A Linear Decomposition of Multiparty Sessions for Safe Distributed Programming

Alceste Scalas¹, Ornela Dardha², Raymond Hu¹, and Nobuko Yoshida¹

¹ Imperial College London, UK
  {alceste.scalas, raymond.hu, n.yoshida}@imperial.ac.uk
² University of Glasgow, UK
  ornela.dardha@glasgow.ac.uk

Abstract

Multiparty Session Types (MPST) is a typing discipline for message-passing distributed processes that can ensure properties such as absence of communication errors and deadlocks, and protocol conformance. Can MPST provide a theoretical foundation for concurrent and distributed programming in “mainstream” languages? We address this problem by (1) developing the first encoding of a full-fledged multiparty session π-calculus into linear π-calculus, and (2) using the encoding as the foundation of a practical toolchain for safe multiparty programming in Scala.

Our encoding is type-preserving and operationally sound and complete. Crucially, it keeps the distributed choreographic nature of MPST, illuminating that the safety properties of multiparty sessions can be precisely represented with a decomposition into binary linear channels. Previous works have only studied the relation between (limited) multiparty and binary sessions via centralised orchestration means. We exploit these results to implement an automated generation of Scala APIs for multiparty sessions, abstracting existing libraries for binary communication channels. This allows multiparty systems to be safely implemented over binary message transports, as commonly found in practice. Our implementation is the first to support distributed multiparty delegation: our encoding yields it for free, via existing mechanisms for binary delegation.

1998 ACM Subject Classification D.1.3 Concurrent Programming; D.3.1 Formal Definitions and Theory; F.3.3 Studies of Program Constructs — Type structure

Keywords and phrases process calculi, session types, concurrent programming, Scala

Digital Object Identifier 10.4230/LIPIcs.ECOOP.2017.18

1 Introduction

Correct design and implementation of concurrent and distributed applications is notoriously difficult. Programmers must confront challenges involving protocol conformance (are messages sent/received according to a specification?) and communication mechanics (how are the interactions actually performed?). These difficulties are worsened by the potential complexity of interactions among multiple participants, and if the communication topology is not fixed.

For example, consider a common scenario for a peer-to-peer multiplayer game: the clients, initially unknown to each other, connect to a “matchmaking” server, whose task is to group players and setup a game session in which they can interact directly. Fig. 1 depicts this

* Partially supported by EPSRC (grants EP/K034413/1, EP/K011715/1, EP/L00058X/1, EP/N027833/1, EP/N028201/1) and EU (FP7 612985 “Upscale”). Dardha was awarded a SICSA PECE bursary for visiting Imperial College London in January–March 2016.
scenario: \( Q \) is the server, connected to three clients \( P_a, P_b \) and \( P_c \). To set up a game, \( Q \) sends to each client some networking information (denoted by \( s[a]/s[b]/s[c] \), payloads of the \( \text{Play}A/b/c \) messages) to “introduce” the clients to each other and allow them to communicate. Then, the clients follow the game protocol (marked as “Game”), consisting in some initial message exchanges (\( \text{Info} \)), and a game loop: \( P_a \) chooses a message to send to \( P_b \) (\( \text{Mov1AB} \) or \( \text{Mov2AB} \)) followed by a message from \( P_b \) to \( P_c \), who chooses which message send back to \( P_a \).

Fig. 1 features structured protocols with inter-role message dependencies, and a dynamic communication topology (starting client-to-server, becoming client-to-client). Implementing them is not easy: programmers would benefit from tools to statically detect protocol violations in source code, and realise the communication topology changes.

**Multiparty Session Types (MPST)** [26] are a theoretical framework for channel-based communication, capable of modelling our example. In MPST, participants are modelled as roles (e.g., game players \( a, b, c \)) and programs are session \( \pi \)-calculus processes; the “networking information payloads” \( s[a]/s[b]/s[c] \) can be modelled as multiparty channels, for interpreting roles \( a/b/c \) on the game session \( s \). Notably, channels can themselves be sent/received: this allows to delegate a multiparty interaction to another process, thus changing the communicating topology. In Fig. 1, the server \( Q \) sends (i.e., delegates) the channel \( s[b] \) to \( P_b \); the latter can then use \( s[b] \) to interact with the processes owning channels \( s[a] \) and \( s[c] \) (i.e., \( P_a \) and \( P_c \), after two more delegations).

The MPST framework formalises protocols as session types: structured sequences of inputs/outputs and choices. The MPST typing system assigns such types to channels, and checks the processes using them. In our example, channel \( s[b] \) could have type:

\[
S_b = \text{c}!\text{InfoBC} \left( \text{String} \right) \cdot \text{a}？\text{InfoAB} \left( \text{String} \right) \cdot \mu t. \left( a \& \{ ?\text{Mov1AB} \left( \text{Int} \right) , \text{c}!\text{Mov1BC} \left( \text{Int} \right) . t , ?\text{Mov2AB} \left( \text{Bool} \right) , \text{c}!\text{Mov2BC} \left( \text{Bool} \right) . t \} \right)
\]

\( S_b \) says that \( s[b] \) must be used to realise the Game interactions of \( P_b \) in Fig. 1: first to send \( \text{InfoBC} \) to \( c \), then receive \( \text{InfoAB} \) from \( a \), then enter the recursive game “loop” \( \mu t. \{ \ldots \} \). Inside the recursion, \( a \& \{ \ldots \} \) is a branching from \( a \): depending on \( a \)’s choice, the channel will deliver either \( \text{Mov1AB} \left( \text{Int} \right) \) (in which case, it must be used to send \( \text{Mov1BC} \) to \( c \), and loop), or \( \text{Mov2AB} \) (then, it must be used to send \( \text{Mov2BC} \) to \( c \), and loop). Analogous types can be assigned to \( s[a] \) and \( s[c] \). **Delegation** is represented by types like \( q ?\text{PlayB} \left( S_b \right) . \text{end} \), meaning: from role \( q \), receive a message \( \text{PlayB} \) carrying a channel that must be used according to \( S_b \) above; then, \text{end} the session. Session type checking ensures that, e.g., process \( P_b \) uses its channels abiding by the types above — thus safely implementing the expected channel dynamics and fulfilling role \( b \) in the game. Finally, MPST can formalise the whole Game protocol in Fig. 1 as a global type, and validate that it is deadlock-free; then, via typing, ensure that a set of processes interacts according to the global type (and is, thus, deadlock-free).

**MPST in practice: challenges** MPST could offer a promising formal foundation for safe distributed programming, helping to develop type-safe and deadlock-free concurrent programs.
However, bridging the gap between theory and implementation raises several challenges:

**C1.** Multiparty sessions can have 2, 3 or more interacting roles; but in practice, communication occurs over binary channels (e.g., TCP sockets). Can multiparty channels be implemented as compositions of binary channels, preserving their type safety properties?

**C2.** MPST are far from the types of “mainstream” programming languages, as shown by $S_b$ above. Can they be rendered, e.g., as objects? If so, what are their API and internals?

**C3.** How should multiparty delegation be realised, especially in distributed settings?

The current state-of-the-art has not addressed these challenges. On one hand, existing theoretical works on encoding multiparty sessions into binary sessions \[7, 8\] introduce centralised medium (or arbiter) processes to orchestrate the interactions between the multiparty session roles: hence, they depart from the choreographic (i.e., decentralised) nature of the MPST framework \[26\], and preclude examples like our peer-to-peer game in Fig. 1. On the other hand, there are no existing implementations of full-fledged MPST; e.g., \[52, 30, 39, 48, 56, 50\] only support binary sessions, while none of \[27, 59, 16, 19\] support session delegation.

**Our approach** In this work, we tackle the three challenges above with a two-step strategy:

**S1.** we give the first choreographic encoding of a “full” MPST calculus into linear $\pi$-calculus;

**S2.** we implement a multiparty session API generation for Scala, based on our encoding.

By step S1, we formally address challenge C1. Linear $\pi$-calculus provides a theoretical framework with typed channels that cater only for binary communication, and may only be used once for input/output. These “limitations” are key to the practicality of our approach. In fact, they force us to figure out whether multiparty channels can be represented by a decomposition into binary channels — and whether multiparty session types can be represented by a decomposition into linear types. To solve these issues, we need study how to “decompose” the intricate MPST theory in (much simpler) $\pi$-calculus terms. This endeavour was not tackled before, and its feasibility was unclear. Its practical payoff is that linear $\pi$-calculus channels/types are amenable for an (almost) direct object-based representation (shown in \[56\]): this tackles challenge C2. Further, using $\pi$-calculus we can prove whether such a decomposition is “correct”, i.e., whether MPST processes can be encoded to only interact on binary channels, preserving their type-safety and behaviour and “inherit” deadlock-freedom.

In step S2, we generate high-level typed APIs for multiparty session programming, ensuring their “correctness” by reflecting the types and process behaviours formalised in step S1. Following the binary decomposition in step S1, we can implement such APIs as a layer over existing libraries for binary sessions (available for Java \[28\], Haskell \[52, 30, 39\], Links \[41\], Rust \[31\], Scala \[56\], ML \[50\]), in a way that solves challenge C3 “for free”.

**Contributions** We present the first encoding (§5) of a full multiparty session $\pi$-calculus (§2) into standard $\pi$-calculus with linear, labelled tuple and variant types (§3).

- We present a novel, streamlined MPST formulation, sharply separating global/local typing. Using this formulation, we “close the gaps” between the intricacies of the MPST theory and the (much simpler) $\pi$-calculus, and spot a longstanding issue with type merging \[17\] (Def. 2.9, §2.1 “On Consistency”). We fix it, with a revised subject reduction (Thm. 2.16).
- At the heart of our encoding there is the discovery that the type safety property of MPST is precisely characterised as a decomposition into linear $\pi$-calculus types (Thm. 6.3). Our encoding of types preserves duality and subtyping (Thm. 6.1); our encoding of processes is type-preserving and operationally sound and complete (Thm. 6.2 and Thm. 6.5).
We subsume the encodings of binary sessions into π-calculus [13, 14], and support recursion (§4), which was not properly handled in [12]. Further, we show that multiparty sessions can be encoded into binary sessions choreographically, i.e., while preserving process distribution (homomorphically w.r.t. parallel composition), in contrast to [7, 8]. In §7, we use our encoding as formal basis for the first implementation of multiparty sessions supporting distributed multiparty delegation, over existing Scala libraries (paper’s artifact).

Conventions Derivations use single/double lines for inductive/coinductive rules. Recursive types \(\mu_t.T\) are always closed, and guarded: e.g., \(\mu_t, \ldots, \mu_t, t\), is not a type. We define \(\text{unf}(\mu_t.T) = \text{unf}(T[\mu_t/s])\), and \(\text{unf}(T) = T\) if \(T \neq \mu_t.T\). Type equality is syntactic: \(\mu_t.T\) is not equal to \(\text{unf}(\mu_t.T)\). We write \(P \rightarrow P'\) for process reductions, \(\rightarrow^*\) for the reflexive+transitive closure of \(\rightarrow\), and \(P \neq P'\) iff \(\not\exists P'\) such that \(P \rightarrow P'\). We assume a basic subtyping \(\preceq_{B}\) capturing e.g. \(\text{Int} \preceq_{B} \text{Real}\). For readability, we use blue/red for multiparty/standard π-calculus.

## 2 Multiparty Session π-Calculus

In this section we illustrate a multiparty session π-calculus [26] (Def. 2.1), and its typing system — including recursion, subtyping [18] and type merging [62, 17] (§2.1). The calculus models processes that interact via multiparty channels connecting two or more participants: this is a departure from many “classic” and simpler process calculi, like the linear π-calculus (§3), that model binary channels. We provide various examples based on the scenario in §1.

| Definition 2.1. The syntax of multiparty session π-calculus processes and values is: |
| Processes \(P, Q ::= 0 \mid P \mid Q \mid (\nu s)P\) (inaction, composition, restriction) |
| \(c[p] \oplus [l(v)].P\) (selection towards role \(p\)) |
| \(c[p] \&_{i \in I} \{l_i(x_i).P_i\}\) (branching from role \(p\) — with \(I \neq \emptyset\)) |
| \(\text{def \(D\)} \in Q \mid X(\bar{x})\) (process definition, process call) |
| Declarations \(D ::= X(\bar{x}) = P\) (process declaration) |
| Channels \(c ::= x \mid s[p]\) (variable, channel with role \(p\)) |
| Values \(v ::= c \mid \text{false} \mid \text{true} \mid 42 \mid \ldots\) (channel, base value) |

\(\text{fc}(P)\) is the set of free channels with roles in \(P\), and \(\text{fv}(P)\) is the set of free variables in \(P\).

A channel \(c\) can be either a variable or a channel with role \(s[p]\), i.e., a multiparty communication endpoint whose user impersonates role \(p\) in the session \(s\). Values \(v\) can be variables, or channels with roles, or base values. The inaction \(0\) represents a terminated process. The parallel composition \(P \mid Q\) represents two processes that can execute concurrently, and potentially communicate. The session restriction \((\nu s)P\) declares a new session \(s\) with scope limited to process \(P\). Process \(c[p] \oplus [l(v)].P\) performs a selection (internal choice) towards role \(p\), using the channel \(c\): the labelled value \([l(v)]\) is sent, and the execution continues as process \(P\). Dually, process \(c[p] \&_{i \in I} \{l_i(x_i).P_i\}\) uses channels \(c\) to wait for a branching (external choice) from role \(p\): if the labelled value \(l_k(v)\) is received (for some \(k \in I\)), then the execution continues as \(P_k\) (with \(x_k\) holding value \(v\)). Note that for all \(i \in I\), variable \(x_i\) is bound with scope \(P_i\). In both branching and selection, the labels \(l_i\) (\(i \in I\)) are all different and their order is irrelevant. Process definition \(\text{def \(D\)} \in Q\) and process call \(X(\bar{x})\) model recursion, with \(D\) being a process declaration \(X(\bar{x}) = P\): the call invokes \(X\) by expanding it into \(P\), and replacing its formal parameters with the actual ones. We postulate that process declarations are closed, i.e., in \(X(\bar{x}) = P\), we have \(\text{fv}(P) \subseteq \bar{x}\) and \(\text{fc}(P) = \emptyset\). Note that our syntax is simplified in the style of [18]: it does not have dedicated input/output prefixes, but they can be easily encoded using \& (with one branch) and \oplus.
of the channel to the client process and a selection process, both operating on the same session. Rule (Loop) received is used to send \( q \) from a channel endpoint to interact in the game session \( s \) (client); e.g., \( P_s \) \( P_z \) \( P_{s'} \) \( P_{s''} \) \( P_{s''' \rightarrow} \), while the server owns \( s_b \) (resp. \( s_c \)) which are composed in parallel with \( s \). Each session has 2 roles: \( q \) (server) and \( p \) (client); e.g., \( s_b \) is accessed by the server (through the channel with role \( s_b[q] \)) and by the client \( P_b \) (through \( s_b[p] \)); similarly, \( s_a \) (resp. \( s_c \)) is accessed by \( P_a \) (resp. \( P_c \)) through \( s_a[p] \) (resp. \( s_c[p] \)), while the server owns \( s_a[q] \) (resp. \( s_c[q] \)). The body of the server process \( Q \equiv \text{Client}_i(s_b[p]) \) (for brevity, we omit the definitions of \( P_a \) and \( P_c \)) defines a session \( s \) (with 3 roles \( a, b, c \)) for playing the game. Note that the scope of \( s \) does not include \( P_a, P_b, P_c \): see Fig. 2(a) for a schema of processes and sessions.

The server \( Q \) uses the channel with role \( s_b[q] \) (resp. \( s_a[q], s_c[q] \)) to send the message \( \text{PlayB} \) (resp. \( \text{PlayA}, \text{PlayC} \)) carrying the channel with role \( s[b] \) (resp. \( s[a], s[c] \)) to \( p \). The result is a delegation of the channel to the client process \( P_b \) (resp. \( P_a, P_c \)). This way, each client obtains a channel endpoint to interact in the game session \( s \), interpreting a role among \( a, b, c \).

The client \( P_b \) is implemented by invoking \( \text{Client}_i(s_b[p]) \) (defined in the 2nd line). Here, \( y[q] \) \& \( \text{PlayB}(z) \) means that \( y \) (that becomes \( s_b[p] \) after the invocation) is used to receive \( \text{PlayB}(z) \) from \( q \), while \( z[c] \oplus \text{Issue}(\ldots) \) means that \( z \) (that becomes \( s[b] \) after the delegation is received) is used to send \( \text{Issue}(\ldots) \) to \( c \). The game loop is implemented with the recursive process call \( \text{Loop}_b(z) \) (defined in the 1st line) — which becomes \( \text{Loop}_b(s[b]) \) after delegation.

**Example 2.2.** The following MPST π-calculus process implements the scenario in Fig. 1:

```plaintext
def Loop_b(x) = x[a] & \{\{s_{1b}(y) . x[c] \oplus \{s_{2b}(z) . Loop_b(x) : s_{2b}(z) . x[c] \oplus \{s_{2b}(z). Loop_b(x) \}\}\}\}
def Client_i(y) = y[q] & \text{PlayB}(z) . z[c] \oplus \text{Issue}(\ldots) . z[a] & \text{Issue}(y) . Loop_b(z)\text{in}

\begin{align*}
(\nu s_a, s_b, s_c)(Q | P_a | P_b | P_c)
\end{align*}
```

where: \( P_b = \text{Client}_i(s_b[p]) \) (for brevity, we omit the definitions of \( P_a \) and \( P_c \))

In the 3rd line, \( s_a, s_b, s_c \) are the sessions between the server process \( Q \) and the clients \( P_a, P_b, P_c \), which are composed in parallel with \( | \). Each session has 2 roles: \( q \) (server) and \( p \) (client); e.g., \( s_b \) is accessed by the server (through the channel with role \( s_b[q] \)) and by the client \( P_b \) (through \( s_b[p] \)); similarly, \( s_a \) (resp. \( s_c \)) is accessed by \( P_a \) (resp. \( P_c \)) through \( s_a[p] \) (resp. \( s_c[p] \)), while the server owns \( s_a[q] \) (resp. \( s_c[q] \)). The body of the server process \( Q \) defines a session \( s \) (with 3 roles \( a, b, c \)) for playing the game. Note that the scope of \( s \) does not include \( P_a, P_b, P_c \): see Fig. 2(a) for a schema of processes and sessions.

The server \( Q \) uses the channel with role \( s_b[q] \) (resp. \( s_a[q], s_c[q] \)) to send the message \( \text{PlayB} \) (resp. \( \text{PlayA}, \text{PlayC} \)) carrying the channel with role \( s[b] \) (resp. \( s[a], s[c] \)) to \( p \). The result is a delegation of the channel to the client process \( P_b \) (resp. \( P_a, P_c \)). This way, each client obtains a channel endpoint to interact in the game session \( s \), interpreting a role among \( a, b, c \).

The client \( P_b \) is implemented by invoking \( \text{Client}_i(s_b[p]) \) (defined in the 2nd line). Here, \( y[q] \) \& \( \text{PlayB}(z) \) means that \( y \) (that becomes \( s_b[p] \) after the invocation) is used to receive \( \text{PlayB}(z) \) from \( q \), while \( z[c] \oplus \text{Issue}(\ldots) \) means that \( z \) (that becomes \( s[b] \) after the delegation is received) is used to send \( \text{Issue}(\ldots) \) to \( c \). The game loop is implemented with the recursive process call \( \text{Loop}_b(z) \) (defined in the 1st line) — which becomes \( \text{Loop}_b(s[b]) \) after delegation.

**Definition 2.3.** The operational semantics of multiparty session processes is:

- (R-Com) \( s[p] \llbracket q \rrbracket \land_{i \in I} \{l_i(x_i).P_i \} | s[q] \llbracket p \rrbracket \oplus (l_j(v_j)).Q \rightarrow P_j \{v_j/s_j\} \) | \( Q \) (if \( j \in I \) and \( fv(v_j) = \emptyset \))
- (R-Call) \( \text{def } X(\overline{x}) = P \in (X(\overline{v}) \mid Q) \rightarrow \text{def } X(\overline{x}) = P \in (P(\overline{v}/\overline{x}) \mid Q) \) (if \( \overline{x} = x_1, \ldots, x_n \), \( \overline{v} = v_1, \ldots, v_n \), \( fv(\overline{x}) = \emptyset \))
- (R-Par) \( P \rightarrow Q \) implies \( P \cup R \rightarrow Q \cup R \) (R-Res) \( P \rightarrow Q \) implies \( (\nu s).P \rightarrow (\nu s)Q \) (R-Def) \( P \rightarrow Q \) implies \( \text{def } D \in P \rightarrow \text{def } D \in Q \) (R-Struct) \( P \equiv P' \) and \( P \rightarrow Q \) and \( Q' \equiv Q \) implies \( P' \rightarrow Q' \) (with \( \equiv \) standard — see [55])

Rule (R-Com) models communication: it says that the parallel composition of a branching and a selection process, both operating on the same session \( s \) respectively as roles \( p \) and \( q \) (i.e., via \( s[p] \) and \( s[q] \)) and targeting each other (i.e., \( s[p] \) is used to branch from \( q \), and \( s[q] \) is used to select towards \( p \)) reduces to the corresponding continuations, with a value
substitution on the receiver side. \((r \text{-} call)\) says that a process call \(X(\overline{v})\) in the scope of \(\text{def } X(\overline{v}) = P\) in \(\ldots\) reduces by expanding \(X(\overline{v})\) into \(P\), and replacing the formal parameters \((\overline{x})\) with the actual ones \((\overline{v})\). The remaining rules are standard: reduction can happen under parallel composition, restriction and process definition. By \((r \text{-} struct)\), reduction is closed under a structural congruence \([55]\) stating, e.g., that \(\lfloor\cdot\rfloor\) is commutative and associative, and has \(0\) as neutral element (i.e., \(P \mid Q \equiv Q \mid P\), \(P \mid (Q \mid R) \equiv (P \mid Q) \mid R\) and \(P \mid 0 \equiv P\)).

\textbf{Example 2.4.} The process in Ex. 2.2 reduces as (see also Fig. 2(b), noting the scope of \(s\)):

\[
(\nu_{s_1}, s_2, s_3)(Q \mid P_s \mid P_1 \mid P_2) \to \text{ (by } (r \text{-} comm)\text{ between } Q \text{ and } P_{s}, \text{ (r-par), (r-struct), (r-res))}
\]

\[
(\nu_{s_1}, s_3)(s_{s_1}[q][p] \oplus \text{play} (s[a]) \mid s_{s_1}[q][p] \oplus \text{play} (s[c])) \mid s[b][c] \oplus \text{interact} ("...") \ldots \mid P_s \mid P_2
\]

### 2.1 Multiparty Session Typing

We now illustrate the typing system for the MPST \(\pi\)-calculus, and its properties. We adopt standard definitions from literature — except for some crucial (and duly noted) adaptations.

The goal of the MPST typing system is to ensure that processes interact on their channels according to given specifications, represented as session types. MPST foster a top-down approach: a global type \(G\) describes a protocol involving various roles — e.g., the game with roles \(a, b, c\) in \(s\); \(G\) is projected into a set of \((local)\) session types \(S_a, S_b, S_c, \ldots\) (one per role) that specify how each role is expected to use its channel endpoint; finally, session types are assigned to channels, and the processes using them are type-checked. Typing ensures that processes \((1)\) never go wrong (i.e., use their channels type-safely), and \((2)\) interact according to \(G\), by respecting its projections — thus realising a multiparty, deadlock-free session.

In the following, we provide a revised and streamlined presentation that clearly outlines the interplay between the global/local typing levels. For this reason, unlike most papers, we discuss local types first, and global types later, at the end of the section.

**Session Types: Local and Partial** Session types describe the expected usage of a channel, as a communication protocol involving two or more \(roles\). They allow to declare structured sequences of input/output actions, specifying who is the source/target role of interaction.

**Definition 2.5** (Types and roles). The syntax of \((local)\) session types is:

\[
S := p \&_{i \in I} ?_{l_i(U_i)} S_i \quad \text{(branching from role } p \text{ — with } I \neq \emptyset)
\]

\[
p \oplus_{i \in I} !_{l_i(U_i)} S_i \quad \text{(selection towards role } p \text{ — with } I \neq \emptyset)
\]

\[
\mu t.S \mid t \mid \text{end} \quad \text{(recursive type, type variable, termination)}
\]

\[
B := \text{Bool} \mid \text{Int} \mid \ldots \quad \text{(base type)}
\]

\[
U := B \mid S \text{ (closed) (payload type)}
\]

We omit \&/\oplus when \(I\) is a singleton: \(pU_i(\text{Int})S_i\) stands for \(p \oplus_{i \in \{1\}} U_i(\text{Int})S_i\).

The set of \(roles\) in \(S\), denoted as \(\text{roles}(S)\), is defined as follows:

\[
\text{roles}(p \&_{i \in I} ?_{l_i(U_i)} S_i) \triangleq \text{roles}(p \&_{i \in I} ?_{l_i(U_i)} S_i) \cup \{p\} \cup \bigcup_{i \in I} \text{roles}(S_i)
\]

\[
\text{roles}(\text{end}) \triangleq \emptyset \quad \text{roles}(t) \triangleq \emptyset \quad \text{roles}(\mu t.S) \triangleq \text{roles}(S)
\]

We will write \(p \in S\) for \(p \in \text{roles}(S)\), and \(p \in S \setminus q\) for \(p \in \text{roles}(S) \setminus \{q\}\).

The \(\text{branching}\) type \(p \&_{i \in I} ?_{l_i(U_i)} S_i\) describes a channel that can receive a label \(l_i\) from role \(p\) (for some \(i \in I\), chosen by \(p\)), together with a \textit{payload} of type \(U_i\); then, the channel must be used as \(S_i\). The \(\text{selection}\) \(p \oplus_{i \in I} !_{l_i(U_i)} S_i\), describes a channel that can choose a label \(l_i\) (for any \(i \in I\)), and send it to \(p\) together with a payload of type \(U_i\); then, the channel must be used as \(S_i\). The labels of branch/select types are all distinct and their order is irrelevant. The \(\text{recursive}\) type \(\mu t.S\) and \text{type variable} \(t\) model infinite behaviours. \text{end} is the type of a \textit{terminated channel} (often omitted). \text{Base types} \(B, B', \ldots\) can be types like \text{Bool}, \text{Int}, \text{etc. Payload types} \(U, U', \ldots\) are either base types, or \text{closed} session types.
Example 2.6. See the definition and description of session type \( S \) in §1 (p. 2).

To define session typing contexts later on, we also need partial session types.

Definition 2.7. Partial session types, denoted by \( H \), are:
\[
H ::= \kappa_{i \in I} \exists_i(U_i).H_i \mid \oplus_{i \in I} \exists_i(U_i).H_i \mid \mu t.H \mid t \mid \text{end}
\]
(branching, selection) (with \( I \neq \emptyset \), \( U_i \) closed)
(recursive type, type variable, termination)

A partial session type \( H \) is either a branching, a selection, a recursion, a type variable, or a terminated channel type. Unlike Def. 2.5, partial types have no role annotations: they are similar to binary session types (but the payloads \( U_i \) can be multiparty) — and similarly, they endow a notion of duality: the outputs of a type match the inputs of its dual, and vice versa.

Definition 2.8. \( \overline{H} \) is the dual of \( H \), defined as:
\[
\overline{\exists_i(U_i).H_i} \equiv \kappa_{i \in I} \exists_i(U_i).H_i^\dagger \quad \kappa_{i \in I} \exists_i(U_i).H_i^\dagger \equiv \exists_{i \in I} \exists_i(U_i).H_i^\dagger \quad \overline{\oplus_{i \in I} \exists_i(U_i).H_i} \equiv \oplus_{i \in I} \exists_i(U_i).H_i^\dagger
\]

The dual of a selection type is a branching with dualised continuations, and vice versa; the payloads \( U_i \) are the same. Duality is the identity on \( \text{end} \) and \( t \), and homomorphic on \( \mu t.H \).

Multiparty session types can be projected onto a role \( q \) (Def. 2.9 below): this yields a partial type that only describes the communications where \( q \) is involved. This is technically necessary for typing rules, as we will see in Def. 2.11 later on.

Definition 2.9. \( S \mid q \) is the partial projection of \( S \) onto \( q \):
\[
\begin{align*}
\text{end} | q & \triangleq \text{end} \\
t | q & \triangleq t \\
(\mu t.S) | q & \triangleq \left\{ \begin{array}{ll}
\mu t.(S | q) & \text{if } S | q \neq t' (\forall t') \\
\text{end} & \text{otherwise}
\end{array} \right.
\end{align*}
\]

where \( \sqcap \) is the merge operator for partial session types:
\[
\begin{align*}
\text{end} \sqcap \text{end} & \triangleq \text{end} \\
t \sqcap t & \triangleq t \\
\mu t.H \sqcap \mu t.H' & \triangleq \mu t.(H \sqcap H') \\
\kappa_{i \in I} \exists_i(U_i).H_i \sqcap \kappa_{i \in I} \exists_i(U_i).H_i' & \triangleq \kappa_{i \in I} \exists_i(U_i).(H_i \sqcap H_i') \\
\oplus_{i \in I} \exists_i(U_i).H_i \sqcap \oplus_{i \in I} \exists_i(U_i).H_i' & \triangleq \left( \oplus_{i \in I} \exists_i(U_i).(H_i \sqcap H_i') \right) \sqcup \left( \oplus_{i \in I} \exists_i(U_i).H_i \right) \sqcup \left( \oplus_{i \in I} \exists_i(U_i).H_i' \right)
\end{align*}
\]

The projection of \( \text{end} \) or a type variable \( t \) onto any role is the identity. Projecting a recursive type \( \mu t.S \) onto \( q \), means projecting \( S \) onto \( q \), if \( S \mid q \) is not some \( t' \), for all possible recursive variables \( t' \); otherwise, the projection is \( \text{end} \). The projection of a selection \( p \oplus_{i \in I} \exists_i(U_i).S_i \) (resp. branching \( p \kappa_{i \in I} \exists_i(U_i).S_i \) on role \( p \)), produces a partial selection type \( \oplus_{i \in I} \exists_i(U_i).(S_i | p) \) (resp. branching \( \kappa_{i \in I} \exists_i(U_i).S_i | p \)) with the continuations projected on \( p \). Otherwise, if projecting on \( q \neq p \), the select/branch is “skipped”, and the projection is the merging of the continuations, i.e., \( \prod_{i \in I} (S_i | q) \). The \( \sqcap \) operator (introduced in [62, 17]) expands the set of session types whose partial projections are defined, which allows to type more processes (as we will see in Def. 2.11 and Ex. 2.14 later on). Crucially, \( \sqcap \) can compose different internal choices, but not external choices (because this could break type safety).

Subtyping The subtyping relation (Def. 2.10) says that a session type \( S \) is “smaller” than \( S' \) when \( S \) is “less demanding” than \( S' \) — i.e., when \( S \) permits more internal choices, and imposes less external choices, than \( S' \). When typing processes (Def. 2.12), a channel with a smaller type can be used whenever a channel with a larger type is required, according to Liskov's Substitution Principle [42]. Subtyping is defined on both local and partial types.
A Linear Decomposition of Multiparty Sessions

\[
\begin{align*}
\forall i \in I, U_i & \leq_S S_i' \quad \text{(S-Bcni)} \quad \forall i \in I, U_i' & \leq_S S_i' \quad \text{(S-Sel)} \\
p \& \in i \subseteq \text{roles}(U_i).S_i \leq_S p \& \in i \subseteq \text{roles}(U_i').S_i' & \quad \text{(S-End)} \quad S \leq_S S' \quad \text{(S-\mu L)} \quad S \leq_S S' \quad \text{(S-\mu R)} \\
B \leq_B B' \quad \text{(S-B)} & \quad \text{end} \leq S \text{ end} \quad \text{(S-End)} \quad H \leq_P H' \quad \text{(S-ParL)} \quad H \leq_P H' \quad \text{(S-ParR)} \\
\forall i \in I, U_i & \leq_S S_i \quad H_i \leq_P H_i' \quad \text{(S-Parbnci)} \quad \forall i \in I, U_i' & \leq_S S_i' \quad H_i \leq_P H_i' \quad \text{(S-ParSel)} \\
& \quad \text{end} \leq \text{end} \quad (\text{S-End}) \quad H \leq_P H' \quad \text{(S-ParbP)} \\
& \quad H \leq_P H' \quad \text{(S-ParbR)} \\
\end{align*}
\]

Figure 3 Subtyping for session types (top) and partial session types (bottom).

Definition 2.10 (Subtyping). The subtyping \( \leq_S \) on multiparty session types is the largest relation such that (i) if \( S \leq_S S' \), then \( \forall p \in (\text{roles}(S) \cup \text{roles}(S')) S[p] \leq_P S'[p] \), and (ii) is closed backwards under coinductive rules at the top of Fig. 3. The subtyping \( \leq_P \) on partial session types is coinductively defined by the rules at the bottom of Fig. 3.

Def. 2.10 uses coinduction to support recursive types [51, § 20 and § 21]. Clause (i) links local and partial subtyping, and ensures that if two types are related, then their partial projections exist: this will be necessary later, for typing contexts (Def. 2.11). The gist of Def. 2.10 lies in clause (ii). Rules (s-Bcni)/(s-Sel) define subtyping on branch/select types. Both rules are covariant in the continuation types, i.e., they require \( S_i \leq_S S_i' \). (s-bnci) is coinductive also in the number of branches offered, whereas (s-Sel) is contravariant. (s-b) relates base types, if they are related by \( \leq_B \). (s-End) relates terminated channel types. (s-\mu L) and (s-\mu R) are standard under coinduction: they say that a recursive session type \( \mu.S \) is related to \( S' \), iff its unfolding is related, too. The subtyping \( \leq_P \) for partial types is similar, except for the lack of role annotations (thus resembling the binary subtyping [21]).

Multiparty Session Typing System Before delving into the session typing rules (Def. 2.12), we need to formalise the notions of typing context and typing judgement, defined below.

Definition 2.11. A session typing context \( \Gamma \) is a partial mapping defined as:

\[
\Gamma ::= \emptyset \mid \Gamma, x:U \mid \Gamma, s[p]:S (\text{with } p \notin S)
\]

We say that \( \Gamma \) is consistent iff for all \( s[p]:S_p, s[q]:S_q \in \Gamma \) with \( p \neq q \), we have \( S_p \leq_P S_q \). We say that \( \Gamma \) is complete iff for all \( s[p]:S_p \in \Gamma \), \( q \in S_p \) implies \( s[q] \in \text{dom}(\Gamma) \). We say that \( \Gamma \) is unrestricted, \( \text{un}(\Gamma) \), iff for all \( c \in \text{dom}(\Gamma) \), \( \Gamma(c) \) is either a base type or end. The typing contexts composition \( \circ \) is the commutative operator with \( \emptyset \) as neutral element:

\[
\begin{align*}
\Gamma_1, c:U \circ \Gamma_2, c':U' & \triangleq (\Gamma_1 \circ \Gamma_2), c:U, c':U' \quad \text{(if } \text{dom}(\Gamma_2) \neq c \neq c' \neq \text{ dom}(\Gamma_1)) \\
\Gamma_1, x:B \circ \Gamma_2, x:B & \triangleq (\Gamma_1 \circ \Gamma_2), x:B
\end{align*}
\]

A typing context can map a channel with role \( s[p] \) to a session type \( S \) (that cannot refer to \( p \) itself, ruling out “self-interactions”), but not to a base type. Variables can be mapped to either session or base types. The clause “\( \forall c:S \in \Gamma : S | p \) is mapped” is discussed below.

On Consistency In Def. 2.11, and in the rest of this work, we emphasise the importance of consistency of the context \( \Gamma \) for session typing: this condition is, in fact, necessary to prove subject reduction, and will be central for our encoding (§5 and §6). As an example of
non-consistent typing context, consider \( s[p]: \text{end}, s[q]: ?!(U).S \): we have \( \text{end} \mid q = \text{end} \not\equiv_p ?!(U).S \mid p \).

Note that our consistency in Def. 2.11 is weaker than the one in previous papers (where it is sometimes called coherency): we use \( \preceq_p \), instead of (syntactic) type equality \( = \), to relate dual partial projections. The reason being: if we use \( = \), and adopt partial projections with type merging (Def. 2.9), subject reduction does not hold. Hence, by relaxing our definition, and proving Thm. 2.16 later on, we fix a longstanding mistake appearing e.g., in [62, 17].

**Definition 2.12 (Session typing judgements).** The process declaration typing context \( \Theta \) maps process variables \( X \) to \( n \)-tuples of types \( \bar{U} \) (one per argument of \( X \)), and is defined as:

\[
\Theta ::= \emptyset \mid \Theta, X: \bar{U}
\]

Typing judgements are inductively defined by the rules in Fig. 4, and have the forms:

- for processes: \( \Theta \cdot \Gamma \vdash P \) (with \( \Gamma \) consistent, and \( \forall c: S \in \Gamma, S \mid p \) is defined \( \forall p \in S \))

- for values: \( \Gamma \vdash \text{v: } \bar{U} \)

The judgement \( \Theta \cdot \Gamma \vdash P \) reads: “process \( P \) is well-typed in \( \Theta \) and \( \Gamma \)”. \( \Theta \) and \( \Gamma \), in turn, type respectively process variables (judgement \( \Theta \vdash X: \bar{U} \)) and values, including channels (judgement \( \Gamma \vdash \text{v: } \bar{U} \)). Rule (T-NAME) says that a channel has the type assumed in the session typing context. (T-BASIC) relates base values to their type. By (T-DEFCTX), a process name has the type assumed in the process declaration typing context. (T-SUB) is the standard subsumption rule, using \( \preceq_5 \) (Def. 2.10). By (T-NIL), the terminated process is well typed in any unrestricted typing context. By (T-PAR), the parallel composition of \( P \) and \( Q \) is well typed under the composition of the corresponding typing contexts, as per Def. 2.11. By (T-RES), \( (\nu s)P \) is well typed in \( \Gamma \), if \( s \) occurs in a complete set of typed channels with roles (denoted with \( \Gamma' \)), and the open process \( P \) is well typed in the “full” context \( \Gamma, \Gamma' \). For convenience, we annotate the restricted \( s \) with \( \Gamma' \) in the process, giving \( (\nu s: \Gamma')P \). (T-BRCH) (resp. (T-SEL)) state that branching (resp. selection) process on \( c[p] \) is well typed if \( c[p] \) is of compatible branching (resp. selection) type, and the continuations \( P_i \), for all \( i \in I \), are well typed with the continuation session types. By (T-DEF), a process definition \( \text{def } X(\bar{x}) = P \text{ in } Q \) is well typed if both \( P \) and \( Q \) are well typed in their typing contexts enriched with \( \bar{x}: \bar{U} \). For convenience, we annotate \( \bar{x} \) with types \( \bar{U} \). By (T-CALL), process call \( X(v_1, \ldots, v_n) \) is well typed if the actual parameters \( v_1, \ldots, v_n \) have compatible types w.r.t. \( X \).

As mentioned above, we emphasise consistency by restricting typing judgements to consistent typing contexts — i.e., those allowing to prove subject reduction. The clause “\( \forall c: S \in \Gamma : S \mid p \) is defined” is unusual in MPST works, but arises naturally: by requiring the existence of partial projections, it rejects processes containing \( (a) \) a channel with role \( s[p]: S \)
that, for some q ∈ S, cannot be (consistently) paired with s[q], or (b) a variable x:S that, in a consistent and complete Γ, cannot be substituted by any s[p]:S. Rejected processes cannot join any complete session (case (a)), or are never-executed “dead code” (case (b)).

► Remark 2.13. Unlike most MPST papers (e.g., [18, 10]), our rule (T-Rns) does not directly map a session s to a global type: this is explained in the next section, “Global Types”.

► Example 2.14. Consider the session type S_b in §1 (p. 2), and the client process P_b = Clients_b(s_b[p]) from Ex. 2.12. By Def. 2.12, the following typing judgement holds:

\[
\text{Client} b \colon q?\text{play}(S_b) \land \text{Loop}_b \colon \mu t. a \land \{ \text{nov1BC}(\text{int}).c \text{!nov1BC}(\text{int}).t, \} \land s_b[p] \colon q?\text{play}(S_b) \vdash \text{Clients}_b(s_b[p])
\]

It says that the channel with role s_b[p] is used following type q?play(S_b).end (with a delegation of a S_b-typed channel); the argument of Clients_b has the same type; the argument of Loop_b is used following the game loop. This example cannot be typed without merging \( \sqcap \) (Def. 2.9): its derivation requires to compute S_b[c \equiv !\text{InfoBC}(\text{string}).\mu t. (\text{mov1BC}(\text{int}).t \sqcap \text{mov2BC}(\text{bool}).t) = !\text{InfoBC}(\text{string}).\mu t. (\text{mov1BC}(\text{int}).t \sqcup \text{mov2BC}(\text{bool}).t), \) which is undefined without merging.

The typing rules in Fig. 4 satisfy a subject reduction property (Thm. 2.16) based on typing context reductions. Reduction relations for typing contexts are common in typed process calculi, and reflect the communications required by the types in Γ.

► Definition 2.15 (Typing context reduction). The reduction \( \Gamma \rightarrow \Gamma' \) is:

\[
\begin{align*}
& \text{s[p]:S}_p, s[q]:S_q \rightarrow s[p]:S_k, s[q]:S_k' & \text{if } & \begin{cases} \\
\text{unf}(S_k) = q \sqcap \{ \exists i \in I. S_i \}, \text{ if } k \in I \\
\text{unf}(S_k) = p \sqcup \{ \exists i \in I. S_i' \}, \text{ if } U_k \subseteq S U_k'
\end{cases} \\
& \text{Γ, c:U \rightarrow Γ', c:U'} & \text{if } & \Gamma \rightarrow \Gamma' \text{ and } U \subseteq S U'
\end{align*}
\]

Our Def. 2.15 is a bit less straightforward than the ones in literature: it accommodates subtyping (hence, uses \( \sqsubseteq \)) and our iso-recursive type equality (hence, unfolds types explicitly).

► Theorem 2.16 (Subject reduction). If \( \Theta \vdash \Gamma \vdash P \text{ and } P \rightarrow P' \), then \( \exists \Gamma' \vdash \Theta \vdash \Gamma' \vdash P' \).

**Global Types**

We conclude this section with global types, mentioned in §2.1 and Remark 2.13.

► Definition 2.17. The syntax of global types, ranged over by \( G \), is:

\[
G \ ::= \ p \rightarrow q : \{ \{i(U_i).G_i\}_{i \in I} \} \quad \text{(interaction — with } U \text{ closed)} \\
\mu t. G \mid t \mid \text{end} \quad \text{(recursive type, type variable, termination)}
\]

Type \( p \rightarrow q : \{ \{i(U_i).G_i\}_{i \in I} \) states that role \( p \) sends to role \( q \) one of the (pairwise distinct) labels \( i \) for \( i \in I \), together with a payload \( U_i \) (Def. 2.5). If the chosen label is \( i_j \), then the interaction proceeds as \( G_j \). Type \( \mu t. G \) and type variable \( t \) model recursion. Type \( \text{end} \) states the termination of a protocol. We omit the braces \( \{ ... \} \) from interactions when \( I \) is a singleton: e.g., \( a \rightarrow b : \{ \{i(U_i).G_i\}_{i \in \{1\}} \).

► Example 2.18. The following global type formalises the Game described in §1 and Fig. 1:

\[
G_{\text{Game}} = b \rightarrow c : \text{InfoBC}(\text{string}).c \rightarrow a : \text{InfoCA}(\text{string}).a \rightarrow b : \text{InfoBC}(\text{string})
\]

\[
\mu t. a \rightarrow b : \begin{cases} \\
\text{nov1BC(\text{int}).b} \rightarrow c : \text{InfoCA}(\text{int}).c \rightarrow a : \{ \text{nov1CA}(\text{int}).t, \text{mov2CA(\text{bool}).t} \} \\
\text{nov2BC(\text{bool}).b} \rightarrow c : \text{Info2BC(\text{bool})}.c \rightarrow a : \{ \text{nov1CA(\text{int}).t}, \text{nov2CA(\text{bool}).t} \}
\end{cases}
\]

In MPST theory, a global type \( G \) with roles \( p_i \) (\( i \in I \)) is used to project\(^1\) a set of session types \( S_i \) (one per role). E.g., projecting \( G_{\text{Game}} \) in Ex. 2.18 onto \( b \) yields the session type \( S_b \)

\(^1\) We use a standard projection with merging [62, 17]: for its definition (not crucial here), see [55].
When all such projections $S_i$ are defined, and all partial projections of each $S_i$ are defined (as per Def. 2.9), then we can define the projected typing context of $G$:

$$\Gamma_G = \{s[p_i] : S_i\}_{i \in I}$$

where $\forall i \in I : S_i$ is the projection of $G$ onto $p_i$. $\Gamma_G$ can be shown to be: (a) consistent and complete, i.e., can be used to type the session $s$ by rule (T-Res) (Fig. 4), and (b) deadlock-free, i.e.: $\Gamma_G \Rightarrow^* \Gamma_G \not\Rightarrow$ implies $\forall i \in I : \Gamma_G(s[p_i]) = \text{end}$. Similarly, it can be shown that $\Gamma_G$ reduces as prescribed by $G$.

Now, from observation (a) above, we can easily define a “strict” version of rule (T-Res) (Fig. 4) in the style of [18, 10], where (1) the clause “T' complete” is replaced with “T' is the projected typing context of some $G$”, and (2) in the conclusion, the annotation $(\nu s : \Gamma)$ is replaced with $(\nu s : G)$. Further, observation (b) allows to prove Thm. 2.19 below, as shown e.g. in [4]: a typed ensemble of processes interacting on a single $G$-typed session is deadlock-free (note: with our rules in Fig. 4, the annotation $(\nu s : G)$ would be $(\nu s : \Gamma_G)$).

**Theorem 2.19 (Deadlock freedom).** Let $P_1 \cdot P_2 \vdash_\bullet P$, where $P \equiv (\nu s : G)_{i \in I} P_i$ and each $P_i$ only interacts on $s[p_i]$. Then, $P$ is deadlock-free: i.e., $P \Rightarrow^* P' \not\Rightarrow$ implies $P' \equiv 0$.

Note that the properties above emerge by placing suitable session types $S_i$ in the premises of (T-Res) — but our streamlined typing rules in Fig. 4 do not require it, nor mention $G$. The main property of such rules is ensuring type safety (Thm. 2.16). We will exploit this insight (obtained by our separation of global/local typing) in our encoding (§5), preserving semantics and types (and thus, Thm. 2.19) without explicit references to global types.

### 3 Linear $\pi$-Calculus

The $\pi$-calculus is the canonical model for communication and concurrency based on message-passing and channel mobility. It was developed in the late 1980’s, with the first publication in 1992 [44], followed by various proposals for types and type systems. In this section we summarise the theory of the $\pi$-calculus with linear types [34], adopting a standard formulation and well-known results from [54]. We will present new $\pi$-calculus-related results in §4.

**Definition 3.1.** The syntax of $\pi$-calculus processes and values is:

$$P, Q := 0 \mid P | Q \mid (\nu x)P \quad \text{(inaction, parallel composition, restriction)}$$

$$P \mid \pi(v).P \mid x(y).P \quad \text{(process replication, output, input)}$$

$$\text{case } v \text{ of } \{l_i(x_i) \triangleright P_i\}_{i \in I} \quad \text{(variant destruct)}$$

$$\text{with } [l_i : x_i]_{i \in I} = v \text{ do } P \quad \text{(labelled tuple destruct)}$$

$$a, v := x, y, w, z \mid l(v) \mid [l_i : v_i]_{i \in I} \quad \text{(name, variant value, labelled tuple value)}$$

$$\text{false} \mid \text{true} \mid 42 \mid \ldots \quad \text{(base value)}$$

In $\pi$-calculus, names $x, y, \ldots$ can be intuitively seen as variables (i.e., they can be substituted with values), and as communication channels (i.e., they can be used for input/output). Values can be names, base values like `false` or 42, variant values $l(v)$ and labelled tuples $[l_i : v_i]_{i \in I}$. The inaction 0 and the parallel composition $P \mid Q$ are similar to Def. 2.1. The restriction $(\nu x)P$ creates a new name $x$ and binds it with scope $P$. The replicated process $*P$ represents infinite replicas of $P$, composed in parallel. The output $\pi(v).P$ uses the name $x$ to send a value $v$, and proceeds as $P$; the input $x(y).P$ uses $x$ to receive a value that will substitute $y$ in the continuation $P$. Process $\text{case } v \text{ of } \{l_i(x_i) \triangleright P_i\}_{i \in I}$ pattern matches a variant value $v$, and if it has label $l_i$, substitutes $x_i$ and continues as $P_i$. Process $\text{with } [l_i : x_i]_{i \in I} = v \text{ do } P$ destructs a labelled tuple $v$, substituting each $x_i$ in $P$. For brevity, we will often write “record” instead of “labelled tuple”.

**Definition 3.2.** The $\pi$-calculus operational semantics is the relation $\rightarrow$ defined as:
A Linear Decomposition of Multiparty Sessions

\[ (\text{R}\_\text{Com}) \quad \pi(v).P \mid x(y).Q \rightarrow P \mid Q \{v/y\} \]
\[ (\text{R}\_\text{Case}) \quad \text{case } l_j(v) \text{ of } \{l_i(x_i) \triangleright P_i\}_{i \in I} \rightarrow P_j \{l_j/v\} \quad (j \in I) \]
\[ (\text{R}\_\text{With}) \quad \text{with } [l_i : x_i]_{i \in I} \triangleright [l_i : v_i]_{i \in I} \quad \text{do } P \rightarrow P \{\forall i \in I \mid l_i/v_i\} \]
\[ (\text{R}\_\text{Res}) \quad P \rightarrow Q \quad \text{implies } (\nu x)P \rightarrow (\nu x)Q \]
\[ (\text{R}\_\text{Par}) \quad P \rightarrow Q \quad \text{implies } P | R \rightarrow Q | R \]
\[ (\text{R}\_\text{Struct}) \quad T \equiv P' \land P \rightarrow Q \land Q' \equiv Q' \quad \text{implies } P' \rightarrow Q' \]

Rule (\text{R}\_\text{Com}) models communication between output and input on a name \( x \): it reduces to the corresponding continuations, with a value substitution on the receiver process. (\text{R}\_\text{Case}) says that case applied on a variant value \( l_j(v) \) reduces to \( P_j \), with \( v \) in place of \( x_j \) — provided that \( l_j \) is one of the supported cases (i.e., \( l_j = l_i \) for some \( i \in I \)). Rule (\text{R}\_\text{With}) deconstructs a labelled tuple \([l_i : v_i]_{i \in I}\): it says that with reduces to its continuation \( P \) with \( v_i \) in place of each \( x_i \), for all \( i \in I \). By (\text{R}\_\text{Res}) and (\text{R}\_\text{Par}), reductions can happen under restriction and parallel composition, respectively. By (\text{R}\_\text{Struct}), reduction is closed under the structural congruence \( \equiv \), whose definition is standard (see [54, Table 1.1] and [55]).

\( \pi \)-Calculus Typing \quad We now summarise the \( \pi \)-calculus types, subtyping, and typing rules.

**Definition 3.3 (\( \pi \)-types).** The syntax of a \( \pi \)-calculus type \( T \) is given by:

\[
T ::= \text{Li}(T) \mid \text{Lo}(T) \mid \text{Lj}(T) \quad \text{(linear input, linear output, linear connection)}
\]

\[
\#(T) \mid \bullet \quad \text{(unrestricted connection, no capability)}
\]

\[
[l_i : T_j]_{i \in I} \quad \text{variant, labelled tuple a.k.a. “record”}
\]

\[
\mu T \mid t \mid \text{Bool} \mid \text{Int} \mid \ldots \quad \text{(recursive type, type variable, base type)}
\]

Linear types \( \text{Li}(T) \), \( \text{Lo}(T) \) denote, respectively, names used exactly once to input/output a value of type \( T \). \( \text{Lj}(T) \) denotes a name used once for sending, and once for receiving, a message of type \( T \). \( \#(T) \) denotes an unrestricted connection, i.e., a name that can be used both for input/output any number of times. \( \bullet \) is assigned to names that cannot be used for input/output. \( [l_i : T_j]_{i \in I} \) is a labelled disjoint union of types, while \([l_i : T_j]_{i \in I} = [l_i : T_j]_{i \in I} \) (that we will often call “record”) is a labelled product type; for both, labels \( l_i \) are all distinct, and their order is irrelevant. As syntactic sugar, we write \( (T_i)_{i \in 1..n} \) for a record with integer labels \([i : T_j]_{i \in 1..n} \). Recursive types and variables, and base types like \text{Bool}, are standard.

The predicate \( \text{lin}(T) \) (Def. 3.4 below) holds if \( T \) has some linear input/output component.

**Definition 3.4 (Linear/Restrictive types).** The predicate \( \text{lin} \) is inductively defined as:

\[
\begin{align*}
\text{lin}(\text{Li}(T)) & \quad \exists j \in I : \text{lin}(T_j) \\
\text{lin}(\text{Lo}(T)) & \quad \exists j \in I : \text{lin}(T_j) \\
\text{lin}(\text{Lj}(T)) & \quad \text{lin} \end{align*}
\]

We write \( \text{un}(T) \) iff \( \neg \text{lin}(T) \) (i.e., \( T \) is unrestricted if \( \neg \text{lin} \)) is not linear.

**Definition 3.5. Subtyping \( \leq \text{pt} \) for \( \pi \)-types is coinductively defined as:

\[
\begin{align*}
B \leq_{\pi} B' & \quad \text{(S-LB)} \quad \text{if } B \subseteq B' \\
\leq_{\pi} B' & \quad \text{(S-END)} \quad \text{if } B \leq_{\pi} B' \\
\forall i \in I \quad T_i \leq_{\pi} T'_i & \quad \text{(S-VARIANT)} \quad \text{if } [l_i : T_i]_{i \in I} \leq_{\pi} [l_i : T'_i]_{i \in I} \\
T \leq_{\pi} T' & \quad \text{(S-LI)} \quad \text{if } \text{Li}(T) \leq_{\pi} \text{Li}(T') \\
\text{Lo}(T) \leq_{\pi} \text{Lo}(T') & \quad \text{(S-Lo)} \quad \text{if } T' \leq_{\pi} T \\
T \{\mu T\} \leq_{\pi} T' & \quad \text{(S-LTUPLE)} \quad \text{if } \mu T \leq_{\pi} T' \\
\end{align*}
\]

By rule (S-LB), \( \leq_{\pi} \) includes basic subtyping \( \leq_{B} \). (S-END) relates types without I/O capabilities. By (S-LI) (resp. (S-Lo)), linear input (resp. output) subtyping is covariant (resp. contravariant) in the carried type. By (S-VARIANT), subtyping for variant types is covariant in both carried types and number of components. By (S-LTUPLE), subtyping for labelled tuples, a.k.a records, is covariant in the carried types. (Note: “full” record subtyping allows to add/remove entries [54, §7.3]; but here, “record” just means “labelled tuple”.) Rule (S-LTUPLE) (and its symmetric, omitted) relates a recursive type \( \mu T \) to \( T' \) iff its unfolding is related to \( T' \).
We introduce some definitions and results on typed §6, to state our encoding and its properties. As we target standard typed π-calculus (§3),

4 Some Typed π-Calculus Extensions and Results

We introduce some definitions and results on typed π-calculus: we will need them in §5 and §6, to state our encoding and its properties. As we target standard typed π-calculus (§3),
A Linear Decomposition of Multiparty Sessions

\[
\text{let } x = v \text{ in } P \triangleq (\nu z) (z(v), 0 \mid z(x), P) \quad (\text{where } z \notin \{x\} \cup \text{fn}(v) \cup \text{fn}(P))
\]

(\text{R}_{\pi} \text{-Let}) \quad \text{let } x = v \text{ in } P \rightarrow P[v/x]

(\text{T}_{\pi} \text{-Let}) \quad \Gamma \vdash v : T \quad \Gamma, x : T \vdash P

(\text{T}_{\pi} \text{-Narrow}) \quad \Gamma, x : P \vdash T' \quad \Gamma, x : T' \vdash P

(\text{T}_{\pi} \text{-MSubst}) \quad \forall i \in I \quad \Gamma_i \vdash v_i : T_i \quad \Gamma_i, \{x_i : T_i\}_{i \in I} \vdash P[\nu_i/x_i]

\hfill \text{Fig. 6} \quad \text{“Let” binder (definition, reduction, typing), and narrowing / substitution rules.}

all our extensions are conservative, so to preserve standard results (e.g., subject reduction).

"Let" binder, narrowing, substitution \quad Fig. 6 shows several auxiliary definitions and typing rules. let \( x = v \text{ in } P \) binds \( x \) in \( P \), and reduces by replacing \( x \) with \( v \) in \( P \). It is a macro on other \( \pi \)-calculus constructs: hence, rules \((\text{R}_{\pi} \text{-Let}) / (\text{T}_{\pi} \text{-Let})\) are based on the reduction/typing of its expansion (details in [55]). Rule \((\text{T}_{\pi} \text{-Narrow})\) derives from the narrowing lemma [54, 7.2.5]. \((\text{T}_{\pi} \text{-MSubst})\) represents zero or more applications of the substitution lemma [54, 8.1.4].

Duality and Recursive \( \pi \)-Types \quad The duality for linear \( \pi \)-types relates opposite but compatible input/output capabilities. Intuitively, the dual of a Li(T) is Lo(T) (and vice versa) [14]. Note that the carried type \( T \) is the same: i.e., dual types can be combined with \( \uplus \) (Def. 3.6), yielding \( \langle T \rangle \). However, defining duality for recursive \( \pi \)-types is not straightforward: what is the dual of \( T = \mu t.\text{Li}(t) \)? Is it maybe \( T' = t.\text{Li}(t) \)? Since \( \uplus \) is not defined for \( \mu \)-types, we can check whether it is defined for the unfoldings of our hypothetical duals \( T \) and \( T' \). Unfortunately, we have \( \text{unf}(T) = \text{Lo}(\mu t.\text{Li}(t)) \) and \( \text{unf}(T') = \text{Li}(\mu t.\text{Li}(t)) \): i.e., \( \uplus \) is again undefined, so \( T, T' \) cannot be considered duals. Solving this issue is crucial: in §5, we will need to encode recursive partial types, preserving their duality (Def. 2.8) in linear \( \pi \)-types.

What we want is a notion of duality that commutes with unfolding, so that if two recursive types are dual, and we unfold them, we get a dual pair \( \text{Lo}(T)/\text{Li}(T) \) that can be combined with \( \uplus \) (since they carry the same \( T \)). We address this issue by extending the \( \pi \)-calculus type variables (Def. 3.3) with their dualised counterpart, denoted with \( \overline{\text{t}} \). We allow recursive types such as \( \mu t.\text{Li}(\overline{t}) \) (but not \( \mu t.\overline{t} \), ...), and postulate that when unfolding, \( \overline{t} \) is substituted by a “dual” type \( t.\text{Li}(t) \), as formalised in Def. 4.1 below. Quite interestingly, our approach reminds of the “logical duality” for session types [40], but we study it in the context of \( \pi \)-calculus (we will further discuss this topic in §8).

\hfill \text{Definition 4.1.} \quad T \text{ is the dual of } T', \text{ and is defined as follows:}

\[
\text{Li}(\overline{T}) \triangleq \text{Lo}(T) \quad \text{Lo}(\overline{T}) \triangleq \text{Li}(T) \quad \bullet \triangleq \bullet \quad \{t\} \triangleq \overline{t} \quad \{\overline{t}\} \triangleq t \quad \mu t.\text{Lo}(\overline{T}) \triangleq \mu t.\text{Li}(T)
\]

The substitution of \( T \) for a type variable \( t \) or \( \overline{t} \) is: \( t\{\overline{t}/t\} \triangleq \overline{T} \quad \overline{t}\{t/\overline{t}\} \triangleq T \).

The dual of a linear input type \( \text{Li}(T) \) is a linear output type \( \text{Lo}(T) \), and vice versa, with the payload type \( T \) unchanged, as expected. The dual of a terminated channel type \( \bullet \) is itself. The dual of a type variable \( t \) is \( \overline{t} \), and the dual of a dualised type variable \( \overline{t} \) is \( t \), implying that duality on linear \( \pi \)-types is convolutive. The dual of \( \mu t.\text{Li}(t) \) is \( \mu t.\text{Lo}(\overline{T}) \), where type \( T \) is dualised to \( \overline{T} \), and every occurrence of \( t \) is replaced by its dual \( \overline{t} \) by Def. 4.1. Now, the desired commutativity between duality and unfolding holds, as per Lemma 4.2 below.

\hfill \text{Lemma 4.2.} \quad \text{unf}(\overline{T}) = \overline{\text{unf}(T)}.

\hfill \text{Example 4.3.} \quad \text{Let } T = \mu t.\text{Li}(t, \overline{t}). \text{ Then:}

\[
\text{unf}(T) = \text{Li}((\mu t.\text{Li}(t, \overline{t}), \mu t.\text{Li}(t, \overline{t}))) = \text{Li}((\mu t.\text{Li}(t, \overline{t}), \mu t.\text{Lo}(\overline{T}, t))) \quad \text{and}
\]

\[
\text{unf}(\overline{T}) = \text{unf}(\mu t.\text{Lo}(\overline{T}, t)) = \text{Lo}((\mu t.\text{Li}(t, \overline{t}), \mu t.\text{Lo}(\overline{T}, t))) = \overline{\text{unf}(T)}
\]
By adding dualised type variables in Def.3.3, we naturally extend the definition of $\text{fv}(T)$ (with $\mu t \ldots$ binding both $t$ and $\bar{t}$), the subtyping relation $\preceq_\pi$ in Def. 3.5 (by letting rules (s-L,R) and (S-L,R) use the substitution in Def. 4.1) and ultimately the typing system in Def. 3.6. These extensions, we will obtain a rather simple encoding of recursive session types (Def. 5.1), and solve a subtle issue involving duality, recursion and continuations (Ex. 5.3).

The reader might be puzzled about the impact of dualised variables in the $\pi$-calculus theory. We show that dualised variables do not increase the expressiveness of linear $\pi$-types, and do not unsafely enlarge subtyping $\preceq_\pi$: this is proved in Lemma 4.4, that allows to erase dualised variables from recursive $\pi$-types. It uses (1) a substitution that only replaces dualised variables, i.e.: $\bar{t} \{ t'/\bar{t} \} = t'$; and (2) the equivalence $= \pi$ defined as: $\preceq_\pi \cap \pi^{-1}$.

- **Lemma 4.4** (Erasure of $\bar{t}$). $\mu t. T =_\pi \mu t. T \{ \mu t'. T \{ t'/\bar{t} \} \}$, for all $t' \notin \text{fv}(T)$.

- **Example 4.5** (Application of erasure). Take $T$ from Ex. 4.3. By Lemma 4.4, we have:

$$T =_\pi \mu t. \text{Li} \left( \left( t, \mu t'. \text{Li}(t, \bar{t}) \{ t'/\bar{t} \} \right) \right) = \mu t. \text{Li}(t, \mu t'. \text{Lo}(t, t')).$$

Since $T =_\pi T'$ implies $T \preceq_\pi T'$ and $T' \preceq_\pi T$, Lemma 4.4 says that any $\mu t. T$ is equivalent to a $\mu$-type without occurrences of $\bar{t}$: i.e., any typing relation with instances of $\bar{t}$ corresponds to a $\bar{t}$-free one. As a consequence, any typing derivation using $\bar{t}$ can be turned into a $\bar{t}$-free one. Summing up: adding dualised variables preserves the standard results of typed $\pi$-calculus.

**Type Combinator $\boxplus$** Def. 4.6 introduces a type combinator that is a “relaxed” version of $\boxplus$ (Def. 3.6) extended with subtyping. We will use it to encode MPST typing contexts (Def. 5.6).

- **Definition 4.6**. The $\pi$-calculus type combinator $\boxplus$ is defined on $\pi$-types as follows (and undefined in other cases), and naturally extended to typing contexts:

$$\begin{align*}
\text{Lo}(T) \cap \text{Li}(T') & \triangleq \text{Li}(T) \cup \text{Lo}(T) \quad \text{if } T \preceq_\pi T' \quad T \cap T & \triangleq T \quad \text{if } \text{un}(T) \\
\text{Li}(T) \cap \text{Lo}(T) & \triangleq \text{Li}(T) \cup \text{Lo}(T) \\
(T_1 \boxplus T_2)(x) & \triangleq \\
& \begin{cases}
\Gamma_1(x) \cap \Gamma_2(x) & \text{if } x \in \text{dom}(\Gamma_1) \cap \text{dom}(\Gamma_2) \\
\Gamma_1(x) & \text{if } x \in \text{dom}(\Gamma_1) \setminus \text{dom}(\Gamma_2)
\end{cases}
\end{align*}$$

The difference between $\cup$ and $\boxplus$ is that the former combines linear inputs/outputs with the same carried type, while $\boxplus$ is more relaxed: it allows a carried type to be subtype of the other — more exactly, the type carried by the output side can be smaller than the type carried by the input side. This is shown in Lemma 4.7 and Ex. 4.8 below.

- **Lemma 4.7**. If $T =_\pi T_1 \boxplus T_2$, and $T_1 \cup T_2 = T$, then either (a) $T_1 \preceq_\pi T_1$ and $T_2 \preceq_\pi T_2$, or (b) $T_1 \preceq_\pi T_2$ and $T_2 \preceq_\pi T_1$.

Lemma 4.7 says that $T_1 \boxplus T_2$ (when defined) is a type that, when split using $\cup$, yields linear I/O types that are subtypes of the originating $T_1, T_2$. Intuitively, it means that $\boxplus$ can be soundly used to simplify typing derivations: if used to type some name $x$, it will yield (when defined) a type that can also be obtained by suitably using $\cup$ and $(T_\pi-,\cup)$ (Fig. 5).

- **Example 4.8**. Let $T_1 = \text{Li}(\text{Real})$, $T_2 = \text{Lo}(\text{Int})$, and $T = T_1 \boxplus T_2$. We have $T = \text{Li}(\text{Int})$; if we let $T_2' = T_2$, then we get either (a) $T_1' = \text{Li}(\text{Int}) \leq_\pi T_1$ and $T_2' = \text{Lo}(\text{Int}) \leq_\pi T_2$, or (b) $T_1' = \text{Lo}(\text{Int}) \leq_\pi T_2$ and $T_2' = \text{Li}(\text{Int}) \leq_\pi T_1$.

5 **Encoding Multiparty Session-$\pi$ into Linear $\pi$-Calculus**

We now present our encoding of MPST $\pi$-calculus into linear $\pi$-calculus. It consists of an encoding of types and an encoding of processes: combined, they preserve the safety properties of MPST communications, both w.r.t. typing and process behaviour.
Encoding of Types  Our goal is to decompose MPST channel endpoints into point-to-point \(\pi\)-calculus channels. This leads to the main intuition behind our approach: encode MPST channel endpoints as labelled tuples, whose labels are roles, and whose values are names (for communication). The idea is that if a multiparty channel of type \(S\) allows to talk with role \(p\), then the corresponding \(\pi\)-calculus record should have a label \(p\), mapping to a name that can send/receive messages to/from the process that plays the role \(p\). This suggests the type of an encoded MPST channel endpoint: it should be a \(\pi\)-calculus record — and since each name appearing in such record is used to communicate, it should have an input/output type.

\[ \text{Example 5.2. Consider the session type } S \triangleq p!_{1}(\text{Int}).q?_{2}(S').\text{end}, \text{ where } S' \triangleq r!_{3}(\text{Bool}).q?_{4}(\text{String}).\text{end}. \text{ By Def. 5.1, the encoding of } S \text{ is:} \]

\[ [S] = [p: [S | p], q: [S | q]] = [p: [l_{1}(\text{Int}), q: [l_{2}(S')]]
\]

\[ = [p: \text{Lo}(l_{1}(\text{Int})), q: \text{Li}(l_{2}(r: \text{Lo}(l_{3}(\text{Bool})), \cdot)), q: \text{Li}(l_{4}(\cdot: \text{String}, \cdot)), \cdot)] \]

Recursion, Continuations and Duality  We now point out a subtle (but crucial) difference between Def. 5.1 and the encoding of binary, non-recursive session types in [14]. When encoding partial selections, our continuation type is the \(\pi\)-calculus record — and since each name appearing in such record is used to communicate, it should have an input/output type.

\[ \text{Recursion, Continuations and Duality.} \]

\[ \text{Let } H = \mu t. !(\text{Bool}).t. \text{ By Def. 5.1, we have:} \]

\[ [H] = [[\mu t. !!(\text{Bool}).t]] = [\mu t. \text{Lo}(l_{-}(\text{Bool}, [t]))] = [\mu t. \text{Lo}(\cdot(\text{Bool}, \cdot))]] \]

Let us now unfold the encoding of \(H\). By Def. 4.1, we have:

\[ \text{unf}([H]) = \text{unf}([\mu t. \text{Lo}(l_{-}(\text{Bool}, \cdot))]) = \text{Lo}(l_{-}(\text{Bool}, \mu t. \text{Li}(l_{-}(\text{Bool}, \cdot)))) \]

This is what we want: since \(H\) requires a recursive output of \text{Booleans}, its encoding should output a \text{Boolean} together with a \text{recursive input name} as continuation. Hence, the recipient
will receive the first Boolean together with a continuation name, whose type mandates to recursively input more Booleans. If encoding continuations as in [14], instead, we would have:

\[
[H] = \mu t. Lo(l_\bot([\text{Bool}], [\bot])) = \mu t. Lo(l_\bot(\text{Bool}, t)) \text{ (t is not dualised)}
\]

\[\text{unf}(\langle H \rangle) = Lo(l_\bot(\text{Bool}, \mu t. Lo(l_\bot(\text{Bool}, t))))\]

which is wrong: the recipient is required to recursively output Boolean. This wrong encoding would also prevent us from obtaining Thm.6.1 later on.

**Encoding of Typing Contexts** In order to preserve type safety, we want to encode a session judgement (Fig.4) into a π-calculus typing judgement (Fig.5). For this reason, we now use the encoding of session types (Def.5.1) to formalise the encoding of session typing contexts.

► **Definition 5.4.** The encoding of a session typing context is:

\[
\begin{align*}
\emptyset & \triangleq \sigma \\
\Theta \cdot \Gamma & \triangleq [\Theta], [\Gamma] \\
\mathcal{C} : \mathcal{U} & \triangleq [\mathcal{C} : U] \\
\mathcal{X} & \triangleq x \\
\mathcal{X} : \mathcal{U}_1, \ldots, \mathcal{U}_n & \triangleq [\mathcal{X} : (\mathcal{U}_i)_{i \in 1..n}]
\end{align*}
\]

When encoding typing contexts, variables \(x\) keep their name, while process variables \(X\) and channels with roles \(s[p]\) are turned into distinguished names with a subscript: e.g., \(X\) becomes \(z_X\). The composition \(\Gamma_1 \circ \Gamma_2\) (Def.2.11) is encoded using \(\uplus\) (Def.3.6): such an operation is always defined, since the domains of \([\Gamma_1],[\Gamma_2]\) can only overlap on basic types.

Note that encoded process variables have an unrestricted connection type, carrying an n-tuple of encoded argument types; encoded sessions, instead, are linearly-typed, similarly to [14]: this will allow to exploit the (partial) confluence properties of linear π-calculus [34] to prove Thm.6.5 later. Moreover, this will lead to the implementation discussed in §7.

**Encoding Typing Judgements: Overview** With these definitions at hand, we can now have a first look at the encoding of session typing judgements in Fig.7 (but we postpone the formal statement to Def.5.7 later on, as it requires some more technical developments).

**Terminated processes** are encoded homomorphically. **Parallel composition** is also encoded homomorphically — i.e., our encoding preserves the choreographic distribution of the originating processes. Note that \([P_1]_\Theta \Gamma_1\) and \([Q_1]_\Theta \Gamma_2\) are the encoded processes yielded respectively by \([\Theta \cdot \Gamma_1]_\Theta P_1\) and \([\Theta \cdot \Gamma_2]_\Theta Q_2\): they exist because such typing judgements hold, by inversion of \((T \text{-PAR})\) (Fig.4). Similar uses of sub-processes encoded w.r.t. their typing occur in the other cases. **Process declaration** \(X(x) : \mathcal{U} = \mathcal{P}\) in \(Q\) is encoded as a replicated π-calculus process that inputs a value \(z\) and a name \(X\) = \(z_X\) (matching Def.5.4), deconstructs it into \(x_1, \ldots, x_n\) (using **with**, and hence assuming that \(z\) is an n-tuple), and then continues as the encoding of the body \(\mathcal{P}\); meanwhile, the encoding of \(\mathcal{Q}\) runs in parallel, enclosed by a delimiter on \(z_X\) (that matches the scope of the original declaration). Correspondingly, a **process call** \(X(v)\) is encoded as a process that sends the encoded values \(\langle v \rangle\) on \(z_X\) and ends (in MPST π-calculus, process calls are in tail position).

**Selection** on \(c[p]\) is encoded using information from the session typing context: the fact that \(c\) has type \(S = p \oplus l(U).S'\) — i.e., \([S]\) is a record type with one entry \(q : z_q\) for each \(q \in S\). Therefore, the encoding first deconstructs \([c]\) (using **with**), then uses the (linear) name in its p-entry to output on \(z_p\). Before performing the output, however, a new name \(z\) is created: it is the **continuation** of the interaction with \(p\). Then, one endpoint of \(z\) is sent through \(z_p\) as part of \(l([v], z)\), which is a variant value carrying a tuple. The other endpoint of \(z\) is kept, and used to rebind \([c]\) (using **let**) with a “new” record, consisting in all the entries of the “original” \([c]\), except \(z_p\) (which has been used for output). More in detail, the
“new” \([c]\) has an entry for \(p\) (mapping \(p\) to \(z\)) iff \(S'\) still involves \(p\) (otherwise, if \(p \not\in S'\), then \(z\) is discarded, since it has type \([S' | p] = \text{end} = \bullet\). After let, the encoding continues as \([P]\).

Symmetrically, branching on \(c[p]\) is also encoded using information from the typing context, i.e., that \(c\) has type \(S = p & z \in S_i(U_i) \cdot S_i'\) — and therefore, \([S]\) is a record type with one entry \(q:z_q\) for each \(q \in S\). As above, the encoded process deconstructs \([c]\) (using with), an then uses the (linear) name in its \(p\)-entry to perform an input \(z_p(y)\); \(y\) is assumed to be a variant, and is pattern matched to determine the continuation. If \(y\) matches \(l_i\) (for some \(i \in I\), and it carries a tuple \(z_i = (x_i, z)\) (where \(z\) is a continuation name), then \([c]\) is rebound (using let) and the process continues as \([P]\). The rebinding of \([c]\) depends on \(l_i\) and the continuation type \(S_i'\): the “new” \([c]\) is a record with all the linear names of the “original” \([c]\), except \(z_p\) (which has been used for input); as above, an entry for \(p\) will exist (and map \(p\) to \(z\)) iff \(S'\) still involves \(p\) (otherwise, if \(p \not\in S_i'\), then \(z\) has type \(\bullet\) and is discarded).

We will explain the encoding of session restriction \((\sigma s)P\) later, after Def. 5.7, as it requires some technicalities: namely, the substitution \(\sigma(\Gamma')\). We can, however, have an intuition about the role of \(\sigma(\Gamma')\) by considering an obvious discrepancy. Consider the following \(\pi\)-calculus process, that reduces by communication (cf. Def. 2.3):

\[
\Gamma, s[p]:S, s[q]:S' \vdash s[p][q] & (\langle l(x), P \rangle | s[q][p] \oplus \langle l(v), Q \rangle) \rightarrow P[\langle v / x \rangle | Q]
\]

We would like its encoding to reduce and communicate, too — but it is not the case:

\[
\text{with } r:x, z_r \in S = [s[p]] \text{ do } \ldots \text{ with } r:x, z_r \in S = [s[q]] \text{ do } \ldots
\]

and the reason is that \([s[p]], [s[q]]\) are “just” record-typed names (respectively \(z_{s[p]}, z_{s[q]}\), as per Def. 5.4), whereas with-prefixes only reduce when applied to record values (cf. Def. 3.2). Hence, to let our encoded terms reduce, we must first substitute \([s[p]], [s[q]]\) with two records; moreover, to let the two encoded processes synchronise and exchange \([v]\), such records must be suitably defined: we must ensure that the entries for \(q\) (in one record) and \(p\) (in the other) map to the same (linear) name. In the following, we show how \(\sigma(\Gamma')\) handles this issue.

Reification of Multiparty Sessions By simply translating a channel with role \(s[p]\) into a \(\pi\)-calculus name \(z_{s[p]}\), we have not yet captured the insight behind our approach, i.e., the idea that a multiparty session can be decomposed into a labelled tuple of linear channels (i.e., \(\pi\)-calculus names), connecting pairs of roles. We can formalise “connections” as follows.

**Definition 5.5.** The connections of \(s\) in \(\Gamma\) are: conn\((s, \Gamma) \triangleq \{ p, q \mid s[p]:S_p \in \Gamma \land q \in S_p \}\)

Intuitively, two roles \(p, q\) are connected by \(s\) in \(\Gamma\) if \(p\) occurs in the type \(\Gamma(s[q])\) but \(q\) might not occur in \(\Gamma(s[p])\); note, however, that \(q\) will always occur if \(\Gamma\) is consistent.

Now, as anticipated above, we want to substitute each \([s[p]]\) with a suitably defined record, containing \(\pi\)-calculus names; moreover, such names must be typed in the typing context. But what are exactly such names, and their types? This is answered by Def. 5.6.

**Definition 5.6** (Reification and decomposition of MPST contexts). The reification of a session typing context \(\Gamma_5\) is the substitution:

\[
\sigma(\Gamma_5) = \{ \{ a : z_{s[p]} \} \mid s[p] \in S_p, \Gamma_s \}
\]

The linear decomposition of \(\Gamma_5\) is the \(\pi\)-calculus typing context \(\delta(\Gamma_5)\), defined as:

\[
\delta(\Gamma_5) = \{ a : z_{s[p]} : \text{unf}(S_p) \} \mid (p, q) \in \text{conn}(s, \Gamma_s) \}
\]

The \(\pi\)-calculus reification typing rule is (note that \(\Gamma_5, \Gamma_5'\) are MPST typing contexts):

\[
\begin{align*}
(\Theta, \Gamma_5) \vdash & P, \Gamma_5' \vdash P[\sigma(\Gamma_5)] \quad \text{(T-R-Reify)}
\end{align*}
\]
\[ \Gamma \vdash 0 \triangleq \Gamma \vdash 0 \]

\[ \Theta \cdot \Gamma \vdash \text{def } X; U = P \text{ in } Q \]

where \( \bar{U} = U_1, \ldots, U_n \) and \( \bar{x} = x_1, \ldots, x_n \) and \( \bar{v} = v_1, \ldots, v_n \)

\[ \Theta, X; \bar{U} : \Gamma_1 \circ \ldots \circ \Gamma_n \circ \Gamma \vdash X(\bar{U}) \]

\[ \Theta, c : S, \Gamma_1 \circ \Gamma_2 \vdash \text{c}[\text{p}] \oplus (l(l(v)), P) \]

where \( S = \text{p} \oplus U(U), S' \)

\[ \Theta, c : S, \Gamma_1 \circ \Gamma_2 \vdash c \text{[i]} \in \ell \{ l(x), P \} \]

where \( S = \text{p}[\in \ell \{ U(U), S' \}] \)

\[ \Theta, c : S, \Gamma_1 \circ \Gamma_2 \vdash c \text{[i]} \in \ell \{ l(x), P \} \]

where \( S = \text{p}[\in \ell \{ U(U), S' \}] \)

where \( \text{conn}(s, \Gamma') = \{ \{ p_i, q_i \}, \ldots, \{ p_n, q_n \} \} \)

\[ \Theta, \Gamma \vdash (\nu s : \Gamma') P \triangleq \Theta, \Gamma \vdash \text{[(\nu s)]} P \oplus \Theta, \Gamma, \nu \sigma(\Gamma') \]

where \( \text{[(\nu s)]} = (\nu z, p, q, \eta)_{i \in \{ 1, 2, \ldots \}} \)

\[ \text{Definition 5.7 (Encoding).} \]

\[ \text{encoding of session typing judgements} \]

The simplest part of Def. 5.6 is \( \sigma(\Gamma_s) \): it is a substitution that, for each \( s[p] : S_p \in \Gamma_s \), replaces \( \text{[s[p]]} \) with a record containing one entry \( q : z_{\{ s, p, q \}} \) for each \( q \in S_p \). Note that if there is also some \( s[q] : S_q \in \Gamma_s \) with \( p \in S_q \), then the corresponding record (replacing \( \text{[s[q]]} \)) has an entry \( p : z_{\{ s, q, p \}} = z_{\{ s, p, q \}} \); i.e., \( p \) (in one record) and \( q \) (in the other) map to the same name. This realises the intuition of “multiparty sessions as records of interconnected binary channels”.

The definition of \( \sigma(\Gamma_s) \) was the last ingredient needed to formalise our encoding, presented in Def. 5.7 below. The rest of Def. 5.6 will be used later on, to prove its correctness (Thm 6.2): hence, we postpone its explanation to page 20.

\[ \text{Definition 5.7 (Encoding).} \]

\[ \text{encoding of session typing judgements} \]

We define \( P[S] \vert P \) if \( \Theta, \Gamma \vdash P \). Sometimes, we write \( P[S] \) for \( P[S] \vert P \) when \( \Theta, \Gamma \) are empty, or clear from the context.

We conclude by explaining the last case in Fig. 7, which was not addressed on p.17. The process \( (\nu s : \Gamma') P \) is encoded by generating one delimitation for each \( z_{\{ s, p, q \}} \) whenever \( \{ p, q \} \) is a connection of \( s \) in \( \Gamma' \) (Def. 5.5). Then, \( P \) is encoded, and the substitution \( \sigma(\Gamma') \) is applied: it replaces each \( \text{[s[p]]} \), \( \text{[s[q]]} \) in \( P \) with records based on the delimited \( z_{\{ s, p, q \}} \).

\[ \text{Example 5.8.} \]

Consider (1). If we delimit \( s \) and encode the resulting process, we obtain a \( \pi \)-calculus process based on (2), enclosed by the delimitations yielded by \( \text{[(\nu s)]} \), and the substitution \( \sigma(s[p] : S, s[q] : S', \ldots) \). Since the latter replaces \( \text{[s[p]]}, \text{[s[q]]} \) with records whose entries reflect roles(\( S \)) and roles(\( S' \)), the encoding can now reduce, firing the two withs.

\[ \text{Example 5.9.} \]

Consider the main server/clients parallel composition in Ex. 2.2:

\[ Q = (\nu s, s, s, s, s) \]

| \( P_s \) \| \( P_b \) \| \( P_c \) \]

where

\[ Q = (\nu s) \{ s \| P_s \} \oplus (\nu a \| s \} \]

\[ s \| P_s \} \oplus (\nu a \| s \} \]

\[ s \| P_s \} \oplus (\nu a \| s \} \]

\[ s \| P_s \} \oplus (\nu a \| s \} \]

\[ s \| P_s \} \oplus (\nu a \| s \} \]

\[ s \| P_s \} \oplus (\nu a \| s \} \]
6 Properties of the Encoding

In this section we present some crucial properties ensuring the correctness of our encoding.

Encoding of Types

Thm. 6.1 below says that our encoding (1) commutes the duality between partial session types (Def. 2.8) and \( \pi \)-types (Def. 4.1), and (2) also preserves subtyping.

**Theorem 6.1 (Duality/subtyping preservation).** \( \mathbb{H} = \mathbb{H'} \); if \( U \leq U' \), then \( [U] \leq [U'] \).

Encoding of Typing Judgements

Thm. 6.2 shows that the encoding of session typing judgements into \( \pi \)-calculus typing judgements is valid. As a consequence, a well-typed MPST process also enjoys the type safety guarantees that can be expressed in standard \( \pi \)-calculus.

**Theorem 6.2 (Correctness of encoding).** \( \Gamma \vdash v:U \) implies \( [\Gamma] \vdash [v]:[U] \), \( \Theta \vdash X:U \) implies \( [\Theta] \vdash [X]:[U] \), and \( \Theta \vdash P \) implies \( [\Theta] \vdash P \).

The proof is by induction on the MPST typing derivation, and yields a corresponding \( \pi \)-calculus typing derivation. One simple case is the following, that relates subtyping:

\[
\begin{align*}
\text{(T-SUB)} & \quad \Theta \cdot \Gamma, c:U \vdash P \quad U' \leq_U U \\
\implies & \quad [\Theta \cdot \Gamma, c:U \vdash P] \quad [U'] \leq [U] \\
\text{(T-NARROW)} & \quad [\Theta \cdot \Gamma, c:U' \vdash P] \quad [P]_{\Theta, \Gamma, c:U}
\end{align*}
\]

and holds by the induction hypothesis and Thm. 6.1. The most delicate case is the encoding of session restriction \( \Theta \cdot \Gamma \vdash (\nu s: \Gamma') P \) (Fig. 7): its encoding turns \( (\nu s) \) into a set of delimited names, used in the substitution \( \sigma(\Gamma') \) applied to \( [P]_{\Theta, \Gamma, c:U} \). Hence, to prove Thm. 6.2 in this case, we need to type such names, i.e., produce a context that types \( [P]_{\Theta, \Gamma, c:U} \). This is where \( \delta(\Gamma') \) and (T-REify) (Def. 5.6) come into play, as we now explain.

More on reification and decomposition

By Def. 5.6, the typing context \( \delta(\Gamma_S) \), when defined, has an entry for each role of each channel in \( \Gamma_S \); more precisely, an entry \( z_{(s,p,q)} \) for each \( s[p]:S_p \in \Gamma_S \) and \( q \in S_p \). Such entries are used to type the records yielded by \( \sigma(\Gamma_S) \).

The type of \( z_{(s,p,q)} \) is based on the encoding of the unfolded partial projection \( S_p \) \mid q, that can be either \( * \), or Li(T)/Lo(T) (for some \( T \)). Note that if there is also some \( s[q]:S_q \in \Gamma_S \), then \( S_q \) \mid \( z_{(s,p,q)} \) (when defined) is \( \left[ \text{unf}(S_p \mid q) \right] \cap \left[ \text{unf}(S_q \mid p) \right] \).

This creates a deep correspondence between the consistency of \( \Gamma_S \) and the existence of \( \delta(\Gamma_S) \), shown in Thm. 6.3: the precondition for MPST type safety (i.e., consistency of \( \Gamma_S \)) is precisely characterised in \( \pi \)-calculus by the linear decomposition at the roots of our encoding.
**Theorem 6.3** (Precise decomposition). \( \Gamma_5 \) is consistent if and only if \( \delta(\Gamma_5) \) is defined.

The final part of Def. 5.6 is the \( \pi \)-calculus typing rule (\( T\pi\text{-Refy} \)), that uses \( \delta(\Gamma_5) \) to type a process on which \( \sigma(\Gamma_5) \) has been applied. Intuitively, \( \delta(\Gamma_5) \) provides a typing context that types each record yielded by \( \sigma(\Gamma_5) \). We now explain how the rule works and why it is sound (with a slight simplification). Let \( \Gamma_5 = \{ s[p]: s \}_{p \in I} \), for some \( I \). Then, by Def. 5.6:

\[
\delta(\Gamma_5) = \bigcap_{p \in I} \{ z(s[p], q) \ | \ \text{unf}(s[p] \vdash q) \} \}
\]

(Note: \( \delta(\Gamma_5) \) is defined iff \( \Gamma_5 \) is consistent, by Thm. 6.3). Take the I/O types yielded by \( \delta(\Gamma_5) \), i.e., \( \{ T(s[p], q) \}_{p \in I} \) such that \( \delta(\Gamma_5) = \bigcup_{\eta \in I} \{ z(s[p], q) \ | \ T(s[p], q) \} \) (note \( T(s[p], q) \) are distinct). If we assume \( [\Theta \cdot \Gamma_5], [\Gamma_5] \vdash P \), this derivation holds:

\[
[\Theta \cdot \Gamma_5], [\Gamma_5] \vdash P \quad \text{(T-Sub)}
\]

In particular, the assumptions \( T(s[p], q) \leq \pi \{ S_p \vdash q \} \) hold by Lemma 4.7, since each \( T(s[p], q) \) is obtained by splitting \( \delta(\Gamma_5) \) (that combines types with \( \Theta \)) using \( \eta \). The equivalence in the conclusion holds since dom([\Theta \cdot \Gamma_5]) \cap dom(\delta(\Gamma_5)) = \emptyset. \) Hence: if the (\( T\pi\text{-Refy} \)) premise \( ([\Theta \cdot \Gamma_5], [\Gamma_5] \vdash P) \) holds, the above derivation holds, proving the conclusion of (\( T\pi\text{-Refy} \)).

Now, we can finish the proof of Thm. 6.2 for the case \( \Theta \cdot \Gamma \vdash ([\nu s \cdot \Gamma']) P \). Assuming that the judgement holds, we also have \( \Theta \cdot \Gamma, \Gamma' \vdash P \) and \( \Gamma' \) complete (by the premise of \( T\text{-Res} \), Fig. 4); hence, \( \Gamma' \) is consistent, and \( \delta(\Gamma') \) is defined by (Thm. 6.3). Assuming that \( [\Theta \cdot \Gamma, \Gamma' \vdash P] \) holds by the induction hypothesis, we obtain:

\[
[\Theta \cdot \Gamma], [\Gamma'] \vdash P_{\Theta \cdot \Gamma, \Gamma'} \quad \text{(T-Sub)}
\]

where \( \delta(\Gamma') \) types all the names \( z(s[p], q) \) in \( \sigma(\Gamma') \), that are also delimited by \( \tau(\nu s) \). We can conclude by applying (\( T\pi\text{-Resl} \)) to type such delimitations (cf. Fig. 5 — this is allowed by the completeness of \( \Gamma' \)): we get \( [\Theta \cdot \Gamma] \vdash \tau(\nu s)[P_{\Theta \cdot \Gamma, \Gamma'}] \sigma(\Gamma'), \) i.e., we match Fig. 7.

Finally, notice (from Fig. 7) that our encoding of processes uses some typing information. In principle, a process could be typed by applying the rules in multiple ways (especially (T-Sub) in Fig. 4), and one might wonder whether an MPST process could have multiple encodings. Proposition 6.4 says that this is not the case: the reason is that the only typing information being used is the set of roles in each session type, which does not depend on the typing rule — and is constant w.r.t. subtyping (i.e., \( S \leq S' \) implies \( \text{roles}(S) = \text{roles}(S') \)).

**Proposition 6.4** (Uniqueness). If \( \Theta \cdot \Gamma \vdash P \) and \( \Theta' \cdot \Gamma' \vdash P \), then \( [P]_{\Theta \cdot \Gamma} = [P]_{\Theta' \cdot \Gamma'} \).

**Encoding and Reduction** One usual way to assess that an encoding is “behaviourally correct” (i.e., a process and its encoding behave “in the same way”) consists in proving operational correspondence. Roughly, it says that the encoding is: (1) complete, i.e., any reduction of the original process is simulated by its encoding; and (2) sound, i.e., any reduction of the encoded process matches some reduction of the original process. This is formalised in Thm. 6.5, where \( \cd \) denotes a reduction induced by (R\pi-\text{Wru}) (Def. 3.2).

**Theorem 6.5** (Operational correspondence). If \( \emptyset \cdot \emptyset \vdash P \), then:

1. (Completeness) \( P \rightarrow P' \) implies \( \exists \emptyset, P'' \) such that \( [P] \rightarrow (\nu \emptyset) P'' \) and \( P'' = [P'] \);
2. (Soundness) \( [P] \rightarrow P' \) implies \( \exists \emptyset, P'', P'' \) s.t. \( P \rightarrow (\nu \emptyset) P'', P \rightarrow P' \) and \( [P'] \rightarrow P'' \).
The statement of Thm. 6.5 is standard [22, §5.1.3]. Item 1 says that if $P$ reduces to $P'$, then the encoding of the former can reduce to the encoding of the latter. Item 2 says (roughly) that no matter how the encoding of $P$ reduces, it can always further reduce to the encoding of some $P''$, such that $P$ reduces to $P''$. Note that when we write $[P']$, we mean $[P']_{s} \circ s$, which implies $s \circ \emptyset \vdash P''$ (cf. Def. 5.7). The restricted variables $\tilde{x}$ in items 1-2 are generated by the encoding of selection (Fig. 7); it creates a delimited linear name to continue the session. To see why item 2 uses $\vdash \circ \circ \vdash P''$, consider the following MPST process:

$\emptyset \circ \Gamma, [s\circ r] ; S \vdash s[p] ; [q] \& \{l(x) \circ P\} \not\rightarrow$ (the process is stuck)

If we encode it (and apply $\sigma(\Gamma, s[p] ; S)$ as per Ex. 5.8), we get a π-calculus process that gets stuck, too — but only after firing one internal with-reduction:

with $[x : z_{r}]_{r \in S} = [x : z_{(s \circ r)}]_{r \in S} \mid do z_{q}(y) \ldots \rightarrow \vdash z_{(s \circ r)}(y) \ldots \not\rightarrow$

This happens whenever a process is deadlocked, because in Fig. 7, the “atomic” MPST branch/select actions are encoded with multiple π-calculus steps: first with to deconstruct the channels tuple, and then input/output. In general, if an MPST process is stuck, its encoding fires one with for each branch/select, then blocks on an input/output.

Thm. 6.5 yields a corollary on deadlock freedom (Cor. 6.6), that in turn allows to transfer deadlock freedom (Thm. 2.19) from MPST to π-calculus processes (Cor. 6.7 below).

**Corollary 6.6.** $P$ is deadlock-free if and only if $[P]$ is deadlock-free, i.e.: $[P] \not\rightarrow^* P' \not\rightarrow$ implies $\exists Q \equiv 0$ such that $P' = [Q]$.

**Corollary 6.7.** Let $\emptyset \circ \circ \vdash P$, where $P \equiv (\nu s : G)_{i \in \Gamma} P_{i}$ and each $P_{i}$ only interacts on $s[p_{i}]$. Then, $[P]$ is deadlock-free.

### 7 From Theory to Implementation

We can now show how our encoding directly guides the implementation of a toolchain for generating safe multiparty session APIs in Scala, supporting distributed delegation. We continue our Game example from §1, focusing on player b: we sketch the API generation and an implementation of a client, following the results in §6. Our approach is to: (1) exploit type safety and distribution provided by an existing library for binary session channels, and then (2) treat the ordering of communications across separate channels in the API generation.

**Scala and lchannels** Our Scala toolchain is built upon the lchannels library [56, 57]. lchannels provides two key classes, Out[T] and In[T], whose instances must be used linearly (i.e., once) to send/receive (by method calls) a τ-typed message: i.e., they represent channel endpoints with π-calculus types $\text{Lo}(T)$ and $\text{Li}(T)$ (Def. 3.3). This approach enforces the typing of I/O actions via static Scala typing; the linear usage of channels, instead, goes beyond the capabilities of the Scala typing system, and is therefore enforced with run-time checks.

lchannels delivers messages by abstracting over various transports: local memory, TCP sockets, Akka actors [38]. Notably, lchannels promotes session type-safety through a continuation-passing-style encoding of binary session types [56] that is close to our encoding of partial projections (formalised in Def. 5.1). Further, lchannels allows to send/receive In[T]/Out[T] instances for binary session delegation [56, Ex. 4.3]; on distributed message transports, instances of In[T]/Out[T] can be sent remotely (e.g., via the Akka-based transport).

**Type-safe, distributed multiparty delegation** By Thm. 6.2, Def. 5.1 and Thm. 6.3, we know that the game player session type $S_{b}$ in our example (see §1, p. 2) provides the type safety
guarantees of a tuple of (linear) channels, whose types are given by the encoded partial projections of $S_b$ onto $a$ and $c$ (Def. 2.9). This suggests that, using $\text{lchannels}$, the delegation of an $S_b$-typed channel (as seen in §1) could be rendered in Scala as:

$$
\text{In}[\text{PlayB}] \text{ with definitions: case class PlayB(payload: } S_b)$$
i.e., as a linear input channel carrying a message of type $\text{PlayB}$, whose payload has type $S_b$; $S_b$, in turn, is a Scala case class, which can be seen as a labelled tuple, that maps $a, c$ to I/O channels — whose types derive from $[S_b]a$ and $[S_b]c$ (in fact, they carry messages of type $\text{InfoAB}/\text{InfoBC}$). In this view, $S_b$ is our Scala rendering of the encoded session type $[S_b]$. As said above, $\text{lchannels}$ allows to send channels remotely — hence, also allows to remotely send tuples of channels (e.g., instances of $S_b$); thus, with this simple approach, we obtain type-safe distributed multiparty delegation of an $[S_b]$-typed channel tuple “for free”.

**Multiparty API generation** Corresponding to the $\pi$-calculus labelled tuple type yielded by the type encoding $[S_b]$, the $S_b$ class outlined above can ensure communication safety, i.e., no unexpected message will be sent or received on any of its binary channels. Like $[S_b]$, however, $S_b$ does not convey any ordering to communications across channels: i.e., $S_b$ does not suggest the order in which its fields $a, c$ should be used. (Indeed, $[S_b]$ may type $\pi$-processes that use its separate channels in any order, while preserving type safety.) To recover the “desired” ordering of communications, and implement it correctly, we can refine our classes so that:

1. each multiparty channel class (e.g., $S_b$) exposes a $\text{send()}$ or $\text{receive()}$ method, according to the I/O action expected by the multiparty session type (e.g., $S_b$);
2. the implementation of such method uses the binary channels as per our process encoding.

E.g., consider again $S_b$ and $S_c$. $S_b$ requires to send towards $c$, so $S_b$ could provide the API:

```scala
case class $S_b(a: \text{In[InfoAB]}, c: \text{Out[InfoBC]})$

def send(v: String) = {
  // v is the payload of InfoBC message
  val c' = c !! \text{InfoBC(v)} // \text{lchannels method: send v, and return continuation}
  $S_b(a, c')$ } } // return a “continuation object”
```

Now, $S_b$.send() behaves exactly as our process encoding in Fig. 7 (case for selection ⊕): it picks the correct channel from the tuple (in this case, $c$), creates a new tuple $S_b'$ where $c$ maps to a continuation channel, and returns it — so that the caller can use it to continue the multiparty session interaction. The class $S_b'$ should be similar, with a $\text{receive()}$ method that uses a for input (by following the encoding of $\&$). This way, a programmer is correctly led to write, e.g., $\text{val x = s.send(...)}.\text{receive()}$ (using method call chaining) — whereas attempting, e.g., $s.\text{receive()}$ is rejected by the Scala compiler (method undefined). These $\text{send()}/\text{receive()}$ APIs are mechanical, and can be automatically generated: we did it by extending Scribble.

**Scribble-Scala Toolchain** Scribble is a practical MPST-based language and tool for describing global protocols [58, 63]. To implement our results, we have extended Scribble (both the language and the tool) to support the full MPST theory in §2, including, e.g., projection, type merging and delegation (not previously supported). Our extension supports protocols with the syntax in Fig. 9 (left), by augmenting Scribble with a projection operator $\exists$: then, it computes the projections/encodings explained in §5, and automates the Scala API generation as outlined above (producing, e.g., the $S_b, S'_b, \ldots$ classes and their $\text{send}/\text{receive}$ methods). This approach reminds the Java API generation in [27] — but we follow a formal foundation and target the type-safe binary channels provided by $\text{lchannels}$ (that, as shown above, takes care of most irksome aspects — e.g., delegation). As a result, the $P_b$ client in Fig. 1 can be written as in Fig. 9 (right); and although conceptually programmed as Fig. 2, the networking mechanisms of the game will concretely follow Fig. 8.
8 Conclusion and Related Works

We presented the first encoding of a full-fledged multiparty session \(\pi\)-calculus into standard \(\pi\)-calculus (§5), and used it as the foundation of the first implementation of multiparty sessions (based on Scala API generation) supporting distributed multiparty delegation, on top of existing libraries (§7). We proved that the type safety property of MPST is precisely characterised by our decomposition into linear \(\pi\)-calculus (Thm.6.3). We encode types by preserving duality and subtyping (Thm.6.1); our encoding of processes is type-preserving, and operationally sound and complete (Thm.6.2 and Thm.6.5); hence, our encoding preserves the type-safety and deadlock-freedom properties of MPST (Cor.6.7). These results ensure the correctness of our (encoding-based) Scala implementation. Moreover, our encoding preserves process distribution (i.e., is homomorphic w.r.t. parallel composition); correspondingly, our implementation of multiparty sessions is decentralised and choreographic.

Session Types for “Mainstream” Languages We mentioned binary session implementations for various languages in §1. Notably, [52, 30, 31, 39, 48, 56, 50] seek to integrate session types in the native host language, without language extensions, to avoid hindering their use in practice. To do so, one approach (e.g. in [56, 50]) is combining static typing of I/O actions with run-time checking of linear channel usage. Our implementation adopts this idea (§7). Haskell-based works exploit its richer typing system to statically enforce linearity — with various expressiveness/usability trade-offs based on their session types embedding strategy.

Implementations of multiparty sessions are few and limited, due to the intricacies of the theory (e.g., the interplay between projections, mergability and consistency), and practical issues (e.g., realising multiparty abstractions over binary transports, including distributed delegation), as discussed in §1. [59] was the first implementation of MPST, based on extending Java with session primitives. [27] proposes MPST-based API generation for Java, based on CFMS [6], but has no formalisation — unlike our implementation, that follows our encoding. [16, 19] develop MPST-influenced networking APIs in Python and Erlang; [46] implements recovery strategies in Erlang. [16, 19, 46] focus on purely dynamic MPST verification via run-time monitoring. [47, 45] extends [16] with actors and timed specifications. [43] uses a
dependent MPST theory to verify MPI programs. Crucially, none of these implementations supports delegation (nor projection merging, needed by our Game example, cf. Ex. 2.14).

**Encodings of Session Types and Processes** [15] encodes binary session \(\pi\)-calculus into an augmented \(\pi\)-calculus with branch/select constructs. [14], following [33], and [20] encode non-recursive, binary session \(\pi\)-calculus, respectively into linear \(\pi\)-calculus and the Generic Type System for \(\pi\)-calculus [29], proving correctness w.r.t. typing and reduction. All the above works investigate binary and (except [15]) non-recursive session types, while in this paper we study the encoding of multiparty session types, subsuming binary ones; and unlike [15], we target standard \(\pi\)-calculus. We encode branching/selection using variants as in [14, 12], but our treatment of recursion, and the rest of the MPST theory, is novel.

Encodings of multiparty into binary sessions are studied in [8, 7]. Both use orchestration approaches that add centralised medium/arbiter processes, and target session calculi (not \(\pi\)-calculus). [49] uses a limited class of global types to extract “characteristic” deadlock-free \(\pi\)-calculus processes — without addressing session calculi, nor proving operational properties.

**Recursion and Duality** The interplay between recursion and duality has been a thorny issue in session types literature, requiring our careful treatment in §4. [5, 1] noticed that the standard duality in [25] does not commute with the unfolding of recursion when type variables occur as payload, e.g., \(\mu t.t.\text{end}\). To solve this issue, [5, 1] define a new notion of duality, called complement [1], then used in [12] to encode recursive binary session types into linear \(\pi\)-types. Unfortunately, [2] later noticed that even complement does not commute, e.g., when unfolding \(\mu t.\mu t'.t.t'\). As observed in §4, to encode recursive session types we encounter similar issues in \(\pi\)-types. The reason seems natural: \(\pi\)-types do not distinguish “payloads” and “continuations”, and in recursive linear inputs/outputs, type variables always occur as “payload”, e.g., \(\mu t.\text{Lo}(t)\). Since, in the light of [2], we could not adopt the approach of [12], we propose a solution similar to [40]: introduce dualised type variables \(\bar{t}\). [40] also sketches a property similar to our Lemma 4.4. The main difference is that we add dualised variables to \(\pi\)-types (while [40] adds \(\bar{t}\) to session types). An alternative idea is given in [56]: encoding recursive session types as non-recursive linear I/O types with recursive payloads. This avoids dualised variables (e.g., \(\text{Lo}(\mu t.\text{Li}(t))\) instead of \(\mu t.\text{Lo}(\bar{t})\)), but if adopted, would complicate Def. 5.1. Moreover, [56] studies the encoding of recursive types, but not processes.

**Future work** On the practical side, we plan to study whether Scala language extensions could provide stronger static channel usage checks. E.g., [24, 23] (capabilities) could allow to ensure that a channel endpoint is not used after being sent; [53, 60] (effects) could allow to ensure that a channel endpoint is actually used in a given method. We also plan to extend our multiparty API generation approach beyond Scala and 1channels, targeting other languages and implementations of binary sessions/channels [52, 30, 31, 39, 48, 50].

On the theoretical side, our encoding provides a basis for reusing theoretical results and tools between MPST \(\pi\)-calculus and standard \(\pi\)-calculus. E.g., we could now exploit Cor. 6.6, to verify deadlock-freedom of processes with interleaved multiparty sessions (studied in [3, 9, 11]) by applying \(\pi\)-calculus deadlock detection methods to their encodings [35, 32, 61]. Moreover, we can prove that our encoding is barb-preserving: hence, we plan to study its full abstraction properties w.r.t. barbed congruence in session \(\pi\)-calculus [37, 36] and \(\pi\)-calculus.

**Thanks** to the reviewers for their remarks, and to B. Toninho for fruitful discussions. Thanks to S.S. Jongmans, R. Neykova, N. Ng, B. Toninho for testing the companion artifact.
References


A Linear Decomposition of Multiparty Sessions


Luca Padovani. Deadlock and lock freedom in the linear π-calculus. Online version of [?], January 2014. URL: https://hal.inria.fr/hal-00932356.


TYPICAL. Type-based static analyzer for the pi-calculus. http://www-kb.is.s.u-tokyo.ac.jp/~koba/typical/.
