Domain-Aware Session Types

Luís Caires
Universidade Nova de Lisboa

Jorge A. Pérez
University of Groningen

Frank Pfenning
Carnegie Mellon University

Bernardo Toninho
Universidade Nova de Lisboa

Abstract
We develop a generalization of existing Curry-Howard interpretations of (binary) session types by relying on an extension of linear logic with features from hybrid logic, in particular modal worlds that indicate domains. These worlds govern domain migration, subject to a parametric accessibility relation familiar from the Kripke semantics of modal logic. The result is an expressive new typed process framework for domain-aware, message-passing concurrency. Its logical foundations ensure that well-typed processes enjoy session fidelity, global progress, and termination. Typing also ensures that processes only communicate with accessible domains and so respect the accessibility relation.

Remarkably, our domain-aware framework can specify scenarios in which domain information is available only at runtime; flexible accessibility relations can be cleanly defined and statically enforced. As a specific application, we introduce domain-aware multiparty session types, in which global protocols can express arbitrarily nested sub-protocols via domain migration. We develop a precise analysis of these multiparty protocols by reduction to our binary domain-aware framework: complex domain-aware protocols can be reasoned about at the right level of abstraction, ensuring also the principled transfer of key correctness properties from the binary to the multiparty setting.

1 Introduction
The goal of this paper is to show how existing Curry-Howard interpretations of session types [10, 11] can be generalized to a domain-aware setting by relying on an extension of linear logic with features from hybrid logic [40, 5]. These extended logical foundations of message-passing concurrency allow us to analyze complex domain-aware concurrent systems (including those governed by multiparty protocols) in a precise and principled manner.

Software systems typically rely on communication between heterogeneous services; at their heart, these systems rely on message-passing protocols that combine mobility, concurrency, and distribution. As distributed services are often virtualized, protocols should span diverse software and hardware domains. These domains can have multiple interpretations, such as the location where services reside, or the principals on whose behalf they act. Concurrent
behavior is then increasingly domain-aware: a partner’s potential for interaction is influenced not only by the domains it is involved in at various protocol phases (its context), but also by connectedness relations among domains. Moreover, domain architectures are rarely fully specified: to aid modularity and platform independence, system participants (e.g., developers, platform vendors, service clients) often have only partial views of actual domain structures. Despite their importance in communication correctness and trustworthiness at large, the formal status of domains within typed models of message-passing systems remains unexplored.

This paper contributes to typed approaches to the analysis of domain-aware communications, with a focus on session-based concurrency. This approach specifies the intended message-passing protocols as session types [30, 31, 24]. Different type theories for binary and multiparty (n-ary) protocols have been developed. In both cases, typed specifications can be conveniently coupled with \(\pi\)-calculus processes [36], in which so-called session channels connect exactly two subsystems. Communication correctness usually results from two properties: session fidelity (type preservation) and deadlock freedom (progress). The former says that well-typed processes always evolve to well-typed processes (a safety property); the latter says that well-typed processes will never get into a stuck state (a liveness property).

A key motivation for this paper is the sharp contrast between (a) the growing relevance of domain-awareness in message-passing, concurrent systems and (b) the expressiveness of existing session type frameworks, binary and multiparty, which cannot adequately specify (let alone enforce) domain-related requirements. Indeed, existing session types frameworks, including those based on Curry-Howard interpretations [10, 47, 14], capture communication behavior at a level of abstraction in which even basic domain-aware assertions (e.g., “Shipper resides in domain AmazonUS”) cannot be expressed. As an unfortunate consequence, the effectiveness of the analysis techniques derived from these frameworks is rather limited.

To better illustrate our point, consider a common distributed design pattern: a middleware agent (\(mw\)) which answers requests from clients (\(cl\)), sometimes offloading the requests to a server (\(serv\)) to better manage local resource availability. In the framework of multiparty session types [32] this protocol can be represented as the global type:

\[
\begin{align*}
& cl \rightarrow mw: \text{request}(\text{req}), \quad mw \rightarrow cl: \text{reply}(\text{ans}), \quad mw \rightarrow serv: \text{done} \cdot end, \\
& serv \rightarrow mw: \text{reply}(\text{ans}), \quad mw \rightarrow cl: \{\text{reply}(\text{ans}), \text{end}\}\}
\end{align*}
\]

The client first sends a request to the middleware, which answers back with either a reply message containing the answer or a wait message, signaling that the server will be contacted to produce the final reply. While this multiparty protocol captures the intended communication behavior, it does not capture that protocols for the middleware and the server often involve some form of privilege escalation or specific authentication—ensuring, e.g., that the server interaction is adequately isolated from the client, or that the escalation must precede the server interactions. These requirements simply cannot be represented in existing frameworks.

Our work addresses this crucial limitation by generalizing Curry-Howard interpretations of session types by appealing to hybrid logic features. We develop a logically motivated typed process framework in which worlds from modal logics precisely and uniformly define the notion of domain in session-based concurrency. At the level of binary sessions, domains manifest themselves through point-to-point domain migration and communication. In multiparty sessions, domain migration is specified choreographically through the new construct \(\text{p moves} q \text{to} \omega \text{for} G_1 \cdot G_2\), where participant \(p\) leads a migration of participants \(q\) to domain \(\omega\) in order to perform protocol \(G_1\), who then migrate back to perform protocol \(G_2\).

Consider the global type \(\text{Offload} \equiv mw \rightarrow serv: \{\text{req}(\text{data}), serv \rightarrow mw: \{\text{reply}(\text{ans}), \text{end}\}\}\) in our previous example. Our framework allows us to refactor the global type above as:

\[
\begin{align*}
& cl \rightarrow mw: \text{request}(\text{req}), \quad mw \rightarrow cl: \{\text{reply}(\text{ans}), mw \rightarrow serv: \{\text{done} \cdot end\}\}, \\
& serv \rightarrow mw: \{\text{init}, mw \text{ moves} serv \text{ to } w_{prev}, \text{for} Offload\}, mw \rightarrow cl: \{\text{reply}(\text{ans}), \text{end}\}\}
\end{align*}
\]
By considering a first-class multiparty domain migration primitive at the type and process levels, we can specify that the offload portion of the protocol takes place after the middleware and the server migrate to a private domain $w_{priv}$, as well as ensuring that only accessible domains can be interacted with. For instance, the type for the server that is mechanically projected from the protocol above ensures that the server first migrates to the private domain, communicates with the middleware, and then migrates back to its initial domain.

Perhaps surprisingly, our domain-aware multiparty sessions are studied within a context of logical binary domain-aware sessions, arising from a propositions-as-types interpretation of hybrid linear logic [22, 18], with strong static correctness guarantees derived from the logical nature of the system. Multiparty domain-awareness arises through an interpretation of multiparty protocols as medium processes [7] that orchestrate the multiparty interaction while enforcing the necessary domain-level constraints and migration steps.

Contributions The key contributions of this work are:

1. A process model with explicit domain-based migration (§2). We present a session π-calculus with domains that can be communicated via novel domain movement prefixes.

2. A session type discipline for domain-aware interacting processes (§3). Building upon an extension of linear logic with features from hybrid logic [22, 18] we generalize the Curry-Howard interpretation of session types [10, 11] by interpreting (modal) worlds as domains where session behavior resides. In our system, types can specify domain migration and communication; domain mobility is governed by a parametric accessibility relation. Judgments stipulate the services used and realized by processes and the domains where sessions should be present. Our type discipline statically enforces session fidelity, global progress and, notably, that communication can only happen between accessible domains.

3. As a specific application, we introduce a framework of domain-aware multiparty sessions (§4) that uniformly extends the standard multiparty session framework of [32] with domain-aware migration and communication primitives. Our development leverages our logically motivated domain-aware binary sessions (§3) to give a precise semantics to multiparty sessions through a (typed) medium process that acts as an orchestrator of domain-aware multiparty interactions, lifting the strong correctness properties of typed processes to the multiparty setting. We show that mediums soundly and completely encode the local behaviors of participants in a domain-aware multiparty session.

We conclude with a discussion of related work (§5) and concluding remarks (§6).

2 Process Model

We introduce a synchronous π-calculus [42] with labeled choice and explicit domain migration and communication. We write $\omega, \omega', \omega''$ to stand for a concrete domain $(w, w', \ldots)$ or a domain variable $(\alpha, \alpha', \ldots)$. Domains are handled at a high-level of abstraction, with their identities being attached to session channels. Just as the π-calculus allows for communication over names and name mobility, our model also allows for domain communication and mobility. These features are justified with the typing discipline of §3.

Definition 2.1. Given infinite, disjoint sets $\Lambda$ of names $(x, y, z, u, v)$, $\mathcal{L}$ of labels $l_1, l_2, \ldots$, $W$ of domain tags $(w, w', w'')$ and $V$ of domain variables $(\alpha, \beta, \gamma)$, respectively, the set of processes $(P, Q, R)$ is defined by

\[
P ::= 0 \mid P \mid Q \mid [x \leftrightarrow y] \mid x \vdash \{k : P\}_{i \in I} \mid (\nu y)P \mid x(y).P \mid x(y).P \mid !x(y).P \mid x(y@\omega).P \mid x(y@\omega).P \mid x(\omega).P \mid x(\alpha).P
\]
Domain-aware prefixes are present only in the last line. As we make precise in the typed setting of §3, these constructs realize mobility and domain communication, in the usual sense of the π-calculus: migration to a domain is always associated with a fresh name.

The operators $\mathbf{0}$ (inaction), $P | Q$ (parallel composition) and $(\nu y)P$ (name restriction) are standard. We then have $x(y).P$ (send $y$ on $x$ and proceed as $P$), $x(y).P$ (receive $z$ on $x$ and proceed as $P$ with parameter $y$ replaced by $z$), and $!x(y).P$ which denotes replicated (persistent) input. The forwarding construct $[x \leftrightarrow y]$ equates $x$ and $y$; it is a primitive representation of a copycat process. The last two constructs in the second line define a labeled choice mechanism: $x \triangleright \{ l_i : P_i \}_{i \in I}$ is a process that awaits some label $l_j$ (with $j \in I$) and proceeds as $P_j$. Dually, the process $x \triangleleft; P$ emits a label $l_i$ and proceeds as $P$.

The first two operators in the third line define explicit domain migration: given a domain $\omega$, $x(y@\omega).P$ denotes a process that is prepared to migrate the communication actions in $P$ on endpoint $x$, to session $y$ on $\omega$. Complementarily, process $x(y@\omega).P$ signals an endpoint $x$ to move to $\omega$, providing $P$ with the appropriate session endpoint that is then bound to $y$. In a typed setting, domain movement will be always associated with a fresh session channel. Alternatively, this form of coordinated migration can be read as an explicit form of agreement (or authentication) in trusted domains. Finally, the last two operators in the third line define output and input of domains, $x(\omega).P$ and $x(\alpha).P$, respectively. These constructs allow for domain information to be obtained and propagated across processes dynamically.

Following [41], we abbreviate $(\nu y)x(y)$ and $(\nu y)x(y@\omega)$ as $\pi(y)$ and $\pi(y@\omega)$, respectively. In $(\nu y)P$, $x(y).P$, and $x(y@\omega).P$ the distinguished occurrence of name $y$ is binding with scope $P$. Similarly for $\alpha$ in $x(\alpha).P$. We identify processes up to consistent renaming of bound names and variables, writing $\equiv_\alpha$ for this congruence. $P[x/y]$ denotes the capture-avoiding substitution of $x$ for $y$ in $P$. While structural congruence $\equiv$ expresses standard identities on the basic structure of processes (cf. [9]), reduction expresses their behavior.

Reduction $(P \to Q)$ is the binary relation defined by the rules below and closed under structural congruence; it specifies the computations that a process performs on its own.

$$
\begin{align*}
 x(y).Q & \to Q | (P[y/z]) & x(y).Q & \to Q | P[y/z] & | !x(z).P & \to Q | P[y/z] & | !x(z).P \\
x(y@\omega).P & \to Q | (P[y@\omega]) & x(\omega).P & \to Q | (P[y]/z) & x(\omega).P & \to Q | (P[y@\omega]) & P & \to Q | (\nu x)(P) & \to Q | (\nu y)(x) \\
(\nu x)[(x \leftrightarrow y) & \to P] & \to (P[y/x]) & Q & \to Q' & \to P | Q & \to P | P' \\
P & \to Q | (\nu y)P & \to (\nu y)Q & x \triangleleft; P & | x \triangleright \{ l_i : Q_i \}_{i \in I} & \to P | Q_j & (j \in I)
\end{align*}
$$

For the sake of generality, reduction allows dual endpoints with the same name to interact, independently of the domains of their subjects. The type system introduced next will ensure, among other things, local reductions, disallowing synchronisations among distinct domains.

## 3 Domain-aware Session Types via Hybrid Logic

This section develops a new domain-aware formulation of binary session types. Our system is based on a Curry-Howard interpretation of a linear variant of so-called hybrid logic, and can be seen as an extension of the interpretation of [10, 11] to hybrid (linear) logic. Hybrid logic is often used as an umbrella term for a class of logics that extend the expressiveness of propositional logic by considering modal worlds as syntactic objects that occur in propositions.

As in [10, 11], propositions are interpreted as session types of communication channels, proofs as typing derivations, and proof reduction as process communication. As main novelties, here we interpret: logical worlds as domains; the hybrid connective $@_\omega.A$ as the type of a session that migrates to an accessible domain $\omega$; and type-level quantification over worlds $\forall \alpha.A$ and $\exists \alpha.A$ as domain communication. We also consider a type-level operator
α.A (read “here”) which binds the current domain of the session to α in A. The syntax of domain-aware session types is given in Def. 3.1, where w, w1, . . . stand for domains drawn from W, and where α, β and ω, ω′ are used as in the syntax of processes.

Definition 3.1 (Domain-aware Session Types). The syntax of types (A, B, C) is defined by

\[
A ::= 1 \mid (\text{down}) A \mid \forall_\alpha A \mid \exists_\alpha A \mid \downarrow A.
\]

Types are the propositions of intuitionistic linear logic where the additives A & B and A ⊕ B are generalized to a labelled n-ary variant. Propositions take the standard interpretation as session types, extended with hybrid logic operators [5], with worlds interpreted as domains that are explicitly subject to an accessibility relation (in the style of [43]) that is tracked by environment Ω. Intuitively, Ω is made up of direct accessibility hypotheses of the form ω₁ ≺ ω₂, meaning that domain ω₂ is accessible from ω₁.

Types are assigned to channel names; a type assignment x : A[ω] enforces the use of name x according to session A, in the domain ω. A type environment is a collection of type assignments. Besides the accessibility environment Ω just mentioned, our typing judgments consider two kinds of type environments: a linear part Δ and an unrestricted part Γ. They are subject to different structural properties: weakening and contraction principles hold for Γ but not for Δ. Empty environments are written as ‘.’. We then consider two judgments:

(i) Ω ⊢ ω₁ ≺ ω₂ and (ii) Ω; Γ; Δ ⊢ P :: x : A[ω]  

Judgment (i) states that ω₁ can directly access ω₂ under the hypotheses in Ω. We write ≺ for the reflexive, transitive closure of ≺, and ω₁ ≺* ω₂ when ω₁ ≺* ω₂ does not hold. Judgment (ii) states that process P offers the session behavior specified by type A on channel x; the session x resides at domain ω, under the accessibility hypotheses Ω, using unrestricted sessions in Γ and linear sessions in Δ. Note that each hypothesis in Γ and Δ is labeled with a specific domain. We omit Ω when it is clear from context.

Typing Rules Selected typing rules are given in Fig. 1; see [9] for the full listing. Right rules (marked with R) specify how to offer a session of a given type, left rules (marked with L) define how to use a session. The hybrid nature of the system induces a notion of well-formedness of sequents: a sequent Ω; Γ; Δ ⊢ P :: x : C[ω₁] is well-formed if Ω ⊢ ω₁ ≺* ω₂ for every x : A[ω₂] ∈ Δ, which we abbreviate as Ω ⊢ ω₁ ≺* Δ, meaning that all domains mentioned in Δ are accessible from ω₁ (not necessarily in a single direct step). No such domain requirement is imposed on Ω. If an end sequent is well-formed, every sequent in its proof will also be well-formed. All rules (read bottom-up) preserve this invariant; only (cut), (copy), (⊗R), (∀L) and (∃R) require explicit checks, which we discuss below. This invariant statically excludes interaction between sessions in accessible domains (cf. Theorem 3.7).

We briefly discuss some of the typing rules, first noting that we consider processes modulo structural congruence; hence, typability is closed under ≡ by definition. Type A → B denotes a session that inputs a session of type A and proceeds as B. To offer z : A → B at domain ω, we input y along z that will offer A at ω and proceed, now offering z : B at ω:

\[
\frac{\text{(- R)}}{\Omega; Γ; Δ; A : Y : A[ω] \vdash P : z : B[ω] \quad \text{(- R)}}}{\Omega; Γ; Δ \vdash z(y). P : z : A \rightarrow B[ω]} \quad (\otimes R) \frac{\Omega; Γ; Δ₁ \vdash P : y : A[ω] \quad \Omega; Γ; Δ₂ \vdash Q : z : B[ω]}{\Omega; Γ; Δ₁ ; Δ₂ \vdash \exists(y)(P \otimes Q) : z : A \otimes B[ω]}
\]

Dually, A ⊗ B denotes a session that outputs a session that will offer A and continue as B. To offer z : A ⊗ B, we output a fresh name y with type A along z and proceed offering z : B.
The (cut) rule allows us to compose process $P$, which offers $x:A[\omega_2]$, with process $Q$, which uses $x:A[\omega_2]$ to offer $z:C[\omega_1]$. We require that domain $\omega_2$ is accessible from $\omega_1$ (i.e., $\omega_1 \prec^* \omega_2$). We also require $\omega_1 \prec^* \Delta_1$: the domains mentioned in $\Delta_1$ (the context for $P$) must be accessible from $\omega_1$, which follows from the transitive closure of the accessibility relation ($\prec^*$) using the intermediary domain $\omega_2$. As in [10, 11], composition binds the name $x$:

$$\frac{\Gamma \vdash \omega_1 \prec^* \omega_2 \quad \Omega \vdash \psi : \tau \quad \Delta \vdash P : x:A[\omega_2] \quad \Omega, \Gamma; \Delta_1 \vdash \varphi : \psi} {\Omega, \Gamma; \Delta_1, \Delta_2 \vdash (\nu x)(P \mid Q) : z:C[\omega_1]}$$

Type 1 means that no further interaction will take place on the session; names of type 1 may be passed around as opaque values. $\&\{l : A_i\}_{i \in I}$ types a session channel that offers its partner a choice between the $A_i$ behaviors, each uniquely identified by a label $l$. Dually, $\oplus\{l : A_i\}_{i \in I}$ types a session that selects some behavior $A_i$ by emitting the corresponding label. For flexibility and consistency with merge-based projectability in multi-party session types, rules for choice and selection induce a standard notion of session subtyping [26].

Type $\forall A$ types a shared (non-linear) channel, to be used by a server for spawning an arbitrary number of new sessions (possibly none), each one conforming to type $A$.

Following our previous remark on well-formed sequents, the only rules that appeal to accessibility are ($\otimes$R), ($\otimes$L), ($\otimes$copy), and (cut). These conditions are directly associated with varying degrees of flexibility in terms of typability, depending on what relationship is imposed between the domain to the left and to the right of the turnstile in the left rules. Notably, our system leverages the accessibility judgment to enforce that communication is only allowed between processes whose sessions are in (transitively) accessible domains.

The type operator $\otimes_{\omega_2}$ realizes a domain migration mechanism which is specified both at the level of types and processes via name mobility tagged with a domain name. Thus, a channel typed with $\otimes_{\omega_2}A$ denotes that behavior $A$ is available by first moving to domain $\omega_2$, directly accessible from the current domain. More precisely, we have:

$$\frac{\Gamma \vdash \omega_1 \prec^* \Delta \quad \Omega \vdash \psi : y:A[\omega_1]} {\Omega, \Gamma; \Delta \vdash x : \otimes_{\omega_2}A[\omega_1]} \quad \frac{\Gamma \vdash \omega_2 \prec \omega_1 \quad \Omega, \omega_2 \prec \omega_1 \quad \Gamma, \Delta \vdash P : x:A[\omega_1]} {\Omega, \Gamma; \Delta \vdash (\nu y)(P \mid Q) : z:C[\omega_1]}$$

Hence, a process offering a behavior $z : \otimes_{\omega_2}A$ at $\omega_1$ ensures: (i) behavior $A$ is available at $\omega_2$ along a fresh session channel $y$ that is emitted along $z$ and (ii) $\omega_2$ is directly accessible from $\omega_1$. To maintain well-formedness of the sequent we also must check that all domains in $\Delta$ are still accessible from $\omega_2$. Dually, using a service $x : \otimes_{\omega_2}A[\omega_2]$ entails receiving a channel $y$ that will offer behavior $A$ at domain $\omega_3$ (and also allowing the usage of the fact that $\omega_2 \prec \omega_3$).

Domain-quantified sessions introduce domains as fresh parameters to types: a particular service can be specified with the ability to refer to any existing directly accessible domain (via universal quantification) or to some a priori unspecified accessible domain:

$$\frac{\Omega, \omega_1 \prec \alpha, \Gamma; \Delta \vdash P : x:A[\omega_1] \quad \alpha \notin \Omega, \Gamma, \Delta, \omega_1} {\Omega, \Gamma; \Delta \vdash z(\alpha).P : \forall \alpha.A[\omega_1]} \quad \frac{\Omega \vdash \omega_2 \prec \omega_1} {\Omega ; \Gamma, \Delta, x : \forall \alpha.A[\omega_2] \vdash Q : z:C[\omega_1]}$$

Rule (\forall R) states that a process seeking to offer $\forall \alpha.A[\omega_1]$ denotes a service that is located at domain $\omega_1$ but that may refer to any fresh domain directly accessible from $\omega_1$ in its specification (e.g. through the use of $\otimes$). Operationally, this means that the process must be ready to receive from its client a reference to the domain being referred to in the type, which is bound to $\alpha$ (occurring fresh in the typing derivation). Dually, Rule (\forall L) indicates that a
process interacting with a service of type $x: \forall \alpha. A[\omega_2]$ must make concrete the domain that is directly accessible from $\omega_2$ it wishes to use, which is achieved by the appropriate output action. Rules (\textit{3L}) and (\textit{3R}) for the existential quantifier have a dual reading.

Finally, the type-level operator $\downarrow \alpha.A$ allows for a type to refer to its current domain:

$$
\frac{
\Omega; \Gamma; \Delta \vdash P \mid z : A[\omega / \alpha][\omega]\n}{
\Omega; \Gamma; \Delta \vdash P \mid z : \downarrow \alpha.A[\omega]\n}
$$

The typing rules that govern $\downarrow \alpha.A$ are completely symmetric and produce no action at the process level, merely instantiating the domain variable $\alpha$ with the current domain $\omega$ of the session. As will be made clear in §4, this connective plays a crucial role in ensuring the correctness of our analysis of multiparty domain-aware sessions in our logical setting.

By developing our type theory with an explicit domain accessibility judgment, we can consider the accessibility relation as a parameter of the framework. This allows changing accessibility relations and their properties without having to alter the entire system. To consider the simplest possible accessibility relation, the only defining rule for accessibility would be Rule (\textit{why}) in Fig. 1. To consider an accessibility relation which is an equivalence relation we would add reflexivity, transitivity, and symmetry rules to the judgment.

\textbf{Discussion and Examples} Being an interpretation of hybridized linear logic, our domain-aware theory is conservative wrt the Curry-Howard interpretation of session types in [10, 11], in the following sense: the system in [10, 11] corresponds to the case where every session resides at the same domain. As in [10, 11], the sequent calculus for the underlying (hybrid) linear logic can be recovered from our typing rules by erasing processes and name assignments.

Conversely, a fundamental consequence of our hybrid interpretation is that it refines the session type structure in non-trivial ways. By requiring that communication only occurs between sessions located at the same (or accessible) domain we effectively introduce a new layer of reasoning to session type systems. To illustrate this feature, consider the following session type $\textsf{WStore}$, which specifies a simple interaction between a web store and its clients:

$$
\textsf{WStore} \triangleq \textsf{addCart} \rightarrow \&\{ \textsf{buy} : \textsf{Pay}, \textsf{quit} : 1 \} \quad \textsf{Pay} \triangleq \textsf{CCNum} \rightarrow \&\{ \textsf{ok} : \textsf{Rcpt} \otimes 1, \textsf{nok} : 1 \}
$$

$\textsf{WStore}$ allows clients to checkout their shopping carts by emitting a $\textsf{buy}$ message or to $\textsf{quit}$. In the former case, the client pays for the purchase by sending their credit card data. If a banking service (not shown) approves the transaction (via an $\textsf{ok}$ message), a receipt is emitted. Representable in existing session type systems (e.g. [10, 47, 31]), types $\textsf{WStore}$ and $\textsf{Pay}$ describe the intended communications but fail to capture the crucial fact that in practice the client’s sensitive information should only be requested after entering a secure domain. To address this limitation, we can use type-level domain migration to refine $\textsf{WStore}$ and $\textsf{Pay}$:

$$
\textsf{WStore}_{\text{sec}} \triangleq \textsf{addCart} \rightarrow \&\{ \textsf{buy} : @\text{sec} \textsf{Pay}_{\text{bank}}, \textsf{quit} : 1 \}
\quad \textsf{Pay}_{\text{bank}} \triangleq \textsf{CCNum} \rightarrow @\{ \textsf{ok} : (@\text{bank} \textsf{Rcpt}) \otimes 1, \textsf{nok} : 1 \}
$$

$\textsf{WStore}_{\text{sec}}$ decrees that the interactions pertinent to type $\textsf{Pay}_{\text{bank}}$ should be preceded by a migration step to the trusted domain $\text{sec}$, which should be directly accessible from $\textsf{WStore}_{\text{sec}}$’s current domain. The type also specifies that the receipt must originate from a bank domain $\text{bank}$ (e.g., ensuring that the receipt is never produced by the store without entering $\text{bank}$). When considering the interactions with a client (at domain $c$) that checks out their cart, we reach a state that is typed with the following judgment:

$$
\textsf{c} : \exists x : x : @\text{sec} \textsf{Pay}_{\text{bank}}[x] \vdash \textsf{Client} :: z : @\text{sec} \cdot 1[c]$$
We state the main results of type safety via type preservation (Theorem 3.3) and global progress (Theorem 3.4). These results directly ensure session fidelity and deadlock-freedom. Typing also ensures termination, i.e., processes do not exhibit infinite reduction paths (Theorem 3.5). We note that in the presence of termination, our progress result ensures that communication actions are always guaranteed to take place. Moreover, as a property specific to domain-aware processes, we show domain preservation, i.e., processes respect their domain accessibility conditions (Theorem 3.7). The formal development of these results relies on a domain-aware labeled transition system [9], defined as a simple generalization of the early labelled transition system for the session π-calculus given in [10, 11].

### Type Safety and Termination

Following [10, 11], our proof of type preservation relies on a simulation between reductions in the session-typed π-calculus and logical proof reductions. At this point, it is impossible for a (typed) client to interact with the behavior that is protected by the domain `sec`, since it is not the case that `c ⊲ ws; z::Pay_bank[sec]` is derivable. This ensures, e.g., that a client cannot exploit the payment platform of the web store by accessing the trusted domain in unforeseen ways. The client can only communicate in the secure domain after the web store service has migrated accordingly, as shown by the judgment

\[
c ⊲ ws; ws ⊲ sec; z::Pay_bank[sec] ⊢ Client' :: z:T[c].\]

**Technical Results** We state the main results of type safety via type preservation (Theorem 3.3) and global progress (Theorem 3.4). These results directly ensure session fidelity and deadlock-freedom. Typing also ensures termination, i.e., processes do not exhibit infinite reduction paths (Theorem 3.5). We note that in the presence of termination, our progress result ensures that communication actions are always guaranteed to take place. Moreover, as a property specific to domain-aware processes, we show domain preservation, i.e., processes respect their domain accessibility conditions (Theorem 3.7). The formal development of these results relies on a domain-aware labeled transition system [9], defined as a simple generalization of the early labelled transition system for the session π-calculus given in [10, 11].

### Type Safety and Termination

Following [10, 11], our proof of type preservation relies on a simulation between reductions in the session-typed π-calculus and logical proof reductions.

#### Lemma 3.2 (Domain Substitution)

Suppose \( \Omega ⊢ \omega_1 ⊲ \omega_2 \). Then we have:

1. If \( \Omega, \omega_3 ⊲ \alpha; \Omega; \Delta ⊢ P :: z:A[\omega] \) then 
   \( \Omega, \omega_3 ⊲ \omega_2/\alpha; \Gamma; \Delta ⊢ P[\omega_2/\alpha] :: z:A[\omega_2/\alpha] \).
2. If \( \Omega, \alpha ⊲ \omega_2; \Omega; \Delta ⊢ P :: z:A[\omega] \) then 
   \( \Omega, \omega_3 ⊲ \omega_1/\alpha; \Gamma; \Delta ⊢ P[\omega_1/\alpha] :: z:A[\omega_1/\alpha] \).

Safe domain communication relies on domain substitution preserving typing (Lemma 3.2).

#### Theorem 3.3 (Type Preservation)

If \( \Omega; \Gamma; \Delta ⊢ P :: z:A[\omega] \) and \( P ⊮ Q \) then 
\( \Omega; \Gamma; \Delta ⊢ Q :: z:A[\omega] \).
Proof (Sketch). The proof mirrors those of [10, 11, 8, 44], relying on a series of lemmas relating the result of dual process actions (via our LTS semantics) with typable parallel compositions through the (cut) rule [9]. For session type constructors of [10], the results are unchanged. For the domain-aware session type constructors, the development is identical that of [8] and [44], which deal with communication of types and data terms, respectively. □

Following [10, 11], the proof of global progress relies on a notion of a live process, which intuitively consists of a process that has not yet fully carried out its ascribed session behavior, and thus is a parallel composition of processes where at least one is a non-replicated process, guarded by some action. Formally, we define live(P) if and only if P ≡ (νn)(π.Q | R), for some R, names n and a non-replicated guarded process π.Q.

**Theorem 3.4** (Global Progress). If Ω; · ⊢ P :: x.1[ω] and live(P) then ∃Q s.t. P ⊑ Q.

Note that Theorem 3.4 is without loss of generality since using the cut rules we can compose arbitrary well-typed processes together and x need not occur in P due to Rule (1R).

Termination (strong normalization) is a relevant property for interactive systems: while from a global perspective they are meant to run forever, at a local level participants should always react within a finite amount of time, and never engage into infinite internal behavior.

We say that a process P terminates, noted P ⊑, if there is no infinite reduction path from P.

**Theorem 3.5** (Termination). If Ω; Γ; ∆ ⊢ P :: x:A[ω] then P ⊑.

Proof (Sketch). By adapting the linear logical relations given in [38, 39, 8]. For the system in §3 without quantifiers, the logical relations correspond to those in [38, 39], extended to carry over Ω. When considering quantifiers, the logical relations resemble those proposed for polymorphic session types in [8], noting that no impredicativity concerns are involved. □

**Domain Preservation.** As a consequence of the hybrid nature of our system, well-typed processes are guaranteed not only to faithfully perform their prescribed behavior in a deadlock-free manner, but they also do so without breaking the constraints put in place on domain accessibility given by our well-formedness constraint on sequents.

**Theorem 3.6.** Let E be a derivation of Ω; Γ; ∆ ⊢ P :: z:A[ω]. If Ω; Γ; ∆ ⊢ P :: z:A[ω] is well-formed then every sub-derivation in E well-formed.

While inaccessible domains can appear in Γ, such channels can never be used and thus can not appear in a well-typed process due to the restriction on the (copy) rule. Combining Theorems 3.3 and 3.6 we can then show that even if a session in the environment changes domains, typing ensures that such a domain will be (transitively) accessible:

**Theorem 3.7.** Let (1) Ω; Γ; ∆; Δ′ ⊢ (νx)(P | Q) :: z : A[ω], (2) Ω; Γ; ∆ ⊢ P :: x:B[ω′], and (3) Ω; Γ; Δ′; x:B[ω′] ⊢ Q :: z:A[ω]. If (νx)(P | Q) ⇒ (νx)(P′ | Q′) then: (a) Ω; Γ; Δ ⊢ P′ :: x′:B′[ω′′], for some x′, B′, ω′′; (b) Ω; Γ; Δ′, x′:B′[ω′′] ⊢ Q′ :: z:A[ω]; (c) ω ≺+ ω′′.

## 4 Domain-Aware Multiparty Session Types

We now shift our attention to multiparty session types [32]. We consider the standard ingredients: global types, local types, and the projection function that connects the two. Our global types include a new domain-aware construct, p moves q to ω for G1; G2; our local types exploit the hybrid session types from Def. 3.1. Rather than defining a separate type system based on local types for the process model of §2, our analysis of multiparty protocols extends...
the approach defined in [7], which uses medium processes to characterize correct multiparty implementations. The advantages are twofold: on the one hand, medium processes provide a precise semantics for global types; on the other hand, they enable the principled transfer of the correctness properties established in §3 for binary sessions (type preservation, global progress, termination, domain preservation) to the multiparty setting. Below, participants are ranged over by $p, q, r, \ldots$; we write $\bar{q}$ to denote a finite set of participants $q_1, \ldots, q_n$.

Besides the new domain-aware global type, our syntax of global types includes constructs from [32, 21]. We consider value passing in branching (cf. $U$ below), fully supporting delegation. To streamline the presentation, we consider global types without recursion.

> **Definition 4.1 (Global and Local Types).** Define global types ($G$) and local types ($T$) as

$$U ::= \text{bool} \mid \text{nat} \mid \text{str} \mid \ldots \mid T$$

$$G ::= \text{end} \mid p \to q; \{l_i(U_i); G_i\}_{i \in I} \mid p \text{ moves } \bar{q} \text{ to } \omega \text{ for } G_1; G_2$$

$$T ::= \text{end} \mid p?\{l_i(U_i); T_i\}_{i \in I} \mid p\{l_i(U_i); T_i\}_{i \in I} \mid \forall \alpha.T \mid \exists \alpha.T \mid \downarrow \alpha.T \mid \uparrow \alpha.T$$

The completed global type is denoted $\text{end}$. Given a finite $I$ and pairwise different labels, $p \to q; \{l_i(U_i); G_i\}_{i \in I}$ specifies that by choosing label $l_i$, participant $p$ may send a message of type $U_i$ to participant $q$, and then continue as $G_i$. We decree $p \neq q$, so reflexive interactions are disallowed. The global type $p \text{ moves } \bar{q} \text{ to } \omega$ for $G_1; G_2$ specifies the migration of participants $p, \bar{q}$ to domain $\omega$ in order to perform the sub-protocol $G_1$; this migration is lead by $p$. Subsequently, all of $p, \bar{q}$ migrate from $\omega$ back to their original domains and protocol $G_2$ is executed. This intuition will be made precise by the medium processes for global types (cf. Def. 4.8). Notice that $G_1$ and $G_2$ may involve different sets of participants. In writing $p \text{ moves } \bar{q} \text{ to } \omega$ for $G_1; G_2$ we assume two natural conditions: (a) all migrating participants intervene in the sub-protocol (i.e., the set of participants of $G_1$ is exactly $p, \bar{q}$) and (b) domain $\omega$ is accessible (via $\leftarrow$) by all these migrating participants in $G_1$. While subprotocols and session delegation may appear as similar, delegation supports a different idiom altogether, and has no support for domain awareness. Unlike delegation, with subprotocols we can specify a point where some of the participants perform a certain protocol within the same multiparty session and then return to the main session as an ensemble.

> **Definition 4.2.** The set of participants of $G$ (denoted $\text{part}(G)$) is defined as: $\text{part}(\text{end}) = \emptyset$,

$\text{part}(p \to q; \{l_i(U_i); G_i\}_{i \in I}) = \{p, q\} \cup \bigcup_{i \in I} \text{part}(G_i)$, $\text{part}(p \text{ moves } \bar{q} \text{ to } \omega \text{ for } G_1; G_2) = \{p\} \cup \bar{q} \cup \text{part}(G_1) \cup \text{part}(G_2)$. We sometimes write $p \in G$ to mean $p \in \text{part}(G)$.

Global types are projected onto participants so as to obtain local types. The terminated local type is $\text{end}$. The local type $p?\{l_i(U_i); T_i\}_{i \in I}$ denotes an offer of a set of labeled alternatives; the local type $p\{l_i(U_i); T_i\}_{i \in I}$ denotes a behavior that chooses one of such alternatives. Exploiting the domain-aware framework in §3, we introduce four new local types. They increase the expressiveness of standard local types by specifying universal and existential quantification over domains ($\forall \alpha.T$ and $\exists \alpha.T$), migration to a specific domain ($\uparrow \alpha.T$), and a reference to the current domain ($\downarrow \alpha.T$, with $\alpha$ occurring in $T$).

We now define (merge-based) projection for global types [21]. To this end, we rely on a merge operator on local types, which in our case considers messages $U$.

> **Definition 4.3 (Merge).** We define $\sqcup$ as the commutative partial operator on base and local types such that $\text{bool} \sqcup \text{bool} = \text{bool}$ (and analogously for other base types), and

1. $T \sqcup T = T$, where $T$ is one of the following: end, $p\{l_i(U_i); T_i\}_{i \in I}$, $\forall \alpha.T$, $\forall \alpha.T$, or $\exists \alpha.T$;
2. $p?\{l_k(U_k); T_k\}_{k \in K} \sqcup p\{l_j(U_j); T_j\}_{j \in J} = \{l_k(U_k); T_k\}_{k \in K \cup J} \cup \{l_j(U_j); T_j\}_{j \in J \cup K} \cup \{l_i(U_i); (T_i \sqcup T_j)\}_{i \in K \cap J}$

and is undefined otherwise.
Therefore, for $U_1 \sqcup U_2$ to be defined there are two options: (a) $U_1$ and $U_2$ are identical base, terminated, selection, or “hybrid” local types; (b) $U_1$ and $U_2$ are branching types, but not necessarily identical: they may offer different options but with the condition that the behavior in labels occurring in both $U_1$ and $U_2$ must be mergeable.

To define projection and medium processes for the global type $p \text{ moves } q \text{ to } \omega$ for $G_1 ; G_2$, we require ways of “fusing” local types and processes. The intent is to capture in a single (sequential) specification the behavior of two distinct (sequential) specifications, i.e., those corresponding to protocols $G_1$ and $G_2$. For local types, we have the following definition, which safely appends a local type to another:

$\blacktriangleright$ **Definition 4.4 (Local Type Fusion).** The fusion of $T_1$ and $T_2$, written $T_1 \circ T_2$, is given by:

$\begin{align*}
\forall \ell \langle U \rangle. T_1 \rangle \circ i \in T &= \forall \ell \langle U \rangle. (T_1 \circ T) \rangle \in T \\
\forall \ell \langle U \rangle. T_1 \rangle \circ i \in T &= \forall \ell \langle U \rangle. (T_1 \circ T) \rangle \in T \\
(1 \circ i) T_1 \circ T 1 &= 1 \circ i (T_1 \circ T)
\end{align*}$

This way, e.g., if $T_1 = 1 \circ \alpha \circ \beta$ and $T_2 = 1 \circ \lambda \circ \mu$ then $T_1 \circ T_2 = 1 \circ \lambda \circ \mu$ (and back).

$\blacktriangleright$ **Definition 4.5 (Merge-based Projection [21]).** Let $G$ be a global type. The merge-based projection of $G$ under participant $r$, denoted $G[r]$, is defined as $\text{end}[r] = \text{end}$ and

$p \rightarrow q \{ l \langle U \rangle. G[r] \rangle i \in T \} r = \begin{cases} p \{ l \langle U \rangle. G[r] \rangle i \in T \} r & \text{if } r = p \\ q \{ l \langle U \rangle. G[r] \rangle i \in T \} r & \text{if } r = q \\ \cup_{i \in T} G[r] & \text{otherwise (as in Def. 4.3)} \end{cases}$

When no side condition holds, the map is undefined.

The projection for the type $p \text{ moves } q \text{ to } \omega$ for $G_1 ; G_2$ is one of the key points in our analysis. The local type for $p$, the leader of the migration, starts by binding the identity of its current domain (say, $\omega_p$) to $\beta$. Then, the (fresh) domain $\omega$ is communicated, and there is a migration step to $\omega$, which is where protocol $G_1[p]$ will be performed. Finally, there is a migration step from $\omega$ back to $\omega_p$; once there, the protocol $G_2[p]$ will be performed. The local type for all of $q_i \in q$ follows accordingly: they expect $\omega$ from $p$; the migration from their original domains to $\omega$ (and back) is as for $p$. For participants in $G_1$, the fusion on local types (Def. 4.4) defines a local type that includes the actions for $G_1$ but also for $G_2$, if any: a participant in $G_1$ need not be involved in $G_2$. Interestingly, the resulting local types $\downarrow \beta. (\forall \alpha. \exists \beta G_1[p] \circ \exists \beta G_2[p]$ and $\downarrow \beta. (\forall \alpha. \exists \beta G_1[q] \circ \exists \beta G_2[q]$ define a precise combination of hybrid connectives whereby each migration step is bound by a quantifier or the current domain.

The following notion of well-formedness for global types is standard:

$\blacktriangleright$ **Definition 4.6 (Well-Formed Global Types [32]).** We say that global type $G$ is well-formed (WF, in the following) if the projection $G[r]$ is defined for all $r \in G$. 

**Analyzing Global Types via Medium Processes** A medium process is a well-typed process from §2 that captures the communication behavior of the domain-aware global types of Def. 4.1. Here we define medium processes and establish two fundamental characterization results for them (Theorems 4.11 and 4.12). We shall consider names indexed by participants: given a name $c$ and a participant $p$, we use $c_p$ to denote the name along which the session behavior of $p$ will be made available. This way, if $p \neq q$ then $c_p \neq c_q$. To define mediums, we need to append or fuse sequential processes, just as Def. 4.4 fuses local types:
Definition 4.7 (Fusion of Processes). We define \( \circ \) as the partial operator on well-typed processes such that (with \( \pi \in \{c(y), c(\omega), c(\alpha), c(y \oplus \omega), c(y \otimes \omega), c(\eta)\} : \)
\[
\begin{align*}
c(y), [u \mapsto v] & \parallel P \triangleq c(y), [u \mapsto v] \parallel (P \circ Q) \\
c \triangleright \{ k : P \}_i \circ Q & \triangleq c \triangleright \{ k : (P_i \circ Q) \}_i \\
\end{align*}
\]
and is undefined otherwise.

The previous definition suffices to define a medium process (or simply medium), which uses indexed names to uniformly capture the behavior of a global type:

Definition 4.8 (Medium Process). Let \( G \) be a global type (cf. Def. 4.1), \( \bar{c} \) be a set of indexed names, and \( \tilde{\omega} \) a set of domains. The medium of \( G \), denoted \( M^\bar{c}[G](\tilde{\omega}) \), is defined as:
\[
\begin{align*}
0 & \quad \text{if } G = \text{end} \\
c_p \triangleright \{ k : c_p(u).c_q \triangleleft k \cdot \tilde{\omega}(v).[u \mapsto v] \parallel M^\bar{c}[G_i](\tilde{\omega}) \}_i & \quad \text{if } G = p \rightarrow q; \{ k_i(U_i) \cdot G_i \}_i \\
\quad \text{if } G = p \text{ moves } q_1, \ldots, q_n \text{ to } w \text{ for } G_1 : G_2 \\
\end{align*}
\]
where \( M^\bar{c}[G_1](\tilde{\omega}) \circ M^\bar{c}[G_2](\tilde{\omega}) \) is as in Def. 4.7.

The medium for \( G = p \rightarrow q; \{ k_i(U_i) \cdot G_i \}_i \) exploits four prefixes to mediate in the interaction between the implementations of \( p \) and \( q \): the first two prefixes (on name \( c_p \)) capture the label selected by \( p \) and the subsequently received value; the third and fourth prefixes (on name \( c_q \)) propagate the choice and forward the value sent by \( p \) to \( q \). We omit the forwarding and value exchange when the interaction does not involve a value payload.

The medium for \( G = p \text{ moves } q_1, \ldots, q_n \text{ to } w \text{ for } G_1 : G_2 \) showcases the expressivity and convenience of our domain-aware process framework. In this case, the medium’s behavior takes place through the following steps: First, \( M^\bar{c}[G](\tilde{\omega}) \) inputs a domain identifier (say, \( \omega \)) from \( p \) which is forwarded to \( q_1, \ldots, q_n \), the other participants of \( G_1 \). Secondly, the roles of \( p, q_1, \ldots, q_n \) migrate from their domains \( \tilde{\omega}_p, \tilde{\omega}_q_1, \ldots, \tilde{\omega}_q_n \) to \( \omega \). At this point, the medium for \( G_1 \) can execute, keeping track the current domain \( \omega \) for all participants. Finally, the participants of \( G_1 \) migrate back to their original domains and the medium for \( G_2 \) executes.

Recalling the domain-aware global type of §1, we produce its medium process:
\[
\begin{align*}
c_{c_1} \triangleright \{ \text{request} : c_{c_1}(y).c_{\text{serv}} \triangleleft \text{request}; \tilde{\omega}(v).[y \mapsto v] \parallel \} \\
c_{\text{serv}} \triangleright \{ \text{reply} : c_{\text{serv}}(a).c_{\text{c1}} \triangleleft \text{reply}; \tilde{\omega}(n).[a \mapsto n] \parallel \} \circ \{ \text{done} : c_{\text{serv}} \triangleleft \text{done}; 0 \} \\
\quad \text{if } G = \text{end} \\
\quad \text{if } G = p \rightarrow q; \{ k_i(U_i) \cdot G_i \}_i \\
\text{wait} : c_{c_1} \triangleright \text{wait}; c_{\text{serv}} \triangleright \{ \text{init} : c_{\text{serv}} \triangleleft \text{init}; c_{\text{serv}}(U_{\text{priv}}) \cdot c_{\text{serv}}(U_{\text{priv}}), c_{\text{serv}}(y_{\text{priv}}).c_{\text{serv}}(y_{\text{priv}}), M^{\bar{c}[G]}(\text{Offload})[y_{\text{serv}}.y_{\text{serv}}] \parallel \} \circ \{ y_{\text{serv}} \cdot y_{\text{serv}}.y_{\text{serv}} \cdot y_{\text{serv}} \} \\
\quad \{ \text{reply} : c_{\text{serv}}(a).c_{\text{c1}} \triangleleft \text{reply}; \tilde{\omega}(n).[a \mapsto n] \parallel 0 \} \} \\
\end{align*}
\]

The medium ensures the client’s domain remains fixed through the entire interaction, regardless of whether the middleware chooses to interact with the server. This showcases how our medium transparently manages domain migration of participants.

Characterization Results. We state results that offer a sound and complete account of the relationship between: (i) a global type \( G \) (and its local types), (ii) its medium process \( M^\bar{c}[G](\tilde{\omega}) \), and (iii) process implementations for the participants \( \{ p_1, \ldots, p_n \} \) of \( G \). In a nutshell, these results say that the typeful composition of \( M^\bar{c}[G](\tilde{\omega}) \) with processes for each
\[ p_1, \ldots, p_n \] (well-typed in the system of §3) performs the intended global type. Crucially, these processes reside in distinct domains and can be independently developed, guided by their local type—never need not know about the medium’s existence or structure. The results generalize those in [7] to the domain-aware setting. Given a global type \( G \) with \( \text{part}(G) = \{ p_1, \ldots, p_n \} \), below we write \( \text{npart}(G) \) to denote the set of indexed names \( \{ c_{p_1}, \ldots, c_{p_n} \} \). We define:

\( \begin{align*}
\mathbf{Definition 4.9 (Compositional Typing).} \quad & \text{We say } \Omega; \Gamma; \Delta \vdash M^G[\tilde{G}](\tilde{c}) :: z : C \text{ is a compositional typing if:} \\
& (i) \text{ it is a valid typing derivation; (ii) } \text{npart}(G) \subseteq \text{dom}(\Delta); \text{ and (iii) } C = 1 .
\end{align*} \)

A compositional typing says that \( M^G[\tilde{G}](\tilde{c}) \) depends on behaviors associated to each participant of \( G \); it also specifies that \( M^G[\tilde{G}](\tilde{c}) \) does not offer any behaviors of its own.

The following definition relates binary session types and local types: the main difference is that the former do not mention participants. Below, \( B \) ranges over base types (\( \text{bool}, \text{nat}, \ldots \)).

\( \begin{align*}
\mathbf{Definition 4.10 (Local Types → Binary Types).} \quad & \text{Mapping } \langle \rangle \text{ from local types } T \text{ (Def. 4.1)} \\
& \text{into binary types } A \text{ (Def. 3.1) is inductively defined as } \langle \langle \text{end} \rangle \rangle = \langle \langle B \rangle \rangle = 1 \text{ and}
\end{align*} \)

\[ \langle \langle \Gamma[1], T_i \rangle \rangle_{i \in I} = \top \{ l : \langle U_i \rangle \otimes \langle T_i \rangle \}_{i \in I} \text{ if } \forall \alpha. T \rangle = \forall \alpha. \langle \langle T \rangle \rangle \]

\[ \langle \langle \alpha, T \rangle \rangle = \top \langle \langle T \rangle \rangle \]

Our first characterization result ensures that well-formedness of a global type \( G \) guarantees the typability of its medium \( M^G[\tilde{G}](\tilde{c}) \) using binary session types. Hence, it ensures that multiparty protocols can be analyzed by composing the medium with independently obtained, well-typed implementations for each protocol participant. Crucially, the resulting well-typed process will inherit all correctness properties ensured by binary typability established in §3.

\( \begin{align*}
\mathbf{Theorem 4.11 (Global Types → Typed Mediums).} \quad & \text{If } G \text{ is WF with } \text{part}(G) = \{ p_1, \ldots, p_n \} \\
& \text{then } \Omega; \Gamma; c_{p_1}; \langle \langle G[\tilde{p}_1] \rangle \rangle_1, \ldots, c_{p_n}; \langle \langle G[p_n] \rangle \rangle_n ; M^G[\tilde{G}](\tilde{c}) :: z : 1[\omega_m] \text{ is a compositional typing for some } \Omega, \Gamma, \text{ with } \tilde{\omega} = \omega_1, \ldots, \omega_n . \text{ We assume that } \omega_i \prec \omega_m \text{ for all } i \in \{ 1, \ldots, n \} \text{ (the medium’s accessibility is accessible by all), and that } i \neq j \text{ implies } \omega_i \neq \omega_j .
\end{align*} \)

The second characterization result, given next, is the converse of Theorem 4.11: binary typability precisely delineates the interactions that underlie well-formed multiparty protocols. We need an auxiliary relation on local types, written \( \preceq_{\alpha} \), that relates types with branching and “here” type operators, which have silent process interpretations (cf. Figure 1 and [9]).

First, we have \( T_1 \preceq_{\alpha} T_2 \) if there is a \( T’ \) such that \( T_1 \sqcup T’ = T_2 \) (cf. Def. 4.3). Second, we have \( T_1 \preceq_{\alpha} T_2 \) if (i) \( T_1 = T’ \) and \( T_2 = \bot \alpha.T’ \) and \( \alpha \) does not occur in \( T’ \); but also if (ii) \( T_1 = \bot \alpha.T’ \) and \( T_2 = T’[\omega/\alpha] \). (See [9] for a formal definition of \( \preceq_{\alpha} \)).

\( \begin{align*}
\mathbf{Theorem 4.12 (Well-Typed Mediums → Global Types).} \quad & \text{Let } G \text{ be a global type (cf. Def. 4.1).}
\end{align*} \)

\[ \text{If } \Omega; \Gamma; c_{p_1}; A_1[\omega_1], \ldots, c_{p_n}; A_n[\omega_n] ; M^G[\tilde{G}](\tilde{c}) :: z : 1[\omega_m] \text{ is a compositional typing then}
\]

\[ \exists T_1, \ldots, T_n \text{ such that } G\{ p_j \} \preceq_{\alpha} T_j \text{ and } \langle T_j \rangle = A_j, \text{ for all } p_j \in \text{part}(G) . \]

The above theorems offer a static guarantee that connects multiparty protocols and well-typed processes. They can be used to establish also dynamic guarantees relating the behavior of a global type \( G \) and that of its associated set of multiparty systems (i.e., the typeful composition of \( M^G[\tilde{G}](\tilde{c}) \) with processes for each of \( p_i \in \text{part}(G) \)). These dynamic guarantees can be easily obtained by combining Theorems 4.11 and 4.12 with the approach in [7].

### 5 Related Work

There is a rich history of works on the logical foundations of concurrency (see, e.g., [4, 27, 1, 3]), which has been extended to session-based concurrency by Wadler [47], Dal Lago and Di
Giamberardino [35], and others. Medium-based analyses of multiparty sessions were developed in [7] and used in an account of multiparty sessions in an extended classical linear logic [14].

Two salient calculi with distributed features are the Ambient calculus [16], in which processes move across ambients (abstractions of administrative domains), and the distributed \( \pi \)-calculus (D\( \pi \)) [29], which extends the \( \pi \)-calculus with flat locations, local communication, and process migration. While domains in our model may be read as locations, this is just one specific interpretation; they admit various alternative readings (e.g., administrative domains, security-related levels), leveraging the partial view of the domain hierarchy. Type systems for Ambient calculi such as [15, 6] enforce security and communication-oriented properties in terms of ambient movement but do not cover issues of structured interaction, central in our work. Garralda et al. [25] integrate binary sessions in an Ambient calculus, ensuring that session protocols are undisturbed by ambient mobility. In contrast, our type system ensures that both migration and communication are safe and, for the first time in such a setting, satisfy global progress (i.e., session protocols never jeopardize migration and vice-versa).

The multiparty sessions with nested protocols of Demangeon and Honda [19] include a nesting construct that is similar to our new global type \( p \text{moves} \tilde{q} \text{to} w \) for \( G_1; G_2 \), which also introduces nesting. The focus in [19] is on modularity in choreographic programming; domains nor domain migration are not addressed. The nested protocols in [19] can have local participants and may be parameterized on data from previous actions. We conjecture that our approach can accommodate local participants in a similar way. Data parameterization can be transposed to our logical setting via dependent session types [44, 46]. Asynchrony and recursive behaviors can also be integrated by exploiting existing logical foundations [23, 45].

Balzer et al. [2] overlay a notion of world and accessibility on a system of shared session types to ensure deadlock-freedom. Their work differs substantially from ours: they instantiate accessibility as a partial-order, equip sessions with multiple worlds and are not conservative wrt linear logic, being closer to partial-order-based typings for deadlock-freedom [34, 37].

6 Concluding Remarks

We developed a Curry-Howard interpretation of hybrid linear logic as domain-aware session types. Present in processes and types, domain-awareness can account for scenarios where domain information is only determined at runtime. The resulting type system features strong correctness properties for well-typed processes (session fidelity, global progress, termination). Moreover, by leveraging a parametric accessibility relation, it rules out processes that communicate with inaccessible domains, thus going beyond the scope of previous works.

As an application of our framework, we presented the first systematic study of domain-awareness in a multiparty setting, considering multiparty sessions with domain-aware migration and communication whose semantics is given by a typed (binary) medium process that orchestrates the multiparty protocol. Embedded in a fully distributed domain structure, our medium is shown to strongly encode domain-aware multiparty sessions; it naturally allows us to transpose the correctness properties of our logical development to the multiparty setting.

Our work opens up interesting avenues for future work. Mediums can be seen as monitors that enforce the specification of a domain-aware multiparty session. We plan to investigate contract-enforcing mediums building upon works such as [28, 33, 20], which study runtime monitoring in session-based systems. Our enforcement of communication across accessible domains suggests high-level similarities with information flow analyses in multiparty sessions (cf. [13, 12, 17]), but does not capture the directionality needed to model such analyses outright. It would be insightful to establish the precise relationship with such prior works.
References


Domain-Aware Session Types

Kaustuv Chaudhuri, Carlos Olarte, Elaine Pimentel, and Joëlle Despeyroux. Hybrid Linear Logic, revisited. Mathematical Structures in Computer Science, 2019. URL: https://hal.inria.fr/hal-01968154.


