Abstract

Human fallibility, unpredictable operating environments, and the heterogeneity of hardware devices are driving the need for software to be able to adapt as seen in the Internet of Things or telecommunications networks. Unfortunately, mainstream programming languages do not readily allow a software component to sense and respond to its operating environment, by discovering, replacing, and communicating with components that are not part of the original system design, while maintaining static correctness guarantees. In particular, if a new component is discovered at runtime, there is no guarantee that its communication behaviour is compatible with existing components.

We address this problem by using multiparty session types with explicit connection actions, a type formalism used to model distributed communication protocols. By associating session types with software components, the discovery process can check protocol compatibility and, when required, correctly replace components without jeopardising safety.

We present the design and implementation of EnsembleS, the first actor-based language with adaptive features and a static session type system, and apply it to a case study based on an adaptive DNS server. We formalise the type system of EnsembleS and prove the safety of well-typed programs, making essential use of recent advances in non-classical multiparty session types.

1 Introduction

The era of single monolithic stand-alone computers has long been replaced by a landscape of heterogeneous and distributed computers and software applications. Technologies such as the IoT [56], self-driving cars [55], or autonomous networks [7] bring the new challenge of needing to successfully operate in face of ever-changing environments, technologies, devices, and human errors, necessitating the need to adapt.

Here, we define dynamic self-adaptation—hereafter referred to as adaptation—as the ability of a software component to sense and respond to its operating environment, by discovering, replacing, and communicating with other software components at runtime that are not part of the original system design [6, 52]. There are many examples of adaptive systems, as well as the mechanisms of adaptation they leverage, such as discovery [37], modularisation [27], dynamic code loading and migration [12, 24]. Commercially, Steam’s in-home streaming system1 enables video games to dynamically transfer their input/output across a range of devices. Academically, RE³ [50] enables software to self-assemble predefined components, using machine learning to reconfigure the software in response to environmental changes.

1 http://store.steampowered.com/streaming/
Despite strong interest in adaption and substantial work on the mechanisms of adaptation, current programming languages either lack the capabilities to ensure that adaptation can be achieved safely and correctly, or they check correctness dynamically, resulting in runtime overheads which may not be acceptable for resource-constrained devices.

Specifically, if an adaptive system discovers new software components at runtime, these components must interact with the system in a purposeful manner. In concurrent and distributed systems, such interaction goes beyond a simple function call / return expressed with standard types and type systems: interaction involves complex communication protocols that constrain the sequence and type of data exchanged. For example, knowing that two components communicate integers and strings does not describe if or when they will be sent or received. In spite of growing interest in the topic, for example, the recent formation of the United Nations group considering creative adaptation\(^2\), mainstream programming languages do not support the specification and verification of communication protocols in concurrent and distributed systems. In turn, errors are discovered late in the development process and potentially after deployment.

Even where all components are known statically, communication safety cannot be guaranteed: as an example, the REX system’s programming language specifies sequential call / return interfaces for components, but not communication protocols for concurrent components. The adaptation in the Steam in-home streaming system is even more limited, being restricted to detection of input/output devices from a set of compatible possibilities. In both cases, the adaptive aspects of the software have been defined and designed ahead of time, as opposed to being composed on-demand at runtime, leaving no scope for extending the system via runtime discovery and replacement.

This situation brings us to a key research question:

RQ: Can a programming language support static (compile-time) verification of safe runtime dynamic self-adaptation, i.e., discovery, replacement and communication?

The problem of static verification of safe communication is addressed by multiparty session types [29–31]. Multiparty session types (MPSTs) are a type formalism used to specify the type, direction and sequence of communication actions between two or more participants. Session types guarantee that software conforms to predefined communication protocols, rather than risking errors manifesting themselves at runtime.

There is already some work in the literature on adaptation and session types, but it does not answer our research question. We discuss related work in §6, but in brief, the state-of-the-art has some combination of the following limitations: theory for a formal model such as the \(\pi\)-calculus [11, 13, 18, 19], rather than a real-world programming language; omission of some aspects of adaptation, such as runtime discovery [32]; or verification by runtime monitoring [21, 47, 48], as opposed to static checking.

To answer our research question, we implement EnsembleS, the first actor language leveraging MPSTs to provide compile-time verification of safe dynamic runtime adaptation: we can statically guarantee that a discovered actor will comply with a communication protocol, and guarantee that replacing an actor’s behaviour (e.g., to fix a bug) will not jeopardise communication safety. Key to our approach is the combination of the actor paradigm [28], for its process addressability and explicit message passing, with explicit connection actions [32] in multiparty session types, which allow discovered actors to be invited into a session.

\(^2\) https://www.itu.int/en/ITU-T/focusgroups/an/Pages/default.aspx
Contributions. The overarching contribution of this work is the design, implementation, and formalisation of a language which supports dynamic self-adaptation while guaranteeing communication safety. We achieve this through a novel integration of an actor-based language and multiparty session types with explicit connection actions. Specifically, we introduce:

1. EnsembleS and its compiler (§3): we present an actor language, EnsembleS, which supports safe adaptable applications using MPSTs. Our framework supports:
   - MPST specifications, both standard and using explicit connection actions (§3.3);
   - MPSTs to provide guarantees of protocol compliance in runtime discovery (§3.4);
   - automatic generation of application code from MPSTs (§3.2)

2. An adaptive DNS case study (§4): using MPSTs and runtime discovery to show safe dynamic self-adaptation can be achieved in a non-trivial software service

3. A core calculus for EnsembleS (§5): we formalise EnsembleS and prove type safety and progress.

The formalism makes several technical contributions: it is the first actor-based calculus with statically-checked MPSTs; and it is the first calculus to provide a language design and semantics for explicit connection actions, which had previously only been explored at the type level. Our design requires exception handling in the style of Mostrous and Vasconcelos [45] and Fowler et al. [22], and the metatheory makes essential (and novel) use of non-classical multiparty session types [53].

The implementation and examples are available in the paper’s companion artifact.

## 2 Multiparty Session Types

Multiparty session types [31] are a type formalism used to describe communication protocols in concurrent and distributed systems. An MPST describes communication among multiple software components or participants, by specifying the type and the direction of data exchanged, which is given as a sequence of send and receive actions.

We first introduce MPSTs (formalised in §5) via Scribble [57], a specification language for communicating protocols based on the theory of multiparty session types. We start with a global type, which describes the interactions among all communicating participants. Using the Scribble tool, a global protocol can be validated, guaranteeing its correctness, and then projected for each participant. Projection returns a local type, which describes communication actions from the viewpoint of that participant.
4 Multiparty Session Types for Safe Runtime Adaptation in an Actor Language

```
1 explicit global protocol OnlineStore
2 { role Customer, role Store, role Courier } {
3   login[string] connect Customer to Store;
4   do Browse(Customer, Store, Courier);
5 }
6
7 aux global protocol Deliver
8 { role Customer, role Store, role Courier } {
9   address[string] from Customer to Store;
10   deliver[string] connect Store to Courier;
11   ref(int) from Courier to Store;
12   disconnect Courier and Store;
13   ref(int) from Store to Customer;
14   disconnect Store and Customer;
15 }
```

Figure 2 Global protocol for OnlineStore

Bookstore example. Fig. 1 shows the classic Bookstore (also known as Two-Buyer) example, written in Scribble. We have three communicating participants (roles): two buyers Buy1 and Buy2, and one seller Sell, where the buyers wish to buy a book from the seller. Buy1 sends the title of the book of type string to Sell (line 3). Next, Sell sends the price of the book of type int to Buy1 (line 4). At this stage, Buy1 invites Buy2 to share the cost of the book, by sending them a quote of type int that Buy2 should pay (line 5). It is Buy2’s internal choice (line 6) to either agree (line 7), or quit the protocol (line 11). After agreement, both Buy1 and Buy2 transfer their quote to Sell (lines 8 and 9, respectively).

Projection the Bookstore global protocol into each of the communicating participants returns their local protocols. Fig. 1 shows the local protocol for Sell; we omit Buy1 and Buy2 as they are similar. Note that the local protocol only includes actions relevant to Sell.

Explicit connection actions. The Bookstore protocol assumes that all roles are connected at the start of the session. This is undesirable when a participant is only needed for part of a session, or the identity of a participant depends on data exchanged in the protocol.

Consider Figure 2, which details the protocol for an online shopping service, inspired by the travel agency protocol detailed by Hu and Yoshida [32]. The protocol is organised as three subprotocols: OnlineStore, the entry-point; Browse, where the customer repeatedly requests quotes for items; and Deliver, where the store requests delivery from a courier. In contrast to Bookstore, each connection must be established explicitly (note that connect replaces from when initiating a connection).

Note in particular that Courier is only involved in the Deliver subprotocol. The store can therefore choose which courier to use based on, for example, the weight of the item or the customer’s location. Furthermore, it is not necessary to involve the courier if the customer does not choose to make a purchase.

3 EnsembleS: An Actor Language for Runtime Adaptation

In this section, we present EnsembleS, a new session-typed actor-based language based on Ensemble [25, 26]. EnsembleS actors are addressable, single-threaded entities with share-nothing semantics, and communicate via message passing. However, differently from the classic definition of the actor model [1, 28], the communication model in EnsembleS is channel-based. EnsembleS supports both static and dynamic topologies:

Static Topologies All participants are present at the start of the session and remain involved for the duration of the session. This is based on traditional MPSTs [31].
Dynamic Topologies Participants can connect and disconnect during a session. This builds on the more recent idea of explicit connection actions [32].

3.1 EnsembleS: basic language features

An EnsembleS actor has its own private state and a single thread of control expressed as a behaviour clause, which is repeated until explicitly told to stop. Every actor executes within a stage, which represents a memory space. Actors do not share state, but instead communicate via message passing along half-duplex, simply-typed channels.

Fig. 3 shows a simple EnsembleS program which defines, instantiates and connects two actors, one of which sends linearly increasing values to the other. The program defines two interfaces Isnd and Ircv, declaring an output and input channel respectively. The boot clause (lines 19–23) is executed first and creates an instance of each actor (lines 20–21), using the appropriate constructor (lines 7 and 13, respectively). This creates and begins executing new threads for each actor, which follow the logic of the relevant behaviour clause. Next, the boot clause binds the actor’s channels together (line 22, discussed later in §3.3). Once bound, the sender actor sends the contents of value on its channel, increments it, and goes back to the beginning of its behaviour loop (lines 8–11). The receiver actor waits for a message, binds the message to data, displays it, and returns to the top of its behaviour loop (lines 14–18). EnsembleS inherits Ensemble’s native support for runtime software adaptation actions [26]:

Discover The ability to locate an arbitrary actor or stage reference at runtime, given an interface and query.

Install Given an actor type, the ability to spawn it at a specified stage.

Migrate The ability for an executing actor to move to another stage.

Replace The ability to replace an executing actor A by a new instantiation of actor B, the latter continuing at the same stage as A, if A and B have the same interface.

Interact : Given an actor reference (either spawned, discovered, or communicated), the ability to connect to its channels at runtime and then communicate.

We focus on the underlined actions and apply session types to guarantee communication safety. The reason for this choice is that discover, replace and interact are actions that modify how actors operate, whereas the other actions, install and migrate, affect where actors operate, but not their behaviour.

3.2 Session types in EnsembleS

A session type in EnsembleS represents a communication protocol for an actor, i.e., a local protocol (or local session type) validated and projected from a global session type.
We extend the StMungo [40] tool to generate EnsembleS template code that supports session types. Fig. 4 shows an overview of the actor template code generation from a global session type, and Fig. 5 shows an example of the generated code.

First, a developer defines a global session type in Scribble [57] (Fig. 4, first stage). The Scribble tool checks that the protocol is well-formed and valid according to MPST theory and projects the global protocol into local protocols for each participant (Fig. 4, second stage). For each local protocol, the StMungo tool produces (Fig. 4, third stage) i) the session type, ii) the interface and type definitions, and iii) the actor template. The generated code is parsed by the EnsembleS compiler, producing executable code (Fig. 4, fourth stage).

Let us now look at the \texttt{Buy1} local protocol, given in Fig. 1. Following the code generation process in Fig. 4, the EnsembleS template items i), ii) and iii) for \texttt{Buy1} correspond respectively to the code blocks starting in lines 3, 14, and 24 in Fig. 5.

The \texttt{Buy1} local protocol is translated as an EnsembleS \texttt{session} type in Fig. 5 (lines 3–12). It shows a sequence of send and receive actions (lines 4–6), followed by a choice at \texttt{Buy2} (lines 7–12), which determines the next set of communication actions.

Following session type specifications, EnsembleS channels define both the payload type and the session that this channel expects to interact with (lines 14–21, Fig. 5). The EnsembleS compiler uses this information to ensure that the session of each channel matches the session associated with the actor it is connected to.

An actor may follow a session type (line 24, Fig. 5). This tells the EnsembleS compiler that the logic within the \texttt{behaviour} clause of that actor must follow the communication protocol defined in the \texttt{session}.

It is important to note that the code generation in Fig. 4 is optional and the EnsembleS typechecker is independent of this process.

### 3.3 Channel connections: static and dynamic

If an actor follows a session type, then its channel connections must be 1-1. This is the standard linearity requirement for session types: if there are multiple senders on one channel, then their messages can interfere and it is not possible to statically check that the session is followed correctly. EnsembleS avoids this problem by using a single channel for each message type between each pair of participants. For example, in Fig. 1, each of the three actors communicates strings and integers with both of the other actors. Because channels are unidirectional, each actor therefore has 8 channels: 2 to send strings and 2 to send integers to both other actors, and similarly 4 channels for receiving.

**Static connections.** When using session types with static topologies, and all actors in the session are known from the beginning of the application, EnsembleS provides the \texttt{establish topology} statement to create the connections between the specified session actors (line 22, Fig. 3; line 51, Fig. 5). A compile-time error is generated if the topology is ill-defined (e.g., if the sessions do not compose or if the channels do not match).

**Dynamic connections.** EnsembleS supports reconfigurable channels and dynamic connec-
3.4 Adaptation via discovery and replacement

EnsembleS supports runtime discovery of local or remote actor instances. As an example, in a sensor network, it may be desirable to connect to a sensor which has a battery level above a certain threshold. The EnsembleS query language allows the user to define a query on non-functional properties (such as battery level, signal strength, or name), as well as the channels exposed by an actor’s interface. This ensures that any discovered actor has the correct number and type of channels, and satisfies user’s preferences. To ensure that the discovered actor also obeys a declared protocol, EnsembleS uses session types in the discovery process. The green box in Fig. 6 shows how a session is used in the actor discovery process, and the yellow box shows how such actors are connected together. Runtime discovery does not appear in the session because it does not affect the behaviour of an application directly.

EnsembleS also supports the replacement of executing actors, much like the hot-code swapping in Erlang [12]. The new actor must present the same interface as it takes over the channels of the actor being replaced at the location it was executing. Replacement happens at the beginning of an actor’s behaviour loop. Replacement has many uses, such as updating, changing, or extending some of the functionalities of existing software, and is particularly...
// session and interface definitions
actor fastA presents accountingI
follows accountingSession{
    constructor() {}
    behaviour{
        receive data on input;
        quicksort(data);
        send data on output;
    }
}

actor slowA presents accountingI
follows accountingSession{
    pS = new property[2]
        of property("serial", 823);
    constructor() {
        pS[0]:= new property("serial", 823);
        pS[1]:= new property("version", 2);
        publish pS;
    }
    query alpha() { $serial==823 && $version<4; }
}

actor main presents mainI {
    constructor() {
        // Find the slow actors matching query
        actor_s = discover(accountingI,
            accountingSession, alpha());
        // Replace them with efficient versions
        if(actor_s[0].length > 1) {
            replace actor_s[0] with fastA();
        }
    }
}

Figure 7 Session type-based replacement

useful in embedded systems [33, 34]. The existing and new actors must follow the same
session type, guaranteeing that replacement will not break existing actor interactions.

Fig. 7 shows an example of a main actor searching for actors of type slowA (line 32), and
replacing them with new actors of type fastA (lines 35–37). The slowA actors are located
by defining a query (line 26) over user-defined properties, which are published (lines 16–18).
The discovery process is the same as above, but now the discovered actors are used for
replacement rather than just communication.

3.5 Implementation

EnsembleS is implemented in C, and supports reference-counted garbage collection and
exceptions. Applications are compiled to Java source code, and then to custom Java class files
for use with a custom VM [10]. These applications can be executed on the desktop, parallel
accelerators (e.g. GPUs), Raspberry Pi, Lego NXT, and Tmote Sky hardware platforms, and
use a range of networking technologies.

Compact representations of session types are retained at runtime in order to support
discovery. EnsembleS skeleton generation code is based on the StMungo tool [40], which is
implemented as an ANTLR listener, and session typechecking is supported by modifying
the original Ensemble typechecker to ensure that each communication action is permitted by the
actor’s declared session type.

Since EnsembleS builds directly on top of the original Ensemble implementation, it inherits
Ensemble’s runtime system. Performance results can be found in [26].
To illustrate the use of session types for adaptive programming, we consider a real-world case study: the domain name system (DNS). DNS is a hierarchical, globally distributed translation system that converts an internet host name (domain name) into its corresponding numerical Internet Protocol (IP) address [43].

The process begins by transmitting a domain name to one of many well-known root servers. This server either rejects bad requests, or provides the information to contact a zone server. The zone server may know the IP address of the domain name; if not it refers the request to another zone server. This process continues until either the IP address is returned, or the name cannot be found.

To develop an adaptive DNS example, we assume no a priori information about server location, and instead use explicit discovery to find root and zone servers based on session types and server properties. We use

```
4  Case study: DNS

To illustrate the use of session types for adaptive programming, we consider a real-world case study: the domain name system (DNS). DNS is a hierarchical, globally distributed translation system that converts an internet host name (domain name) into its corresponding numerical Internet Protocol (IP) address [43].

The process begins by transmitting a domain name to one of many well-known root servers. This server either rejects bad requests, or provides the information to contact a zone server. The zone server may know the IP address of the domain name; if not it refers the request to another zone server. This process continues until either the IP address is returned, or the name cannot be found.

To develop an adaptive DNS example, we assume no a priori information about server location, and instead use explicit discovery to find root and zone servers based on session types and server properties. We use

```

```

Figure 8 EnsembleS DNS client

```

Figure 9 EnsembleS DNS client session type
discovery to find root and zone servers based on session types and server properties. We use
an existing Scribble description of DNS as a starting point [21]. To illustrate adaptation we focus on the client who is querying DNS.

Fig. 9 shows the session type for the client actor which asks DNS to resolve a domain name. The client first asks for a root server (lines 2–3), and then either is informed that the request is invalid (lines 24–25) or recursively queries zone servers (lines 7–22) until the IP address is found (lines 19–20), or an error is reported (lines 16–17). Based on this session, StMungo generates EnsembleS types and interface definitions and a skeleton actor. Minimally completing the generated skeleton produces the code in Fig. 8.

In this example, discovery is used to locate the root server (lines 21–25, in Fig. 8) and the zone server (line 37). In each case, the session for the relevant server is provided to ensure that the discovered actor follows the expected protocol. When either server is located, the client links with it (lines 27 and 39), enabling communication. When communication with the server is no longer required, the client unlinks explicitly (lines 34, 47, 51, 55, 62).

Although explicit discovery is used at the language level, there is nothing to prevent the implementation of discovery from caching the addresses of the root and zone servers. This does not affect the use of sessions in discovery or the safety they provide, as the type-based guarantees are still enforced. However, this would potentially improve performance of the system. Additionally, if a cached entry becomes stale, the full discovery process can again be used without code modification or degradation in trust.

A version of DNS which uses discovery allows the system to become more flexible and resilient to changing operational conditions, such as topology changes in the servers and their data. Session types ensure compatibility with the discovered actors.

5 A Core Calculus for EnsembleS

In this section, we provide a formal characterisation of EnsembleS. In doing so, we show that our integration of adaptation with multiparty session types is safe, allowing adaptation while ruling out communication mismatches.

Relationship to implementation. Our core calculus aims to distil the essence of the interplay between adaptation and session-typed communication with explicit connection actions. Therefore, we concentrate on a functional core calculus rather than an imperative one: imperative variable binding serves only to clutter the formalism, and our fine-grain call-by-value representation can be thought of as an intermediate language.

Interfaces and unidirectional, simply-typed channels in EnsembleS are an implementation artifact: sending on a channel whose type changes is equivalent to sending on multiple channels with different types. Moreover, following theoretical accounts of multiparty session types [14, 31, 32], instead of having send and receive (resp. connect and accept) operations followed by branching (as done in Mungo and StMungo), we have unified send and receive constructs which communicate a label along with the message payload.

Since session typing is the interesting part of discovery, we omit properties and queries from the formalism; their inclusion is routine. Finally, we concentrate on dynamic topologies with explicit connection actions rather than static topologies since they are important for adaptation and more interesting technically.

5.1 Syntax

Definitions. Figure 10 shows the syntax of Core EnsembleS terms and types. We let $u$ range over actor class names and $D$ range over definitions; each definition $\text{actor } u \text{ follows } S \{M\}$
Syntax of Types and Terms

Actor class names | \( u \)

Actor definitions | \( D ::= \text{actor } u \text{ follows } S \{ M \} \)

Roles | \( p, q, s, t \)

Recursion Labels | \( l \)

Behaviours | \( \kappa ::= M \mid \text{stop} \)

Types | \( A, B ::= \text{Pid}(S) \mid 1 \)

Values | \( V, W ::= x \mid () \)

Actions | \( L ::= \text{return } V \mid \text{continue } l \mid \text{raise } V \mid \text{self } V \mid \text{replace } V \mid \text{discover } S \)

| \( \mid \text{connect } \ell(V) \text{ to } W \mid \text{accept from } p \{ \ell_i(x_i) \mapsto M_i \}_i \mid \text{send } \ell(V) \text{ to } p \mid \text{receive from } p \{ \ell_i(x_i) \mapsto M_i \}_i \mid \text{wait } p \mid \text{disconnect from } p \)

Computations | \( M, N ::= \text{let } x \leftarrow M \text{ in } N \mid \text{try } L \text{ catch } M \mid 1::M \mid L \)

Syntax of Session Types

Session Actions | \( \alpha, \beta ::= p!t(A) \mid p?t(A) \mid p?r(A) \mid p?r(A) \mid \#p \)

Session Types | \( S, T, U ::= \Sigma_{i \in I}(\alpha_i \cdot S_i) \mid \mu X. S \mid X \mid \#p \mid \text{end} \)

Communication Actions | \( \uparrow ::= ! \mid ? \)

Disconnection Actions | \( \downarrow ::= \#\uparrow \mid \#\downarrow \)

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure10}
\caption{Syntax}
\end{figure}

specified the actor’s class name, session type, and behaviour. Like class tables in Featherweight Java [36], we assume a fixed mapping from class names to definitions.

Values. Since our calculus is inherently effectful, we work in the setting of fine-grain call-by-value [41], where we have an explicit static stratification of values and computations and an explicit evaluation order similar to A-normal form [20]. Values \( V, W \) describe data that has been computed, and for the sake of simplicity, consist of variables and the unit value. Other base values (such as integers or booleans) can be encoded or added straightforwardly.

Computations. The \texttt{let } \( x \leftarrow M \text{ in } N \) construct evaluates \( M \), binding its result to \( x \) in \( N \). The calculus supports exception handling over a single action \( L \) using \texttt{try } \texttt{L catch } \texttt{M} \text{ where } \texttt{M} \text{ is evaluated if } \texttt{L} \text{ raises an exception, and labelled recursion using } \texttt{L::M}, \text{ stating that inside term } \texttt{M}, \text{ a process can recurse to label } \texttt{L} \text{ using } \texttt{continue } \texttt{L}. \texttt{Actions } \texttt{L} \text{ denote the basic steps of a computation. The return } \texttt{V} \text{ construct denotes a value.}

Concurrency and adaptation constructs. The \texttt{new } \texttt{u} \text{ construct spawns a new actor of class } \texttt{u} \text{ and returns its PID. The } \texttt{self} \text{ construct returns the current actor’s PID. An actor can replace the behaviour of itself or another actor } \texttt{V} \text{ using } \texttt{replace } \texttt{V with } \texttt{K}. \text{ An actor can discover other actors following a session type } \texttt{S} \text{ using the } \texttt{discover } \texttt{S} \text{ construct, which returns the PID of the discovered actor.}

Session communication constructs. An actor can connect to an actor } \texttt{W} \text{ playing role } \texttt{p} \text{ using } \texttt{connect } \ell(V) \text{ to } W \text{ as } p, \text{ sending a message with label } \ell \text{ and payload } x. \text{ An actor can accept a connection from another actor playing role } p \text{ using } \texttt{accept from } p \{ \ell_i(x_i) \mapsto M_i \}_i \text{, which allows an actor to receive a choice of messages; given a message with label } \ell_j, \text{ the payload is bound to } x_j \text{ in the continuation } N_j. \text{ Once connected, an actor can communicate using the } \texttt{send} \text{ and } \texttt{receive} \text{ constructs. An actor can disconnect from } p \text{ using } \texttt{disconnect from } p, \text{ and await the disconnection of } p \text{ using } \texttt{wait p}. \]
Types. Types, ranged over by $A, B$, include the unit type $1$ and process IDs $\text{Pid}(S)$; the parameter $S$ refers to the statically-known initial session type of the actor (i.e., the session type declared in the follows clause of a definition). Unlike in channel-based session-typed systems, process IDs themselves need not be linear: any number of actors can have a reference to another actor, but each actor may only be in a single session at a time. PIDs can be passed as payloads in session communications.

Session types. Session types are ranged over by $S, T, U$ and follow the formulation of Hu and Yoshida [32]. A session type can be a choice of actions, written $\Sigma_{i \in I}(\alpha_i . S_i)$, a recursive session type $\mu X . S$ binding recursion variable $X$ in continuation $S$, a recursion variable $X$, a disconnection action $\# \downarrow p$, or the finished session $\text{end}$. The syntax of session types is more liberal than traditional ‘directed’ presentations in order to allow output-directed choices to send or connect to different roles.

Session actions $\alpha$ involve sending ($!$), receiving ($?$), connecting ($!!$), or accepting ($??$) a message $\ell(A)$ with label $\ell$ and type $A$; or awaiting another participant’s disconnection ($\# \uparrow$).

As well as disallowing self-communication, following Hu and Yoshida [32], we require the following syntactic restrictions on session types:

- **Definition 1 (Syntactic validity).** A choice type $S = \Sigma_{i \in I}(\alpha_i . S_i)$ is syntactically valid if:
  1. it is an output choice, i.e., each $\alpha_i$ is a send or connection action; or
  2. it is a directed input choice, i.e., $S = \Sigma_{i \in I}(p ? \ell_i(A_i) . S_i)$ or $S = \Sigma_{i \in I}(p ?? \ell_i(A_i) . S_i)$; or
  3. the choice consists of single wait action $\# \uparrow p . S$.

In the remainder of the paper, we assume that all session types are syntactically valid.

Session correlation. The most general form of explicit connection actions allows a participant to leave and re-join a session, or accept connections from multiple different participants. Such generality comes at a cost, since care must be taken to ensure that the same participant plays the role throughout the session.

To address this session correlation issue, Hu and Yoshida [32] propose two solutions: either augment global types with type-level assertions and check conformance dynamically, or adopt a lightweight syntactic restriction which requires that each local type must contain at most a single accept action as its top-level construct. We opt for the latter, enforcing the constraint as part of our safety property (§5.4.2), and by requiring that $\# \downarrow p$ does not have a continuation. (Note that the behaviour will repeat, so $p$ will be able to accept again after disconnecting). As Hu and Yoshida [32] show, this design still supports the most common use cases of explicit connection actions.

Global types. Traditional MPST works [14, 31] use global types to describe the interactions between participants at a global level, which are then projected into local types; projectability ensures safety and deadlock-freedom.

Since we are using explicit connection actions, traditional approaches are insufficiently flexible as they do not account for certain roles being present in certain branches but not others. Following Scalas et al. [54] and subsequently non-classical MPSTs [53], we instead formulate our typing rules and safety properties using collections of local types.

It is, however, still convenient to write a global type and have local types computed programatically. Global types are defined as follows:

\[
\begin{align*}
\text{Global Actions} & \quad \pi ::= \ p \rightarrow q : \ell(A) \mid p \rightarrow q : \ell(A) \mid p \# q \\
\text{Global Types} & \quad G ::= \Sigma_{i \in I}(\pi_i . G_i) \mid \mu X . G \mid X \mid \text{end}
\end{align*}
\]
Global actions $\pi$ describe interactions between participants: $p \rightarrow q : \ell(A)$ states that role $p$ sends a message with label $\ell$ and payload type $A$ to $q$. Similarly, $p \rightarrow q : \ell(A)$ states that $p$ connects to $q$ by sending a message with label $\ell$ and payload type $A$. The disconnection action $p \# q$ states that role $p$ disconnects from role $q$.

We can write the OnlineStore example from §2 as follows:

$$\begin{align*}
\text{Customer} & \rightarrow \text{Store} : \text{login(String)}, \mu \text{Browse}, \\
\text{Customer} & \rightarrow \text{Store} : \text{item(String)}, \text{Store} \rightarrow \text{Customer} : \text{price(Int)}. \mu \text{Browse} \\
& \quad + \text{Store} \rightarrow \text{Customer} : \text{address(String)}, \text{Store} \rightarrow \text{Courier} : \text{deliver(String)}. \\
\text{Courier} & \rightarrow \text{Store} : \text{ref(Int)}. \text{Courier} \# \text{Store}. \text{Store} \rightarrow \text{Customer} : \text{ref(Int)}. \\
& \quad \text{Store} \# \text{Customer}. \mu \text{end} \\
& \quad + \text{Customer} \rightarrow \text{Store} : \text{quit(1)}. \text{Store} \# \text{Customer}. \mu \text{end}
\end{align*}$$

Although projectability in our setting does not necessarily guarantee safety and deadlock-freedom, we show a projection algorithm, adapted from that of Hu and Yoshida [32], in Appendix A. The resulting local types can then be checked for safety (§5.4.2).

Protocols and Programs. Terms do not live in isolation; they refer to a set of protocols, and evaluate in the context of an actor. A protocol maps role names to local session types.

- **Definition 2 (Protocol).** A protocol is a set $\{p_i : S_i\}$ mapping role names to session types.

As an example, consider the protocol for the online shop example:

$$\begin{align*}
\text{Customer} : \text{Store}!! \text{login(String)}, \mu \text{Browse}, \\
& \quad \text{Store}!! \text{item(String)}, \text{Store}!! \text{price(Int)}. \mu \text{Browse} \\
& \quad \quad + \text{Store}!! \text{address(String)}, \text{Store}!! \text{ref(Int)}. \mu \text{Browse} \\
& \quad \quad + \text{Store}!! \text{quit(1)}. \mu \text{Browse}
\end{align*}$$

We can now consider an implementation of a Store actor, which uses discovery to find a courier. We write receive $\ell(x)$ from $p; M$ and accept $\ell(x)$ from $p; M$ as syntactic sugar for receive from $p \{\ell(x) \rightarrow M\}$ and accept from $p \{\ell(x) \rightarrow M\}$ respectively, and write $M; N$ as syntactic sugar for let $x \leftarrow M \text{in} N$ for a fresh variable $x$. We assume the existence of a function lookupPrice, and define CourierType as Store?? deliver(String). Store!! ref(Int). #\text{Store}.

actor Store follows try(Store) { 
accept login(credentials) from Customer;
Browse ::
receive from Customer {
\quad item(name) \rightarrow
\quad \quad send price(lookupPrice(name)) to Customer;
\quad continue Browse
\quad address(addr) \rightarrow
\quad \quad let pid \leftarrow discover CourierType in
\quad \quad connect deliver(addr) to pid as Courier;
\quad \quad receive ref(r) from Courier;
\quad \quad wait Courier;
\quad \quad send ref(r) to Customer;
\quad \quad disconnect from Customer
\quad quit(() \rightarrow disconnect from Customer
}
A program consists of actor definitions, protocol definitions, and the 'boot' clause to be run in order to set up initial actor communication.

Definition 3 (Program). An EnsembleS program is a 3-tuple \((\mathcal{D}, \mathcal{P}, M)\) of a set of definitions, protocols, and an initial term to be evaluated.

In the context of a program, we write \(\text{ty}(p)\) to refer to the session type associated with role \(p\) as defined by the set of protocols. Given an actor definition \(\text{actor } u \text{ follows } S \{M\}\), we define \(\text{sessionType}(u) = S\) and \(\text{behaviour}(u) = M\).

5.2 Typing rules

Figures 11 and 12 show the typing rules for EnsembleS. Value typing, with judgement \(\Gamma \vdash V : A\), states that under environment \(\Gamma\), value \(V\) has type \(A\). Judgement \(\Gamma \vdash D\) states that an actor definition \(\text{actor } u \text{ follows } S \{M\}\) is well-typed if its body is typable under, and fully consumes, its statically-defined session type \(S\). The behaviour typing judgement \(\{S\} \Gamma \vdash \kappa\) states that given static session type \(S\), behaviour \(\kappa\) is well-typed under \(\Gamma\). Specifically, \(\text{stop}\) is always well-typed, and \(M\) is well-typed if it is typable under and fully consumes \(S\).

5.2.1 Term typing.

The typing judgement for terms \(\{T\} \Gamma \vdash M : A \triangleleft S'\) reads "in an actor following \(T\), under typing environment \(\Gamma\) and with current session type \(S\), term \(M\) has type \(A\) and updates..."


We take an equi-recursive view of session types, identifying recursive sessions with their

\[ T\text{-}\text{Continue} \]

ensures that the pre-condition must match the label stored in the environment,

\[ \Gamma \vdash \text{M} \]

where

\[ T\text{-}\text{Replacement} \]

and returns the unit type.

\[ \Gamma \vdash \text{A} : \text{U} \]

local actor (i.e., the

\[ \text{a PID for the current actor, parameterised by the statically-defined session type of the} \]

Actor and adaptation rules. Rule T-New states that creating an actor of class \( \text{u} \) returns

a PID parameterised by the session type declared in the class of \( \text{u} \). Rule T-Self retrieves

a PID for the current actor, parameterised by the statically-defined session type of the

local actor (i.e., the \( T \) in the judgement \( \{ T \} \Gamma \vdash \text{M} : \text{A} \triangleq \text{S'} \)). Rule T-Discover states

\text{discover} \( \text{U} \) returns a PID of type \( \text{Pid}(\text{U}) \). Finally, given a behaviour \( \kappa \) typable under a static

session type \( \text{U} \), and a process ID with the matching static type \( \text{Pid}(\text{U}) \), T-Replacement allows

replacement, and returns the unit type.

Figure 12 Typing rules (2)
Exception handling rules. Figure 12 shows the rules for exception handling and session communication. T-Raise denotes raising an exception; since it does not return, it can have an arbitrary return type and postcondition. Rule T-Try types an exception handler try \( L \).catch \( M \) which acts over a single action \( L \). If \( L \) raises an exception, then \( M \) is evaluated instead. Since \( L \) only scopes over a single action, the try and catch clauses have the same pre- and post-conditions to allow the action to be retried if necessary.

▶ Remark 4. Following Mostrous and Vasconcelos [45], our try \( L \).catch \( M \) construct scopes over a single action and is discarded afterwards. We opt for this simple approach since in our setting exceptions are a means to an end, but (at the cost of a more involved type system) we could potentially scope over multiple actions as long as the handler is compatible with all potential exit conditions [23]. We leave a thorough exploration to future work.

Session communication rules. Rule T-Conn types a term connect \( \ell_j(V) \) to \( W \) as \( p_j \). Given the precondition is a choice type containing a branch \( p!!\ell_j(A_i) \). \( S_j \), and the remote actor reference is \( W \) of type Pid(S), the rule ensures that \( S \) is compatible with the type of \( p_j \), and ensures that the label and payload are compatible with the session type. The session type is then advanced to \( S_j \). Rule T-Send follows the same pattern.

Given a session type \( \Sigma_{i \in I} (p??\ell_i(A_i)) \cdot S \), rule T-Accept types term accept from \( p \{ \ell_i(x_i) \mapsto M_i \}_{i \in I} \), enabling an actor to accept connections with messages \( \ell_i \), binding the payload \( x_i \) in each continuation \( M_i \). Like case expressions in functional languages, each continuation must be typable under an environment extended with \( x_i : A_i \), under session type \( S \), and each branch must have same result type and postcondition. Rule T-Recv is similar.

Rule T-Wait handles waiting for a participant \( p \) to disconnect from a session, requiring a pre-condition of \( \# \mid p . S \), returning the unit type and advancing the session type to \( S \). Rule T-Disconnect is similar and advances the session type to end.

5.3 Operational semantics

We describe the semantics of EnsembleS via a deterministic reduction relation on terms, and a nondeterministic reduction relation on configurations.

5.3.1 Runtime syntax

Figure 13 shows the runtime syntax and the first part of the reduction rules for EnsembleS.

Whereas static syntax and typing rules describe code that a user would write, runtime syntax arises during evaluation. We introduce two types of runtime name: \( s \) ranges over session names, which are created when a process initiates a session, and \( a \) ranges over actor names, which uniquely identify each actor once it has been spawned by new.

Configurations. Configurations, ranged over by \( \mathcal{C}, \mathcal{D}, \mathcal{E} \), represent the concurrent fragment of the language. Like in the π-calculus [42], name restrictions \((\nu n) \mathcal{C}\) bind name \( n \) in \( \mathcal{C} \). \( \mathcal{C} \parallel \mathcal{D} \) denotes \( \mathcal{C} \) and \( \mathcal{D} \) running in parallel, and the 0 configuration denotes the inactive process.

Actors are represented at runtime as a 4-tuple \( (a, M, \sigma, \kappa) \), where \( a \) is the actor’s runtime name; \( M \) is the term currently evaluating; \( \sigma \) is the connection state; and \( \kappa \) is the actor’s current behaviour. A connection state is either disconnected, written \( \bot \), or playing role \( p \) in session \( s \) and connected to roles \( q \), written \( s[p](q) \).

Inspired by Mostrous and Vasconcelos [45] and Fowler et al. [22], a zapper thread \( \# s[p] \) indicates that participant \( p \) in session \( s \) cannot be used for future communications, for example due to the actor playing the role crashing due to an unhandled exception.
Runtime syntax

Names

Configurations

Connection state

Runtime environments

Evaluation contexts

Top-level contexts

Pure contexts

Definition 5

Whereas

Runtime typing environments. Whereas Γ is an unrestricted typing environment used for typing values and configurations, we introduce Δ as a linear runtime environment. Runtime environments can contain entries of type a : S, stating that actor a has statically-defined session type S, and entries of type s[p][q]:S, stating that in session s, role p is connected to roles q and currently has session type S.

Evaluation contexts. Due to our fine-grain call-by-value presentation, evaluation contexts E allow nesting only in the immediate subterm of a let expression. The top-level frame F can either be a hole, or a single, top-level exception handler. Pure contexts Ep do not include exception handling frames.

To run a program, we place it in an initial configuration.

Definition 5 (Initial configuration). An initial configuration for an EnsembleS program with boot clause M is of the form (va)((a, M, ⊥, stop)).
Configuration reduction (2)

Session reduction rules

\[ E-\text{CONN} \]

\[
\begin{align*}
\langle a, E[F\{\text{connect } \ell_j(V) \text{ to } b \text{ as } q]\}, \bot, \kappa_1 \rangle & \parallel \langle b, E'[F\{\text{accept from } p \{ \ell_i(x_i) \mapsto M_i \}_{i \in I}\}]\rangle, \bot, \kappa_2 \rangle \\
\langle a, E[F]\{\text{return } ()\} , s[p\{q\}, \kappa_1]\} & \parallel \langle b, E'[M_j(V/x_j)]\}, s[q\{p\}, \kappa_2]\rangle
\end{align*}
\]

\[ E-\text{CONN} \]

\[
\begin{align*}
\langle a, E[F\{\text{connect } \ell_j(V) \text{ to } b \text{ as } q]\}, s[p\{\bar{r}\}, \kappa_1]\} & \parallel \langle b, E'[F\{\text{accept from } p \{ \ell_i(x_i) \mapsto N_i \}_{i \in I}\}]\rangle, \bot, \kappa_2 \rangle \\
\langle a, E[F]\{\text{return } ()\} , s[p\{\bar{r}\}, \kappa_1]\} & \parallel \langle b, E'[N_j(V/x_j)]\}, s[q\{p\}, \kappa_2]\rangle
\end{align*}
\]

\[ E-\text{DISCON} \]

\[
\begin{align*}
\langle a, E[F\{\text{wait } q\}], s[p\{\bar{r}\}, \kappa_1]\} & \parallel \langle b, E'[F\{\text{disconnect from } p\}], s[q\{p\}, \kappa_2]\rangle \\
\langle a, E[F]\{\text{return } ()\} , s[p\{\bar{r}\}, \kappa_1]\} & \parallel \langle b, E'[F\{\text{return } ()\}], \bot, \kappa_2 \rangle
\end{align*}
\]

\[ E-\text{COMM} \]

\[
\begin{align*}
\langle a, E[F\{\text{send } \ell_j(V) \text{ to } q\}], s[p\{\bar{r}\}, \kappa_1]\} & \parallel \langle b, E'[F\{\text{receive from } p \{ \ell_i(x_i) \mapsto M_i \}_{i \in I}\}], s[q\{\bar{s}\}, \kappa_2]\rangle \\
\langle a, E[F]\{\text{return } ()\} , s[p\{\bar{r}\}, \kappa_1]\} & \parallel \langle b, E'[M_j(V/x_j)]\}, s[q\{\bar{s}\}, \kappa_2]\rangle
\end{align*}
\]

\[ E-\text{COMPLETE} \]

\[
\langle a, E[F]\{\text{return } V, s[p\{\emptyset\}, \kappa]\} \rightarrow \langle a, E[F]\{\text{return } V, \bot, \kappa\}
\]

\[ \text{Figure 14} \] Operational semantics (2)

5.3.2 Reduction rules

Term reduction \( \longrightarrow_M \) is standard \( \beta \)-reduction, save for \( E-\text{TRYRAISE} \) which evaluates the failure continuation in the case of an exception. We consider four subcategories of configuration reduction rules: actor and adaptation rules; session communication rules; exception handling rules; and administrative rules.

Actor / adaptation rules. Given a fully-evaluated actor, \( E-\text{LOOP} \) runs the term specified by the actor’s behaviour. Rule \( E-\text{NEW} \) allows actor \( a \) to spawn a new actor of class \( u \) by creating a fresh runtime actor name \( b \) and a new actor process of the form \( \langle b, M, \bot, M \rangle \) where \( M \) is the behaviour specified by \( u \), returning the process ID \( b \). Rules \( E-\text{REPLACE} \) and \( E-\text{REPLACESELF} \) handle replacement by changing the behaviour of an actor, returning the unit value to the caller. Rule \( E-\text{DISCOVER} \) returns the process ID of an actor \( b \) if it has the desired static session type \( S \). Rule \( E-\text{SELF} \) returns the PID of the local actor.

Session communication rules. An actor begins a session by connecting to another actor while disconnected; such a case is handled by rule \( E-\text{CONNINIT} \). Suppose we have a disconnected actor \( a \) evaluating a connection statement \( \text{connect } \ell_j(V) \text{ to } b \text{ as } p \), evaluating in parallel with a disconnected actor \( b \) evaluating an accept statement \( \text{accept from } p \{ \ell_i(x_i) \mapsto M_i \}_{i \in I} \). Rule \( E-\text{CONNINIT} \) returns the unit value to actor \( a \); creates a fresh session name restriction \( s \), sets the connection state of \( a \) to \( s[p\{q\}] \) and of \( b \) to \( s[q\{p\}] \); accepting actor \( b \) then evaluates continuation \( M_j \) with \( V \) substituted for \( x_j \). Since exception handlers only scope
Configuration reduction (3)

**Exception handling rules**

\[ \text{E-CommRaise} \quad \text{subj}(M) = q \]
\[ \langle a, E[M], s[p][\bar{p}], \kappa \rangle \parallel \langle q, \bar{p} \rangle \rightarrow \langle a, E[\text{raise}], s[p][\bar{p}], \kappa \rangle \parallel \langle q, \bar{p} \rangle \]

\[ \text{E-Fails} \]
\[ \langle a, E[p][\text{raise}], s[p][\bar{p}], \kappa \rangle \rightarrow \langle a, E[\text{raise}], s[p][\bar{p}], \kappa \rangle \parallel \langle a, \bot \rangle \]

\[ \text{E-FailS} \quad \langle a, E[P][\text{raise}], s[p][\bar{p}], \kappa \rangle \rightarrow \langle a, \text{raise}, \bot, \kappa \rangle \parallel \langle a, \bot \rangle \]

\[ \text{E-FailLoop} \quad \langle a, E[P][\text{raise}], s[p][\bar{p}], \kappa \rangle \rightarrow \langle a, \bot, \bot, \kappa \rangle \parallel \langle a, \bot \rangle \]

**Administrative rules**

\[ \text{E-LiftM} \quad M \rightarrow_{\text{M}} M' \]
\[ \langle a, E[M], \sigma, \kappa \rangle \rightarrow \langle a, E[M'], \sigma, \kappa \rangle \]

\[ \text{E-Equiv} \quad C \equiv C' \]
\[ \text{E-Par} \quad C \rightarrow C' \parallel D \rightarrow C' \parallel D \]

\[ \text{E-Nu} \quad C \rightarrow D \]

\[ \langle v_n C \rightarrow (v_n) D \]

**Configuration equivalence**

\[ \mathcal{C} \parallel D \equiv \mathcal{C} \parallel \mathcal{C} \]

\[ \mathcal{C} \parallel (\mathcal{C} \parallel D) \equiv (\mathcal{C} \parallel D) \parallel \mathcal{C} \]

\[ (v_{n_1})(v_{n_2})C \equiv (v_{n_2})(v_{n_1})C \]

\[ \mathcal{C} \parallel (v_n)D \equiv (v_n)(\mathcal{C} \parallel D) \quad \text{if } n \notin \text{fn}(\mathcal{C}) \]

\[ (v_s)(\parallel s[p_1] \parallel \cdots \parallel s[p_n]) \parallel \mathcal{C} \equiv \mathcal{C} \quad \mathcal{C} \parallel \bot \equiv \mathcal{C} \]

**Figure 15** Operational semantics (3)

Over a single communication action, the top-level frames \(F, F'\) in each actor are discarded if the communication succeeds. Rule E-CONN handles the case where the connecting actor is already part of a session and behaves similarly to E-CONNINIT, without creating a new session name restriction. A connection can fail if an actor attempts to connect to another actor which is terminated or is already involved in a session; in these cases, E-CONNFAIL raises an exception in the connecting actor.

Rule E-Disconn handles the case where an actor \(b\) leaves a session, synchronising with an actor \(a\). In this case, the unit value is returned to both callers, and the connection state of \(b\) is set to \(\bot\). Rule E-Comm handles session communication when two participants are already connected to the same session, and is similar to E-Conn. Rule E-Complete garbage collects a session after it has completed and sets the initiator’s connection state to \(\bot\).

**Exception handling rules.** Exception handling rules allow safe session communication in the presence of exceptions. Rule E-CommRaise states that if an actor is attempting to communicate with a role no longer present due to an exception, then an exception should be raised. We write \(\text{subj}(E[M]) = p\) if \(M \in \{\text{send } \ell(V) \rightarrow p, \text{receive from } p \{\ell_i(x_i) \rightarrow N_i\}, \text{wait } p, \text{disconnect from } p\}\). Rule E-Fails states that if a connected actor encounters an unhandled exception, then a zapper thread will be generated for the current role, the actor will become disconnected, and the current evaluation context will be discarded. Rule E-FailLoop restarts an actor encountering an unhandled exception.

**Administrative rules.** The remaining rules are administrative: E-LiftM allows term reduction inside an actor; E-Equiv allows reduction modulo structural congruence; E-Par allows reduction under parallel composition; and E-Nu allows reduction under name restrictions.

**Configuration equivalence.** Reduction includes configuration equivalence \(\equiv\), defined as the smallest congruence relation satisfying the axioms in Figure 15. The equivalence rules extend
We now turn our attention to showing that session typing allows runtime adaptation and discovery while precluding communication mismatches and deadlocks.

5.4 Metatheory

We now turn our attention to showing that session typing allows runtime adaptation and discovery while precluding communication mismatches and deadlocks.

5.4.1 Runtime typing

To reason about the metatheory, we introduce typing rules for configurations (Fig. 16): the judgement $\Gamma; \Delta \vdash C$ states that configuration $C$ is well-typed under term typing environment $\Gamma$ and runtime typing environment $\Delta$.

Rule T-Pid types actor name restriction $(\nu a)C$ by adding a PID into the term environment, and extending the runtime typing environment $a : S$; the linearity of the runtime typing environment therefore means that the system must contain precisely one actor with name $a$.

Session name restrictions $(\nu s)C$ are typed by T-Session. We follow the formulation of Scalas and Yoshida [53] which types multiparty sessions using a parametric safety property $\varphi$; we discuss safety properties in more depth in Section 5.4.2. Let $\Delta'$ be a runtime typing environment containing only mappings of the form $s[p] : (p : q) : S$. Assuming $\Delta$ does not contain any mappings involving session $s$ and $\Delta'$ satisfies $\varphi$, the rule states that $C$ is typable under typing environment $\Gamma$ and runtime typing environment $\Delta, \Delta'$. It is sometimes convenient to annotate session $\nu$-binders with their environment, e.g., $(\nu s : \Delta)C$.

Rule T-Par types each subconfiguration of a parallel composition by splitting the linear runtime environment. Rule T-Zap types a zapper thread $\downarrow s[p]$, assuming the runtime environment contains an entry $s[p,q] : S$ for any session type $S$.

Finally, rules T-DisconnectedActor and T-ConnectedActor type disconnected and connected actor configurations respectively. Given an actor with name $a$ and static session type $T$, both rules require that the typing environment contains $a : \text{Pid}(T)$ and runtime environment contains $a : T$. Both rules require that the current session type is fully consumed by the currently-evaluating term and that the actor's behaviour should be typable under $T$. Rule T-DisconnectedActor requires that the currently-evaluating term must be typable under either $T$ or end, whereas to type a connection state of $s[p,q]$ and current session type $S$, T-ConnectedActor requires an entry $s[p,q] : S$ in the runtime environment.
We now prove that reduction preserves typability and thus that actors only perform communication actions specified in their session types. Due to our use of explicit connection actions, classical MPST approaches are too limited for our purposes. Our approach, following that of Scalas and Yoshida [53], is to introduce a labelled transition system (LTS) on local types, and specify a generic safety property based around local type reduction. The property can then refined; in our case, we will later specialise the property in order to prove progress.

5.4.2 Preservation

We now prove that reduction preserves typability and thus that actors only perform communication actions specified in their session types. Due to our use of explicit connection actions, classical MPST approaches are too limited for our purposes. Our approach, following that of Scalas and Yoshida [53], is to introduce a labelled transition system (LTS) on local types, and specify a generic safety property based around local type reduction. The property can then refined; in our case, we will later specialise the property in order to prove progress.

Reduction on runtime typing environments. Figure 17 shows the LTS on runtime typing environments. There are two judgements: $\Delta \overset{\gamma}{\rightarrow} \Delta'$, which handles reduction of individual local types, and a synchronisation judgement $\Delta \overset{\rho}{\rightarrow} \Delta'$. Rule ET-CONN handles the reduction of role $p$, where the choice session type contains a connection action $q!\ell_j(A_j)$. If $q$ has a statically-defined session type $\Sigma_{k \in K}(p ? \ell_k(B_k) \cdot T_k)$ which can accept $\ell_j$ from from $p$, and the payload types match, reduction advances $p$’s session type, adds $q$ to $p$’s connected role set, and introduces an entry for $q$ into the environment. The reduction emits a label $s.p \rightarrow q::\ell_j$.

Given a role $p$ connected to $q$ with a session choice containing a send or receive action $q!\ell_j(A_j) \cdot S_j$, rule ET-ACT will emit a label $s.p::\ell_j(A_j)$ and advance the session type of $p$.

Rule ET-WAIT handles the reduction of $#q \cdot S$ actions, $s[p](\widehat{r}, q, \#q) \cdot S$, where $p$ waits for $q$ to disconnect: the reduction emits label $p.q#\uparrow$ and removes $q$ from $p$’s connected roles.
Similarly, rule ET-DISCONN handles disconnection, by emitting label $p\cdot q\downarrow$ and removing the entry from the environment. ET-REC handles recursive types, and the ET-CONG rules handle reduction of sub-environments.

Rule ET-CONNSYNC states that connection is a synchronisation action, and rules ET-COMM and ET-DISCONN handle synchronisation between dual actions in sub-environments, emitting synchronisation labels $s\cdot p, q\cdot \ell$ and $s\cdot p\#q$ respectively. We omit the congruence rules for synchronisation actions.

We say that a runtime environment reduces, written $\Delta \Longrightarrow$, if there exists some $\Delta'$ such that $\Delta \Longrightarrow \Delta'$.

**Safety.** A safety property describes a set of invariants on typing environments which allow us to prove preservation. Since the type system is parametric in the given safety property, we can tweak the property to permit or rule out different typing environments satisfying particular behavioural properties; however, we need only prove type preservation once, using the weakest safety property. Our safety property is different to the safety property described by Scalas and Yoshida [53] in order to account for explicit connection actions.

\[\text{Definition 6 (Safety Property). } \varphi \text{ is a safety property of runtime typing contexts } \Delta \text{ if:}\]

1. $\varphi(\Delta, s[p]\langle r \rangle : \Sigma_{i \in I}(\alpha_i, S_i), s[q]\langle s \rangle : \Sigma_{j \in J}(p?\ell_j(B_j)) \cdot T_j) \) implies that if $q!\ell_k(A_k) \in \{\alpha_i\}_{i \in I}$, then $k \in J$, $q \in r$, $p \in s$, and $A_k = B_k$.
2. $\varphi(\Delta, s[p]\langle r \rangle : \Sigma_{i \in I}(\alpha_i, S_i)) \) implies that if $\alpha_i = q!\ell_j(A_j) \in \{\alpha_i\}_{i \in I}$, then $q \notin r$, $s[q]\langle s \rangle \notin \text{dom}(\Delta)$, and $\text{ty}(q) = \Sigma_{k \in K}(p?\ell_k(B_k)) \cdot T_k$ with $j \in K$ and $A_j = B_j$.
3. $\varphi(\Delta, s[p]\langle q \rangle : S) \) implies $\varphi(\Delta, s[p]\langle q \rangle : S[\mu X.S/X])$.
4. $\varphi(\Delta)$ and $\Delta \Longrightarrow \Delta'$ implies $\varphi(\Delta')$.

A runtime typing environment is safe, written $\text{safe}(\Delta)$, if $\varphi(\Delta)$ for a safety property $\varphi$.

Clause (1) ensures that communication actions between participants are compatible: if $p$ is sending a message with label $\ell$ and payload type $A$ to $q$, and $q$ is receiving from $p$, then the two roles must be connected, and $q$ must be able to receive $\ell$ with a matching payload.

Clause (2) states that if $p$ is connecting to a role $q$ with label $\ell$, then $q$ should not already be involved in the session, and should be able to accept from $p$ on message label $\ell$ with a compatible payload type. The requirement that $q$ is not already involved in the session rules out the correlation errors described in Section 5.2.1. Clause (3) handles recursion, and clause (4) requires that safety is preserved under environment reduction.

**Concretising the safety property.** In order to deduce that a runtime typing environment $\Delta$ is safe, we define $\varphi(\Delta) = \{\Delta' \mid \Delta \Longrightarrow^* \Delta'\}$ and verify that $\varphi$ is a safety property by ensuring that it satisfies all clauses in Definition 6.

**Properties on protocols and programs.** It is useful to distinguish active and inactive session types, depending on whether their associated role is currently involved in a session, and identify the initiator of a session.

\[\text{Definition 7 (Active and Inactive Session Types). } A \text{ session type } S \text{ is inactive, written } \text{inactive}(S), \text{ if } S = \text{end} \text{ or } S = \Sigma_{i \in I}(p?\ell_i(A_i) \cdot S_i). \text{ Otherwise, } S \text{ is active, written } \text{active}(S).\]

\[\text{Definition 8 (Initiator, unique initiator). } \text{Given a protocol } P, \text{ a role } p : S_p \in P \text{ is an initiator if } S_p = \Sigma_{i \in I}(\alpha_i, S_i), \text{ and each } \alpha_i \text{ is a connection action } q!\ell_i(A_i). \text{ Role } p \text{ is a unique initiator of } P \text{ if inactive}(S_q) \text{ for all } q \in P \setminus \{p : S_p\}.\]
A protocol is well-formed if it is safe and has a unique initiator.

**Definition 9** (Well-formed protocol). A protocol \( P = \{ p_i : S_i \}_{i \in I} \) is well-formed if it has a unique initiator \( q \) of type \( S \) and \( \text{safe}(s[q](\emptyset):s) \) for any \( s \).

By way of example, the online shopping protocol is well-formed: Customer is the protocol’s unique initiator, and it is straightforward to verify that \( \text{safe}(s[\text{Customer}](\emptyset):\text{ty}(\text{Customer})) \).

**Definition 10** (Well-formed program). A program \((\overrightarrow{D}, \overrightarrow{P}, M)\) is well-formed if:

1. For each actor definition \( D = \text{actor} u \text{ follows} S \{ N \} \in \overrightarrow{D}, \) there exists some role \( p \in \overrightarrow{P} \) such that \( \text{ty}(p) = S \), and \( \{ S \} \cdot | S \triangleright N : A \triangleright \text{end} \)
2. Each protocol \( P \in \overrightarrow{P} \) is well-formed and has a distinct set of roles
3. The ‘boot clause’ \( M \) is typable under the empty typing environment and does not perform any communication actions: \( \{ \text{end} \} \cdot | \text{end} \triangleright M : A \triangleright \text{end} \)

When discussing the metatheory, we only consider configurations defined with respect to a well-formed program. Specifically, we henceforth assume that each actor definition in the system follows a session type matched by a role in a given protocol, assume each role belongs to a single protocol, and assume that all protocols are well-formed.

Given a safe runtime environment, configuration reduction preserves typability; details can be found in Appendix B. We write \( \mathcal{R}^n \) for the reflexive closure of a relation \( \mathcal{R} \).

**Theorem 11** (Preservation (Configurations)). Suppose \( \Gamma; \Delta \vdash C \) with \( \text{safe}(\Delta) \) and where \( C \) is defined wrt. a well-formed program. If \( C \rightarrow C' \), then there exists some \( \Delta' \) such that \( \Delta \rightarrow^* \Delta' \) and \( \Gamma; \Delta' \vdash C' \).

Preservation shows that each actor conforms to its session type, and that communication never introduces unsoundness due to mismatching payload types.

### 5.4.3 Progress

We now show a progress property, which shows that given protocols which satisfy a progress property, EnsembleS configurations do not get stuck due to deadlocks.

A final runtime typing environment contains a single, disconnected role of type end, reflecting the intuition that all roles will eventually disconnect from a protocol initiator.

**Definition 12** (Final environment). An environment \( \Delta \) is final, written end(\( \Delta \)), \( \Delta = \{ s[p](\emptyset):\text{end} \} \) for some \( s \) and \( p \).

So far, we have considered safe protocols, which ensure the absence of communication mismatches. We say that an environment satisfies progress if each active role can eventually perform an action, each potential send is eventually matched by a receive, and non-reducing environments are final. Let \( \text{roles}(\rho) \) denote the roles referenced in a synchronisation label (i.e., \( \text{roles}(\rho) = \{ p, q \} \) for \( \rho \in \{ s;p \rightarrow q::{\ell}, s;p,q::{\ell}, s;p\#q \} \).

**Definition 13** (Progress (Runtime typing environments)). A runtime typing environment \( \Delta \) satisfies progress, written prog(\( \Delta \)), if:

- (Role progress) for each \( s[p](\emptyset):S_i \in \Delta \) s.t. \( \text{active}(S_i) \), \( \Delta \rightarrow^* \Delta' \) \( \Downarrow \) with \( p \in \text{roles}(\rho) \)
- (Eventual comm.) if \( \Delta \rightarrow^* \Delta' \xrightarrow{p:q::{\ell}(A)} \), then \( \Delta' \xrightarrow{\vec{\rho}} \Delta'' \xrightarrow{\vec{\rho}'p:q::{\ell}(A)} \), with \( p \notin \text{roles}(\vec{\rho}') \)
- (Correct termination) \( \Delta \rightarrow^* \Delta' \not\rightarrow \) implies end(\( \Delta \))
The online shopping example satisfies progress, since all roles will always eventually be able to fire an action once connected, and since all roles disconnect, the non-reducing final environment will be of the form \( s[\text{Customer}](\emptyset) : \text{end} \).

**Definition 14 (Progress (Programs)).** A well-formed program \((\overrightarrow{P}, \overrightarrow{P}, M)\) satisfies progress if each \( P \in \overrightarrow{P}\) has a unique initiator \( q \) of type \( S \) and \( \text{prog}(s[q](\emptyset) : S) \) for any \( s \).

It is useful to define a configuration context \( G \) as the one-hole context \( G := [ ] | (\nu s)G | G \parallel C \). A session consists of a session name restriction and all connected actors and zapper threads. Each well-typed configuration can be written as a sequence of sessions, followed by all disconnected actors.

**Definition 15 (Session).** A configuration is a session \( S \) if it can be written:

\[
(\nu s)\langle a_1, M_1, s[p_1]\rangle(q_1, \kappa_1) \parallel \cdots \parallel \langle a_m, M_m, s[p_m]\rangle(q_m, \kappa_m) \parallel \xi s[p_{m+1}] \parallel \cdots \parallel \xi s[p_n] 
\]

An actor is terminated if it has reduced to a value or has an unhandled exception, and has the behaviour stop. An unmatched discover occurs when no other actors match a given session type. An actor is accepting if it is ready to accept a connection.

**Definition 16 (Terminated actor, unmatched discover, accepting actor).**

- An actor \( \langle a, M, \sigma, \kappa \rangle \) is terminated if \( M = \text{return} V \) or \( M = E_p[\text{raise}] \), and \( \kappa = \text{stop} \).
- An actor \( \langle a, E[\text{discover} S], \sigma, \kappa \rangle \) which is a subconfiguration of \( C \) has an unmatched discover if no other non-terminated actor in \( C \) has session type \( S \).
- An actor \( \langle a, M, \sigma, \kappa \rangle \) is accepting if \( M = E[\text{accept from} p \{ \ell_j(x_j) \rightarrow N_j \}] \) for some evaluation context \( E \) and role \( p \).

Unhandled exceptions will propagate through a session, progressively cancelling all roles. A failed session consists of only zapper threads.

**Definition 17 (Failed session).** We say that a session \( S \) is a failed session, written failed\((S)\), if \( S \equiv (\nu s)\{ \xi s[p_1] \parallel \cdots \parallel \xi s[p_n] \} \).

The key session progress lemma establishes the reducibility of each session which does not contain an unmatched discover and is typable under a reducible runtime typing environment.

**Lemma 18 (Session Progress).** If \( \vdash C \) where \( C \) does not contain an unmatched discover, \( C \equiv G[S] \) and \( S = (\nu s : \Delta)D \) with \( \text{prog}(\Delta) \), and \( S \) is not a failed session, then \( C \rightarrow \).

There are several steps to proving Lemma 18. First, we introduce exception-aware reduction on runtime typing environments, which explicitly accounts for zapper threads at the type level, and show that exception-aware environments threads retain safety and progress. Second, we introduce flattenings, which show that runtime typing environments containing only unary output choices can type configurations blocked on communication actions, and that flattenings preserve environment reducibility. Finally, we show that configurations typable under flat, reducible typing environments can reduce. Full details can be found in Appendix B.

We can now show our second main result: in the absence of unmatched discovers, a configuration can either reduce, or it consists only of accepting and terminating actors.

**Theorem 19 (Progress).** Suppose \( \vdash C \) where \( C \) is defined wrt. a well-formed program which satisfies progress, and \( \text{prog}(\Delta) \) for each \( (\nu s : \Delta)C' \) in \( C \). If \( C \) does not contain an unmatched discover, either \( \exists D \) such that \( C \rightarrow D \), or \( C \equiv 0 \), or \( C \equiv (\nu b_1 \cdots \nu b_n)((b_1, N_1, \bot, \kappa_1) \parallel \cdots \parallel (b_n, N_n, \bot, \kappa_n)) \) where each \( b_i \) is terminated or accepting.
The proof eliminates all failed sessions by the structural congruence rules; shows that the presence of sessions implies reducibility (Lem. 18); and reasons about disconnected actors.

In addition to each actor conforming to its session type (Thm. 11), Theorem 19 guarantees that the system does not deadlock. It follows that session types ensure safe communication.

Theorem 19 assumes the absence of unmatched discovers. This is not a significant limitation in practice, however, as unmatched discovers can be mitigated with timeouts, where a timeout would trigger an exception.

6 Related Work

**Behavioural typing for actors.** Mostrous and Vasconcelos [46] present the first theoretical account of session types in an actor language; their work effectively overlays a channel-based session typing discipline on mailboxes using Erlang’s reference generation capabilities.

Neykova and Yoshida [48] use MPSTs to specify communication in an actor system, implemented in Python. Fowler [21] implements similar ideas in Erlang, with extensions to allow subsessions [17] and failure handling. Neykova and Yoshida [49] later improve the recovery mechanism of Erlang by using MPSTs to calculate a minimal set of affected roles. The above works check multiparty session typing dynamically. We are first to both formalise and implement static multiparty session type checking for an actor language.

Active objects (AOs) [15] are actor-like concurrent objects where results of asynchronous method invocations are returned through futures. Bagherzadeh and Rajan [4] study order types for an AO calculus, which characterise causality and statically rule out data races. In contrast to MPSTs, order types work bottom-up through type inference. Kamburjan et al. [39] apply an MPST-like system to Core ABS [38], a core AO calculus; they establish soundness via a translation to register automata rather than via an operational semantics.

de’Liguoro and Padovani [16] introduce mailbox types, a type system for first-class, unordered mailboxes. Their calculus generalises the actor model, since each process can be associated with more than one mailbox. Their type discipline allows multiple writers and a single reader for each mailbox, and ensures conformance, deadlock-freedom, and for many programs, junk-freedom. Our approach is based on MPSTs and is more process-centric.

**Non-classical multiparty session types.** MPSTs were introduced by Honda et al. [31]. Classical MPST theories are grounded in binary duality: safety follows as a consequence of consistency (pointwise binary duality of interactions between participants), and deadlock-freedom follows from projectability from a global type.

Unfortunately, classical MPSTs are restrictive: there are many protocols which are intuitively safe but not consistent. Scalas and Yoshida [53] introduced the first non-classical multiparty session calculus. Instead of ensuring safety using binary duality, they define an LTS on local types and safety property suitable for proving type preservation; since the type system is parametric in the safety property (inspired by Igarashi and Kobayashi [35] in the π-calculus), the property can be customised in order to guarantee different properties such as deadlock-freedom or liveness. Hu and Yoshida [32] formalise MPSTs with explicit connection actions via an LTS on types rather than providing a concrete language design or calculus; in our setting, a calculus is vital in order to account for the impact of adaptation constructs. A key contribution of our work is the use of non-classical MPSTs to prove preservation and progress properties for a calculus incorporating MPSTs with explicit connection actions.
Adaptation. None of the above work considers adaptation. The literature on formal studies of adaptation is mainly based on process calculi, without programming language design or implementation. Bravetti et al. [8] develop a process calculus that allows parts of a process to be dynamically replaced with new definitions. Their later work [9] uses temporal logic rather than types to verify adaptive processes. Di Giusto and Pérez [18] define a session type system for the same process calculus, and prove that adaptation does not disrupt active sessions. Later, Di Giusto and Pérez [19] use an event-based approach so that adaptation can depend on the state of a session protocol. Anderson and Rathke [2] develop an MPST-like calculus and study dynamic software update providing guarantees of communication safety and liveness. Differently from our work, they do not consider runtime discovery of software components and do not provide an implementation.

Coppo et al. [13] consider self-adaptation, in which a system reconfigures itself rather than receiving external updates. They define an MPST calculus with self-adaptation and prove type safety. Castellani et al. [11] extend [13] to also guarantee properties of secure information flow, but neither of these works have been implemented. Dalla Preda et al. [51] develop the AIOCJ system based on choreographic programming for runtime updates. Their work is implemented in the Jolie language [44], but they do not consider runtime discovery.

In this work we focus on correct communication in the absence of adversaries, and do not consider security. The literature on security and behavioural types is surveyed by Bartoletti et al. [5] and could provide a basis for future work on security properties.

7 Conclusion and Future Work

Modern computing increasingly requires software components to adapt to their environment, by discovering, replacing, and communicating with other components which may not be part of the system’s original design. Unfortunately, up until now, existing programming languages have lacked the ability to support adaptation both safely and statically. We therefore asked:

Can a programming language support static (compile-time) verification of safe runtime dynamic self-adaptation, i.e., discovery, replacement and communication?

We have answered this question in the affirmative by introducing EnsembleS, an actor-based language supporting adaptation, which uses multiparty session types to guarantee communication safety, using explicit connection actions to invite discovered actors into a session. We have demonstrated the safety of our system by proving type soundness theorems which state that each actor follows its session type, and that communication does not introduce deadlocks. Our formalism makes essential use of non-classical MPSTs.

Future work. Currently, in both the theory and implementation, each actor only takes part in a single session. Unlike dynamically-checked implementations of session typing for actors [21, 47], this means that a message received by an actor in one session cannot trigger an interaction in another (e.g., the Warehouse example in [47]). A key focus for future work will be to allow actors to partake in multiple sessions.

Currently, EnsembleS discovery and replacement requires type equality. We envisage that we could relax this constraint to subtyping [54] or perhaps bisimilarity on local types to increase expressiveness.

In order to avoid session correlation errors, we require that each role includes at most a single top-level accept construct (c.f. [32]). It would be interesting to investigate the more general setting, which would likely require dependent types.
References


REFERENCES


36 Atsushi Igarashi, Benjamin C Pierce, and Philip Wadler. Featherweight Java: a minimal core calculus for Java and GJ. ACM Transactions on Programming Languages and Systems, 23(3):396–450, 2001.


30 REFERENCES


A Global types and projection

In this section, we show how global types can be projected into the local types used in the core formalism. Unlike in classic MPST works, it is not the case that projection alone guarantees safety and deadlock-freedom in itself. Rather, projection produces local types, which can be validated separately as described in the main body of the paper.

This section is mostly a straightforward adaptation of the work of Hu and Yoshida [32] to our setting.

Syntax of types. Similar to the presentation of local types, the key difference between this presentation of global types and standard MPST systems is that instead of having branching of the form \( r \rightarrow s(\ell_i : G_i) \), where a single role makes a choice, this presentation of global types provides arbitrary summations of global actions. The standard sending action is therefore \( p \rightarrow q : \ell(A). G \) which involves role \( p \) sending message \( \ell(A) \) to \( q \).

A key technical innovation is explicit connection actions \( (p \rightarrow q : \ell(A)) \) which establish a connection between two roles \( p \) and \( q \) by sending a label \( \ell \). Conversely, disconnection \( p \# q \) is a directed disconnection where \( p \) disconnects from \( q \), and \( q \) waits for \( p \)’s disconnection.

Instead of assuming that all roles are connected at the start of the the session, in order to communicate, each role must be connected explicitly. This allows communication paths where one party isn’t involved (as in Hu and Yoshida’s travel agent example).

Projection. Global types can be projected at a role in order to obtain a local type. In standard MPST systems, a global type is well-formed if it is closed, contractive, and projectable at all roles. A well-formed global type is then guaranteed to be deadlock-free.

Definition 20 (Initiator (global type)). We say that \( p \) is an initiator of \( G \) if \( p \in \text{roles}(G) \) and \( G \vdash p = \Sigma_{i \in I}(p_i \cdot G_i) \), where each \( p_i \) is a connection action. We say that \( p \) is the unique initiator of \( G \) if it is the only initiator.

Given the above definitions, we can show that the set of projected local types are syntactically valid.

Syntactic validity of projected local types.

REFERENCES
Meta-level definitions

\[
\begin{align*}
\text{isOutput}(L) & \triangleq L \in \{p!\ell(A), p!!\ell(A)\} \\
\text{isInput}(L) & \triangleq L \in \{p?\ell(A), p??\ell(A)\} \\
\text{subj}(p \rightarrow q : \ell(A)), \text{subj}(p \rightarrow q : \ell(A)), \text{subj}(p \# q) & \triangleq p \\
\text{obj}(p \rightarrow q : \ell(A)), \text{obj}(p \rightarrow q : \ell(A)), \text{obj}(p \# q) & \triangleq q
\end{align*}
\]

Projection

\[
\begin{align*}
G[r] & \Rightarrow G[r] \\
(p \rightarrow q : \ell(A), G)[r] & \Rightarrow \begin{cases} 
q!\ell(A). (G[r]) & r = p \\
p?\ell(A). (G[r]) & r = q \\
G[r] & r \notin \{p, q\}
\end{cases} \\
(p \rightarrow q : \ell(A), G)[r] & \Rightarrow \begin{cases} 
q!!\ell(A). (G[r]) & r = p \\
p??\ell(A). (G[r]) & r = q \\
G[r] & r \notin \{p, q\}
\end{cases} \\
(p \# q, G)[r] & \Rightarrow \begin{cases} 
\#\downarrow q & r = p \text{ and } G[r] = \text{end} \\
\#\uparrow p \cdot (G[r]) & r = q \\
G[r] & r \notin \{p, q\}
\end{cases} \\
\Sigma_{i \in I}(G_i)[r] & \Rightarrow \begin{cases} 
X & \forall i \in I. (G_i[r]) = X \\
\text{end} & \forall i \in I. (G_i[r]) = \text{end} \\
|I| > 1, |J| > 0, \text{ and} & \\
\Sigma_{j \in J \subseteq I}(L_j = G_j[r]) & \forall k \in I \setminus J. G_k[r] = \text{end or } X \in \Phi, \text{ and} \\
\text{either} & \forall j \in J. \text{isOutput}(L_j) \\
& \exists p. \forall j \in J. \text{isInput}(L_j) \land \text{subj}(L_j) = q
\end{cases} \\
\mu X.G[r] & \Rightarrow \begin{cases} 
\text{end} & G[r] = X' \text{ or end} \\
G[\Delta, X][r] & \text{otherwise}
\end{cases} \\
X[r] & = X \\
\text{end}[r] & = \text{end}
\end{align*}
\]

\hspace{1cm} Figure 18 Global types and projection
Lemma 21. Suppose $p$ is the unique initiator of $G$. If $p \vdash \text{unf}(G)$ and $(G | q = L_q)_{q \in \text{roles}(G)}$, then each $L_q$ is syntactically valid.

Proof sketch. The result can be established by induction on the derivation of $G \models_{\phi} p$.

Due to the partiality of the projection operation, disconnection actions must only occur as unary choices, and role enabling coupled with the conditions on the projection of non-unary choices preclude mixed choice.
B Proofs for Section 5

B.1 Preservation

► Lemma 22 (Preservation (Terms)). If \{T\} Γ ⊢ S ▷ M:A ▷ S′ and M → M N, then \{T\} Γ ⊢ S ▷ M N:A ▷ S′.

Proof. By induction on the derivation of M → M N.

► Lemma 23 (Preservation (Equivalence)). If Γ; ∆ ⊢ C and C ≡ D, then Γ; ∆ ⊢ D.

Proof. By induction on the derivation of C ≡ D.

► Lemma 24 (Substitution). If \{T\} Γ; x : A ⊢ S ▷ M:B ▷ S′ and Γ ⊢ V : A, then \{T\} Γ ⊢ S ▷ M\{V/x\}:B ▷ S′.

Proof. By induction on the derivation of \{T\} Γ; x : A ⊢ S ▷ M:B ▷ S′.

► Lemma 25 (Subterm typability). Suppose D is a derivation of \{T\} Γ ⊢ S ▷ E[M]:A ▷ S′. Then there exists some subderivation D′ of D concluding \{T\} Γ ⊢ S ▷ E[M]:A ▷ S′" for some type B and local type S′", where the position of D′ in D corresponds to that of the hole in E.

Proof. By induction on the structure of E.

► Lemma 26 (Replacement). If:

1. D is a derivation of \{U\} Γ ⊢ S ▷ E[M]:A ▷ T
2. D′ is a subderivation of D concluding \{U\} Γ ⊢ S ▷ M:B ▷ T′, where the position of D′ in D corresponds to that of the hole in E
3. \{U\} Γ ⊢ S ▷ N:B ▷ T′

Then \{U\} Γ ⊢ S ▷ E[N]:A ▷ T.

Proof. By induction on the structure of E.

Due to the absence of exception handling frames which constrain the pre-condition to match that of the failure continuation, pure contexts admit a more liberal replacement lemma.

► Lemma 27 (Replacement (Pure contexts)). If:

1. D is a derivation of \{U\} Γ ⊢ S ▷ E[M]:A ▷ T
2. D′ is a subderivation of D concluding \{U\} Γ ⊢ S ▷ M:B ▷ T′, where the position of D′ in D corresponds to that of the hole in E
3. \{U\} Γ ⊢ S ▷ N:B ▷ T′

Then \{U\} Γ ⊢ S ▷ E[N]:A ▷ T.

Proof. By induction on the structure of E, noting that S is not constrained by exception handling frames.

► Theorem 11 (Preservation (Configurations)). Suppose Γ; ∆ ⊢ C with \text{safe}(∆) and where C is defined wrt. a well-formed program. If C → C′, then there exists some ∆′ such that ∆ → ∆′ and Γ; ∆′ ⊢ C′.

Proof. By induction on the derivation of C → C′. Where there is a choice of whether \(\sigma = \bot\) or \(\sigma = s[p][q]:S\), we show the latter case; the technique for proving the former case is identical.

Case E-Loop
(\(a, \text{return}\ V, \bot, M\)) \(\rightarrow\) (\(a, M, \bot, M\))

**Assumption:**
\[
\begin{array}{c}
    a : \text{Pid}(T) \in \Gamma \quad S = T \lor S = \text{end} \quad \{T\} \Gamma \mid S \triangleright \text{return} V : B \triangleleft \text{end} \\
    \Gamma; a : T \triangleright (a, \text{return} V, \bot, M)
\end{array}
\]

Recomposing:
\[
\begin{array}{c}
    a : \text{Pid}(T) \in \Gamma \quad \{T\} \Gamma \mid T \triangleright M : A \triangleleft \text{end} \\
    \Gamma; a : T \triangleright (a, M, \bot, M)
\end{array}
\]

as required.

**Case E-New**
\[
(\langle a, E [\text{new}\ u], \sigma, \kappa \rangle \rightarrow (\nu b)((\langle a, E [\text{return}\ b], \sigma, \kappa \rangle \parallel \langle b, M, \bot, M \rangle))\]

where \(b\) is fresh, and \(u.\text{behaviour} = M\).

**Assumption:**
\[
\begin{array}{c}
    a : \text{Pid}(S) \in \Gamma \quad S = \text{end} \quad \{T\} \Gamma \mid S \triangleright E [\text{new}\ u] : A \triangleleft \text{end} \\
    \Gamma; a : S, s[p[\hat{q}]] : S' \triangleright (a, E [\text{new}\ u], s[p[\hat{q}]], \kappa_1)
\end{array}
\]

By Lemma 25:
\[
\text{u.\sessionType} = T \\
\{S\} \Gamma \mid S' \triangleright \text{new}\ u : \text{Pid}(T) \triangleleft S'
\]

By Lemma 26, \(\{S\} \Gamma, b : \text{Pid}(T) \mid T \triangleright \text{return} b : \text{Pid}(T) \triangleleft S'\).

Let \(\Gamma' = \Gamma, b : \text{Pid}(T)\). Note that by weakening, everything typable under \(\Gamma\) is also typable under \(\Gamma'\).

By T-DEF:
\[
\{T\} \cdot \mid T \triangleright M : B \triangleleft \text{end} \\
\vdash \text{actor}\ u\ \text{follows}\ T\ \{M\}
\]

Again by weakening, \(\{T\} \Gamma' \mid T \triangleright M : B \triangleleft \text{end}\).

Recomposing:
\[
\begin{array}{c}
    a : \text{Pid}(S) \in \Gamma' \quad b : \text{Pid}(T) \in \Gamma' \quad \{T\} \Gamma' \mid T \triangleright M : B \triangleleft \text{end} \\
    \Gamma; a : S, s[p[\hat{q}]] : S' \triangleright (a, E [\text{return}\ b], s[p[\hat{q}]], \kappa_1) \\
    \Gamma' ; b : T \triangleright (b, M, \bot, M)
\end{array}
\]

as required.
Case E-Replace

\[ \langle a, E[\text{replace } b \text{ with } \kappa_2'], \sigma, \kappa_1 \rangle \| \langle b, M, \sigma, \kappa_2 \rangle \]

Assumption:

\[ \{ U_a \} \Gamma \vdash S \triangleright E[\text{replace } b \text{ with } \kappa_2']; A \triangleleft \text{end} \quad \{ U_a \} \Gamma \vdash \kappa_1 \]

By Lemma 25:

\[ \{ U_a \} \Gamma \vdash \kappa_2' \quad \Gamma \vdash b \triangleright \text{Pid}(U_b) \]

\[ \{ U_a \} \Gamma \vdash b \triangleright \text{return}(\kappa_2') \]

By Lemma 26, \{ U_a \} \Gamma \vdash S \triangleright E[\text{return ()}]; A \triangleleft \text{end}.

Recomposing:

\[ \{ U_a \} \Gamma \vdash \text{return ()}; S \triangleright E[\text{return ()}]; A \triangleleft \text{end} \]

as required.

Case E-ReplaceSelf

\[ \langle a, E[\text{replace } a \text{ with } \kappa'], \sigma, \kappa \rangle \rightarrow \langle a, E[\text{return ()}], \sigma, \kappa' \rangle \]

Assumption:

\[ a : \text{Pid}(T) \in \Gamma \quad \{ T \} \Gamma \vdash S \triangleright E[\text{replace } a \text{ with } \kappa']; A \triangleleft \text{end} \quad \{ T \} \Gamma \vdash \kappa \]

By Lemma 25:

\[ \{ T \} \Gamma \vdash \kappa' \quad \Gamma \vdash a : \text{Pid}(T) \]

\[ \{ T \} \Gamma \vdash S \triangleright E[\text{return ()}]; A \triangleleft \text{end} \]

(noting that \( \Gamma \vdash b : \text{Pid}(T) \) because \( a : \text{Pid}(T) \in \Gamma \), as per the T-CONNECTED-ACTOR and T-DISCONNECTED-ACTOR rules).

By Lemma 26, \{ T \} \Gamma \vdash S \triangleright E[\text{return ()}]; A \triangleleft \text{end}.
REFERENCES

Recomposing:

\[ a : \text{Pid}(T) \in \Gamma \quad \{ T \} \quad \Gamma \mid S \triangleright E[\text{return }()] : A \triangleq \text{end} \quad \{ T \} \quad \Gamma \vdash \kappa' \]

\[ \Gamma ; a : T, s[p](S) : q \vdash \langle a, E[\text{return }()], s[p](q), \kappa' \rangle \]

as required.

Case E-Discover

\[ \langle a, E[\text{discover } T], \sigma_1, \kappa_1 \rangle \parallel \langle b, M, \sigma_2, \kappa_2 \rangle \longrightarrow \langle a, E[\text{return } b], \sigma_1, \kappa_1 \rangle \parallel \langle b, M, \sigma_2, \kappa_2 \rangle \]

where \( b.\text{sessionType} = T \) and \( \neg(M = \text{return } V \land \kappa_2 = \text{stop}) \).

Assumption:

a : \text{Pid}(S) \in \Gamma

\[ \{ S \} \quad \Gamma \mid S' \triangleright E[\text{discover } T] : A \triangleq \text{end} \quad \{ S \} \quad \Gamma \vdash \kappa_1 \]

\[ \Gamma ; a : S, s[p](\tau) : S' \vdash \langle a, E[\text{discover } T], s[p](\tau), \kappa_1 \rangle \]

b : \text{Pid}(T) \in \Gamma

\[ \{ T \} \quad \Gamma \mid T' \triangleright M : B \triangleq \text{end} \quad \{ T \} \quad \Gamma \vdash \kappa_2 \]

\[ \Gamma ; b : T, s[q](\delta) : T' \vdash \langle b, E[\text{return } S], \sigma_1, \kappa_1 \rangle \parallel \langle b, M, \sigma_2, \kappa_2 \rangle \]

By Lemma 25:

\[ \{ T \} \quad \Gamma \mid S' \triangleright \text{discover } T : \text{Pid}(T) \triangleq S' \]

Since \( b : \text{Pid}(T) \in \Gamma \), we can show \( \{ T \} \quad \Gamma \mid S' \triangleright \text{discover } T : \text{Pid}(T) \triangleq S' \).

By Lemma 26, \( \{ T \} \quad \Gamma \mid S' \triangleright E[\text{return } b] : A \triangleq S' \).

Thus, recomposing:

a : \text{Pid}(S) \in \Gamma

\[ \{ S \} \quad \Gamma \mid S' \triangleright E[\text{return } b] : A \triangleq \text{end} \quad \{ S \} \quad \Gamma \vdash \kappa_1 \]

\[ \Gamma ; a : S, s[p](\tau) : S' \vdash \langle a, E[\text{return } b], s[p](\tau), \kappa_1 \rangle \]

b : \text{Pid}(T) \in \Gamma

\[ \{ T \} \quad \Gamma \mid T' \triangleright M : B \triangleq \text{end} \quad \{ T \} \quad \Gamma \vdash \kappa_2 \]

\[ \Gamma ; b : T, s[q](\delta) : T' \vdash \langle b, E[\text{return } b], s[p](\tau), \kappa_1 \rangle \parallel \langle b, M, t[q](\delta), \kappa_2 \rangle \]

as required.

Case E-Self

\[ \langle a, E[\text{self}], \sigma, \kappa \rangle \longrightarrow \langle a, E[\text{self}], \sigma, \kappa \rangle \]

Assumption:

a : \text{Pid}(T) \in \Gamma

\[ \{ T \} \quad \Gamma \mid S \triangleright E[\text{self}] : A \triangleq S \]

\[ \Gamma ; a : T, s[p](\delta) : S \vdash \langle a, E[\text{self}], s[p](\delta), \kappa \rangle \]

By Lemma 25:
\{T\} \quad \Gamma \mid S \triangleright \text{self:Pid}(T) \triangleleft S

We can show:

\[ \Gamma \vdash a:\text{Pid}(T) \]
\[ \{T\} \quad \Gamma \mid S \triangleright \text{return} \ a:\text{Pid}(T) \triangleleft S \]

By Lemma 26, \(\{T\} \quad \Gamma \mid S \triangleright E[\text{return} a]; A \triangleleft \text{end} \).

Recomposing:

\[ a : \text{Pid}(T) \in \Gamma \quad \{T\} \quad \Gamma \mid S \triangleright E[\text{return} a]; A \triangleleft S \]
\[ \Gamma ; a : T, s[p(q)] : S \vdash (a, E[\text{return} a], s[p(q)], \kappa) \]

as required.

Case E-ConnInit

\[ \langle a, E[F] \text{connect } \ell_j(V) \text{ to } b \text{ as } q \rangle, \bot, \kappa_1 \rangle \parallel \langle b, E'[F'] \text{accept from } p \{ \ell_i(x_i) \mapsto M_i \}_{i \in I} \rangle, \bot, \kappa_2 \rangle \longrightarrow
\]

\[ \nu s((a, E[\text{return } i], s[p(q)], \kappa_1) \parallel \langle b, E'[M_j(V/x_i)] \rangle, s[q[p]], \kappa_2) \]

Assumption:

\[ a : \text{Pid}(U_a) \in \Gamma \quad S = U_a \lor S = \text{end} \]
\[ \{U_a\} \quad \Gamma \mid S \triangleright E[\text{connect } \ell_j(V) \text{ to } b \text{ as } q ]; A \triangleleft \text{end} \]
\[ \Gamma ; a : U_a \vdash \langle a, E[\text{connect } \ell_j(V) \text{ to } b \text{ as } q ]; \bot, \kappa_1 \rangle \]
\[ \Gamma ; a : U_a, b : U_b \vdash \langle a, E[\text{connect } \ell_j(V) \text{ to } b \text{ as } q ]; \bot, \kappa_1 \rangle \parallel \langle b, E'[\text{accept from } p \{ \ell_i(x_i) \mapsto M_i \}_{i \in I} ]; B \triangleleft \text{end} \]
\[ \Gamma ; b : U_b \vdash \langle b, E'[\text{accept from } p \{ \ell_i(x_i) \mapsto M_i \}_{i \in I} ]; \bot, \kappa_2 \rangle \]

By Lemma 25, by case analysis on \( F \), we either have:

\[ q!!\ell_j(A_j) . S_j' \in \{ S_j \}, \quad \Gamma \vdash b; T_b \quad \text{ty}(q) = T_b \]
\[ \{U_a\} \quad \Gamma \mid \Sigma_i \in I(S_i) \triangleright \text{connect } \ell_j(V) \text{ to } b \text{ as } q; 1 \triangleleft S_j' \]

or

\[ q!!\ell_j(A_j) . S_j' \in \{ S_j \}, \quad \Gamma \vdash b; T_b \quad \text{ty}(q) = T_b \]
\[ \{U_a\} \quad \Gamma \mid \Sigma_i \in I(S_i) \triangleright \text{try connect } \ell_j(V) \text{ to } b \text{ as } q \text{ catch } M.1 \triangleleft S_j' \]

Since the evaluation context will be discarded, WLOG we proceed assuming that \( F = [ ] \).

As \( b : \text{Pid}(U_b) \in \Gamma \), we have that \( T_b = U_b \) and therefore that \( \text{ty}(q) = U_b \).
REFERENCES

Again by Lemma 25, \{U_k\}  \Gamma | \Sigma_{i \in I}(p ? \ell_k(C_k) \cdot T_k) \triangleright \text{accept from } p \{\ell_i(x_k) \mapsto M_k\}_{k \in K} : B' \triangleleft T'.

By case analysis on \(F'\), we either have:

\[
\frac{\{U_k\}  \Gamma, x : C_k \mid T_k \triangleright M_k : B' \triangleleft T'}{\{U_k\}  \Gamma | \Sigma_{i \in I}(p ? \ell_k(C_k) \cdot T_k) \triangleright \text{accept from } p \{\ell_i(x_k) \mapsto M_k\}_{k \in K} : B' \triangleleft T'}
\]

or

\[
\frac{\{U_k\}  \Gamma, x : C_k \mid T_k \triangleright M_k : B' \triangleleft T'}{\{U_k\}  \Gamma | \Sigma_{i \in I}(p ? \ell_k(C_k) \cdot T_k) \triangleright \text{try (accept from } p \{\ell_i(x_k) \mapsto M_k\}_{k \in K} \text{) catch } M : B' \triangleleft T'}
\]

Again, we consider the first case.

Thus, \(U_k = \text{accept from } p \{\ell_i(x_k) \mapsto M_k\}_{k \in K}\).

We now need to introduce the new runtime typing environment for the new session. We begin with a singleton runtime typing environment \{s[p](\emptyset)\}:U_a, and recall that \(U_a = \{\Sigma_{i \in I}(S_i)\}\) and \(q!!u_j(A_j)\). \(S'_j \in \{S_i\}\).

Since \(C\) is defined wrt. a well-formed program and thus protocols are well-formed, \(p\) is a unique initiator, and we know that \(U_a = \text{ty}(p)\) and \(\text{safe}(\{s[p](\emptyset)\}:U_a)\).

As a consequence of safety, we know that \(C_j = A_j\).

We can then reduce on typing environments:

\[
\exists j \in I, S_j = q!!u_j(A_j), S'_j \quad \text{ty}(q) = p ? \ell_k(C_k) \cdot T_k \\
\Gamma | S'_j \triangleright \text{return } ():A \triangleleft S'_j \quad \text{and so by Lemma 27, } \{U_a\}  \Gamma | \Sigma_{i \in I}(S_i) \triangleright \text{return } ():1 \triangleleft \text{end.}
\]

Similarly, we can show \(\{U_b\}  \Gamma | S'_j \triangleright \text{return } ():M_{j\{V/x\}} : B \triangleleft \text{end} \) and so by Lemma 27, \(\{U_b\}  \Gamma | S'_j \triangleright E'[M_{j\{V/x\}} : B] \triangleleft \text{end} \).

Recomposing:

\[
\frac{\text{a} : \text{Pid}(U_a) \in \Gamma \\ \{U_a\}  \Gamma | S'_j \triangleright E'[\text{return } ()] : A \triangleleft S'_j \quad \{U_a\}  \Gamma | T_j \triangleright E'[M_{j\{V/x\}} : B] \triangleleft \text{end} \\ \text{b} : \text{Pid}(U_b) \in \Gamma \\ \{U_b\}  \Gamma | T_j \triangleright E'[M_{j\{V/x\}} : B] \triangleleft \text{end} \quad \{U_b\}  \Gamma | \kappa_2}{\Gamma | a : U_a, \kappa_1 \triangleright (a, E'[\text{return } ()], s[p](\emptyset), \kappa_1) \\ \Gamma | b : U_b, \kappa_2 \triangleright (b, E'[M_{j\{V/x\}}], s[p](\emptyset), \kappa_2)}
\]

as required.

Note: in the remaining communication cases, we consider the case where the top-level frame is empty, since the frame will be discarded in the result.

Case E-Conn
with \( j \in K \).

Assumption:

\[
\begin{align*}
\& a: \text{P}d(U_a) \in \Gamma \\
\& U_a \vdash S : E \xrightarrow{\text{connect } \ell_j(V) \text{ to } b \text{ as } q} A \xrightarrow{\text{end}} \end{align*}
\]

\[
\begin{align*}
\& b: \text{P}d(U_b) \in \Gamma \\
\& T = U_b \lor T = \text{end} \\
\& U_b \vdash \Gamma \vdash E' \xrightarrow{\text{accept from } p} \ell_i(x_i) \rightarrow M_i, i \in I, \bot, \kappa_2 \xrightarrow{\text{end}}
\end{align*}
\]

where \( j \in I \) and safe\((a: U_a, b: U_b, s[p](\tilde{r}) : S)\).

Consider the subderivation \( \{U_a\} \vdash S \vdash E \xrightarrow{\text{connect } \ell_j(V) \text{ to } b \text{ as } q} A \xrightarrow{\text{end}}. \)

By Lemma 25:

\[
\begin{align*}
\& q! \ell_j(A_j) \cdot S_j' \in \{S_i\}_i \\
\& \Gamma \vdash b: \text{P}d(T_b) \vdash \text{ty}(q) = T_b \\
\& \{U_a\} \vdash \Gamma \vdash \Sigma_{i \in I}(S_i) \vdash \text{connect } \ell_j(V) \text{ to } b \text{ as } q \cdot 1 \xrightarrow{\text{end}} S_j'
\end{align*}
\]

Since \( b: \text{P}d(U_b) \in \Gamma \), we have that \( T_b = U_b \). We also deduce that \( S = \Sigma_{i \in I}(S_i) \) where \( q! \ell_j(A_j) \cdot S_j' \in \{S_i\}_i \).

Also by Lemma 25:

\[
\begin{align*}
\& (\{U_b\} \vdash x: C_b \rightarrow M_b : B' \xrightarrow{\text{end}} T')_{k \in K} \\
\& \{U_b\} \vdash \Gamma \vdash \Sigma_{i \in I}(p ? (\ell_i(C_i), T_k)) \vdash \text{accept from } p \ell_i(x_i) \rightarrow M_i, i \in I, B' \xrightarrow{\text{end}} T'
\end{align*}
\]

Thus, \( U_b = \text{accept from } p \ell_i(x_i) \rightarrow M_i, i \in I \).

We can then show a reduction on typing environments:

\[
\exists j \in I. S_j = q! \ell_j(A_j) \cdot S_j' \quad \text{ty}(q) = p ? (\ell_j(C_j), T_k) \\
\quad j \in K \\
\quad C_j = A_j \\
\quad s[p](\tilde{r}) \Sigma_{i \in I}(S_i) \xrightarrow{\text{end}} s[p](\tilde{r}, q) : S_j', s[q](p) : T_j
\]

(noting that as a consequence of safety, we know that \( C_j = A_j \)).

Since \( s[p](\tilde{r}) : \Sigma_{i \in I}(S_i) \xrightarrow{\text{end}} s[p](\tilde{r}, q) : S_j', s[q](p) : T_j \), it follows by safety that safe\((s[p](\tilde{r}, q) : S_j', s[q](p) : T_j)\).

Noting that only top-level frames (i.e., \( E, E' \)) can contain exception-handling frames, \( E, E' \) are pure. We can show \( \{U_a\} \vdash S_j' \vdash \text{return } \cdot \mathcal{A} \xrightarrow{\text{end}} \) and so by Lemma 27, \( \{U_a\} \vdash S_j' \vdash E \xrightarrow{\text{return } \cdot \mathcal{A}} 1 \xrightarrow{\text{end}}. \)

Similarly, we can show \( \{U_b\} \vdash T_j \vdash M_j \{V/x_j\} : B' \xrightarrow{\text{end}} T' \) and so by Lemma 27, \( \{U_b\} \vdash T_j \vdash E' \rightarrow M_j \{V/x_j\} \xrightarrow{\text{end}} B \xrightarrow{\text{end}}. \)

Recomputing:

\[
\begin{align*}
\& a: \text{P}d(U_a) \in \Gamma \\
\& \{U_a\} \vdash S_j' \vdash E \xrightarrow{\text{connect } \ell_j(V) \text{ to } b \text{ as } q} A \xrightarrow{\text{end}} \end{align*}
\]

\[
\begin{align*}
\& b: \text{P}d(U_b) \in \Gamma \\
\& \{U_b\} \vdash T_j \vdash E' \rightarrow M_j \{V/x_j\} : B \xrightarrow{\text{end}} \end{align*}
\]

with safe\((a: U_a, b: U_b, s[p](\tilde{r}, q) : S_j', s[q](p) : T_j)\) as required.
Case E-Comm

Let $\Delta_1 = a : U_a, s[p](\bar{r}); S_a$ and $\Delta_2 = b : U_b, s[q](\bar{s}); S_b$.

Assumption:

$\begin{align*}
\Gamma; \Delta_1 &\vdash \{a, E[\text{send} \ell_j(V) \text{ to } q] : A \bowtie \text{end}\} \\
\Gamma; \Delta_2 &\vdash \{b, E'[\text{receive from } p \{\ell_i(x_i) \mapsto M_i\}_{i \in I}] : B \bowtie \text{end}\}
\end{align*}$

where $j \in I$ and $\text{safe}(\Delta_1, \Delta_2)$.

Consider the subderivation $\{U_a\} \Gamma \vdash S_a \triangleright E[\text{send} \ell_j(V) \text{ to } q] : A \bowtie \text{end}$. By Lemma 25:

$\begin{array}{c}
\begin{array}{c}
q[\ell_j(A_j)] \in \{S_i\}_{i \in I} \\
\Gamma \vdash V : A_j
\end{array}
\end{array}
\quad
\frac{\begin{array}{c}
\begin{array}{c}
\{U_a\} \Gamma \vdash \Sigma_{i \in I}(S_i) \triangleright \text{send} \ell_j(V) \text{ to } q : 1 \bowtie S_j
\end{array}
\end{array}}{}

Next, consider the subderivation $\{U_b\} \Gamma \vdash S_b \triangleright E'[\text{receive from } p \{\ell_i(x_i) \mapsto M_i\}_{i \in I}] : B \bowtie \text{end}$. Again by Lemma 25:

$\begin{array}{c}
\begin{array}{c}
\{U_b\} \Gamma \vdash i_k : B \bowtie \text{end}
\end{array}
\end{array}
\quad
\frac{\begin{array}{c}
\begin{array}{c}
\{U_b\} \Gamma \vdash \Sigma_{k \in K}(p?\ell_k(B_k), T_k) \triangleright \text{receive from } p \{\ell_i(x_i) \mapsto M_i\}_{i \in I} : A \bowtie T'
\end{array}
\end{array}}{}

From the assumption we know that $j \in I$. As a result of the two subderivations above, we can refine our definitions of $\Delta_1$ and $\Delta_2$:

$\begin{align*}
\Delta_1 &= a : U_a, s[p](\bar{r}); \Sigma_{i \in I}(S_i), \text{ where } q[\ell_j(A_j)] \cdot S_j' \in \{S_i\}_{i \in I} \\
\Delta_2 &= b : U_b, s[q](\bar{s}); \Sigma_{k \in K}(p?\ell_k(B_k), T_k)
\end{align*}$

Since $\text{safe}(\Delta_1, \Delta_2)$, we have that $j \in K$, $B_j = A_j$.

Thus we can construct a reduction on typing environments:

$\begin{align*}
\begin{array}{c}
\begin{array}{c}
\{U_a\} \Gamma \vdash S_a \triangleright E[\text{return }()] : A \bowtie \text{end}
\end{array}
\end{array}
\end{align*}$

Let $\Delta' = a : U_a, b : U_b, s[p](S_j') ; s[q](T_j)$.

Since $\text{safe}(\Delta_1, \Delta_2)$ and $\Delta_1, \Delta_2 \rightarrow \Delta'$, by the definition of safety, $\text{safe}(\Delta')$.

Noting that only top-level frames (i.e., $F, F'$) can contain exception-handling frames, $E, E'$ are pure. By Lemma 27, $\{U_a\} \Gamma \vdash S_a \triangleright E'[\text{return }()] : A \bowtie \text{end}$.

By Lemma 24, $\{U_b\} \Gamma \vdash T_j \triangleright M_j[V/x_j] : B \bowtie T'$.

By Lemma 27, $\{U_b\} \Gamma \vdash T_j \triangleright E'[M_j[V/x_j]] : B \bowtie \text{end}$.

Letting $\Delta'_1 = a : U_a, s[p](S_j')$ and $\Delta'_2 = b : U_b, s[q](T_j)$; recomposing:
We can show a reduction on runtime typing environments:

\[
\gamma; \Delta_1 \vdash (a, E[\text{return}]), s[p](\bar{r}), \kappa_1 \quad \gamma; \Delta_2 \vdash (b, E'[M_j\{V/x_j\}], s[q](\bar{\delta}), \kappa_2)
\]

\[
\gamma; \Delta' \vdash (a, E[\text{return}]), s[p](\bar{r}), \kappa_1 \parallel (b, E'[M_j\{V/x_j\}], s[q](\bar{\delta}), \kappa_2)
\]

with \( \text{safe}(\Delta') \), as required.

**Case E-Disconn**

\[
\langle a, E[\text{wait q}], s[p](\bar{r}, q), \kappa_1 \rangle \parallel \langle b, E'[\text{disconnect from p}], s[q](\bar{p}), \kappa_2 \rangle \rightarrow \langle a, E[\text{return}]), s[p](\bar{r}), \kappa_1 \parallel \langle b, E'[\text{return}]), \bot, \kappa_2 \rangle
\]

Let \( \Delta = a : U_a, s[p](\bar{r}) : S, b : U_b, s[q](\bar{p}) : T \).

**Assumption:**

\[
\begin{align*}
\text{PId}(U_a) \in \Gamma & \quad \{U_a\} \quad S \triangleright E[\text{wait q}] : B \triangleleft \kappa_1 \\
\text{PId}(U_b) \in \Gamma & \quad \{U_b\} \quad T \triangleright E'\{\text{disconnect from p}\} : B \triangleleft \kappa_2 \\
\gamma; a : U_a, s[p](\bar{r}) : S & \vdash \langle a, E[\text{wait q}], s[p](\bar{r}, q), \kappa_1 \rangle \\
\gamma; b : U_b, s[q](\bar{p}) : T & \vdash \langle b, E'[\text{disconnect from p}], s[q](\bar{p}), \kappa_2 \rangle
\end{align*}
\]

\[
\gamma; \Delta \vdash \langle a, E[\text{wait q}], s[p](\bar{r}, q), \kappa_1 \rangle \parallel \langle b, E'[\text{disconnect from p}], s[q](\bar{p}), \kappa_2 \rangle
\]

By Lemma 25:

\[
\{U_a\} \quad \Gamma \vdash \#^\uparrow q : S' \triangleright \text{wait q} \cdot 1 \triangleleft S'
\]

Also by Lemma 25:

\[
\{U_b\} \quad \Gamma \vdash \#^\downarrow p \triangleright \text{disconnect from p} : 1 \triangleleft T'
\]

Thus, \( S = \#^\uparrow q \cdot S' \) and \( T = \#^\downarrow p \cdot T' \).

We can show a reduction on runtime typing environments:

\[
\begin{align*}
\frac{s[p](\bar{r}, q) : \#^\uparrow q \cdot S' \triangleright s[p](\bar{r}) : S' \quad s[q](\bar{p}) : \#^\downarrow p \triangleright S'}{s[p](\bar{r}, q), \#^\uparrow q \cdot S', s[q](\bar{p}) : \#^\downarrow p \triangleright S'} \equiv \quad a : U_a, s[p](\bar{r}) : \#^\uparrow q \cdot S', b : U_b, s[q](\bar{p}) : \#^\downarrow p \triangleright a : U_a, s[p](\bar{r}) : S', b : U_b}
\end{align*}
\]

Since \( \text{safe}(\Delta) \), and \( \Delta \implies \Delta' \), by the definition of safety, we have that \( \text{safe}(\Delta') \).

Noting that only top-level frames (i.e., \( F, F' \)) can contain exception-handling frames, \( E, E' \) are pure. We can show that \( \{U_a\} \quad \Gamma \mid S' \triangleright \text{return}() : 1 \triangleleft S' \), so by Lemma 27, we have that \( \{U_a\} \quad \Gamma \mid S' \triangleright E[\text{return}()] : A \triangleleft S' \).

By the same argument, \( \{U_b\} \quad \Gamma \mid \text{end} \triangleright E'[\text{return}()] : 1 \triangleleft \kappa_2 \).

Thus we can show (by T-UNCONNECTEDACTOR, noting that \( \text{end} \) is a permissible precondition):

\[
\text{PId}(U_a) \in \Gamma \quad \{U_a\} \quad \Gamma \mid \text{end} \triangleright E'[\text{return}()] : B \triangleleft \kappa_2 \quad \{U_b\} \quad \Gamma \vdash \kappa_2
\]

\[
\gamma; b : U_b \vdash \langle b, E'[\text{return}()], \bot, \kappa_2 \rangle
\]
Recomposing:

\[
\begin{align*}
T \Gamma \quad | \quad S \triangleright E[\text{wait } q]: B \triangleleft & \quad \{T\} \Gamma \vdash \kappa_1 \\
T \Gamma \quad | \quad a : \text{P}(U_a) \in \Gamma \\
& \quad \Gamma; a : U_a, s[p](\bar{r}); S' \triangleright \langle a, E[\text{reset } ()], s[p](\bar{r}), \kappa_1 \rangle \\
T \Gamma \quad | \quad \Gamma; b : U_b \triangleright (b, E'[\text{return } ()]: B \triangleleft & \quad \{U_b\} \Gamma \vdash \kappa_2 \\
& \quad \Gamma; b : U_b \triangleright (b, E'[\text{return } ()], \bot, \kappa_2) \\
\end{align*}
\]

with safe(\(a : U_a, s[p](\bar{r}); S' \quad b : U_b\), as required.

**Case E-Complete**

\[(\nu s)(\langle a, \text{return } V, s[p](\emptyset), \kappa \rangle) \rightarrow \langle a, \text{return } V, \bot, \kappa \rangle\]

Assumption:

\[
\begin{align*}
a : \text{P}(T) \quad & \{T\} \Gamma \vdash \text{return } V: A \triangleleft \quad \{T\} \Gamma \vdash \kappa \\
& \quad \Gamma; a : T, s[p](\emptyset); S \triangleright \langle a, \text{return } V, s[p](\emptyset), \kappa \rangle \\
& \quad \Gamma; \vdash (\nu s)((\langle a, \text{return } V, s[p](\emptyset), \kappa \rangle)
\end{align*}
\]

Since by T-RETURN, the pre- and post-conditions must match, it must be the case that \(S = \text{end}\). Thus we can show:

\[
\begin{align*}
a : \text{P}(T) \quad & \{T\} \Gamma \vdash \text{return } V: A \triangleleft \quad \{T\} \Gamma \vdash \kappa \\
& \quad \Gamma; a : T \vdash \langle a, \text{return } V, s[p](\emptyset), \kappa \rangle
\end{align*}
\]

as required.

**Case E-CommRaise**

\[
\langle a, E[M], s[p](\bar{r}), \kappa \rangle \parallel \triangledown s[q] \rightarrow \langle a, E[\text{raise } q], s[p](\bar{r}), \kappa \rangle \parallel \triangledown s[q]
\]

where subj(\(M\) = \(p\).

The proof is by cases on \(M\), where \(M\) must be a communication action. The cases have the same structure, so we show the case where \(M = \text{wait } q\).

Assumption:

\[
\begin{align*}
\{T\} \Gamma \quad | \quad \# q . S' \triangleright E[\text{wait } q]: A \triangleleft \quad \{T\} \Gamma \vdash \kappa \\
& \quad \Gamma; a : T, s[p](\bar{r}); \# q . S' \triangleright \langle a, E[\text{wait } q], s[p](\bar{r}), \kappa \rangle \\
& \quad \Gamma; s[q](\bar{s}) : U \vdash \triangledown s[q] \\
& \quad \Gamma; a : T, s[p](\bar{r}); \# q . S' \triangleright \langle a, E[\text{wait } q], s[p](\bar{r}), \kappa \rangle \parallel \triangledown s[q]
\end{align*}
\]

By Lemma 25, there exists some \(S''\) such that:

\[
\begin{align*}
\{T\} \Gamma \quad | \quad \# q . S' \triangleright \text{wait } q: 1 \triangleleft S''
\end{align*}
\]

By T-Raise, \(\text{raise } q\) can have any precondition, return type, and postcondition. Therefore, by Lemma 27, \(\{T\} \Gamma \quad \# q \triangleright E[\text{raise } q]: A \triangleleft \), and therefore:
as required.

Case E-FailS

\[ \langle a, P[\text{raise}], s[p](\bar{r}), \kappa \rangle \longrightarrow \langle a, \text{raise}, \bot, \kappa \rangle \parallel \delta s[p] \]

Assumption:

\[ a : \text{Pid}(T) \in \Gamma \]

\[ \{ T \} \Gamma \mid S \triangleright E[\text{raise}] : A \triangleleft \end \{ T \} \Gamma \vdash \kappa \]

\[ \Gamma; a : T, s[p](\bar{r}) : \# \uparrow q . S' \vdash \langle a, E[\text{wait}] q, s[p](\bar{r}), \kappa \rangle \]

Since \text{raise} is typable under any precondition and postcondition, and has an arbitrary return type, it follows that \( \{ T \} \Gamma \mid \text{end} \triangleright E[\text{raise}] : A \triangleleft \end \).

Recomposing:

\[ a : \text{Pid}(T) \in \Gamma \]

\[ \{ T \} \Gamma \mid \text{end} \triangleright E[\text{raise}] : A \triangleleft \end \{ T \} \Gamma \vdash \kappa \]

\[ \Gamma; a : T, s[p](\bar{r}) : \# \uparrow q . S' s[q](\bar{s}) \triangleright \langle a, E[\text{raise}], s[p](\bar{r}), \kappa \rangle \parallel \delta s[p] \]

Case E-FailLoop

Similar to E-LOOP.

Case E-LiftM

Immediate by Lemma 22.

Case E-Equiv

Immediate by Lemma 23.

Case E-Par

Immediate by the IH and rules E-Cong1 and E-Cong2.

Case E-Nu

Immediate by the IH, noting that the IH ensures that the resulting environment is also safe.
C Progress

C.1 Overview

The progress proof requires several steps. We overview them below.

**Canonical forms** Canonical forms allow us to reason globally about a configuration by putting it in a structured form. Lemma 31 states that any well-typed, closed configuration can be put into canonical form.

**Exception-aware runtime typing environments** Runtime typing environments do not account explicitly for zapper threads. This makes sense when analysing protocols statically to check their safety and progress properties, but is inconvenient when reasoning about configurations.

The second step is to introduce *exception-aware* runtime typing environments which account explicitly for zapper threads and the propagation of exceptions, and an exception-aware runtime typing system (Definition 32). We then show that configurations including zapper threads are typable under the exception-aware runtime typing system (Lemma 36).

We refine our notion of environment progress to include the possibility of failed sessions (Definition 39), and show that given a runtime environment \( \Delta \) satisfying safety and progress, a derived exception-aware runtime environment \( \Theta \) also satisfies safety and progress (Lemma 40).

**Flattenings** Hu & Yoshida’s formulation of multiparty session types relaxes the directedness constraint for output choices, but this relaxation makes it more difficult to reason about reduction of environments being reflected by configurations.

In this step, we introduce *flattenings* (Definitions 43 and 44), which restrict each top-level output choice to a single option, and show that if a configuration is *ready* (i.e., all actors are blocked on communication actions), then it is typable under a flattened environment (Lemma 46). We then show that flattenings preserve environment reducibility (Lemma 47).

**Session progress** The penultimate step is to show that sessions can make progress. A key result is Lemma 49, which states that a ready configuration typable under a flat exception-aware typing environment can reduce. The session progress lemma (Lemma 18) follows from Lemma 49 and the previous results.

**Progress** Finally, progress follows from Lemma 18 and case analysis on the disconnected actors.

C.2 Auxiliary Definitions

Let \( \Psi \) range over typing environments containing only runtime names: \( \Psi ::= \cdot | \Psi, a : \text{Pid}(S) \).

Term reduction satisfies a form of progress: a well-typed term is a value, can reduce, or is a communication or concurrency construct:

▶ **Lemma 28 (Progress (terms)).** If \( \{T\} \Psi \vdash M : A \triangleleft S' \), then either \( M = \text{return} V \) for some value \( V \); there exists some \( N \) such that \( M \triangleleft M N \); or there exists some \( E \) such that \( M \) can be written \( E[N] \) for some \( E, N \) where \( N \) is either \( \text{raise} \) or an adaptation, communication, or concurrency construct.

▶ **Lemma 29 (Session typability).** If \( \cdot \vdash G[S] \), then there exist \( \Psi, \Delta \) such that \( \Psi; \Delta \vdash S \) and \( \Delta \) only consists of entries of the form \( a : S \).

Proof. By induction on the structure of \( G \), noting that entries of the form \( s[p/q]:S \) are linear; by the definition of \( S = (\nu s)C \), actors and zapper threads in \( C \) must refer to only to \( s \).

C.3 Canonical forms

To help us state a progress property, we consider configurations in canonical form.

A canonical form consists of binders for all connected actor names, followed by binders for all disconnected actor names, followed by all sessions, followed by all disconnected actors.

▶ **Definition 30 (Canonical form).** A configuration is in canonical form if it is either \( 0 \) or can be written: \( (\nu a_1 \cdots a_l)(\nu b_1 \cdots b_m)(S_1 \parallel \cdots \parallel S_n \parallel \langle b_1, M_1, \bot, \kappa_1 \rangle \parallel \cdots \parallel \langle b_m, M_m, \bot, \kappa_m \rangle) \).
Every well-typed, closed configuration can be written in canonical form.

Lemma 31 (Canonical forms). If $\vdash \Gamma \vdash C$, then $\exists D \equiv C$ where $D$ is in canonical form.

Proof sketch. Due to Lemma 23, by induction on typing derivations we can move all actor name restrictions to the top level, followed by all session name restrictions, followed by all connected actors, followed by all zapper threads, followed by all disconnected actors.

Since the typing rules ensure each actor only participates in a single session, we can then group each actor and zapper thread according to its session, in order to arrive at a canonical form.

C.4 Exception-aware runtime typing environments

Due to E-RAISEP, zapper threads expose additional reductions to those allowed by standard environment reduction. In particular, given the presence of a zapper thread $\delta s[p]$, any other participant in the remainder of the session blocked on $p$ can reduce. In order to account for this, we introduce the notion of exception-aware runtime typing environments, environment reduction, and runtime typing.

Definition 32 (Exception-aware runtime typing environments, environment reduction, and runtime typing). An exception-aware runtime typing environment $\Theta$ is defined as follows:

$$\Theta \ ::= \ a : S \mid s[p]{\bar{q}} : S \mid s[p] : \ \delta$$

The exception-aware runtime typing relation $\Gamma ; \Theta \vdash C$ is defined to be the standard runtime typing relation $\Gamma ; \Delta \vdash C$ but with rule T-ZAP defined as:

$$T-ZAP$$

$$\Gamma ; s[p] : \ \delta \vdash \delta s[p]$$

We extend the set of labels $\rho$ with a zapper label $s : p \vdash q$, which states that role $q$ has attempted to interact with a cancelled role $p$ and has become cancelled itself as a result.

The exception-aware environment reduction relation is defined as the rules of the standard runtime typing relation $\Delta \Rightarrow \Delta'$ with the addition of the following rules:

ET-CommFail

$$\exists j \in I. S_j = p \downarrow j(A_j) \cdot S_j'$$

$$s[p] : \ \delta, s[q]{\bar{r}} : S_{\iota} \vdash s[p] : \ \delta, s[q] : \ \delta$$

ET-DisconnFail

$$s[p] : \ \delta, s[q]{\bar{q}} : \# \downarrow q \cdot S \vdash s[p] : \ \delta, s[q] : \ \delta$$

ET-WaitFail

$$s[p] : \ \delta, s[q]{\bar{q}} : \# \uparrow q \cdot S \vdash s[p] : \ \delta, s[q] : \ \delta$$

Definition 33 (Zapped roles). Define the zapped roles of session

$$S = (vs)((a_1, M_1, s[p_1]{\bar{q_1}})_{1 \cdots 1} \cdot \cdots \cdot (a_m, M_m, s[p_m]{\bar{q_m}})_{1 \cdots 1} \cdot \# s[p_{m+1}] \cdot \cdots \cdot \# s[p_n])$$

as $p_{m+1}, \ldots, p_n$.

Definition 34 (Zapped environment). Given a runtime environment

$$\Delta = a_1 : S_1, \ldots, a_t : S_t, s[p_1]{\bar{r_1}} : T_1, \ldots, s[p_m]{\bar{r_m}} : T_m, s[q_1]{\bar{r_1}} : T'_1, \ldots, s[q_n]{\bar{r_n}} : T'_n$$

and a set of roles $\bar{q} = q_1, \ldots, q_n$, the zapped environment $\Theta = zap(\Delta, \bar{q})$ is defined as:

$$\Delta = a_1 : S_1, \ldots, a_t : S_t, s[p_1]{\bar{r_1}} : T_1, \ldots, s[p_m]{\bar{r_m}} : T_m, s[q_1] : \ \delta, \ldots, s[q_n] : \ \delta$$
REFERENCES

Definition 35 (Failed environment). An exception-aware runtime typing environment $\Theta$ is a failed environment, written $\text{failed}(\Theta)$, if $\Theta$ is of the form $s[p_1]:\xi, \ldots, s[p_n]:\xi$.

Lemma 36 (Zapped Typeability). If $\Gamma; \Delta \vdash S$ where $S = (\nu s: \Delta') C$, the zapped roles of $S$ are $\tilde{p}$, and $\Theta = \text{zap}(\Delta', \tilde{p})$, then $\Gamma; \Delta; \Theta \vdash \gamma C$.

Proof. A straightforward induction on the derivation of $\Gamma; \Delta \vdash C$, noting that the definition of sessions and T-SESSION ensures that $\Delta$ only contains actor runtime names, and that the modified T-ZAP rule is satisfied by the fact that $\Theta = \text{zap}(\Delta, \tilde{p})$.

Corollary 37. If $\vdash_i C$ where $C$ is in canonical form, then $\vdash_i C$.

Proof. Follows directly by applying Lemma 36 to each session.

Corollary 38 (Exception-aware session typability). If $\vdash_i G[S]$, then there exist $\Psi, \Delta$ such that $\Delta$ only consists of entries of the form $a : S$ and $\vdash_i S$.

Definition 13 extends straightforwardly to exception-aware runtime typing environments.

Definition 39 (Progress (exception-aware environments)). An exception-aware runtime typing environment $\Theta$ satisfies progress, written $\text{prog}(\Theta)$, if:

- (Role progress) for each $s[p_i](q_i):S_i \in \Theta$ such that $\text{active}(S_i)$, it is the case that $\Theta \rightarrow^* \Theta' \xrightarrow{\nu p} \rho$ with $p \in \text{roles}(\gamma)$.
- (Eventual communication) if $\Theta \rightarrow^* \Theta' \xrightarrow{s[p':\gamma](A)}$, then either $\Theta' \xrightarrow{\gamma} \Theta'' \xrightarrow{s[q':\gamma](A)}$, or $\Theta' \xrightarrow{\gamma} \Theta'' \xrightarrow{s[q,p]:\gamma}$, where $p \notin \text{roles}(\rho)$.
- (Correct termination) $\Theta \rightarrow^* \Theta' \xrightarrow{\gamma} \Theta''$ implies either $\text{end}(\Theta)$ or $\text{failed}(\Theta)$.

If a runtime typing environment is deadlock-free, then any corresponding zapped environment will be deadlock-free.

Lemma 40 (Exception-aware environments preserve safety and progress). Suppose $\text{safe}(\Delta)$ and $\text{prog}(\Delta)$ for some $\Theta$.

If $\Theta = \text{zap}(\Delta, \tilde{p})$ for some set of roles $\tilde{p}$, then $\text{safe}(\Theta)$ and $\text{prog}(\Theta)$.

Proof sketch.

Safety. Safety follows since exception-aware environments do not modify session types, but only replace them with zappers. Interaction with a zapper is vacuously safe, so it follows that if $\text{safe}(\Delta)$ then $\text{safe}(\Theta)$.

Progress. For (role progress), we know that any active role in $\Delta$ will eventually reduce. Presence of a zapped role means that any other role in the session trying to reduce with the zapped role will itself be zapped due to ET-COMMFAL, ET-DISCONNFAL, or ET-WAITFAIL; connections will not occur, but this does not matter since the accepting role will not be in the session.

For (eventual communication), we have that if $\Delta \rightarrow^* \Delta' \xrightarrow{s[p':\gamma](A)}$, then $\Delta' \xrightarrow{\gamma} \Delta'' \xrightarrow{s[q,p]:\gamma} \Delta'''$, where $p \notin \text{roles}(\rho)$.

Suppose $\Theta \rightarrow^* \Theta' \xrightarrow{s[p':\gamma](A)}$. If $\Theta'$ contains zapped roles, either they are irrelevant to $p$’s reduction and we can use the original reduction sequence to show $\Theta \rightarrow^* \Theta'' \xrightarrow{s[q,p]:\gamma} \Delta'''$, or they are relevant to reduction and the exception propagates, resulting in $\Theta' \xrightarrow{\gamma} \Theta'' \xrightarrow{s[q,p]:\gamma} \Delta'''$.

For (correct termination), we know that $\Delta \xrightarrow{\gamma}$ implies that $\text{end}(\Delta)$. By (1), we know that each active role in $\Theta$ will eventually reduce, so it follows that either $\text{end}(\Theta)$ (if all communications occur successfully) or $\text{failed}(\Theta)$ if a role has failed and the failure has propagated to all other participants.
C.5 Flattenings

Definition 41 (Input / Output-Directed Choices). A choice session type $\Sigma_{i \in I}(\alpha_i . S_i)$ is a output-directed choice if each $\alpha_i$ is either of the form $p_i!\ell_i(A_i)$.

A choice session type is input-directed if it is of the form $\Sigma_{i \in I}(p_i!\ell_i(A_i))$ for some $i \in \{?, ??\}$.

For convenience, we write $S^*$ and $\Sigma_{i \in I}(\alpha_i . S_i)$ to denote an output-directed choice, and $S^\circ$ and $\Sigma_{i \in I}(\alpha_i . S_i)$ to denote an input-directed choice.

Definition 42 (Output-flat session type). An output-directed session type $\Sigma_{i \in I}(S_i . S_i)$ is output-flat if it is a unary choice, i.e., can be written $p!f(A) . S$ or $p!!f(A) . S$.

An exception-aware runtime typing environment $\Theta$ is output-flat, written $\text{flat}(\Theta)$, if each output-directed choice type in $\Theta$ is output-flat.

We now define a flattening of an output choice. A session type is a flattening of an output sum if it is a unary sum consisting of one of the choices.

Definition 43 (Flattening (types)). A session type $S'$ is a flattening of an output-directed choice $S = \Sigma_{i \in I}(\alpha_i . T_i)$ if $S' = \alpha_j . T_j$ for some $j \in I$.

We can extend flattening to environments by flattening all output-directed choices.

Definition 44 (Flattening (environments)). Given an exception-aware runtime typing environment:

$$\Theta = s[p_1](\vec{r}_1); S^*_1, \ldots, s[p_2](\vec{r}_2): S^*_2, \ldots, s[q_1](\vec{s}_1):T_1, \ldots, s[q_m](\vec{s}_m):T_m, s[t_1]: \ell_1, \ldots, s[t_n]: \ell_n$$

where each $T$ is not an output-directed choice, we say that $\Theta'$ is a flattening of $\Theta$ if:

$$\Theta' = s[p_1](\vec{r}_1); S'^*_1, \ldots, s[p_2](\vec{r}_2): S'^*_2, \ldots, s[q_1](\vec{s}_1):T_1, \ldots, s[q_m](\vec{s}_m):T_m, s[t_1]: \ell_1, \ldots, s[t_n]: \ell_n$$

where each $S'^*_i$ is a flattening of $S^*_i$.

Progress states that however an environment reduces, an active role will be eventually be able to reduce. In the case that the environment does not reduce, it is final.

Definition 45 (Ready). A configuration $C$ is ready, written $\text{ready}(C)$, if all subconfigurations are either zapper threads or actors evaluating terms of the form $E[M]$ where $M$ is a communication action.

Lemma 46 (Flattening typability). If $\vdash \ell_j : G[S]$ where $S = (\nu\ell : \Theta)C$ and $\text{ready}(C)$, then there exists some $\Theta'$ such that $\text{flat}(\Theta')$ where $\Theta'$ is a flattening of $\Theta$, and $\vdash \ell_j : G[\nu\ell : \Theta']C$.

Proof. By Lemma 38, we have that there exist $\Psi, \Delta$ such that $\Delta$ does not contain session entries, and $\Psi; \Delta \vdash \ell_j S$.

By T-Session, $\Psi; \Delta, \Theta \vdash \ell_j C$.

The result follows by induction on the derivation of $\Psi; \Delta, \Theta \vdash \ell_j C$. In the case of T-ZAP, the result follows immediately.

In the case of E-Actor, we have that:

1. $C = \langle a, M, s[p](\vec{r}), \kappa \rangle$
2. $\Psi; a : T, s[p](\vec{r}) : S \vdash \ell_j C$
3. $\{T\} \Psi | S \triangleright M : A \triangleright \text{end}$

Since $\text{ready}(C)$, it must be the case that the actor is evaluating a term of the form $E[N]$ where $N$ is a communication action.

By Lemma 25, $\{T\} \Psi | S \triangleright N : B \triangleleft S'$ for some $B, S'$.

In the case that $N$ is a disconnect, wait, receive, or accept action, then the session type cannot be output-directed and the result follows immediately.

In the case that $M = \text{connect} \ell_j V_j$ to $W$ as $q$, by T-Connect it must be the case that $S = \Sigma_{i \in I}(\alpha_i . S_i')$ where $q!!\ell_j(A_j)$ $\in \{\alpha_i\}_{i \in I}$ and $\Psi \vdash V_j : A_j$. Again by T-Connect and Lemma 26, we can show that $\{T\} \Psi | q!!\ell_j(A_j) . S' \triangleright E[\text{connect} \ell_j V_j] W$ as $q : B \triangleleft S'$, where $q!!\ell_j(A_j) . S'_i$ is a flattening of $S$, as required.

The same argument holds for send actions.

Lemma 47 (Flattening preserves reducibility). Suppose $\text{safe}(\Theta)$, $\text{prog}(\Theta)$, and $\Theta \Rightarrow \Rightarrow$.

If $\Theta$ is a flattening of $\Theta$, then $\Theta \Rightarrow \Rightarrow$. 
Proof. Assume for the sake of contradiction that \( \hat{\Theta} \not\Rightarrow \).

For this to be the case, each \( \rho \) such that \( \Theta \xrightarrow{\rho} \) must either be \( s;p,q:\ell \) or \( s:p \xrightarrow{\ell} \), but instead, \( \hat{\Theta} \xrightarrow{s;p,q';:\ell'(A)} \) for some \( q' \neq q \). Note that \( \rho \) cannot be a disconnection action, since these are unaffected by flattening, and it cannot be the case that \( \hat{\Theta} \xrightarrow{s;p \xrightarrow{\ell'} A} \), since this is a synchronisation action and could reduce.

By (eventual communication), either \( \Theta \xrightarrow{\rho} \Theta' \xrightarrow{s;p,q':\ell'(A)} \) or \( \Theta' \xrightarrow{\rho'} s;\hat{q} \).

Pick some \( \rho \) such that \( \rho' \) contains no roles affected by flattening; one such \( \rho \) must exist since otherwise there would be a cycle, contradicting progress.

It follows that either:

\[
\hat{\Theta} \xrightarrow{\rho} \Theta' \xrightarrow{s;p,q':\ell'(A)} \xrightarrow{s;p,q':\ell'} A \xrightarrow{\rho'} s;\hat{q} \]

meaning \( \hat{\Theta} \xrightarrow{\rho} \Theta' \xrightarrow{s;p,q':\ell'(A)} \xrightarrow{s;p,q':\ell'} A \xrightarrow{\rho'} s;\hat{q} \), a contradiction; or

\[
\Theta \xrightarrow{\rho} \Theta' \xrightarrow{\rho'} \hat{q} \]

also a contradiction.

\[\Box\]

### C.6 Session progress

#### Lemma 48 (Readiness)

Suppose \( \cdot \vdash \cdot C \) where \( C \equiv G[S] \), \( C \) does not contain unmatched discovers, \( S \) is not a failed session, \( S = (\nu s : \Theta)D \), and \( \text{prog}(\Theta) \).

Either \( C \xrightarrow{\cdot} \) or \( \text{ready}(D) \).

Proof. For each \( \langle a,M,s[p\langle\hat{q}\rangle],\kappa \rangle \), by Lemma 28, \( M \) can either reduce or is either a value, adaptation construct, or communication construct.

- If \( M \) can reduce, then the configuration can reduce by \( E\text{-LiftM} \).
- If \( M = E\text{[raise]} \), then the configuration either can reduce by \( E\text{-TryRaise} \) and \( E\text{-LiftM} \), or \( E\text{-FailS} \).
- If \( M \) is an adaptation action, due to the absence of unmatched discovers, the configuration can reduce by \( E\text{-New} \), \( E\text{-Replace} \), \( E\text{-ReplaceSelf} \), \( E\text{-Discover} \), or \( E\text{-Self} \).
- If \( M \) is a value, then by \( T\text{-ConnectedActor} \), \( \{T\} \Psi \mid \text{end} \xrightarrow{\text{return}} V:A \triangleleft \text{end} \). As a consequence of \( \text{prog}(\Theta) \), \( a \) must be the only actor in the session and thus the configuration could reduce by \( E\text{-Complete} \).
- It follows that all terms must be evaluating communication actions, satisfying \( \text{ready}(D) \).

\[\Box\]

#### Lemma 49 (Exception-aware session progress)

If \( \cdot \vdash \cdot C \) where:

1. \( C \equiv G[S] \),
2. \( S = (\nu s : \Theta)D \),
3. \( \text{flat}(\Theta) \),
4. \( \text{ready}(C) \),
5. \( \Theta \Rightarrow \)

then \( C \xrightarrow{\cdot} \).

Proof. Since \( \Theta \Rightarrow \), there exists some environment \( \Theta' \) and label \( \rho \) such that \( \Theta \xrightarrow{\rho} \Theta' \).

The proof is by induction on the derivation of \( \Theta \xrightarrow{\rho} \Theta' \).

Case ET-Conn
By Lemma 29,
\[ \exists j \in I, S_j = q!\ell_j(A_j) \cdot S'_j \]
\[ s[p][r]:\Sigma_{i\in I}(S_i) \triangleq s[p][r]:\Sigma_{i\in I}(S'_i) \]
\[ s[p][r]:\Sigma_{i\in I}(S_i) \triangleq s[p][r]:\Sigma_{i\in I}(S'_i) \]
\[ s[p][r]:\Sigma_{i\in I}(S_i) \triangleq s[p][r]:\Sigma_{i\in I}(S'_i) \]

Since flat(\Theta), we have that \( s[p][r]:q!\ell_j(A_j) \cdot S'_j \). Thus, \( C \) must contain an actor evaluating \( E[\text{connect } \ell_j(A_j) \to V \text{ as } b] \) for some actor name \( b \). Due to the definition of canonical forms, \( b \) must be a subconfiguration of \( G[S] \) and thus the configuration can reduce by either E-CONN or E-CONNFAIL.

Case ET-Comm

\[ \begin{align*}
\text{ET-Comm} & \quad \Theta_1 \xrightarrow{s,p:q: \ell(A)} \Theta'_1 \\
& \quad \Theta_2 \xrightarrow{s,q:p: \ell(A)} \Theta'_2
\end{align*} \]

By ET-Act, \( \Theta_1 \) must contain \( s[p][r]:S \); since flat(\Theta), \( S = q!\ell(A) \).

Also by ET-Act, \( \Theta_2 \) must contain \( s[p][r]:\Sigma_{i\in I}(\beta_i, T'_i) \) with \( p!\ell(A) \in \{\beta_i\} \).

Thus by typing, \( C \) must contain an actor \( \langle a, E[\text{send } \ell(V) \to q] \rangle, s[p][r], \kappa_a \rangle \), and another actor \( \langle b, E'[\text{receive from } p \{ \ell_i(x_i) \mapsto M_i \}], s[q](\bar{s}), \kappa_b \rangle \), which would reduce by E-Comm.

Case ET-CommFail

\[ \exists j \in I, S_j = p!\ell_j(A_j) \cdot S'_j \]
\[ s[p]:\ell, s[q]:\Sigma_{i\in I}(\alpha_i, S'_i) \triangleq s[p]:\ell, s[q]:\ell \]

We prove the case where \( \ell = ! \). Since flat(\Theta), by typing we have that \( \Sigma_{i\in I}(\alpha_i, S'_i) = \ell!A(q) \cdot S' \) and \( C \) must contain an actor \( \langle a, E[\text{send } \ell(V) \to q] \rangle, s[p][r], \kappa_a \rangle \) and a zapped thread \( \bar{s}[q] \), which could then reduce by E-RAISEP.

Case E-Disconn is similar to E-CONN, and cases E-DisconnFail and E-WaitFail are similar to E-CommFail.

Cases ET-Rec, ET-Comm1, and ET-Comm2 follow by the induction hypothesis.

\[ \text{Lemma 50. If prog(\Theta) and neither end(\Theta) nor failed(\Theta), then } \Theta \Rightarrow. \]

\textbf{Proof.} By contradiction. Assume that prog(\Theta) and neither end(\Theta) nor failed(\Theta).

By prog(\Theta), each active role must eventually reduce.

If no roles are active, then end(\Theta) or failed(\Theta) is a contradiction.

Otherwise, by the definition of prog(\Theta) for each \( s[p][q]:S \) there must exist some \( \bar{p} \) such that \( \Theta \Rightarrow \bar{p} \Rightarrow \bar{\Theta} \Rightarrow \) where \( p \in subj(\rho) \): a contradiction.

\[ \text{Lemma 51. If } \vdash \exists \bar{f} S \text{ where } S = (\nu s : \Theta)C \text{ and ready(C), then } \Theta \text{ is not final.} \]

\textbf{Proof.} By contradiction. If \( \Theta \) were final, it would consist only of session types of type end. No communication actions are typable under end, contradicting ready(C).

\[ \text{Lemma 18 (Session Progress). If } \vdash \exists \bar{c} C \text{ where } C \text{ does not contain an unmatched discover, } C \equiv G[S] \text{ and } S = (\nu s : \Delta)D \text{ with prog(\Delta), and } S \text{ is not a failed session, then } C \Rightarrow. \]

\textbf{Proof.} By Lemma 29, \( \exists \Psi, \Delta' \text{ such that } \Psi; \Delta' \vdash S. \)

By definition, \( S = (\nu s : \Delta)D \), where \( D = \langle a_1, M_1, s[p_1](\bar{q}_1), \kappa_1 \rangle \parallel \cdots \parallel \langle a_m, M_m, s[p_m](\bar{q}_m), \kappa_m \rangle \parallel \bar{s}[p_{m+1}] \parallel \cdots \parallel \bar{s}[p_n] \).

By T-SESSION, safe(\Delta).

By definition, the zapped roles of \( C \) are \( p_{m+1}, \ldots, p_n \). Let us denote this set as \( \bar{p} \).

Let \( \Theta = \text{zap}(\Delta, \bar{p}) \).

By Lemma 36, \( \Psi; \Delta', \Theta \vdash \bar{c} D \) and so by Corollary 37, \( \vdash \exists \bar{c} G[S] \).
By Lemma 40, safe(Θ) and prog(Θ).

By Lemma 48, either C → or ready(D). As C → satisfies the theorem statement, we proceed assuming ready(D).

By Lemma 46, there exists some Θ such that Θ is a flattening of Θ and · ⊢ G[(νs : Θ)D].

By Lemma 51, Θ is not final.

By Lemma 47, Θ →.

Thus, by Lemma 49, C → as required.

C.7 Progress

Theorem 19 (Progress). Suppose · ⊢ C where C is defined wrt. a well-formed program which satisfies progress, and prog(Δ) for each (νs : Δ)C′ in C. If C does not contain an unmatched discover, either ∃D such that C → D, or C ≡ 0, or C ≡ (νb1 · · · νbn)(⟨b1, N1, ⊥, κ1⟩ ∥ · · · ∥ ⟨bn, Nn, ⊥, κn⟩) where each bi is terminated or accepting.

Proof. By Lemma 31, write C in canonical form.

Eliminate all failed sessions via the equivalence (νs)(s1 ∥ · · · ∥ sn) · ⊢ C ≡ C. Henceforth assume no sessions are failed.

Thus we only need to consider disconnected actors. For each disconnected actor ⟨a, M, ⊥, κ⟩, by Lemma 28, either:

1. M = return V. If κ = N, then the configuration can reduce by E-LOOP. Otherwise, if κ = stop, then the actor is terminated, as required.

2. M = E[raise]. If E contains an exception handler, the configuration can reduce by E-TRYRAISE. If not, E is pure:
   a. if κ = N, then the configuration can reduce by E-FAILLOOP. Otherwise, if κ = stop, then the actor is terminated, as required.
   b. M = E[N] where N is a communication or concurrency action, which, following the logic in Lemma 18, can either reduce by a configuration reduction rule or is a communication action. Since:
      a. by T-UNCONNECTEDACTOR each disconnected actor must either have type end or be following its statically-defined session type
      b. by well-formedness, each statically-defined session type must correspond to a role in a protocol
      c. by well-formedness, each protocol must have a unique initiator
   c. since the program satisfies progress, all protocols satisfy progress
   it must be the case that either a is an initiator of a session and blocked on connect, which could either reduce by E-CONNINIT or E-CONNFAIL, or be accepting, as required.