ ,\ \ell_1(\mathtt{int}).\mathsf{r}\oplus\{\ell_2(\mathtt{int}).\mathsf{end}\}\}$$
$$\mathsf{T}_{\mathsf{r}} = \mathsf{q}\&\{\ell_2(\mathtt{int}).\mathsf{end}\}$$

and $\Gamma = \{\mathsf{p} : \mathsf{T}_{\mathsf{p}},\ \mathsf{q} : \mathsf{T}_{\mathsf{q}},\ \mathsf{r} : \mathsf{T}_{\mathsf{r}}\}$. We have the reductions $\Gamma \xrightarrow{\mathsf{p}:\mathsf{q}\oplus\ell_0(\mathtt{int})} \Gamma$ and $\Gamma \xrightarrow{\mathsf{q}:\mathsf{p}\&\ell_0(\mathtt{int})} \Gamma$, which synchronise to give the reduction and $\Gamma \xrightarrow{(\mathsf{p},\mathsf{q})\ell_0} \Gamma$. Similarly via synchronised communication of p and q via message label ℓ_1 we get $\Gamma \xrightarrow{(\mathsf{p},\mathsf{q})\ell_1} \Gamma'$ where Γ' is defined as $\{\mathsf{p} : \mathsf{end},\ \mathsf{q} : \mathsf{r}\oplus\{\ell_2(\mathtt{int}).\mathsf{end}\}, \mathsf{r} : \mathsf{T}_{\mathsf{r}}\}$. We further have that $\Gamma' \xrightarrow{(\mathsf{q},\mathsf{r})\ell_2} \Gamma_{\mathsf{end}}$ where Γ_{end} is defined as $\{\mathsf{p} : \mathsf{end},\ \mathsf{q} : \mathsf{end},\ \mathsf{r} : \mathsf{end}\}$.

In Rocq, Γ is defined the following way:

```
Definition prt_p≜0.
Definition prt_q≜1.
Definition prt_r≜2.
CoFixpoint T_p ≜ ltt_send prt_q [Some (sint,T_p); Some (sint,ltt_end); None].
CoFixpoint T_q ≜ ltt_recv prt_p [Some (sint,T_q); Some (sint, ltt_send prt_r [None;None;Some (sint,ltt_end)]); None].
Definition T_r ≜ ltt_recv prt_q [None;None; Some (sint,ltt_end)].
Definition gamma ≜ M.add prt_p T_p (M.add prt_q T_q (M.add prt_r T_r M.empty)).
```

Now $\Gamma \xrightarrow{(\mathsf{p},\mathsf{q})\ell_0} \Gamma$ can be expressed as `tctxR gamma (lsend prt_p prt_q (Some sint) 0) gamma`.

4.3 Global Type Reductions

As with local typing contexts, we can also define reductions for global types.

▶ **Definition 4.6** (Global type reductions). *The global type transition* $\xrightarrow{\alpha}$ *is defined coinductively as follows.*

$$\frac{k \in I}{\mathsf{p} \to \mathsf{q} : \{\ell_i(S_i).\mathsf{G}_i\}_{i \in I} \xrightarrow{(\mathsf{p},\mathsf{q})\ell_k} \mathsf{G}_k} \ [\text{GR-}\oplus\&]$$

$$\frac{\forall i \in I \ \ \mathsf{G}_i \xrightarrow{\alpha} \mathsf{G}'_i \qquad \text{subject}(\alpha) \cap \{\mathsf{p},\mathsf{q}\} = \emptyset \qquad \forall i \in I \ \ \{\mathsf{p},\mathsf{q}\} \subseteq \mathtt{pt}\{\mathsf{G}_i\}}{\mathsf{p} \to \mathsf{q} : \{\ell_i(S_i).\mathsf{G}_i\}_{i \in I} \xrightarrow{\alpha} \mathsf{p} \to \mathsf{q} : \{\ell_i(S_i).\mathsf{G}'_i\}_{i \in I}} \ [\text{GR-CTX}]$$

[GR-⊕&] says that a global type tree with root $\mathsf{p} \to \mathsf{q}$ can transition to any of its children corresponding to the message label choosen by p. [GR-CTX] says that if the subjects of α are disjoint from the root and all its children can transition via α, then the whole tree can also transition via α, with the root remaining the same and just the subtrees of its children transitioning.

In Rocq global type reductions are expressed using the coinductively defined predicate `gttstepC`. For example, $\mathsf{G} \xrightarrow{(\mathsf{p},\mathsf{q})\ell_k} \mathsf{G}'$ translates to `gttstepC G G' p q k`. We refer to [14] for details.

4.4 Association Between Local Type Contexts and Global Types

We have defined local type contexts which specifies protocols bottom-up by directly describing the roles of every participant, and global types, which give a top-down view of the whole protocol, and the transition relations on them. We now relate these local and global definitions by defining *association* between local type context and global types.

▶ **Definition 4.7** (Association). *A local typing context* Γ *is associated with a global type tree* G*, written* $\Gamma \sqsubseteq \mathsf{G}$*, if the following hold:*

- *For all* $\mathsf{p} \in \mathtt{pt}(\mathsf{G})$, $\mathsf{p} \in \text{dom}(\Gamma)$ *and* $\Gamma(\mathsf{p}) \leqslant \mathsf{G} \upharpoonright \mathsf{p}$.
- *For all* $\mathsf{p} \notin \mathtt{pt}(\mathsf{G})$*, either* $\mathsf{p} \notin \text{dom}(\Gamma)$ *or* $\Gamma(\mathsf{p}) = \mathtt{end}$.

In Rocq this is defined with the following:

```
Definition assoc (g: tctx) (gt:gtt) ≜
    ∀ p, (isgPartsC p gt  →  ∃ Tp, M.find p g=Some Tp ∧
       issubProj Tp gt p) ∧
        (~ isgPartsC p gt  →  ∀ Tpx, M.find p g = Some Tpx  →  Tpx=ltt_end).
```

Informally, $\Gamma \sqsubseteq \mathsf{G}$ says that the local type trees in Γ obey the specification described by the global type tree G.

▶ **Example 4.8.** In Example 4.5, we have that $\Gamma \sqsubseteq \mathsf{G}$ where

$$\mathsf{G} := \mathsf{p} \to \mathsf{q} : \{\ell_0(\mathtt{int}).\mathsf{G}, \ell_1(\mathtt{int}).\mathsf{q} \to \mathsf{r} : \{\ell_2(\mathtt{int}).\mathtt{end}\}\}$$

In fact, we have $\Gamma(\mathsf{s}) = \mathsf{G} \upharpoonright \mathsf{s}$ for $\mathsf{s} \in \{\mathsf{p},\mathsf{q},\mathsf{r}\}$. Similarly, we have $\Gamma' \sqsubseteq \mathsf{G}'$ where

$$\mathsf{G}' := \mathsf{q} \to \mathsf{r} : \{\ell_2(\mathtt{int}).\mathtt{end}\}$$

It is desirable to have the association be preserved under local type context and global type reductions, that is, when one of the associated constructs "takes a step" so should the other. We formalise this property with soundness and completeness theorems.

▶ **Theorem 4.9** (Soundness of Association). *If* `assoc gamma G` *and* `gttstepC G G' p q ell`*, then there is a local type context* `gamma'`*, a global type tree* `G''` *and a message label* `ell'` *such that* `gttStepC G G'' p q ell'`*,* `assoc gamma' G''` *and* `tctxR gamma (lcomm p q ell') gamma'`*.*

▶ **Theorem 4.10** (Completeness of Association). *If* `assoc gamma G` *and* `tctxR gamma (lcomm p q ell) gamma'`*, then there exists a global type tree* `G'` *such that* `assoc gamma' G'` *and* `gttstepC G G' p q ell`*.*

▶ Remark 4.11. Note that in the statement of soundness we allow the message label for the local type context reduction to be different to the message label for the global type reduction. This is because our use of subtyping in association causes the entries in the local type context to be less expressive than the types obtained by projecting the global type. For example consider

$$\Gamma = \mathsf{p} : \mathsf{q}\oplus\{\ell_0(\mathtt{int}).\mathtt{end}\},\ \mathsf{q} : \mathsf{p}\&\{\ell_0(\mathtt{int}).\mathtt{end}, \ell_1(\mathtt{int}).\mathtt{end}\}$$

and

$$\mathsf{G} = \mathsf{p} \to \mathsf{q} : \{\ell_0(\mathtt{int}).\mathtt{end}, \ell_1(\mathtt{int}).\mathtt{end}\}$$

We have $\Gamma \sqsubseteq \mathsf{G}$ and $\mathsf{G} \xrightarrow{(\mathsf{p},\mathsf{q})\ell_1}$. However $\Gamma \xrightarrow{(\mathsf{p},\mathsf{q})\ell_1}$ is not a valid transition. Note that soundness still requires that $\Gamma \xrightarrow{(\mathsf{p},\mathsf{q})\ell_x}$ for some x, which is satisfied in this case by the valid transition $\Gamma \xrightarrow{(\mathsf{p},\mathsf{q})\ell_0}$.

5 Properties of Local Type Contexts

We now use the LTS semantics to define some desirable properties on type contexts and their reduction sequences. Namely, we formulate safety, liveness and fairness properties based on the definitions in [44].

5.1 Safety

We start by defining safety:

▶ **Definition 5.1** (Safe Type Contexts). *We define* safe *coinductively as the largest set of type contexts such that whenever we have* $\Gamma \in \mathsf{safe}$*:*

$$\Gamma \xrightarrow{\mathsf{p}:\mathsf{q}\oplus\ell(S)} \textit{ and } \Gamma \xrightarrow{\mathsf{q}:\mathsf{p}\&\ell'(S')} \textit{ implies } \Gamma \xrightarrow{(\mathsf{p},\mathsf{q})\ell} \qquad \text{[S-\&}\oplus\text{]}$$

$$\Gamma \to \Gamma' \textit{ implies } \Gamma' \in \mathsf{safe} \qquad \text{[S-}\to\text{]}$$

We write $\mathsf{safe}(\Gamma)$ *if* $\Gamma \in \mathsf{safe}$.

Informally, safety says that if p and q communicate with each other and p requests to send a value using message label ℓ, then q should be able to receive that message label. Furthermore, this property should be preserved under any typing context reductions. Being a coinductive property, to show that $\mathsf{safe}(\Gamma)$ it suffices to give a set φ such that $\Gamma \in \varphi$ and φ satisfies [S-&⊕] and [S-→] . This amounts to showing that every element of Γ' of the set of reducts of Γ, defined $\varphi := \{\Gamma' \mid \Gamma \to^* \Gamma'\}$, satisfies [S-&⊕] . We illustrate this with some examples:

▶ **Example 5.2.** Let $\Gamma_A = \mathsf{p} : \mathtt{end}$, then Γ_A is safe: the set of reducts is $\{\Gamma_A\}$ and this set respects [S- ⊕&] as its elements can't reduce, and it respects [S-→] as it's closed with respect to $\to$.

Let $\Gamma_B = \mathsf{p} : \mathsf{q}\oplus\{\ell_0(\mathtt{int}).\mathtt{end}\}, \mathsf{q} : \mathsf{p}\&\{\ell_0(\mathtt{nat}).\mathtt{end}\}$. Γ_B is not safe as as we have $\Gamma_B \xrightarrow{\mathsf{p}:\mathsf{q}\oplus\ell_0}$ and $\Gamma_B \xrightarrow{\mathsf{q}:\mathsf{p}\&\ell_0}$ but we don't have $\Gamma_B \xrightarrow{(\mathsf{p},\mathsf{q})\ell_0}$ as $\mathtt{int} \not\leq \mathtt{nat}$.

Let $\Gamma_C = \mathsf{p} : \mathsf{q}\oplus\{\ell_1(\mathtt{int}).\mathsf{q}\oplus\{\ell_0(\mathtt{int}).\mathtt{end}\}\}, \mathsf{q} : \mathsf{p}\&\{\ell_1(\mathtt{int}).\mathsf{p}\&\{\ell_0(\mathtt{nat}).\mathtt{end}\}\}$. Γ_C is not safe as we have $\Gamma_C \xrightarrow{(\mathsf{p},\mathsf{q})\ell_1} \Gamma_B$ and Γ_B is not safe.

Consider Γ from Example 4.5. All the reducts satisfy [S-&⊕], hence Γ is safe.

Being a coinductive property, safe can be expressed in Rocq using Paco:

```
Definition weak_safety (c: tctx ) ≜
∀ p q s s'  k k', tctxRE (lsend p q (Some s) k) c  →  tctxRE (lrecv q p (Some s') k') c  →
                            tctxRE (lcomm p q k) c.

Inductive safe (R: tctx  →  Prop): tctx  →  Prop ≜
  | safety_red :  ∀ c, weak_safety c  →  (∀ p q c' k,
   tctxR c (lcomm p q k) c'  →  R c')
    →   safe R c.

Definition safeC c ≜ paco1 safe bot1 c.
```

`weak_safety` corresponds [S-&⊕] where `tctxRE l c` is shorthand for `∃ c', tctxR c l c'`. In the inductive `safe`, the constructor `safety_red` corresponds to [S-→]. Then `safeC` is defined as the greatest fixed point of `safe`.

We have that local type contexts with associated global types are always safe.

▶ **Theorem 5.3** (Safety by Association). *If* `assoc gamma g` *then* `safeC gamma`.

5.2 Fairness and Liveness

We now focus our attention to fairness and liveness. We first restate the definition of fairness and liveness for local type context paths from [44].

▶ **Definition 5.4** (Fair, Live Paths). *A local type context reduction path (also called executions or runs) is a possibly infinite sequence of transitions $\Gamma_0 \xrightarrow{\lambda_0} \Gamma_1 \xrightarrow{\lambda_1}$ .. such that λ_i is a synchronous transition label, that is, of the form $(\mathsf{p},\mathsf{q})\ell$, for all i.*

We say that a local type context reduction path $\Gamma_0 \xrightarrow{\lambda_0} \Gamma_1 \xrightarrow{\lambda_2}$ .. is fair if, for all $n \in N : \Gamma_n \xrightarrow{(\mathsf{p},\mathsf{q})\ell}$ implies $\exists k, \ell'$ such that $N \ni k \geq n$ and $\lambda_k = (\mathsf{p},\mathsf{q})\ell'$, and therefore $\Gamma_k \xrightarrow{(\mathsf{p},\mathsf{q})\ell'} \Gamma_{k+1}$. We say that a path $(\Gamma_n)_{n\in N}$ is live iff, $\forall n \in N$:

1. *$\forall n \in N : \Gamma_n \xrightarrow{\mathsf{p}:\mathsf{q}\oplus\ell(S)}$ implies $\exists k, \ell'$ such that $N \ni k \geq n$ and $\Gamma_k \xrightarrow{(\mathsf{p},\mathsf{q})\ell'} \Gamma_{k+1}$*
2. *$\forall n \in N : \Gamma_n \xrightarrow{\mathsf{q}:\mathsf{p}\&\ell(S)}$ implies $\exists k, \ell'$ such that $N \ni k \geq n$ and $\Gamma_k \xrightarrow{(\mathsf{p},\mathsf{q})\ell'} \Gamma_{k+1}$*

▶ **Definition 5.5** (Live Local Type Context). *A local type context Γ is live if whenever $\Gamma \to^* \Gamma'$, every fair path starting from Γ' is also live.*

In general, fairness assumptions are used so that only the reduction sequences that are "well-behaved" in some sense are considered when formulating other properties [42]. For our purposes we define fairness such that, in a fair path, if at any point p attempts to send to q *and* q attempts to send to p then eventually a communication between p and q takes place. Then live paths are defined to be paths such that whenever p attempts to send to q *or* q attempts to send to p, eventually a p to q communication takes place. Informally, this means that every communication request is eventually answered. Then live typing contexts are defined to be the Γ where all fair paths that start from Γ are also live.

▶ **Example 5.6.** Consider the contexts Γ, Γ' and Γ_{end} from Example 4.5. One possible reduction path is $\Gamma \xrightarrow{(\mathsf{p},\mathsf{q})\ell_0} \Gamma \xrightarrow{(\mathsf{p},\mathsf{q})\ell_0} \dots$. Denote this path as $(\Gamma_n)_{n\in\mathbb{N}}$, where $\Gamma_n = \Gamma$

for all $n \in \mathbb{N}$. We have $\forall n, \Gamma_n \xrightarrow{(\mathsf{p},\mathsf{q})\ell_0}$ and $\Gamma_n \xrightarrow{(\mathsf{p},\mathsf{q})\ell_1}$ as the only possible synchronised reductions from Γ_n. Accordingly, we also have $\forall n, \Gamma_n \xrightarrow{(\mathsf{p},\mathsf{q})\ell_0} \Gamma_{n+1}$ in the path so this path is fair. However, this path is not live as we have $\Gamma_1 \xrightarrow{\mathsf{r}:\mathsf{q}\&\ell_2(\mathtt{int})}$ but there is no n, ℓ' with $\Gamma_n \xrightarrow{(\mathsf{q},\mathsf{r})\ell'} \Gamma_{n+1}$ in the path. Consequently, Γ is not a live type context.

Now consider the reduction path $\Gamma \xrightarrow{(\mathsf{p},\mathsf{q})\ell_0} \Gamma \xrightarrow{(\mathsf{p},\mathsf{q})\ell_0} \Gamma' \xrightarrow{(\mathsf{q},\mathsf{r})\ell_2} \Gamma_{\mathsf{end}}$. This path is fair and live as it contains the (q,r) transition from the counterexample above.

Definition 5.4 , while intuitive, is not really convenient for a Rocq formalisation due to the existential statements contained in them. It would be ideal if these properties could be expressed as a least or greatest fixed point, which could then be formalised via Rocq's inductive or (via Paco) coinductive types. To achieve this, we recast fairness and liveness for local type context paths in Linear Temporal Logic (LTL) [33]. $\Diamond$ and $\Box$ can be characterised as least and greatest fixed points using their expansion laws [2, Chapter 5.14]. Hence they can be implemented in Rocq as the inductive type `eventually` and the coinductive type `alwaysCG`. We can further represent reduction paths as *cosequences*, or *streams*. Then the Rocq definition of Definition 5.4 amounts to the following:

```
CoInductive coseq (A: Type): Type ≜
  | conil : coseq A
  | cocons: A → coseq A → coseq A.
Notation local_path ≜ (coseq (tctx*option label)).
```

```
Definition fair_path_local_inner (pt: local_path): Prop ≜
  ∀ p q n, to_path_prop (tctxRE (lcomm p q n)) False pt →
      eventually (headComm p q) pt.
Definition fair_path ≜ alwaysCG fair_path_local_inner.
Definition live_path_inner (pt: local_path) : Prop ≜ ∀ p q s n,
(to_path_prop (tctxRE (lsend p q (Some s) n)) False pt →
      eventually (headComm p q) pt) ∧
(to_path_prop (tctxRE (lrecv p q (Some s) n)) False pt →
      eventually (headComm q p) pt).
Definition live_path ≜ alwaysCG live_path_inner.
```

With these definitions we can now prove that local type contexts associated with a global type are live, which is the most involved of the results mechanised in this work. We now detail the Rocq Proof that associated local type contexts are also live.

▶ Remark 5.7. We once again emphasise that all global types mentioned are assumed to be balanced (Definition 3.9). Indeed association with non-balanced global types doesn't guarantee liveness. As an example, consider Γ from Example 4.5, which is associated with G from Example 4.8. Yet we have shown in Example 5.6 that Γ is not a live type context. This is not surprising as G is not balanced.

▶ **Theorem 5.8** (Liveness by Association). *If* `assoc gamma g` *then* `gamma` *is live.*

Proof. (Simplified, Outline) Our proof proceeds in two steps. First, we prove that the typing context obtained by direct projections [1] of `g`, that is, `gamma_proj` $= \{\mathsf{p}_i : \mathsf{G} \upharpoonright_{\mathsf{p}_i} \mid \mathsf{p}_i \in \mathsf{pt}\{\mathsf{G}\}\}$, is live. We then leverage Theorem 4.10 to show that if `gamma_proj` is live, so is `gamma`.

The proof that `gamma_proj` is live proceeds by well-founded induction on the tree height [12] of the grafting (Lemma 3.12) of the global type `g`. Suppose `gamma_proj` $\xrightarrow{\mathsf{p}:\mathsf{q}\oplus\ell(S)}$ (the case for the receive is similar and omitted), and `xs` is a fair local type context reduction path beginning with `gamma_proj`. To show that `xs` is live we need to show the existence of a $(\mathsf{p},\mathsf{q})\ell$ transition in `xs`. We prove the following helper lemmas:

- The height of the `p`-grafting of `g` is not smaller than the `q`-grafting.

[1] Note that the actual Rocq proof defines an equivalent "enabledness" predicate on global types instead of working with direct projections. The outline given here is a slightly simplified presentation.

- If the p-grafting and q-grafting of a global type `g'` have the same height, then any fair path beginning with the direct projection context of `g'` eventually contains a $(\mathsf{p},\mathsf{q})\ell$ transition.
- The height of the p-grafting of `g` strictly decreases with every transition involving `q`, and doesn't increase with the transitions not involving `q`.

These lemmas followed by well-founded induction on the height of the p-grafting of the global type the head of `xs` is projected from gives the desired transition.

In the second step of the proof we extend association on to paths to get, for each local type context reduction path `xs` that begins with `gamma`, another local type context reduction path `ys` beginning with `gamma_proj` such that the elements of `xs` are subtypes (subtyping on contexts defined pointwise) of the corresponding elements of `ys`. This is obtained from Theorem 4.10, however the statement of Theorem 4.10 is implemented as an ∃ statement that lives in `Prop`, hence we need to use the `constructive_indefinite_description` axiom to construct a `CoFixpoint` returning the desired cosequence `ys`. The proof then follows by the definition of subtyping (Definition 3.4). ◀

6 Properties of Sessions

We give typing rules for the session calculus introduced in 2, and prove subject reduction and progress for them. Then we define a liveness property for sessions, and show that processes typable by a local type context that's associated with a global type tree are guaranteed to satisfy this liveness property.

6.1 Typing rules

We give typing rules for our session calculus based on [17] and [14].

We distinguish between two kinds of typing judgements and type contexts.

1. A local type context Γ associates participants with local type trees, as defined in cdef-type-ctx. Local type contexts are used to type sessions (Definition 2.2) i.e. a set of pairs of participants and single processes composed in parallel. We express such judgements as $\Gamma \vdash_{\mathcal{M}} \mathcal{M}$, or as `typ_sess M gamma` or `gamma ⊢ M` in Rocq.
2. A process variable context Θ_{T} associates process variables with local type trees, and an expression variable context Θ_{e} assigns sorts to expresion variables. Variable contexts are used to type single processes and expressions (Definition 2.1). Such judgements are expressed as $\Theta_{\mathsf{T}}, \Theta_{\mathsf{e}} \vdash_{\mathsf{P}} \mathsf{P} : \mathsf{T}$, or in Rocq as `typ_proc theta_T theta_e P T` or `theta_T, theta_e ⊢ P : T`.

$$\Theta \vdash_{\mathsf{P}} n \colon \mathtt{nat} \qquad \Theta \vdash_{\mathsf{P}} i \colon \mathtt{int} \qquad \Theta \vdash_{\mathsf{P}} \mathtt{true} \colon \mathtt{bool} \qquad \Theta \vdash_{\mathsf{P}} \mathtt{false} \colon \mathtt{bool} \qquad \Theta, x \colon \mathsf{S} \vdash_{\mathsf{P}} x \colon \mathsf{S}$$

$$\frac{\Theta \vdash_{\mathsf{P}} e \colon \mathtt{nat}}{\Theta \vdash_{\mathsf{P}} \mathtt{succ}\ e \colon \mathtt{nat}} \qquad \frac{\Theta \vdash_{\mathsf{P}} e \colon \mathtt{int}}{\Theta \vdash_{\mathsf{P}} \mathtt{neg}\ e \colon \mathtt{int}} \qquad \frac{\Theta \vdash_{\mathsf{P}} e \colon \mathtt{bool}}{\Theta \vdash_{\mathsf{P}} \neg\ e \colon \mathtt{bool}}$$

$$\frac{\Theta \vdash_{\mathsf{P}} e_1 \colon \mathsf{S} \quad \Theta \vdash_{\mathsf{P}} e_2 \colon \mathsf{S}}{\Theta \vdash_{\mathsf{P}} e_1 \oplus e_2 \colon \mathsf{S}} \qquad \frac{\Theta \vdash_{\mathsf{P}} e_1 \colon \mathtt{int} \quad \Theta \vdash_{\mathsf{P}} e_2 \colon \mathtt{int}}{\Theta \vdash_{\mathsf{P}}\ e_1 > e_2 \colon \mathtt{bool}} \qquad \frac{\Theta \vdash_{\mathsf{P}} e \colon \mathsf{S} \quad \mathsf{S} \leq \mathsf{S}'}{\Theta \vdash_{\mathsf{P}} e \colon \mathsf{S}'}$$

Table 4 Typing expressions

$$\frac{[\text{T-END}]}{\Theta \vdash_{\mathsf{P}} \mathbf{0}\colon \mathtt{end}} \qquad \frac{[\text{T-VAR}]}{\Theta, \mathbf{X}\colon \mathsf{T} \vdash_{\mathsf{P}} \mathbf{X}\colon \mathsf{T}} \qquad [\text{T-REC}]\ \frac{\Theta, \mathbf{X}\colon \mathsf{T} \vdash_{\mathsf{P}} \mathsf{P}\colon \mathsf{T}}{\Theta \vdash_{\mathsf{P}} \mu\mathbf{X}.\mathsf{P}\colon \mathsf{T}} \qquad [\text{T-IF}]\ \frac{\Theta \vdash_{\mathsf{P}} e\colon \mathtt{bool} \quad \Theta \vdash_{\mathsf{P}} \mathsf{P}_1\colon \mathsf{T} \quad \Theta \vdash_{\mathsf{P}} \mathsf{P}_2\colon \mathsf{T}}{\Theta \vdash_{\mathsf{P}} \mathtt{if}\ \mathtt{e}\ \mathtt{then}\ \mathsf{P}_1\ \mathtt{else}\ \mathsf{P}_2\colon \mathsf{T}}$$

$$[\text{T-SUB}]\ \frac{\Theta \vdash_{\mathsf{P}} \mathsf{P}\colon \mathsf{T} \quad \mathsf{T} \leqslant \mathsf{T}'}{\Theta \vdash_{\mathsf{P}} \mathsf{P}\colon \mathsf{T}'} \qquad [\text{T-IN}]\ \frac{\forall i \in I, \quad \Theta, x_i\colon \mathsf{S}_i \vdash_{\mathsf{P}} \mathsf{P}_i\colon \mathsf{T}_i}{\Theta \vdash_{\mathsf{P}} \sum_{i\in I} \mathsf{p}?\ell_i(x_i).\mathsf{P}_i\colon \mathsf{p}\&\{\ell_i(\mathsf{S}_i).\mathsf{T}_i\}_{i\in I}} \qquad [\text{T-OUT}]\ \frac{\Theta \vdash_{\mathsf{P}} e\colon \mathsf{S} \quad \Theta \vdash_{\mathsf{P}} \mathsf{P}\colon \mathsf{T}}{\Theta \vdash_{\mathsf{P}} \mathsf{p}!\ell(\mathsf{e}).\mathsf{P}\ :\ \mathsf{p}\oplus\{\ell(\mathsf{S}).\mathsf{T}\}}$$

Table 5 Typing processes

Table 4 and Table 5 state the standard typing rules for expressions and processes which we don't elaborate on. We have a single rule for typing sessions:

$$[\text{T-SESS}]\ \frac{\forall i \in I: \quad \vdash_{\mathsf{P}} \mathsf{P}_i\colon \Gamma(\mathsf{p}_i) \qquad \Gamma \sqsubseteq \mathsf{G}}{\Gamma \vdash_{\mathcal{M}} \prod_i \mathsf{p}_i \triangleleft \mathsf{P}_i}$$

[T-SESS] says that a session made of the parallel composition of processes $\prod_i \mathsf{p}_i \triangleleft \mathsf{P}_i$ can be typed by an associated local context Γ if the local type of participant p_i in Γ types the process

6.2 Properties of Typed Sessions

give theorem no

The subject reduction, progress and non-stuck theorems from [14] also hold in this setting, with minor changes in their statements and proofs. We won't discuss these proofs in detail.

▶ **Lemma 6.1.** *If* `gamma` $\vdash_{\mathcal{M}}$ `M` *and* `M` $\Rrightarrow$ `M'` *then* `typ_sess M' gamma`.

▶ **Theorem 6.2** (Subject Reduction). *If* `gamma` $\vdash_{\mathcal{M}}$ `M` *and* `M` $\xrightarrow{(\mathsf{p},\mathsf{q})\ell}$ `M'`*, then there exists a typing context* `gamma'` *such that* `gamma` $\xrightarrow{(\mathsf{p},\mathsf{q})\ell}$ `gamma'` *and* `gamma` $\vdash_{\mathcal{M}}$ `M` *.*

▶ Remark 6.3. Note that in Theorem 6.2 one transition between sessions corresponds to exactly one transition between local type contexts with the same label. That is, every session transition is observed by the corresponding type. This is the main reason for our choice of reactive semantics (Section 2.2) as τ transitions are not observed by the type in ordinary semantics. In other words, with τ-semantics the typing relation is a *weak simulation* [29], while it turns into a strong simulation with reactive semantics. For our Rocq implementation working with the strong simulation turns out be more convenient.

▶ **Theorem 6.4** (Deadlock Freedom). *If* `gamma` $\vdash_{\mathcal{M}}$ `M` *, one of the following hold :*

1. *Either* `M` $\Rrightarrow$ `M_inact` *where every process making up* `M_inact` *is inactive, i.e.* `M_inact` $\equiv \prod_{i=1}^{n} \mathsf{p}_i \triangleleft \mathbf{0}$ *for some* n*.*
2. *Or there is a* `M'` *such that* `M` $\rightarrow$ `M'`*.*

We can also prove the following correspondence result in the reverse direction to Theorem 6.2, analogous to Theorem 4.9.

▶ **Theorem 6.5** (Session Fidelity). *If* `gamma` $\vdash_{\mathcal{M}}$ `M` *and* `gamma` $\xrightarrow{(\mathsf{p},\mathsf{q})\ell}$ `gamma'`*, there exists a message label* ℓ'*, a context* `gamma''` *and a session* `M'` *such that* `M` $\xrightarrow{(\mathsf{p},\mathsf{q})\ell'}$ `M'` *,* `gamma` $\xrightarrow{(\mathsf{p},\mathsf{q})\ell'}$ `gamma''` *and* `typ_sess M' gamma''`*.*

▶ Remark 6.6. Again we note that by Theorem 6.5 a single-step context reduction induces a single-step session reduction on the type. With the τ-semantics the session reduction induced by the context reduction would be multistep.

Now the following type safety property follows from the above theorems:

▶ **Theorem 6.7** (Type Safety). *If* `gamma` $\vdash_{\mathcal{M}}$ `M` *and* `M` $\to^*$ `M'` $\Rrightarrow$ `(p` $\leftarrow$ `p_send q ell P ||| q` $\leftarrow$ `p_recv p xs ||| M'')`, *then* `onth ell xs` $\neq$ `None`.

The final, and the most intricate, session property we prove is liveness.

▶ **Definition 6.8** (Session Liveness). *Session $\mathcal{M}$ is live iff*

1. $\mathcal{M} \longrightarrow^* \mathcal{M}' \Rrightarrow \mathsf{q} \triangleleft \mathsf{p}!\ell_i(x_i).Q \mid \mathcal{N}$ *implies* $\mathcal{M}' \longrightarrow^* \mathcal{M}'' \Rrightarrow \mathsf{q} \triangleleft Q \mid \mathcal{N}'$ *for some* $\mathcal{M}'', \mathcal{N}'$
2. $\mathcal{M} \longrightarrow^* \mathcal{M}' \Rrightarrow \mathsf{q} \triangleleft \bigwedge_{i \in I} \mathsf{p}?\ell_i(x_i).Q_i \mid \mathcal{N}$ *implies* $\mathcal{M}' \longrightarrow^* \mathcal{M}'' \Rrightarrow \mathsf{q} \triangleleft Q_i[v/x_i] \mid \mathcal{N}'$ *for some* $\mathcal{M}'', \mathcal{N}', i, v$.

In Rocq this is expressed with the predicate `live_sess`*:*

```
Definition live_sess Mp ≜ ∀ M, betaRtc Mp M  →
  (∀ p q ell e P' M', p ≠q  → unfoldP M ( (p ←- p_send q ell e P') ||| M')  → ∃ M'',
  betaRtc M ((p ←- P')\|\|\|M''))
  ∧
  (∀ p  q llp M', p ≠q  → unfoldP M ( (p ←- p_recv q llp) ||| M')  →
    ∃ M'' P' e k, onth k llp = Some P' ∧ betaRtc M ((p ←- subst_expr_proc P' e 0 0) |||M'')).
```

Session liveness, analogous to liveness for typing contexts (Definition 5.4), says that when $\mathcal{M}$ is live, if $\mathcal{M}$ reduces to a session $\mathcal{M}'$ containing a participant that's attempting to send or receive, then $\mathcal{M}'$ reduces to a session where that communication has happened. It's also called *lock-freedom* in related work ([41, 30]).

We can now prove that typed sessions are live. First we prove the following lemma:

▶ **Lemma 6.9** (Fair Extension of Typed Sessions). *If* `typ_sess M gamma`*, then there exists a session reduction path* `xs` *starting from* `M` *such that the following fairness property holds:*

- *On* `xs`*, whenever a transition with label* $(\mathsf{p}, \mathsf{q})\ell$ *is enabled, a transition with label* $(\mathsf{p}, \mathsf{q})\ell'$ *eventually occurs for some* ℓ'*.*

Proof. The desired path can be constructed by repeatedly cycling through all participants, checking if there is a transition involving that participant, and executing that transition if there is. Correctness follows from Theorem 6.2 and Theorem 6.5. ◀

Lemma 6.9 defines a "fairness" property for sessions analogous to Definition 5.4. It then shows that there exists a fair path from any typable session. This resembles the *feasibility* property expected from sensible notions of fairness [42], which states that any partial path can be extended into a fair one [2].

▶ Remark 6.10. As in the proof of Theorem 5.8, the construction in Lemma 6.9 uses the `constructive_indefinite_description` axiom to construct a `CoFixpoint`. Additionally, we use the axiom `excluded_middle_informative` for the "check if there is a transition involving a participant" part of the scheduling algorithm. The use of this axiom is probably not necessary but it makes the proof easier.

[2] Note that this fairness property for sessions is not actually feasible as there are partial paths starting with an untypable session that can't be extended into a fair one. Nevertheless, Lemma 6.9 turns out to be enough to prove our liveness property.

▶ **Theorem 6.11** (Liveness by Typing). *For a session* $\texttt{Mp}$*, if* $\exists$ $\texttt{gamma}$ $\texttt{gamma} \vdash_{\mathcal{M}} \texttt{Mp}$ *then* $\texttt{live\_sess Mp}$*.*

Proof. We detail the proof for the send case of Definition 6.8, the case for the receive is similar. Suppose that $\texttt{Mp} \to^* \texttt{M}$ and $\texttt{M} \Rrightarrow \texttt{((p} \leftarrow \texttt{p\_send q ell e P') ||| M')}$. Our goal is to show that there exists a $\texttt{M''}$ such that $\texttt{M} \to^* \texttt{((p} \leftarrow \texttt{P')|||M'')}$. First, observe that by [R-Unfold] it suffices to show that $\texttt{((p} \leftarrow \texttt{p\_send q ell e P') ||| M')} \to^* \texttt{M''}$ for some $\texttt{M''}$. Also note that $\texttt{gamma} \vdash_{\mathcal{M}} \texttt{M}$ for some $\texttt{gamma}$ by Theorem 6.2, therefore $\texttt{gamma} \vdash_{\mathcal{M}}$ $\texttt{((p} \leftarrow \texttt{p\_send q ell e P') ||| M')}$ by Lemma 6.1.

Now let $\texttt{xs}$ be a fair session reduction path starting from $\texttt{((p} \leftarrow \texttt{p\_send q ell e P')}$ $\texttt{||| M')}$, which exists by Lemma 6.9. By Theorem 6.2, let $\texttt{ys}$ be a local type context reduction path starting with $\texttt{gamma}$ such that every session in $\texttt{xs}$ is typed by the context at the corresponding index of $\texttt{ys}$, and the transitions of $\texttt{xs}$ and $\texttt{ys}$ at every step match. Now it can be shown that $\texttt{ys}$ is fair. Therefore by Theorem 5.8 $\texttt{ys}$ is live, so a $\texttt{lcomm p q ell'}$ transition eventually occurs in $\texttt{ys}$ for some $\texttt{ell'}$. Therefore $\texttt{ys} = \texttt{gamma} \to^* \texttt{gamma\_0} \xrightarrow{(\texttt{p},\texttt{q})\ell'}$ $\texttt{gamma\_1} \to ..$ for some $\texttt{gamma\_0}$, $\texttt{gamma\_1}$. Now consider the session $\texttt{M\_0}$ typed by $\texttt{gamma\_0}$ in $\texttt{xs}$. We have $\texttt{((p} \leftarrow \texttt{p\_send q ell e P') ||| M'')} \to^* \texttt{M\_0}$ by $\texttt{M\_0}$ being on $\texttt{xs}$. We also have that
$\texttt{M\_0} \xrightarrow{(\texttt{p},\texttt{q})\ell''} \texttt{M\_1}$ for some ℓ'', $\texttt{M\_1}$ by Theorem 6.5. Now observe that $\texttt{M\_0} \equiv \texttt{((p} \leftarrow \texttt{p\_send q}$ $\texttt{ell e P') ||| M'')}$ for some $\texttt{M''}$ as no transitions involving $\texttt{p}$ have happened on the reduction path to $\texttt{M\_0}$. Therefore $\ell = \ell''$, so $\texttt{M\_1} \equiv \texttt{((p} \leftarrow \texttt{P') ||| M'')}$ for some $\texttt{M''}$, as needed. ◀

7 Conclusion and Related Work

Liveness Properties. Examinations of liveness, also called *lock-freedom*, guarantees of multiparty session types abound in literature, e.g. [31, 23, 44, 35, 3]. Most of these papers use the definition liveness proposed by Padovani [30], which doesn't make the fairness assumptions that characterize the property [16] explicit. Contrastingly, van Glabbeek et. al. [41] examine several notions of fairness and the liveness properties induced by them, and devise a type system with flexible choices [6] that captures the strongest of these properties, the one induced by the *justness* [42] assumption. In their terminology, Definition 6.8 corresponds to liveness under strong fairness of transitions (ST), which is the weakest of the properties considered in that paper. They also show that their type system is complete i.e. every live process can be typed. We haven't presented any completeness results in this paper. Indeed, our type system is not complete for Definition 6.8, even if we restrict our attention to safe and race-free sessions. For example, the session described in [41, Example 9] is live but not typable by a context associated with a balanced global type in our system.

Fairness assumptions are also made explicit in recent work by Ciccone et. al [10, 11] which use generalized inference systems with coaxioms [1] to characterize *fair termination*, which is stronger than Definition 6.8, but enjoys good composition properties.

Mechanisation. Mechanisation of session types in proof assistants is a relatively new effort. Our formalisation is built on recent work by Ekici et. al. [14] which uses a coinductive representation of global and local types to prove subject reduction and progress. Their work uses a typing relation between global types and sessions while ours uses one between associated local type contexts and sessions. This necessiates the rewriting of subject reduction and progress proofs in addition to the operational correspondence, safety and liveness properties we have proved. Other recent results mechanised in Rocq include Ekici and Yoshida's [15] work on the completeness of asynchronous subtyping, and Tirore's work [37, 39, 38] on projections and subject reduction for π-calculus.

Castro-Perez et. al. [8] devise a multiparty session type system that dispenses with projections and local types by defining the typing relation directly on the LTS specifying the global protocol, and formalise the results in Agda. Ciccone's PhD thesis [9] presents an Agda formalisation of fair termination for binary session types. Binary session types were also implemented in Agda by Thiemann [36] and in Idris by Brady[5]. Several implementations of binary session types are also present for Haskell [24, 28, 34].

Implementations of session types that are more geared towards practical verification include the Actris framework [18, 21] which enriches the seperation logic of Iris [22] with binary session types to certify deadlock-freedom. In general, verification of liveness properties, with or without session types, in concurrent seperation logic is an active research area that has produced tools such as TaDa [13], FOS [25] and LiLo [26] in the past few years. Further verification tools employing multiparty session types are Jacobs's Multiparty GV [21] based on the functional language of Wadler's GV [43], and Castro-Perez et. al's Zooid [7], which supports the extraction of certifiably safe and live protocols.

References

1 Davide Ancona, Francesco Dagnino, and Elena Zucca. Generalizing Inference Systems by Coaxioms. In Hongseok Yang, editor, *Programming Languages and Systems*, pages 29–55, Berlin, Heidelberg, 2017. Springer Berlin Heidelberg.

2 Christel Baier and Joost-Pieter Katoen. *Principles of Model Checking (Representation and Mind Series)*. The MIT Press, 2008.

3 Franco Barbanera and Mariangiola Dezani-Ciancaglini. Partially Typed Multiparty Sessions. *Electronic Proceedings in Theoretical Computer Science*, 383:15–34, August 2023. arXiv:2308.10653 [cs]. URL: http://arxiv.org/abs/2308.10653, doi:10.4204/EPTCS.383.2.

4 Yves Bertot and Pierre Castran. *Interactive Theorem Proving and Program Development: Coq'Art The Calculus of Inductive Constructions*. Springer Publishing Company, Incorporated, 1st edition, 2010.

5 Edwin Charles Brady. Type-driven Development of Concurrent Communicating Systems. *Computer Science*, 18(3), July 2017. URL: https://journals.agh.edu.pl/csci/article/view/1413, doi:10.7494/csci.2017.18.3.1413.

6 Ilaria Castellani, Mariangiola Dezani-Ciancaglini, and Paola Giannini. Reversible sessions with flexible choices. *Acta Informatica*, 56(7):553–583, November 2019. doi:10.1007/s00236-019-00332-y.

7 David Castro-Perez, Francisco Ferreira, Lorenzo Gheri, and Nobuko Yoshida. Zooid: a dsl for certified multiparty computation: from mechanised metatheory to certified multiparty processes. In *Proceedings of the 42nd ACM SIGPLAN International Conference on Programming Language Design and Implementation*, PLDI 2021, page 237–251, New York, NY, USA, 2021. Association for Computing Machinery. doi:10.1145/3453483.3454041.

8 David Castro-Perez, Francisco Ferreira, and Sung-Shik Jongmans. A synthetic reconstruction of multiparty session types. *Proc. ACM Program. Lang.*, 10(POPL), January 2026. doi:10.1145/3776692.

9 Luca Ciccone. Concerto grosso for sessions: Fair termination of sessions, 2023. URL: https://arxiv.org/abs/2307.05539, arXiv:2307.05539.

10 Luca Ciccone, Francesco Dagnino, and Luca Padovani. Fair termination of multiparty sessions. *Journal of Logical and Algebraic Methods in Programming*, 139:100964, 2024. URL: https://www.sciencedirect.com/science/article/pii/S2352220824000221, doi:10.1016/j.jlamp.2024.100964.

11 Luca Ciccone and Luca Padovani. Fair termination of binary sessions. *Proc. ACM Program. Lang.*, 6(POPL), January 2022. doi:10.1145/3498666.

12 Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. *Introduction to Algorithms, Third Edition*. The MIT Press, 3rd edition, 2009.

13 Emanuele D'Osualdo, Julian Sutherland, Azadeh Farzan, and Philippa Gardner. Tada live: Compositional reasoning for termination of fine-grained concurrent programs. *ACM Trans. Program. Lang. Syst.*, 43(4), November 2021. doi:10.1145/3477082.

14 Burak Ekici, Tadayoshi Kamegai, and Nobuko Yoshida. Formalising Subject Reduction and Progress for Multiparty Session Processes. In Yannick Forster and Chantal Keller, editors, *16th International Conference on Interactive Theorem Proving (ITP 2025)*, volume 352 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 19:1–19:23, Dagstuhl, Germany, 2025. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. URL: https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.ITP.2025.19, doi:10.4230/LIPIcs.ITP.2025.19.

15 Burak Ekici and Nobuko Yoshida. Completeness of Asynchronous Session Tree Subtyping in Coq. In Yves Bertot, Temur Kutsia, and Michael Norrish, editors, *15th International Conference on Interactive Theorem Proving (ITP 2024)*, volume 309 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 13:1–13:20, Dagstuhl, Germany, 2024. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. ISSN: 1868-8969. URL: https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.ITP.2024.13, doi:10.4230/LIPIcs.ITP.2024.13.

16 Nissim Francez. *Fairness*. Springer US, New York, NY, 1986. URL: http://link.springer.com/10.1007/978-1-4612-4886-6, doi:10.1007/978-1-4612-4886-6.

17 Silvia Ghilezan, Svetlana Jakšić, Jovanka Pantović, Alceste Scalas, and Nobuko Yoshida. Precise subtyping for synchronous multiparty sessions. *Journal of Logical and Algebraic Methods in Programming*, 104:127–173, 2019. URL: https://www.sciencedirect.com/science/article/pii/S2352220817302237, doi:10.1016/j.jlamp.2018.12.002.

18 Jonas Kastberg Hinrichsen, Jesper Bengtson, and Robbert Krebbers. Actris: Session-type based reasoning in separation logic. *Proceedings of the ACM on Programming Languages*, 4(POPL):1–30, 2019.

19 Kohei Honda, Nobuko Yoshida, and Marco Carbone. Multiparty asynchronous session types. *SIGPLAN Not.*, 43(1):273–284, January 2008. doi:10.1145/1328897.1328472.

20 Chung-Kil Hur, Georg Neis, Derek Dreyer, and Viktor Vafeiadis. The power of parameterization in coinductive proof. *SIGPLAN Not.*, 48(1):193–206, January 2013. doi:10.1145/2480359.2429093.

21 Jules Jacobs, Jonas Kastberg Hinrichsen, and Robbert Krebbers. Deadlock-free separation logic: Linearity yields progress for dependent higher-order message passing. *Proceedings of the ACM on Programming Languages*, 8(POPL):1385–1417, 2024.

22 Ralf Jung, Robbert Krebbers, Jacques-Henri Jourdan, Aleš Bizjak, Lars Birkedal, and Derek Dreyer. Iris from the ground up: A modular foundation for higher-order concurrent separation logic. *Journal of Functional Programming*, 28:e20, 2018.

23 Naoki Kobayashi. A Type System for Lock-Free Processes. *Information and Computation*, 177(2):122–159, September 2002. URL: https://www.sciencedirect.com/science/article/pii/S0890540102931718, doi:10.1006/inco.2002.3171.

24 Wen Kokke and Ornela Dardha. Deadlock-free session types in linear haskell. In *Proceedings of the 14th ACM SIGPLAN International Symposium on Haskell*, Haskell 2021, page 1–13, New York, NY, USA, 2021. Association for Computing Machinery. doi:10.1145/3471874.3472979.

25 Dongjae Lee, Minki Cho, Jinwoo Kim, Soonwon Moon, Youngju Song, and Chung-Kil Hur. Fair operational semantics. *Proc. ACM Program. Lang.*, 7(PLDI), June 2023. doi:10.1145/3591253.

26 Dongjae Lee, Janggun Lee, Taeyoung Yoon, Minki Cho, Jeehoon Kang, and Chung-Kil Hur. Lilo: A higher-order, relational concurrent separation logic for liveness. *Proceedings of the ACM on Programming Languages*, 9(OOPSLA1):1267–1294, 2025.

27 Pierre Letouzey and Andrew W. Appel. Modular Finite Maps over Ordered Types. URL: https://github.com/rocq-community/mmaps.

28 Sam Lindley and J Garrett Morris. Embedding session types in haskell. *ACM SIGPLAN Notices*, 51(12):133–145, 2016.

29 Robin MILNER. Chapter 19 - operational and algebraic semantics of concurrent processes. In JAN VAN LEEUWEN, editor, *Formal Models and Semantics*, Handbook of Theoretical Computer Science, pages 1201–1242. Elsevier, Amsterdam, 1990. URL: https://www.sciencedirect.com/science/article/pii/B978044488074150024X, doi:10.1016/B978-0-444-88074-1.50024-X.

30 Luca Padovani. Deadlock and lock freedom in the linear pi-calculus. In *Proceedings of the Joint Meeting of the Twenty-Third EACSL Annual Conference on Computer Science Logic (CSL) and the Twenty-Ninth Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, CSL-LICS '14, New York, NY, USA, 2014. Association for Computing Machinery. doi:10.1145/2603088.2603116.

31 Luca Padovani, Vasco Thudichum Vasconcelos, and Hugo Torres Vieira. Typing Liveness in Multiparty Communicating Systems. In Eva Kühn and Rosario Pugliese, editors, *Coordination Models and Languages*, pages 147–162, Berlin, Heidelberg, 2014. Springer Berlin Heidelberg.

32 Kai Pischke and Nobuko Yoshida. *Asynchronous Global Protocols, Precisely*, pages 116–133. Springer Nature Switzerland, Cham, 2026. doi:10.1007/978-3-031-99717-4_7.

33 Amir Pnueli. The temporal logic of programs. In *18th annual symposium on foundations of computer science (sfcs 1977)*, pages 46–57. ieee, 1977.

34 Riccardo Pucella and Jesse A Tov. Haskell session types with (almost) no class. In *Proceedings of the first ACM SIGPLAN symposium on Haskell*, pages 25–36, 2008.

35 Alceste Scalas and Nobuko Yoshida. Less is more: multiparty session types revisited. *Proc. ACM Program. Lang.*, 3(POPL), January 2019. doi:10.1145/3290343.

36 Peter Thiemann. Intrinsically-typed mechanized semantics for session types. In *Proceedings of the 21st International Symposium on Principles and Practice of Declarative Programming*, PPDP '19, New York, NY, USA, 2019. Association for Computing Machinery. doi:10.1145/3354166.3354184.

37 Dawit Tirore. A mechanisation of multiparty session types, 2024.

38 Dawit Tirore, Jesper Bengtson, and Marco Carbone. A sound and complete projection for global types. In *14th International Conference on Interactive Theorem Proving (ITP 2023)*, pages 28–1. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2023.

39 Dawit Tirore, Jesper Bengtson, and Marco Carbone. Multiparty asynchronous session types: A mechanised proof of subject reduction. In *39th European Conference on Object-Oriented Programming (ECOOP 2025)*, pages 31–1. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2025.

40 Thien Udomsrirungruang and Nobuko Yoshida. Top-down or bottom-up? complexity analyses of synchronous multiparty session types. *Proceedings of the ACM on Programming Languages*, 9(POPL):1040–1071, 2025.

41 Rob van Glabbeek, Peter Höfner, and Ross Horne. Assuming just enough fairness to make session types complete for lock-freedom. In *Proceedings of the 36th Annual ACM/IEEE Symposium on Logic in Computer Science*, LICS '21, New York, NY, USA, 2021. Association for Computing Machinery. doi:10.1109/LICS52264.2021.9470531.

42 Rob van Glabbeek and Peter Höfner. Progress, justness, and fairness. *ACM Computing Surveys*, 52(4):1–38, August 2019. URL: http://dx.doi.org/10.1145/3329125, doi:10.1145/3329125.

43 Philip Wadler. Propositions as sessions. *SIGPLAN Not.*, 47(9):273–286, September 2012. doi:10.1145/2398856.2364568.

44 Nobuko Yoshida and Ping Hou. Less is more revisited, 2024. URL: https://arxiv.org/abs/2402.16741, arXiv:2402.16741.