A Dependently Typed Ambient Calculus

Cédric Lhoussaine and Vladimiro Sassone
University of Sussex, UK

Abstract

The Ambient calculus is a successful model of distributed, mobile computation, and has been the vehicle of new ideas for resource access control. Mobility types have been used to enforce elementary access control policies, expressed indirectly via classification of ambients in groups by means of 'group types.' The paper presents a theory of dependent types for the Ambient calculus which allows greater flexibility, while keeping the complexity away from the programmer into the type system.

1 Introduction

The calculus of *Mobile Ambients* [11] (MA) is a distributed calculus of mobile processes based on three fundamental notions: locations as computational environments, (subjective) mobility of locations, and local communication. Processes live inside ambients, and inside ambients compute and interact. Ambients relocate themselves, carrying along all their contents: their migration, triggered by the processes they enclose, models mobility of entire domains and active computational loci. Relevant variations of the basic calculus include Safe Ambients [19], Boxed Ambients [4], and NBA [5]. The theory of MA has developed in several directions, including behavioural semantics [21, 23], logics [13, 26, 18], and model checking [6, 14], while applications are flourishing: resource control [27, 2], semistructured data and query languages [8, 7] and, lately, modelling of biological processes [25].

The work on types for ambients, initiated in [12], has introduced some interesting innovations. In particular, it led to natural concepts of mobility types (cf., e.g. [9, 4, 22, 15]). The common framework proposed so far in the literature for mobility control relies on *groups* and *group types*. Groups represent collections of ambients with uniform access rights, and policies like '*n CanMoveTo m*' are expressed by saying, for instance, '*n belongs to group G* and all ambients of *group G can move to m*.' These and similar simple constraints, such as '*m accepts ambients of group G*,' are then enforced statically by embodying groups in types. This approach's merit is to simplify considerably the type system. It allows to avoid the difficulties of dependent types, since it replaces (variable) ambient names with (constant) group names. The loss in expressiveness and flexibility, however, is self-evident.

This paper generalises the approaches to access control based on groups by using types explicitly dependent on ambient names, so that policies like '*n CanMoveTo m*' can be expressed directly. The task involves issues of technical complexity, and we believe that our approach contributes significantly to advance the theory of type-based resource access control in the Ambient calculus. The guiding principle behind our work is to allow for flexibility in control policies, while pushing the complexity to the type system. We elaborate further on this below.

Dependent types vs groups

At the formal level, dependent types are indeed trickier to work with than groups, as already suggested in [9]. However, they are very expressive and ultimately, at the programming level, not necessarily more difficult to use than groups. It may indeed be challenging, if not impossible, to partition ambient names into groups in order to implement the desired security policy in complex applications. By referring directly to names, instead, a programmer avoids a level of indirection, and is less prone to policy specification errors. The type systems we propose here aim at harnessing the complexity of dependent types and relegating it to inner working of the type system, so as to keep the burden off the programmer, and consequently make programs more robust.

To illustrate the point, let us consider a naive and specialised taxi server whose intention is to provide a taxi service usable only by ambient n:

$$TaxiServ(n) = !(\nu\, taxi : A)\,(taxi[\,] \mid n[\mathsf{in}\, taxi]).$$

The process creates a new ambient called *taxi*, with some type A, together with an ambient n which can move to it. Due to the scoping rules, an external ambient $m[P]$ can only move into the taxi by first moving to n and then escaping it after being transported to *taxi*. For instance, for $P = \mathsf{in}\, n.\mathsf{out}\, n.P'$, the system may evolve as follows.

$$m[\,\mathsf{in}\, n.\mathsf{out}\, n.P'\,] \mid TaxiServ(n) \rightarrow^{*} taxi[\,m[P']\mid n[\,]\,] \mid TaxiServ(n).$$

To avoid this, A must restrict the children allowed of *taxi* to, say, only ambient n. Using groups – for instance in the setting of [22], where an ambient type $a : \mathsf{amb}[G, \mathsf{mob}[\mathcal{G}]]$ assigns group G to a and specifies that $\mathcal{G}$ is the set of groups of those ambients which a is allowed to move to – to prevent any ambient other than n to occupy the taxi, n must be the *only* ambient with a type of the form $\mathsf{amb}[H, \mathsf{mob}[\{G\} \cup \mathcal{H}]]$, where G is the group of *taxi*. Such condition is clearly beyond the control $TaxiServ(n)$ application, as the environment may create new names with types that violate it. Making G private is not a solution, as it forces n to be private too, so defeating its very purpose. Indeed, in a term such as $(\nu\, G)\,(\nu\, n : A)\, P \mid Q$, where G occurs in A, n can not be communicated to Q (not even via subtyping [22]).

With dependent types we would simply and directly mention n as a possible (or perhaps the only) child for *taxi*. This leads to ambient types of the form $\mathsf{amb}[\mathsf{mob}[\mathcal{P}, C]]$, where $\mathcal{P}$ is the set of names of those ambients allowed to contain *taxi* and, dually, C is the set of names of those ambients allowed to reside within *taxi*. Type A above can be simply $\mathsf{amb}[\mathsf{mob}[\{top\}, \{n\}]]$, where name *top* represents the top-level ambient. Yet, the *taxi* ambient would be guaranteed to have n and only n as a possible child, with no need for n to be private. Of course, such simplicity in expressing types comes at the cost of additional complexity at the type system level. Primarily, we need to enforce consistency between the type of a parent ambient and those of its children. To exemplify, when a taxi is created, n receives a new capability to have *taxi* as its parent; the type of n – which actually predates the creation of the fresh instance of *taxi* – must then be updated accordingly. Observe that in a conventional type system, the effect of the new name would be confined inside the scope of its definition, and would certainly not affect the type of n. In our case, however, leaving n's type unchanged leads to an unsound system (cf. Example 1).

In order for n to be aware of any additional capability it may acquire over time, we introduce the pivotal notion of *abstract names*. Such names are used only in the derivation of typing judgements, to record potential name creations, either by a process or by its environment. As it will be clear later, abstract names intuitively play the role of group names in their ability to cross the scope of name restrictions.

Flexibility

The main contribution on this paper is the use of dynamic types to increase expressiveness, which can be fleshed out as the ability to deploy security policies at run time. More precisely, we want servers flexible enough to provide services specialised to each particular client, so leading towards secure, highly modular programming. In other words, a service specifically provided for client c_1 must be unusable by client c_2. Such objectives may be achieved in several different ways, as for instance by adding special operators to the calculus. In this paper we stick to the basic primitives of the Ambient calculus and investigate the issue of personalised services at the level of types.

The taxi server discussed above is not particularly interesting, essentially because it is not a server at all: it does not interact with any client, but provides again and again the same 'secure' service to the same specific client. To illustrate our ideas, let us first explore a generic, or *dynamic*, version of the taxi server, *GTaxiServ*, using groups. A most natural protocol seems to require the ability to communicate both group and ambient names, as below.

$$GTaxiServ = !(x)(y)(\nu\, taxi : \mathsf{amb}[x, \mathsf{mob}[\,\mathcal{G}\,]])\,(taxi[\,] \mid y[\,\mathsf{in}\, taxi\,])$$

The protocol consists of two exchanges: a client n with type $\mathsf{amb}[H, \mathsf{mob}[\,\mathcal{H}\,]]$ sends a group name G which belongs to $\mathcal{H}$ and its name n; the server creates a taxi specialised for n. Some security issues

arise. Firstly, G should be a fresh (i.e. restricted) group name, and again this forces to restrict n as well. Secondly, by communicating group names we expose ourselves to the risk of unintentionally disclosing G to malicious eavesdroppers. We definitely need to devise more sophisticated protocols. In any case, a brief reflection on the guarantees that a satisfactory type system is expected to make, shows the need to track information about the group names *GTaxiServ* may receive. That is, communications have to be typed as well as movements. It then follows that *DTaxiServ* can not be written as above: communicating a group and an ambient name to the same ambient is impossible, since only one topic of conversation is allowed inside an ambient [9]. Finally, group types would have the form $\mathsf{gr}[\mathcal{G}]$, for $\mathcal{G}$ a set of groups (which incidentally is similar to the approach of [15]). But then, we would be essentially using (group) dependent types...

The type system we propose for dynamic types is a natural extension of the one we illustrated above, which only deals with mobility. Namely, we simply require that communications of ambient names and variables be reflected in the types. For instance, the dynamic taxi server will have the form:

$$!(x)\mathit{TaxiServ}(x) = !(x)(\nu\, \mathit{taxi} : \mathsf{amb}[\mathsf{mob}[\{\mathit{top}\}, \{x\}]])\,(\mathit{taxi}[\,] \mid x[\mathsf{in}\ \mathit{taxi}]).$$

Communication increases the complexity of the type system, because the rules need to track information about receivers, too. It makes little sense to type communication via the usual exchange types, because receiving different names may lead to orthogonal behavioural and mobility properties. Subtyping does not help towards a unifying treatment (cf. Example 2). We approach the problem by tracking the names that may be received at a given variable. This enriches ambient types which, in addition to a mobility component, acquire a communication one. A typing assignment $n : \mathsf{amb}[\,\mathsf{mob}[\mathcal{P}, C], \mathsf{com}[\mathcal{E}, \mathcal{L}]\,]$, where $\mathcal{E}$ and $\mathcal{L}$ are sets of ambient names, means that n may be communicated inside any ambient in $\mathcal{E}$, and dually, that any ambient in $\mathcal{L}$ may be communicated within n. It is important to remark that even if such components only carry finite sets, the volume of information exchanged is in general not bounded. Indeed, the joint effect of name creation and the use of abstract names, allows to distribute new communication capabilities at run time, and communicate infinitely many names.

Plan. The paper proceeds as follows. Section 2 presents a simple type system with dependent types. We focus on mobility, that is the Ambient calculus with no communication at all. Then, in Section 3, we investigate dynamic types allowing communication of ambient names. For the sake of simplicity, we do not address the issue of communication of capabilities, even though this can easily be integrated following our approach to a dependently typed ambients. The appendices contain complementary material which can safely skipped. Sections A and B lists syntax and semantics of the Mobile Ambients; Section C give the full typing proof of the (dynamic) taxi servers of Sections 2 and 3; Section D sketches the main proofs.

2 A Simple Dependent Type System

In the paper we use the standard Ambient calculus with *asynchronous*, *monadic* communication. (We remark that our results do not depend on such choice.) For the reader's convenience, syntax and reduction semantics are reported in the Appendix. In this section we consider the pure Ambient calculus, that is the calculus restricted to the mobility features. Communication will be studied in Section 3.

2.1 Types and definitions

The syntax of types is given in Figure 1 where N denotes an infinite set of *abstract ambient names* and the symbol $\star$ stands for the *self*-ambient, whose meaning is explained below. The type $\mathsf{cap}[\mathcal{P}]$ denotes the type of a capability which can be exercised within any ambient whose name occurs in $\mathcal{P}$. An ambient type has, for the moment, just one component: a mobility type. Ambient n with mobility type $\mathsf{mob}[\mathcal{P}, C]$ is allowed to be a sub-ambient of all ambients whose name occurs in $\mathcal{P}$; i.e. $\mathcal{P}$ is the set of *possible parents* of n. Moreover, an ambient is allowed to occur as sub-ambient of n if its name occurs in C, the set of *possible children* of n. We define some useful notations on types:

$$\mathsf{amb}[M]^{\mathsf{mob}} = M \qquad \mathsf{mob}[\mathcal{P}, C]^{\uparrow} = \mathcal{P} \qquad \mathsf{mob}[\mathcal{P}, C]^{\downarrow} = C$$

Ambient (concrete) names	$n, m, \ldots \in \mathcal{N}$			*Abstract names*	$\mathsf{n}, \mathsf{m}, \ldots \in \mathsf{N}$		
Capability types	K	::=	$\mathsf{cap}[\mathcal{P}]$	*Mobility types*	M, N	::=	$\mathsf{mob}[\mathcal{P}, C]$
Ambient types	A	::=	$\mathsf{amb}[M]$	where $\mathcal{P}, C \subseteq \mathcal{N} \cup \mathsf{N} \cup \{\star\}$			

Figure 1: Types

We use two kinds of typing contexts: *abstract contexts* (ranged over by $\Xi, \Theta, \ldots$) and *concrete contexts* (ranged over by $\Gamma, \Delta, \ldots$), which map respectively abstract and concrete names to ambient types. We use Π to denote either an abstract or a concrete context. We note by (Π, Π') the union of disjoint contexts of the same kind. According to the informal meaning of types, type assignments in concrete typing contexts are related to each other. Consider for instance

$$\Gamma = n : \mathsf{amb}[\,\mathsf{mob}[\mathcal{P}, C]\,],\ m : \mathsf{amb}[\,\mathsf{mob}[\emptyset, \{n\}]\,],$$

where the type of m allows it to have n as a child. Coherently, the type of n should allow n to have m as a parent, i.e. $m \in \mathcal{P}$. This can be expressed by the central notion of *context update* $\Gamma^{(n:A)}$, which updates Γ with respect to a fresh type assignment $n : A$:

$$(\Gamma, \Delta)^{(n:A)} = \Gamma^{(n:A)}, \Delta^{(n:A)}$$
$$(m : \mathsf{amb}[M_0])^{(n:\mathsf{amb}[N])} = m : \mathsf{amb}[M_1],$$

where

$$M_1^{\uparrow} = \begin{cases} M_0^{\uparrow} \cup \{n\} & \text{if } m \in N^{\downarrow} \\ M_0^{\uparrow} & \text{otherwise} \end{cases} \qquad \text{and} \qquad M_1^{\downarrow} = \begin{cases} M_0^{\downarrow} \cup \{n\} & \text{if } m \in N^{\uparrow} \\ M_0^{\downarrow} \end{cases}$$

Context update is pivotal in our type systems to express the typing of name creation. We define union (resp. inclusion and equality) of types as component-wise set union (resp. inclusion and equality); the notation $nm(A)$ (resp. $an(A)$) stands for the set of (abstract) names occurring in A. It is extended to all types and typing contexts.

2.2 The type system

Our type system deals with typing judgements for values and processes, that is

$$\Gamma \vdash^{\Theta} V : T \qquad \text{and} \qquad \Gamma \vdash_{a}^{\Xi;\Theta} P,$$

where T is either an ambient or a capability type. The first judgement reads as "V has type T with respect to the concrete context Γ and the abstract context Θ." In the second one, ambient name a stands for the ambient where P is running, which we call the *current location* of P. In other words, P is guaranteed to be well-typed if run in a. Abstract contexts Ξ and Θ are used to account for potential name creations: those arising from P are registered in the *local* abstract context Ξ, those performed by the environment appear in the *external* abstract context Θ. The role of such contexts is to "internalise" (a dynamic notion of) group names, which move from being part of the language to being a inner mechanism of the type system.

Example 1. Let

$$\mathit{TaxiServ}(n) = !(\nu\, \mathit{taxi} : A)\,(\mathit{taxi}[\,] \mid n[\mathsf{in}\, \mathit{taxi}]), \qquad \text{for} \quad A = \mathsf{amb}[\,\mathsf{mob}[\{\mathit{top}\}, \{n\}]\,].$$

Let $Q = n[\,\mathsf{in}\, n \mid m[\mathsf{out}\, n.\mathsf{out}\, n]\,]$. We study the system $P = \mathit{TaxiServ}(n) \mid Q$, which we assume running in some ambient named *top*. The server $\mathit{TaxiServ}(n)$ creates an ambient *taxi* whose type allows it to accept only n as a child. The scope (or "visibility") of *taxi* is $(\mathit{taxi}[\,] \mid n[\mathsf{in}\, \mathit{taxi}])$. We assume that Q is an ambient n which may move in an ambient of the same name n and contains a child ambient m, willing to escape

$$\frac{A \in \mathit{Types}(\Gamma,\Theta,a)}{\Gamma \vdash^{\Theta} a : A}\ (\textsc{VAmb}) \qquad \frac{\Gamma \vdash^{\Theta} U : K, V : K}{\Gamma \vdash^{\Theta} U.V : K}\ (\textsc{VPfx}) \qquad \frac{\Gamma \vdash^{\Theta} a : A, a_i : A_i \qquad A^{\mathsf{mob}} \subseteq A_i^{\mathsf{mob}\uparrow}\ \forall i \in \{1,\ldots,n\}}{\Gamma \vdash^{\Theta} \mathsf{out}\, a : \mathsf{cap}[\{a_1,\ldots,a_n\}]}\ (\textsc{VOut})$$

$$\frac{\Gamma \vdash^{\Theta} a : A \qquad \mathcal{P} \subseteq A^{\mathsf{mob}\downarrow}}{\Gamma \vdash^{\Theta} \mathsf{in}\, a : \mathsf{cap}[\mathcal{P}]}\ (\textsc{VIn}) \qquad \frac{\Gamma \vdash^{\Theta} a : A, a_i : A_i \qquad A^{\mathsf{mob}} \subseteq A_i^{\mathsf{mob}} \qquad \forall i \in \{1,\ldots,n\}}{\Gamma \vdash^{\Theta} \mathsf{open}\, a : \mathsf{cap}[\{a_1,\ldots,a_n\}]}\ (\textsc{VOpen})$$

$$\frac{\Gamma \vdash_a^{\Xi;\Theta} P \qquad \Gamma \vdash^{\Xi,\Theta} a : A \qquad b \in A^{\mathsf{mob}\uparrow}}{\Gamma \vdash_b^{\Xi;\Theta} a[P]}\ (\textsc{Amb}) \qquad \frac{}{\Gamma \vdash_a^{\emptyset;\Theta} \mathbf{0}}\ (\textsc{Nil}) \qquad \frac{\Gamma \vdash_a^{\Xi;\Theta} P \qquad \Gamma \vdash^{\Theta,\Xi} V : \mathsf{cap}[a]}{\Gamma \vdash_a^{\Xi;\Theta} V.P}\ (\textsc{Pfx})$$

$$\frac{\Gamma \vdash_a^{\Xi_1;\Xi_2,\Theta} P \qquad \Gamma \vdash_a^{\Xi_2;\Xi_1,\Theta} Q}{\Gamma \vdash_a^{\Xi_1,\Xi_2;\Theta} P \mid Q}\ (\textsc{Par}) \qquad \frac{\Gamma^{(n:A)}, n : A\{n/\star\} \vdash_a^{\Xi\{n/n\};\Theta} P}{\Gamma \vdash_a^{n:A,\Xi;\Theta} (\nu\, n : A)\, P}\ (\textsc{Res}) \qquad \frac{\Gamma \vdash_a^{\Xi;\Theta,\Xi\sigma} P}{\Gamma \vdash_a^{\Xi;\Theta} !P}\ (\textsc{Rep})$$

Figure 2: Simple Type System

twice out n. Thus, m must be allowed to run at the same level of n, and a type system should ensure that any possible parent for n is also a possible one for m. This leads, for instance, to the following assignment.

$$\Gamma = \begin{cases} \mathit{top} : \mathsf{amb}[\ \mathsf{mob}[\emptyset, \{n, m\}]\ ], \\ \quad n : \mathsf{amb}[\ \mathsf{mob}[\{\mathit{top}, n\}, \{n, m\}]\ ], \\ \quad m : \mathsf{amb}[\ \mathsf{mob}[\{\mathit{top}, n\}, \emptyset]\ ]. \end{cases}$$

In $(\mathit{taxi}[\,] \mid n[\mathsf{in}\, \mathit{taxi}])$, ambient n gains access to *taxi* by means of name creation, viz. *taxi*, and the type assignment must evolve to Δ below (which actually is of the form $\Gamma^{(\mathit{taxi}:A)}, \mathit{taxi} : A$).

$$\Delta = \begin{cases} \mathit{top} : \mathsf{amb}[\ \mathsf{mob}[\emptyset, \{n, m, \mathit{taxi}\}]\ ], \\ \quad n : \mathsf{amb}[\ \mathsf{mob}[\{\mathit{top}, n, \mathit{taxi}\}, \{n, m\}]\ ], \\ \quad m : \mathsf{amb}[\ \mathsf{mob}[\{\mathit{top}, n\}, \emptyset]\ ], \\ \mathit{taxi} : \mathsf{amb}[\ \mathsf{mob}[\{\mathit{top}\}, \{n\}]\ ]. \end{cases}$$

However, running P may obviously lead to ambient m becoming a child of *taxi*, thus violating the specification expressed by the type of *taxi*. Indeed, we have

$$P \to \mathit{TaxiServ}(n) \mid \underbrace{(\nu\, \mathit{taxi} : A)\, (\mathit{taxi}[\,] \mid n[\mathsf{in}\, \mathit{taxi}]) \mid Q}_{P'} \qquad \text{and}$$

$$P' \equiv (\nu\, \mathit{taxi} : A)\, (\mathit{taxi}[\,] \mid n[\mathsf{in}\, \mathit{taxi}] \mid n[\ \underline{\mathsf{in}\, n} \mid m[\mathsf{out}\, n.\mathsf{out}\, n]\ ]) \to^{*} (\nu\, \mathit{taxi} : A)\, (\mathit{taxi}[\ m[\,] \mid n[\ n[\,]\ ]\ ]).$$

Therefore, P must be considered ill-typed. A naive approach would however try to typecheck $(\mathit{taxi}[\,] \mid n[\mathsf{in}\, \mathit{taxi}])$ (against Δ) and Q (against Γ) independently, and therefore accept P. Indeed, from Q's point of view, *taxi* does not exist (it is bound in $\mathit{TaxiServ}(n)$), and Q behaves well. From the viewpoint of $\mathit{TaxiServ}(n)$, although *taxi* exists, the specification given by its type is respected: ambient n is allowed to move into *taxi*. Considering $\mathit{TaxiServ}(n)$ and Q as stand-alone processes prevents from realising that their interaction may lead to a breach of the intended access policy. □

Example 1 motivates the use of abstract contexts. They are a means to record the new capabilities which may potentially arise from name creations performed in external processes. Since such names are bound, they cannot be referred to by name in typing contexts: we use *abstract names* to represent them. The typechecking of process Q in Example 1 must then be carried out with an *external* abstract context $\Theta = \mathsf{taxi} : A$, representing the potential creation of a name of type A, and an empty *local* abstract context, as Q does not create names. In other words, we are led to prove $\Gamma \vdash_{\mathit{top}}^{\emptyset;\Theta} Q$. From Γ and Θ, we can deduce a more informative type for n, viz. its *global type* $\mathsf{amb}[\ \mathsf{mob}[\{\mathit{top}, n, \mathsf{taxi}\}, \{n, m\}]\ ]$, which states that n is allowed to run within *top*, n and some ambient taxi, to be created by its environment and whose actual name we do not known yet. (We stress that the name taxi is just a placeholder; the information that leads to the global type is carried by A.) Since m does not appear in Θ, its global type remains $\mathsf{amb}[\mathsf{mob}[\{\mathit{top}, n\}, \emptyset]]$, and we can conclude that Q is ill-typed. Indeed, there exists a possible parent of n which is not a possible one for m, namely taxi.

We define the *symmetric type* $\Pi[\alpha]$ of a name α with respect to a typing context Π, as $\Pi[\alpha] = \mathsf{amb}[\mathsf{mob}[\mathcal{P}, C]]$, where $\mathcal{P} = \{\beta \mid \alpha \in \Pi(\beta)^{\mathsf{mob}\downarrow}\}$ and $C = \{\beta \mid \alpha \in \Pi(\beta)^{\mathsf{mob}\uparrow}\}$.

Definition 1. The *global type* of a name α with respect to typing contexts Γ and Θ is defined as

$$gt(\Gamma;\Theta)(\alpha) = \begin{cases} \Gamma(\alpha) \cup \Theta[\alpha] & \text{if } \alpha \in \mathcal{N} \\ \Theta(\alpha)\{\alpha/\star\} \cup \Theta[\alpha] & \text{if } \alpha \in \mathsf{N} \end{cases} \qquad \square$$

We define $\mathit{Types}(\Gamma, \Theta, a) = \{gt(\Gamma;\Theta)(a)\}$. (We use a singleton set here for uniformity with next section.) Turning back to the previous discussion, one can verify that indeed

$$gt(\Gamma;\Theta)(n) = \mathsf{amb}[\mathsf{mob}[\{top, n, \mathsf{taxi}\}, \{n, m\}]].$$

The notion of symmetric type leads to the obvious definition of *symmetric typing context*.

Definition 2. A concrete typing context Γ is said *symmetric* if, for all $n \in nm(\Gamma)$, we have $\Gamma(n) = \Gamma[n]$. $\square$

Symmetric typing context formalises the notion of "consistency" of a typing context. It ensures that a name n has a type allowing m as a child of n if and only if m itself has a type allowing n as a parent. It also guarantees that a typing context is "complete," i.e. that any name occurring in it has a type assignment. In the following we will assume all concrete typing contexts to be symmetric, and all abstract contexts to be "complete" for abstract names, that is $dom(\Theta) = an(\Theta)$.

Symmetric typing replicates parenthood information both in children and in parents types. Nevertheless, both components of mobility types are necessary to give sufficient access control in the presence of name creation. We remark that comparable mechanisms play in groups based approaches via the assignment of names to groups. Using the types of [22] to exemplify, recall that $\mathcal{G}$ in $n : \mathsf{amb}[G, \mathsf{mob}[\mathcal{G}]]$ is the set of groups of ambients allowed as parents of n. Therefore, assigning n to G to has the effect of determining the children allowed of n: namely, those ambients whose mobility component contains G.

Let us now comment on the rules of the Figure 2, starting with the judgements for values. (A complete derivation is exemplified in §C.) We look at the rules from conclusions to premises. A judgement $\Gamma \vdash^{\Theta} U : T, V : T'$ stands for $\Gamma \vdash^{\Theta} U : T$ and $\Gamma \vdash^{\Theta} V : T'$. Axiom (Vamb) simply gives the global type of a name, while (VPfx) asserts that the prefix $U.V$ has the capability type K if both U and V have such type. In order to type a $\mathsf{out}\, a$ performed in some ambient a_i, (Vout) checks that the possible parents of a are allowed for a_i (for $i \in \{1, \ldots, n\}$). Rule (VIn) typechecks the capability of ambient b (a member of $\mathcal{P}$) to move to ambient a. This is allowed if b is a possible child of a. Finally, (VOpen) states that some ambient a_i can open a if both the allowed parents and children of a are allowed for a_i, $i \in \{1, \ldots, n\}$.

A process is always typed with respect to a current location. Process $a[P]$ is well-typed in ambient b (rule Amb) if b is allowed as a's parent and P is well-typed in a. Process $\mathbf{0}$ is always well-typed with local abstract context empty. Process $V.P$ is well-typed in a if P is well-typed in a and V is a capability that can be exercised in a. In order to type a parallel composition of processes (rule (Par)), the local abstract context must be split in two parts: in the typing of each component one of these remains local, the other becomes external.

Rule (Res) deserves a close analysis. The typing of $(\nu\, n : A)\, P$ requires the local abstract context to assign type A to some abstract name (here n). The rule consumes such assignment, and P is then typed with its concrete typing context updated with n's typing. We apply the substitution $\{n/\star\}$ to A, where $\star$ is an "alias" for the self ambient (n here). This is necessary, since in the conclusion n cannot occur in A. Indeed, we make the usual assumption that a bound name does not occur in the typing contexts and in the current location (which here means $n \neq a$). Finally, the substitution $\{n/\mathsf{n}\}$ is applied to the local abstract context, as types in Ξ may refer to n. This would be the case of, e.g., the term

$$(\nu\, n : \mathsf{amb}[\,\mathsf{mob}[\{top\}, \emptyset]\,])\,(\nu\, m : \mathsf{amb}[\,\mathsf{mob}[\{n\}, \emptyset]\,])\, P$$

typed with the local abstract context $\mathsf{n} : \mathsf{amb}[\,\mathsf{mob}[\{top\}, \emptyset]\,]$, $\mathsf{m} : \mathsf{amb}[\,\mathsf{mob}[\{\mathsf{n}\}, \emptyset]\,]$.

In Rule (Rep) we assume that σ is an *abstract renaming*. By this we mean an injective substitution whose domain is the set of abstract names occurring in Ξ and whose codomain is a set of fresh abstract

names. In other words, if σ is an abstract renaming, then $\Xi\sigma$ is a fresh copy of Ξ. Process $!P$ can be seen as an infinite parallel composition of copies of P. Therefore, typing $!P$ is equivalent to typing P in an environment which can provide new capabilities as P can. These are represented by the local abstract context of $!P$, which explains why we add a copy of the local abstract context to the external one. It is easy to prove that one copy is sufficient (cf. Lemmas 2 and 3 in §D).

It is worth remarking that there are behavioural properties which are expressible with groups but not with this system of dependent types. This is because in the present system, name creation assigns types which may only refer to names already in the scope of the created name. For instance, in

$$(\nu\, n : A)\, P \mid (\nu\, m : A')\, Q$$

m (resp. n) can not occur in A (resp. A'). This means that n and m will not be able to interact. With group types one may use group names shared by m and n, i.e. whose scope contains both names. The extension of the type system to dynamic types introduced in the next section circumvents the problem by the usual mechanisms of scope extrusion in name passing calculi. Indeed, in order for m to give (and acquire) new capabilities to n, we send n to m, which then may refer in A' to the received name.

3 Dynamic Types

As illustrated in the previous section, name creation is itself a means to dynamically change ambient capabilities. In the type system, abstract names track the relevant changes outside the actual scope of the name. New names may refer directly in their types to known ambient names. For instance, the taxi server

$$(\nu\, taxi : \mathsf{amb}[\mathsf{mob}[\{top\}, \{n\}]])\,(taxi[\,] \mid n[\mathsf{in}\, taxi])$$

creates a name *taxi* which may have n as a child. At the same time, the type of n is enriched with the capability to have *taxi* as a parent. This process, however, is restricted in that it provides a private taxi for one and only one ambient, namely n. By enabling communication of ambient names, types in name creation constructs may also refer to a received name, so boosting the dynamic aspects of the calculus. This allows, for instance, to write a *generic* taxi server which dynamically provides private taxis for any ambient whose name is received by a communication:

$$DTaxiServ = !(x)(\nu\, taxi : \mathsf{amb}[\,\mathsf{mob}[\{top\}, \{x\}]\,])\,(taxi[\,] \mid x[\mathsf{in}\, taxi]),$$

Such an increase in dynamic adaptation, and therefore in expressiveness, comes with a corresponding increase in the complexity of the typing system. There are two reasons:

- firstly, types may now refer to ambients indirectly, via variables;
- secondly, upon communication a variable may become instantiated by a name or by another, thus leading to different capabilities, that is different access control policies. Moreover, such policies are not necessarily comparable, which, for instance, makes subtyping useless.

Example 2. Let *DTaxiServ* be as above, and consider

$$P = \langle n \rangle \mid \langle m \rangle \mid DTaxiServ.$$

Process P may evolve to either

$$P_1 = \langle n \rangle \mid taxi[\,] \mid m[\mathsf{in}\, taxi] \mid DTaxiServ \quad \text{or} \quad P_2 = \langle m \rangle \mid taxi[\,] \mid n[taxi] \mid DTaxiServ$$

according to whether *DTaxiServ* receives m or n. As regards to the type assigned to *taxi*, in P_1 only m – that is the received name – is allowed to go inside *taxi*, whereas in P_2 only n is. Such situations are orthogonal and thus incomparable: in the first one, m acquires a new capability ('*CanMoveTo*' *taxi*) and n remains unchanged, whereas in the second it is the other way around. This means that the type system will have to deal with all possible communications. □

Example 2 suggests that an ambient name may have different possible types depending on the communications that may happen.

Abstract variables	$\mathsf{x}, \mathsf{y}, \ldots \in \mathsf{X}$			*Capability types*	K	::=	$\mathsf{cap}[\mathcal{P}]$
Mobility types	M, N	::=	$\mathsf{mob}[\mathcal{P}, C]$	*Communication types*	C	::=	$\mathsf{com}[\mathcal{E}, \mathcal{L}]$
Ambient types	A	::=	$\mathsf{amb}[M, C]$	*Variable types*	B	::=	$\mathsf{var}[\mathcal{B}]$

where $\mathcal{P}, C \subseteq \mathcal{N} \cup \mathsf{N} \cup \mathcal{X} \cup \mathsf{X} \cup \{\star\}$ and $\mathcal{B}, \mathcal{E}, \mathcal{L} \subseteq \mathcal{N} \cup \mathsf{N} \cup \{\star\}$

Figure 3: New types for communication

3.1 New types and definitions

The needed additional types are given in Figure 3, where X is an infinite set of *abstract variables*. Ambient types have now two components: one for mobility, which remains unchanged, and one for communication. Following our "symmetric style" for types, a communication type consists of two sets of names: an *external* one, $\mathcal{E}$, which describes the ambients where the name in object may be communicated, and a *local* one, $\mathcal{L}$, which describes the names which may be communicated within the object ambient. For instance, if n has type $\mathsf{amb}[M, \mathsf{com}[\{m\}, \{o\}]]$, then n can be exchanged inside m, and o can be communicated inside n; two terms which satisfy such specification appear below.

$$m[\langle n \rangle] \quad \text{and} \quad n[\langle o \rangle]$$

A variable type is the set of ambients where a variable may be bound. For instance, in $n[(x)P]$ the variable x may have type $\mathsf{var}[\{n\}]$. Because we deal with an ambient calculus with the open capability, a variable may of course be bound in several places. Variable x in

$$n[\langle o_1 \rangle \mid \mathsf{open}\, m \mid m[\langle o_2 \rangle \mid (x)P]$$

may be bound in n or in m, depending on whether m is opened before x is bound or not. The type of x in the term above must therefore be $\mathsf{var}[\{m, n\}]$.

We remark that, contrary to usual type systems, but as in [1], we do not use the so-called *exchange* types, which build on the notion of "topic of conversation" permitted within a given ambient. This is a particular type (modulo subtyping) which all processes within that ambient agree to exchange. Indeed, suppose that n is an ambient whose exchange type is A, and m_1 and m_2 have type A. Then, the term

$$n[\langle m_1 \rangle \mid \langle m_2 \rangle \mid (x : A)P]$$

would be well-typed. However, if an external process gives a new capabilities to m_1 via name creation, then $\langle m_1 \rangle$ may become ill-typed. An instance of this is the following term.

$$(\nu\, o : \mathsf{amb}[\mathsf{mob}[\{m_1\}, \emptyset], C])\, Q \mid n[\langle m_1 \rangle \mid \langle m_2 \rangle \mid (x : A)P]$$

Here, $\langle m_2 \rangle$ is still well-typed, but $\langle m_1 \rangle$ is manifestly not. In fact, after scope extrusion, m_1 has not anymore type A, but A enriched with the capability to admit o as a child, which leads to a type error when trying to bind x to m_1. Our type system does not feature uniform exchange types, but it allows in principle to bind a variable to names which may have completely different types. This also leads to an increase in expressiveness.

Assuming the set of possible communicable ambient names to appear in types may at first appear to give a very restricted form of communication, where only a finite number of names are communicable in a given ambient. Due to the dynamic nature of types, this is actually not the case: name creation can give new communication capabilities to existing ambients. For instance, if ambient n has a communication type $\mathsf{com}[\emptyset, \{o\}]$ – that is, only o may be sent in n – the creation of name m with communication type $\mathsf{com}[\{n\}, \emptyset]$ gives n the new capability to have m has communicable ambient. Combining name creation with replication leads to potentially infinite communicable names in a given ambient.

Finally, we remark that variable and communication types, contain only ambient names and no variables. This means that communication is forbidden inside ambients created using a received name, as

in $(x)x[P]$. We embraced such restriction for the sake of simplicity: allowing variables in such types is possible, at the price of a more complex definition of the set of types (Definition 7) and of additional side conditions in the type system rules.

As for mobility types, we define corresponding useful notations for communication types.

$$\mathsf{amb}[M, C]^{\mathsf{com}} = C \qquad \mathsf{com}[\mathcal{E}, \mathcal{L}]^{\uparrow} = \mathcal{E} \qquad \mathsf{mob}[\mathcal{E}, \mathcal{L}]^{\downarrow} = \mathcal{L}.$$

Now, concrete (resp. abstract) typing contexts may also map concrete (resp. abstract) variables to variable types. As in Section 2, typing contexts have to be consistent with communication types. The typing context update is therefore extended as follows:

$$\begin{aligned}(\Gamma, \Delta)^{(n:A)} &= \Gamma^{(n:A)}, \Delta^{(n:A)}\\ (x : B)^{(n:A)} &= x : B\\ (m : \mathsf{amb}[M_0, C_0])^{(n:\mathsf{amb}[M,C])} &= m : \mathsf{amb}[M_1, C_1],\end{aligned}$$

where M_1 is as before, and C_1 is defined analogously, i.e.

$$C_1^{\uparrow} = \begin{cases} C_0^{\uparrow} \cup \{n\}, & \text{if } m \in C^{\downarrow},\\ C_0^{\uparrow}, & \text{otherwise;}\end{cases} \qquad C_1^{\downarrow} = \begin{cases} C_0^{\downarrow} \cup \{n\}, & \text{if } m \in C^{\uparrow},\\ C_0^{\downarrow}, & \text{otherwise.}\end{cases}$$

Updating has no effect on (the type of) variables because we only require consistency for concrete ambient names. The notion of *symmetric type* has now to take into account the communication component. It is defined by

$$\Pi[\alpha] = \mathsf{amb}[\,\mathsf{mob}[\mathcal{P}, C], \mathsf{com}[\mathcal{E}, \mathcal{L}]\,],$$

where

$$\begin{aligned}\mathcal{P} &= \{\beta \in \mathsf{N} \cup \mathcal{N} \mid \alpha \in \Pi(\beta)^{\mathsf{mob}^{\downarrow}}\} \qquad C = \{\beta \in \mathsf{N} \cup \mathcal{N} \mid \alpha \in \Pi(\beta)^{\mathsf{mob}^{\uparrow}}\}\\ \mathcal{E} &= \{\beta \in \mathsf{N} \cup \mathcal{N} \mid \alpha \in \Pi(\beta)^{\mathsf{com}^{\downarrow}}\} \qquad \mathcal{L} = \{\beta \in \mathsf{N} \cup \mathcal{N} \mid \alpha \in \Pi(\beta)^{\mathsf{com}^{\uparrow}}\}\end{aligned}$$

No variable occurs in symmetric types, therefore the notion of symmetric typing context must be defined accordingly.

Definition 3. A concrete typing context Γ is *symmetric* if, for all $n \in nm(\Gamma)$, we have $\Gamma(n) - (\mathsf{X} \cup \mathcal{X}) = \Gamma[n]$.

Here $\Gamma(n) - (\mathsf{X} \cup \mathcal{X})$ denotes the type of n in Γ with all variables removed. Definition 1 of global types for ambient names remains unchanged; we complete it below for variables.

Definition 4. The *global type* of a variable α with respect to typing contexts Γ and Θ is defined by

$$gt(\Gamma; \Theta)(\alpha) = \begin{cases} \Gamma[\alpha] \cup \Theta[\alpha] & \text{if } \alpha \in \mathcal{X}\\ \Theta[\alpha] & \text{if } \alpha \in \mathsf{X}\end{cases} \quad \square$$

The global type of a variable is the ambient type constructed from the capabilities the variable is given by typing contexts. In case of an abstract variable, only the abstract context provides the information, as no abstract variable occurs in the concrete context.

We finally define the *local type* of a name, as the usual notion of type provided by a typing context.

Definition 5. The *local type* of a name α with respect to typing contexts Γ and Θ is defined by

$$lt(\Gamma; \Theta)(\alpha) = \begin{cases} \Gamma(\alpha) & \text{if } \alpha \in dom(\Gamma)\\ \Theta(\alpha) & \text{if } \alpha \in dom(\Theta)\\ \text{undefined} & \text{otherwise.}\end{cases}$$

For $B = \mathsf{var}[\mathcal{B}]$, we usually identify B and $\mathcal{B}$ writing, for instance, $\alpha \in B$ instead of $\alpha \in \mathcal{B}$.

$$\frac{\begin{array}{c}\text{for any } \alpha,\ \text{if } lt(\Gamma;\Theta)(\alpha) = B \text{ then } a \in B \text{ iff } a_i \in B \\ \Gamma \vdash^{\Theta} a : A, a_i : A_i \qquad A^{\mathsf{mob}} \subseteq A_i^{\mathsf{mob}} \qquad A^{\mathsf{com}} = A_i^{\mathsf{com}} \qquad \forall i \in \{1, \ldots n\}\end{array}}{\Gamma \vdash^{\Theta} \mathsf{open}\, a : \mathsf{cap}[\{a_1, \ldots, a_n\}]}\ (\textsc{VOpen'})$$

$$\frac{\Gamma, x : B \vdash_a^{\Xi\{x/\mathsf{x}\};\Theta} P \qquad a \in B}{\Gamma \vdash_a^{\mathsf{x}:B,\Xi;\Theta} (x)P}\ (\textsc{Input}) \qquad \frac{\Gamma \vdash^{\Theta} V : A \qquad a \in A^{\mathsf{com}\uparrow}}{\Gamma \vdash_a^{\emptyset;\Theta} \langle V \rangle}\ (\textsc{Ouput})$$

Figure 4: Revised typing system and additional ones for communication

3.2 Revised typing system

The type system for the calculus with communication of ambient names is obtained from Figure 2 adding rules (Input) and (Ouput) for communication in Figure 4, and replacing (VOpen) with (VOpen').

Rule (VOpen') has two new conditions. The first verifies that the communication type is the same in the opened ambient and in the enclosing one. The condition on the top line checks that variables may be bound in the opened ambient if and only if they may in the opening one. Rule (Input) is similar to (Res): we pick up an abstract variable from the local abstract context whose type contains the current location. We do not perform any context update, since such updates only concern ambient names. Finally, rule (Output) says that we can send the value V inside a if that is allowed by the type of V.

The most significant revision is in the definition of $\mathit{Types}(\Gamma, \Theta, a)$, which is not anymore just a singleton, since names may now have several types. This means that any typing derivation with an axiom (VAmb) as a premise has to be read as: "for all types A such that $\Gamma \vdash^{\Theta} a : A$." Before we give the formal definition of $\mathit{Types}(\Gamma, \Theta, a)$, let us focus on an example to gather some intuition.

Example 3. Let us consider a non-replicated version of the taxi server of Example 2, but with the new communication types:

$$\mathit{DTaxiServ}_1 = (x)(\nu\, \mathit{taxi} : \mathsf{amb}[M, C])\,(\mathit{taxi}[\,] \mid x[\mathsf{in}\, \mathit{taxi}]),$$

with $M = \mathsf{mob}[\{\mathit{top}\}, \{x\}]$ and $C = \mathsf{com}[\emptyset, \emptyset]$. Let $P = \langle n \rangle \mid \langle m \rangle \mid \mathit{DTaxiServ}_1$, and suppose to work with the following typing context which assigns types to the free ambient names:

$$\Gamma = \left\{ \begin{array}{l} n : A_n, \\ m : A_m, \\ \mathit{top} : \mathsf{amb}[\,\mathsf{mob}[\emptyset, \{m, n\}], \mathsf{com}[\emptyset, \{m, n\}]\,], \end{array} \right.$$

where

$$A_n = \mathsf{amb}[\,\mathsf{mob}[\{\mathit{top}\}, \{m\}], \mathsf{com}[\{\mathit{top}\}, \emptyset]\,] \quad \text{and} \quad A_m = \mathsf{amb}[\,\mathsf{mob}[\{\mathit{top}, n\}, \emptyset], \mathsf{com}[\{\mathit{top}\}, \emptyset]\,].$$

Here, n and m can be communicated in *top*, and have *top* as a parent. Moreover, n may have m as child and, consequently, m may have n as parent. One can verify that Γ is symmetric. In order to type $\mathit{DTaxiServ}_1$ we need an abstract context which assigns variable type $\mathsf{var}[\{\mathit{top}\}]$ to an abstract variable, say x, because x may be bound in *top*. Also, it has to assign an ambient type A to an abstract ambient name, say taxi. Type A has to match $\mathsf{amb}[M, C]$, but we cannot directly use the latter, since M contains x which is initially bound. However, we can refer to the abstract name x, meant to correspond to x. Therefore the abstract context is

$$\Xi = \mathsf{x} : \mathsf{var}[\{\mathit{top}\}], \mathsf{taxi} : \mathsf{amb}[N, C],$$

for $N = \mathsf{mob}[\{\mathit{top}\}, \{\mathsf{x}\}]$. It is easy to check that the proof of $\Gamma \vdash_{\mathit{top}}^{\Xi;\emptyset} \mathit{DTaxiServ}_1$ leads to the judgement $\Delta \vdash_{\mathit{top}}^{\emptyset;\emptyset} (\mathit{taxi}[\,] \mid x[\mathsf{in}\, \mathit{taxi}])$, by application of the rules (Input) and (Res), where

$$\Delta = \left\{ \begin{array}{l} n : A_n, \\ m : A_m, \\ \mathit{top} : \mathsf{amb}[\,\mathsf{mob}[\emptyset, \{m, n, \mathit{taxi}\}], \mathsf{com}[\emptyset, \{m, n\}]\,], \\ x : \mathsf{var}[\{\mathit{top}\}], \\ \mathit{taxi} : \mathsf{amb}[\,\mathsf{mob}[\{\mathit{top}\}, \{x\}], \mathsf{com}[\emptyset, \emptyset]\,]. \end{array} \right.$$

In $(taxi[] \mid x[taxi])$, x is an ambient whose global *ambient* type is

$$A_x = \Delta[x] = \mathsf{amb}[\ \mathsf{mob}[\{taxi\}, \emptyset], \mathsf{com}[\emptyset, \emptyset]\ ].$$

This is actually the least type assignable to x, since x is intended to be instantiated by an ambient name. Indeed, x may be bound to n or m, which means that the global types it may possibly assume include

$$A_x \cup A_n = \mathsf{amb}[\ \mathsf{mob}[\{top, taxi\}, \{m\}], \mathsf{com}[\{top\}, \emptyset]\ ],$$

if n is received for x, and

$$A_x \cup A_m = \mathsf{amb}[\ \mathsf{mob}[\{top, taxi, n\}, \emptyset], \mathsf{com}[\{top\}, \emptyset]\ ],$$

if m is received for x. Type $A_x \cup A_n$ is possible for n in the scope of the restriction. Indeed, if n is received, then the newly created ambient *taxi* gives to n – the received name – the capability to be its child. Outside the scope of the restriction, a possible type for n is rather

$$\Xi[\mathsf{x}] \cup A_n = \mathsf{amb}[\ \mathsf{mob}[\{top, \mathsf{taxi}\}, \{m\}], \mathsf{com}[\{top\}, \emptyset]\ ].$$

Since *taxi* is not visible, we have to refer to its abstract representative taxi. Inspecting the various possibilities, we are therefore led to consider the following sets of possible ambient types.
(1) Outside the scope of *taxi*:

$$\mathit{Types}(\Gamma, \Xi, n) = \{\, A_n, A_n \cup \Xi[\mathsf{x}]\,\} \quad \text{and} \quad \mathit{Types}(\Gamma, \Xi, m) = \{A_m, A_m \cup \Xi[\mathsf{x}]\,\};$$

(2) Inside the scope of *taxi*:

$$\mathit{Types}(\Delta, \emptyset, n) = \{\, A_n, A_n \cup \Delta[x]\,\}, \qquad \mathit{Types}(\Delta, \emptyset, m) = \{\, A_m, A_m \cup \Delta[x]\,\}$$
$$\text{and} \quad \mathit{Types}(\Delta, \emptyset, x) = \{\, A_x \cup A_n, A_x \cup A_m\,\}. \quad \square$$

3.3 Estimating the set of possible types

In this section we give the formal estimate of the set of possible types for name a with respect to chosen typing contexts. As illustrated by Example 3, the possible types of an ambient name n are given by its global type merged with those of the variables n might instantiate. Consider the term

$$R = !\langle n\rangle \mid \langle m\rangle \mid (x)P \mid (y)Q,$$

and suppose that n and m have respectively global types A_n and A_m. Then, n may instantiate variables x and y with global types, say, A_x and A_y respectively. The possible types of n are, therefore, A_n, $A_n \cup A_x$, $A_n \cup A_y$ and $A_n \cup A_x \cup A_y$. The latter corresponds to the case in which n instantiates both x and y. Observe that m may instantiate only one variable, because $\langle m\rangle$ is not replicated. This means that its possible types are only A_m, $A_m \cup A_x$ and $A_m \cup A_y$. Symmetrically, the possible types for x are $A_x \cup A_n$, $A_x \cup A_m$ and $A_x \cup A_y \cup A_n$. The latter corresponds to the case where n instantiates both x and y.

We first define the set of names which a given name may possibly instantiate or be instantiated by. To this aim we use binary relations over names. Intuitively, if a name α can instantiate a variable β, then the pair (α, β) is in one such a relation. We focus exclusively on so-called binding relations, which only depend on types and typing contexts. Basically, this amounts to saying that α is related to β if β is a variable which might be bound in some ambient where α may also communicated, as formalised by the definition below.

Definition 6. The *binding relation* with respect to typing contexts Γ and Θ is

$$\mathit{Bind}(\Gamma; \Theta) = \{\, (\alpha, \beta) \mid \mathit{gt}(\Gamma; \Theta)(\alpha) = A \text{ and } \mathit{gt}(\Gamma; \Theta)(\beta) = B \text{ with } A^{\mathsf{com}\uparrow}\{\alpha/\star\} \cap B \neq \emptyset\,\} \quad \square$$

Observe that $Bind(\Gamma, \Theta)$ is actually a subset of $(\mathsf{N} \cup \mathcal{N}) \times (\mathsf{X} \cup \mathcal{X})$. Indeed, due to our restrictions, the global (ambient) type of a variable is always empty – more precisely, it is always $\mathsf{com}[\emptyset, \emptyset]$. It follows that a variable cannot be related to another variable.

Relying on binding relations, we can estimate which variables may be instantiated by a given ambient name, and which ambient names may instantiate a given variable.

$$Vars(\Gamma; \Theta; \alpha) = \{\beta \mid (\alpha, \beta) \in Bind(\Gamma; \Theta)\}; \qquad Ambs(\Gamma; \Theta; \alpha) = \{\beta \mid (\beta, \alpha) \in Bind(\Gamma; \Theta)\}.$$

Example 4. Going back to the example of process R above, let us suppose that it is running in ambient *top*, and x and y have variable type $\mathsf{var}[\{top\}]$. From the point of view of the whole R, variables x and y are bound. Thus we only know such variables by means of their abstract representatives, say x and y. If we assume that R is a stand-alone process, the external abstract context is empty. We should therefore be able to prove $\Gamma \vdash^{\Xi;\emptyset}_{top} R$, where

$$\Xi = \mathsf{x} : \mathsf{var}[\{top\}], \mathsf{y} : \mathsf{var}[\{top\}], \Xi' \qquad \text{and} \qquad \Gamma = n : A_n, m : A_m, \Gamma',$$

for some auxiliary typing contexts Ξ' and Γ'. (These will depend on P and Q; we leave them unspecified as well as the actual types A_n and A_m.) In order for n and m to be communicable in *top*, we must have $top \in A_n^{\mathsf{com}\uparrow}$ and $top \in A_m^{\mathsf{com}\uparrow}$. Therefore, we have

$$Bind(\Gamma; \Xi) = \{(n, \mathsf{x}), (n, \mathsf{y}), (m, \mathsf{x}), (m, \mathsf{y})\},$$

$$Vars(\Gamma; \Xi; n) = \{\mathsf{x}, \mathsf{y}\} \qquad \text{and} \qquad Vars(\Gamma; \Xi; m) = \{\mathsf{x}, \mathsf{y}\}.$$

Observe that when typing P, variable x is not anymore bound and we can prove $\Delta \vdash^{\Xi'_1;\Theta}_{top} P$ with

$$\Theta = \mathsf{y} : \mathsf{var}[\{top\}], \Xi'_2 \qquad \text{and} \qquad \Delta = n : A_n, m : A_m, x : \mathsf{var}[\{top\}], \Gamma',$$

where $\Xi'_1, \Xi'_2 = \Xi'$. Indeed, we have to split Ξ' in Ξ'_1, used by the bound names of P, and Ξ'_2, used by the bound names of Q. Now, we have

$$Bind(\Delta; \Xi'_1, \Theta) = \{(n, x), (n, \mathsf{y}), (m, x), (m, \mathsf{y})\};$$

$$Vars(\Delta; \Xi'_1, \Theta; n) = \{x, \mathsf{y}\}; \qquad Vars(\Delta; \Xi'_1, \Theta; m) = \{x, \mathsf{y}\}; \qquad Ambs(\Delta; \Xi'_1, \Theta; x) = \{n, m\}.$$

It is easy to verify that the global type of the abstract variable x in R is the same as the one of the concrete variable x in P, that is $gt(\Gamma; \Xi)(\mathsf{x}) = gt(\Delta; \Xi'_1, \Theta)(x) = A_x$.

In R, the set of possible types for n is the set of all possible combinations of the global type of n and the global types of variables in $Vars(\Gamma; \Xi; n)$, that is

$$Types(\Gamma; \Xi; n) = \{A_n, A_n \cup A_x, A_n \cup A_y, A_n \cup A_x \cup A_y\}.$$

Similarly, we have

$$Types(\Gamma; \Xi; m) = \{A_m, A_m \cup A_x, A_m \cup A_y, A_m \cup A_x \cup A_y\}.$$

Note that, contrary to a previous observation, type $A_m \cup A_x \cup A_y$ is guessed as a possible type for m. This is because our types are not fine enough to provide the information that m is actually sent only once. To address and remove this problem, we would need to use linear types.

In P, the set of possible types for x are those for the ambient names which x may be substituted by – given by $Ambs(\Delta; \Xi'_1, \Theta; x)$ – augmented with the global type of x:

$$Types(\Delta; \Xi'_1, \Theta; x) = \{A_n \cup A_x, A_n \cup A_x \cup A_y, A_m \cup A_x, A_m \cup A_x \cup A_y\}. \quad \square$$

The discussion above is formalised by the following definition, where we use the notation $A \triangleright \mathcal{T}$, for $\mathcal{T}$ a set of ambient types, to denote the set $\{A \cup B \mid B \in \mathcal{T}\}$, and $A \triangleright^\star \mathcal{T}$ for $\{A\} \cup A \triangleright \mathcal{T}$.

Definition 7. The set $\mathit{Types}(\Gamma;\Theta;\alpha)$ of possible types for α with respect to typing contexts Γ and Θ is defined by

$$\mathit{Types}(\Gamma;\Theta;\alpha) = \mathit{gt}(\Gamma;\Theta)(\alpha) \triangleright^{\star} \left\{ \mathit{gt}(\Gamma;\Theta)(\beta) \;\middle|\; \beta \in \mathit{Vars}(\Gamma;\Theta;\alpha) \right\}, \qquad \text{if } \alpha \in \mathsf{N} \cup \mathcal{N}, \text{ and}$$

$$\mathit{Types}(\Gamma;\Theta;\alpha) = \bigcup_{\beta \in \mathit{Ambs}(\Gamma;\Theta;\alpha)} \mathit{gt}(\Gamma;\Theta)(\alpha) \triangleright \mathit{Types}(\Gamma;\Theta;\beta), \qquad \text{if } \alpha \in \mathsf{X} \cup \mathcal{X}. \quad \square$$

Observe that the constraints on our typing rules are expressed essentially as type inclusion constraints. Therefore, we do not really need to consider all the possible types of an ambient name. In practice, as well as in proofs, it is more convenient the use notions of maximum and minimum types. For instance, if a name n with global type A_n may be bound to variables $x_1, \ldots, x_k$ with global types $A_{x_1}, \ldots, A_{x_k}$ respectively, then the possible types of n useful for the purpose of typechecking are A_n and $A_n \cup A_{x_1} \ldots \cup A_{x_k}$. Formally, we can define maximum and minimum types respectively as follows.

$$\mathit{Types}_{\top}(\Gamma;\Theta;\alpha) = \bigcup_{A \in \mathit{Types}(\Gamma;\Theta;\alpha)} A, \qquad \text{and} \qquad \mathit{Types}_{\bot}(\Gamma;\Theta;\alpha) = \bigcap_{A \in \mathit{Types}(\Gamma;\Theta;\alpha)} A.$$

Then, for instance, the rule (VIN) is equivalent to the rule

$$\frac{\mathcal{P} \subseteq \mathit{Types}_{\bot}(\Gamma;\Theta;a)^{\mathsf{mob}^{\downarrow}}}{\Gamma \vdash^{\Theta} \mathsf{in}\, a : \mathsf{cap}[\mathcal{P}]} \text{ (VIN}')$$

and (VOUT) is equivalent to

$$\frac{\mathit{Types}_{\top}(\Gamma;\Theta;a)^{\mathsf{mob}^{\uparrow}} \subseteq \mathit{Types}_{\bot}(\Gamma;\Theta;a_i)^{\mathsf{mob}^{\uparrow}}}{\Gamma \vdash^{\Theta} \mathsf{out}\, a : \mathsf{cap}[\{a_1, \ldots, a_n\}]} \text{ (VOUT}')$$

The reader can easily state the other alternate rule for (VOPEN'), (AMB) and (OUTPUT).

The main result of this paper is a 'Subject Reduction' theorem for the type systems we introduced. Write $\Gamma \vdash_a P$ if there exist some abstract contexts Ξ and Θ such that $\Gamma \vdash_a^{\Xi;\Theta} P$, it can be expressed as follows. (A sketch of the proofs – exploiting the minimum and maximum types of this section – is given in §D. A complete example of a typing derivation is in §C.)

Theorem 1 (Subject Reduction). *If* $\Gamma \vdash_n P$ *and* $P \to Q$, *then* $\Gamma \vdash_n Q$.

4 Conclusion, related and future work

The paper proposed a type system to describe access control policies and related behavioural properties of processes in the Ambient calculus. Whilst all type systems in the literature make use of groups to describe such properties [9, 22, 15], ours is based on dependent types. Despite an additional complexity in building typing derivations, our system has simple, natural types which may make policy specifications easier, and, therefore, simplify the programming task.

The major technical device of our approach is the novel notion of *abstract names*, which mimic the role of groups internally to typing derivations. More precisely, they keep track of – and dynamically embody in an ambient's type – any new capability that the ambient may gain during its lifespan. Abstract names are, in a sense, a dynamic notion of group, made internal to the type system rather than part of the language.

We showed how to extend a basic system to deal with communication of ambient names. The resulting type system is, we believe, the main contribution of this paper. It allows modular, per-client programming and is, to the best of our knowledge, the first one dealing at such a level with dynamic specifications of security policies in the ambient calculus. Communication types come together with a noticeable increase of complexity of typing derivations in the system. Indeed, when typing a communication, one has to consider all ambient names that can possibly instantiate a given variable. However, only a finite number of

names are necessary for the proofs, and the notions of maximum and minimum types simplify the matter considerably.

We plan to study in future work the question of decidability of type checking, as a positive answer would make our type system usable in practice. We conjecture that it should be possible to devise a type checking algorithm, for the following reasons.

- The use of abstract contexts is not a concern: for a typeable term P, it is easy to provide (algorithmically or "by hand"), an abstract context Θ, such that $\Gamma \vdash_n^{\Theta;\emptyset} P$ for some Γ and n. Indeed, Θ is essentially the collection of bound names in P.
- Communication is quite hard to manage "manually" because they it require the synthesis of several global types. However, given variable types and communication types, it does not seem difficult to design an algorithm that does the job.

Because processes are typed against an environment – represented by the external abstract contexts – our type system is not compositional. This may be problematic in the framework of open (or partially typed) systems which have to deal with the arrival of unknown agents. Thus, the following questions arises: if $\Gamma \vdash_n^{\Xi;\emptyset} P$ is provable, does a class exist of external abstract contexts Θ such that $\Gamma \vdash_n^{\Xi;\Theta} P$? Such a class would determine the environments which make P typeable. Another question concerns the design of a type inference algorithm, which is a crucial component in open systems, where information coming from external sources cannot always be trusted. As studied in [20] for $D\pi$, dependent types call for a very accurate treatment, which would certainly be required for our type system as well. Such challenging questions are topics of our current and future research.

Related work

Beside the already mentioned work on groups [9, 22, 15], which provided direct inspiration for our research, related work includes [29, 17]. These papers introduce dynamic and dependent types for a distributed π calculus, and study their impact on behavioural semantics. A difficulty arises in [29] with referring to bound names created in external processes, at all analogous to the one we tackled here with the introduction of *abstract names*. As a matter of fact, it is pointed out in *loc. cit.* as the main limitation of their work. As we just learnt, the problem has been addressed in [28], completely independently of our work, using existential types. There appear to be analogies between Yoshida's existential types and our approach, although at this stage it is difficult to assess them in the details.

Since our type system works linearly on internal abstract contexts, and classically on external ones, the closest match appears to be with Yoshida's linear type discipline. However, while we conjecture we can reformulate local abstract names with some form of existential types, it looks unlikely we may find a notion corresponding to our external abstract contexts. But such contexts are the keystones of our work. They allow, in particular, a correct treatment of parallel composition and replication (cf. Figure 2), where it is not always the case that if P is correct so is $P \mid P$ or, a fortiori, $!P$.

Concerning typing systems for the ambient calculus, [1] uses dependent types for communication in order to achieve advanced type polymorphism of the sort usually encountered in lambda calculi. Types in *loc. cit.* track – like ours – all messages exchanged, and not rely on topics of conversation. They are also used to bound the nesting of ambients.

We conclude by observing that, as pointed out in [10] there are intriguing connections between groups and channels and binders of the flow analysis, as in [3, 16]. Indeed, our approach has a lot to share with control flow analysis, and we believe our work can shed further light on such connections.

References

[1] T. Amtoft and J. Wells. Mobile processes with dependent communication types and singleton types for names and capabilities. Technical Report 2002-3, Kansas State University, 2002.

[2] F. Barbanera, M. Bugliesi, M. Dezani, and V. Sassone. A calculus of bounded capacities. In *ASIAN 2003*, Lecture Notes in Computer Science. Springer, 2003. To appear.

[3] C. Bodei, P. Degano, F. Nielson, and H. R. Nielson. Static analysis for the π calculus with applications to security. *Information and Computation*, 168:68–92, 2001.

[4] M. Bugliesi, G. Castagna, and S. Crafa. Boxed ambients. In *TACS'01*, volume 2215 of *Lecture Notes in Computer Science*, pages 38–63. Springer, 2001.

[5] M. Bugliesi, S. Crafa, M. Merro, and V. Sassone. Communication interference in mobile boxed ambients. In *FST&TCS'02*, volume 2556 of *Lecture Notes in Computer Science*, pages 71–84. Springer, 2002.

[6] C. Calcagno, L. Cardelli, and A. D. Gordon. Deciding validity in a spatial logic for trees. In *TLDI'03*, pages 62–73. ACM Press, 2003.

[7] L. Cardelli, P. Gardner, and G. Ghelli. Manipulating trees with hidden labels. In *FOSSACS'03*, volume 2620 of *Lecture Notes in Computer Science*, pages 216–232. Springer, 2002.

[8] L. Cardelli, P. Gardner, and G. Ghelli. A spatial logic for querying graphs. In *ICALP'02*, volume 2380 of *Lecture Notes in Computer Science*, pages 597–610. Springer, 2003.

[9] L. Cardelli, G. Ghelli, and A. Gordon. Ambient groups and mobility types. In *International Conference IFIP TCS*, volume 1872 of *Lecture Notes in Computer Science*, pages 333–347. Springer, 2000.

[10] L. Cardelli, G. Ghelli, and A. Gordon. Secrecy and group creation. In *CONCUR'00*, volume 1877 of *Lecture Notes in Computer Science*, pages 365–379. Springer, 2000.

[11] L. Cardelli and A. Gordon. Mobile ambients. In *FOSSACS'98*, volume 1378 of *Lecture Notes in Computer Science*, pages 140–155. Springer, 1998.

[12] L. Cardelli and A. Gordon. Types for mobile ambients. In *POPL'99*, pages 79–92. ACM Press, 1999.

[13] L. Cardelli and A. D. Gordon. Anytime, anywhere. Modal logics for mobile ambients. In *POPL'00*, pages 365–377. ACM Press, 2000.

[14] W. Charatonik, A. Gordon, and J.-M. Talbot. Finite-control mobile ambients. In *ESOP'02*, volume 2305 of *Lecture Notes in Computer Science*, pages 295–313. Springer, 2002.

[15] M. Coppo, M. Dezani-Ciancaglini, E. Giovannetti, and I. Salvo. M3: Mobility types for mobile processes in mobile ambients. In *CAT'03*, volume 78 of *Electronic Notes in Theoretical Computer Science*. Elsevier, 2003.

[16] P. Degano, F. Levi, and C. Bodei. Safe ambients: Control flow analysis and security. In *Proceedins of ASIAN'00*, volume 1961 of *LNCS*, pages 199–214. Springer-Verlag, 2000.

[17] M. Hennessy, M. Merro, and J. Rathke. Towards a behavioural theory of access and mobility control in distributed systems. In *FOSSACS'03*, Lecture Notes in Computer Science. Springer, 2003.

[18] D. Hirschkoff, E. Lozes, and D. Sangiorgi. Separability, expressiveness, and decidability in the ambient logic. In *LICS'02*. IEEE Press, 2002.

[19] F. Levi and D. Sangiorgi. Controlling interference in Ambients. In *POPL'00*, pages 352–364. ACM Press, 2000.

[20] C. Lhoussaine. Type inference for a distributed π-calculus. In *ESOP'03*, volume 2618 of *Lecture Notes in Computer Science*, pages 253–268. Springer, 2003.

[21] M. Merro and M. Hennessy. Bisimulation Congruences in Safe Ambients. In *POPL'02*, pages 71–80. ACM Press, 2002.

[22] M. Merro and V. Sassone. Typing and subtyping mobility in boxed ambients. In *CONCUR'02*, volume 2421 of *Lecture Notes in Computer Science*, pages 304–320. Springer, 2002.

[23] M. Merro and F. Zappa-Nardelli. Bisimulation proof methods for mobile ambients. In *ICALP'03*, volume 2719. Lecture Notes in Computer Science, 2003.

[24] R. Milner, J. Parrow, and D. Walker. A calculus of mobile processes, parts i and ii. *Information and Computation*, 100(1):1–77, 1992.

[25] A. Regev, E. Panina, W. Silverman, L. Cardelli, and E. Shapiro. Bioambients: An abstraction for biological compartments. To appear, 2003.

[26] D. Sangiorgi. Extensionality and intensionality of the ambient logic. In *POPL'01*, pages 4–13. ACM Press, 2001.

[27] D. Teller, P. Zimmer, and D. Hirschkoff. Using ambients to control resources. In *CONCUR'02*, volume 2421 of *LNCS*, pages 288–303. Springer, 2002.

[28] N. Yoshida. Channel dependent types for higher-order mobile processes. In *POPL04*, 2004. To appear.

[29] N. Yoshida and M. Hennessy. Assigning types to processes. In *LICS'00*, pages 334–345, 2000.

Ambient names	$n, m, \ldots \in \mathcal{N}$		*Processes*	$P, Q ::= \mathbf{0}$	nil process
Variables	$x, y, \ldots \in \mathcal{X}$			$\mid (\nu\, n : A)\, P$	restriction
Names	$a, b, \ldots \in \mathcal{N} \cup \mathcal{X}$			$\mid (P \mid Q)$	composition
Values	$V, U ::= a$	name		$\mid\ !P$	replication
	$\mid\ \mathsf{in}\, a$	may enter a		$\mid\ V[P]$	ambient
	$\mid\ \mathsf{out}\, a$	may exit of a		$\mid\ V.P$	prefixing
	$\mid\ \mathsf{open}\, a$	may dissolve a		$\mid\ (x)P$	input
	$\mid\ V.U$	path		$\mid\ \langle V \rangle$	output

Figure 5: Mobile Ambients

A Mobile Ambients

The syntax of processes is given in Figure 5, where $\mathcal{N}$ denotes an infinite set of *concrete ambient names* and $\mathcal{X}$ denotes an infinite set of *concrete variables*. Moreover, A is an ambient type as described elsewhere in the paper. Inaction, composition, restriction and replication are inherited from concurrent calculi such as the π-calculus [24]. The inactive process, $\mathbf{0}$, does nothing. Parallel composition is denoted by a binary operator, $P \mid Q$, that is commutative and associative. The restriction operator, $(\nu\, n : A)\, P$, creates a new (unique) name n within a scope P and which is assigned a type A. Replication, $!P$, allows to create as many parallel replicas as needed and it is equivalent to $P \mid !P$. Specific of ambient calculus are the *ambients*, $V[P]$, and the *prefix* via capabilities, $V.P$. In $V[P]$, V is the name of the ambient and P is the process running inside the ambient. The process $V.P$ executes an action regulated by the capability V, and then continues as the process P. Given a name n, the capability $\mathsf{in}\, n$ allows to move in n, the capability $\mathsf{out}\, n$ allows to move out of n, and the capability $\mathsf{open}\, n$ allows to open or dissolve n. Meaningless terms such as $\mathsf{in}\, n[P]$ and $n.P$ are ruled out by the type system.

Communication is *asynchronous* (though a synchronous version could be treated as well), *monadic* (for the sake of simplicity), and *local* which means that any message, $\langle V \rangle$, sent within some ambient may only be received by a process, $(x)P$, running in the same ambient.

We use some notational conventions. Parallel composition has the lowest precedence among the operators. The process $V.U.P$ is read as $V.(U.P)$. As usual, we omit trailing dead processes, writing V for $V.\mathbf{0}$, and $n[]$ for $n[\mathbf{0}]$. Restriction $(\nu\, n : A)\, P$ and input prefix $(x)P$ act as binders for n and x respectively. The set of free names of P, $fn(P)$ is defined accordingly.

The dynamic of the calculus is given in the form of a reduction relation. It is based on an auxiliary relation, called *structural congruence*, which brings the participants of a potential interaction to contiguous positions. The full operational semantics is given in the Appendix B.

B Operational Semantics

$$
\begin{array}{lrcl}
\text{(R-In)} & n[\mathsf{in}\, m.P \mid Q] \mid m[R] & \to & m[n[P \mid Q] \mid R] \\
\text{(R-Out)} & n[m[\mathsf{out}\, n.P \mid Q] \mid R] & \to & n[R] \mid m[P \mid Q] \\
\text{(R-Open)} & \mathsf{open}\, n.P \mid n[Q] & \to & P \mid Q \\
\text{(R-Com)} & \langle V \rangle \mid (x)P & \to & P\{^{V}/_{x}\} \\
\text{(R-Garb)} & (\nu\, n : A)\, \mathbf{0} & \to & \mathbf{0} \\
\text{(R-Rep)} & !P & \to & P \mid !P \\
\text{(R-Cont)} & P \to Q & \Rightarrow & \mathbf{C}[P] \to \mathbf{C}[Q] \\
\text{(R} - \alpha\text{)} & P =_{\alpha} P' \to Q' =_{\alpha} Q & \Rightarrow & P \to Q
\end{array}
$$

where $\mathbf{C}$ is an evaluation context defined by:

$$\mathbf{C} = (\mathbf{C} \mid P) \mid n[\mathbf{C}] \mid (\nu\, n : A)\, \mathbf{C} \mid \bullet$$

and where $\mathbf{C}[P]$ stands for $\mathbf{C}$ with $\bullet$ replaced by P.

The structural congruence is the least congruence satisfying the following axioms.

$$P \mid Q \equiv Q \mid P \qquad (P \mid Q) \mid R \equiv P \mid (Q \mid R)$$
$$P \mid \mathbf{0} \equiv P \qquad !\mathbf{0} \equiv \mathbf{0} \qquad (V.U).P \equiv V.U.P$$

$$\begin{aligned}
(\nu\, n : A)\,(\nu\, m : A')\,P &\equiv (\nu\, m : A')\,(\nu\, n : A)\,P, && n \neq m,\ n \notin nm(A') \text{ and } m \notin nm(A);\\
(\nu\, n : A)\,(P \mid Q) &\equiv (\nu\, n : A)\,P \mid Q, && n \notin fn(Q);\\
a[(\nu\, n : A)\,P] &\equiv (\nu\, n : A)\,a[P], && a \neq n.
\end{aligned}$$

C Examples of Typing Derivations

C.1 Typing the taxi server

Example 5. In order to illustrate the type system, let us consider a taxi server as in Example 1, but with a more liberal control policy $A' = \mathsf{amb}[\,\mathsf{mob}[\{top\},\{n,m\}]\,]$, which allows both n and m as children ot *taxi*. To keep notations simple, we consider a non-replicated version.

$$TaxiServ'_1(n) = (\nu\, taxi : A')\,(taxi[\,] \mid n[\mathsf{in}\, taxi])$$

Let $P' = TaxiServ'_1(n) \mid Q$ with $Q = n[\,\mathsf{in}\, n \mid m[\mathsf{out}\, n.\mathsf{out}\, n]\,]$, as in Example 1. We can then prove that P' is well-typed with current location *top*, local abstract context $(\mathsf{taxi} : A')$, and empty external context. Let

$$\Gamma = \begin{cases} top : \mathsf{amb}[\,\mathsf{mob}[\emptyset,\{n,m\}]\,], \\ \quad n : \mathsf{amb}[\,\mathsf{mob}[\{top,n\},\{n,m\}]\,], \\ \quad m : \mathsf{amb}[\,\mathsf{mob}[\{top,n\},\emptyset]\,] \end{cases}$$

and $\Delta' = \Gamma^{(taxi:A')}, taxi : A'$, that is

$$\Delta' = \begin{cases} top : \mathsf{amb}[\,\mathsf{mob}[\emptyset,\{n,m,taxi\}]\,], \\ \quad n : \mathsf{amb}[\,\mathsf{mob}[\{top,n,taxi\},\{n,m\}]\,], \\ \quad m : \mathsf{amb}[\,\mathsf{mob}[\{top,n,taxi\},\emptyset]\,], \\ taxi : \mathsf{amb}[\,\mathsf{mob}[\{top\},\{n,m\}]\,] \end{cases}$$

Let π_1 be the proof below of $\Delta' \vdash^{\emptyset;\emptyset}_{top} taxi[\,] \mid n[\mathsf{in}\, taxi]$:

$$\dfrac{\dfrac{(1)}{\Delta' \vdash^{\emptyset;\emptyset}_{top} taxi[\,]} \qquad \dfrac{\dfrac{(3)}{\Delta' \vdash^{\emptyset;\emptyset} \mathsf{in}\, taxi : \mathsf{cap}[\{n\}]}}{\Delta' \vdash^{\emptyset;\emptyset}_{n} \mathsf{in}\, taxi} \qquad (2)}{\Delta' \vdash^{\emptyset;\emptyset}_{top} n[\mathsf{in}\, taxi]}}{\Delta' \vdash^{\emptyset;\emptyset}_{top} taxi[\,] \mid n[\mathsf{in}\, taxi]}$$

where

(1) checks that the type of *taxi* in Δ' has *top* as a possible parent;

(2) checks that the type of m in Δ' has *top* as a possible parent;

(3) checks that the type of *taxi* in Δ' has n as a possible child.

Let π_2 be the proof below of $\Gamma \vdash^{\emptyset;\mathsf{n}:A'}_{top} Q$:

$$\dfrac{\dfrac{\dfrac{(1)}{\Gamma \vdash^{\mathsf{taxi}:A'} \mathsf{in}\, n : \mathsf{cap}[\{n\}]}}{\Gamma \vdash^{\emptyset;\mathsf{taxi}:A'}_{n} \mathsf{in}\, n} \qquad \dfrac{\dfrac{(2)}{\Gamma \vdash^{\mathsf{taxi}:A'} \mathsf{out}\, n : \mathsf{cap}[\{m\}]}}{\Gamma \vdash^{\emptyset;\mathsf{taxi}:A'}_{m} \mathsf{out}\, n.\mathsf{out}\, n} \qquad (3)}{\Gamma \vdash^{\emptyset;\mathsf{taxi}:A'}_{n} m[\mathsf{out}\, n.\mathsf{out}\, n]}}{\dfrac{\Gamma \vdash^{\emptyset;\mathsf{taxi}:A'}_{n} \mathsf{in}\, n \mid m[\mathsf{out}\, n.\mathsf{out}\, n] \qquad (4)}{\Gamma \vdash^{\emptyset;\mathsf{taxi}:A'}_{top} n[\mathsf{in}\, n \mid m[\mathsf{out}\, n.\mathsf{out}\, n]]}}$$

where the global types of *top*, *n* and *m* with respect to Γ and the abstract context $(\mathsf{taxi} : A')$ are

$$gt(\Gamma; \mathsf{taxi} : A')(top) = \mathsf{amb}[\ \mathsf{mob}[\emptyset, \{n, m, \mathsf{taxi}\}]\ ]$$
$$gt(\Gamma; \mathsf{taxi} : A')(n) = \mathsf{amb}[\ \mathsf{mob}[\{top, n, \mathsf{taxi}\}, \{n, m\}]\ ]$$
$$gt(\Gamma; \mathsf{taxi} : A')(m) = \mathsf{amb}[\ \mathsf{mob}[\{top, n, \mathsf{taxi}\}, \emptyset]\ ]$$

Regarding those types,

(1) checks that *n* is a possible child of itself,

(2) checks that the possible parents of *n* are possible one for *m*,

(3) checks that *n* is possible parent for *m*, and

(4) checks that *top* is a possible parent for *n*.

Finally,

$$\dfrac{\dfrac{\dfrac{\pi_1}{\Delta' \vdash_{top}^{\emptyset;\emptyset} taxi[\,] \mid n[\mathsf{in}\, taxi]}}{\Gamma \vdash_{top}^{\mathsf{taxi}:A';\emptyset} (\nu\, taxi : A')\,(taxi[\,] \mid n[\mathsf{in}\, taxi])} \qquad \dfrac{\pi_2}{\Gamma \vdash_{top}^{\emptyset;\mathsf{taxi}:A'} Q}}{\Gamma \vdash_{top}^{\mathsf{taxi}:A';\emptyset} (\nu\, taxi : A')\,(taxi[\,] \mid n[\mathsf{in}\, taxi]) \mid Q}$$

which concludes the proof that P' is typeable. □

C.2 Typing the dynamic taxi server

As an example, we give here the full proof of the typing of the dynamic taxi server:

$$DTaxiServ = !(x)(\nu\, taxi : \mathsf{amb}[M, C])\,(taxi[\,] \mid x[\mathsf{in}\, taxi])$$

where $M = \mathsf{mob}[\{top\}, \{x\}]$ and $C = \mathsf{com}[\emptyset, \emptyset]$. Let

$$A_n = \mathsf{amb}[\ \mathsf{mob}[\{top\}, \{m\}], \mathsf{com}[\{top\}, \emptyset]\ ] \quad \text{and} \quad A_m = \mathsf{amb}[\ \mathsf{mob}[\{top, n\}, \emptyset], \mathsf{com}[\{top\}, \emptyset]\ ]$$

be, respectively, the types of *n* and *m*. As in Example 3, we need the concrete context

$$\Gamma = \left\{ \begin{array}{l} n : A_n, \\ m : A_m, \\ top : \mathsf{amb}[\ \mathsf{mob}[\emptyset, \{m, n\}], \mathsf{com}[\emptyset, \{m, n\}]\ ], \end{array} \right.$$

and the abstract context

$$\Xi = \mathsf{x} : \mathsf{var}[\{top\}],\ \mathsf{taxi} : \mathsf{amb}[N, C]$$

for $N = \mathsf{mob}[\{top\}, \{\mathsf{x}\}]$. We prove $\Gamma \vdash_{top}^{\Xi;\emptyset} DTaxiServ$ step by step, and bottom up. Let $\sigma = \{\mathsf{x}'/\mathsf{x}, \mathsf{taxi}'/\mathsf{taxi}\}$ for some fresh x' and taxi', and $\Xi' = \Xi\sigma$, that is

$$\Xi' = \mathsf{x}' : \mathsf{var}[\{top\}],\ \mathsf{taxi}' : \mathsf{amb}[N', C].$$

for $N' = \mathsf{mob}[\{top\}, \{\mathsf{x}'\}]$. By the rule (Rep), we need to prove $\Gamma \vdash_{top}^{\Xi;\Xi'} DTaxiServ_1$, where $DTaxiServ_1$ is as in Example 3. The proof tree is of the form,

$$\dfrac{\dfrac{\pi_1}{\Delta \vdash_{top}^{\mathsf{taxi}:\mathsf{amb}[M,C];\Xi'} (\nu\, taxi : \mathsf{amb}[M, C])\,(taxi[\,] \mid x[\mathsf{in}\, taxi])}}{\Gamma \vdash_{top}^{\mathsf{x}:\mathsf{var}[\{top\}],\mathsf{taxi}:\mathsf{amb}[N,C];\Xi'} (x)(\nu\, taxi : \mathsf{amb}[M, C])\,(taxi[\,] \mid x[\mathsf{in}\, taxi])}$$

where $\Delta = \Gamma, x : \mathsf{var}[\{top\}]$, as obtained by application of rule (Input).
Fixed $\Delta' = \Delta^{(taxi:\mathsf{amb}[M,C])}, taxi : \mathsf{amb}[M, C]$:

$$\Delta' \quad = \quad \left\{ \begin{array}{l} n : A_n, m : A_m, \\ top : \mathsf{amb}[\mathsf{mob}[\emptyset, \{n, m, taxi\}], \mathsf{com}[\emptyset, \{n, m\}]], \\ x : \mathsf{var}[\{top\}], \\ taxi : \mathsf{amb}[M, C] \end{array} \right.$$

then π_1 unfolds as follows

$$\dfrac{\dfrac{(1)}{\Delta' \vdash_{top}^{\emptyset;\Xi'} taxi[]} \qquad \dfrac{\dfrac{\dfrac{(2)}{\Delta' \vdash^{\Xi'} \mathsf{in}\, taxi : \mathsf{cap}[x]}}{\Delta' \vdash_{x}^{\emptyset;\Xi'} \mathsf{in}\, taxi} \qquad (3)}{\Delta' \vdash_{top}^{\emptyset;\Xi'} x[\mathsf{in}\, taxi]}}{\Delta' \vdash_{top}^{\emptyset;\Xi'} taxi[] \mid x[\mathsf{in}\, taxi]}}{\Delta \vdash_{top}^{\mathsf{taxi}:\mathsf{amb}[M,C];\Xi'} (\nu\, taxi : \mathsf{amb}[M,C])\,(taxi[] \mid x[\mathsf{in}\, taxi])}$$

where:

(1) is $top \in Types_{\perp}(\Delta'; \Xi'; taxi)^{\mathsf{mob}\uparrow}$

(2) is $x \in Types_{\perp}(\Delta'; \Xi'; taxi)^{\mathsf{mob}\downarrow}$

(3) is $top \in Types_{\perp}(\Delta'; \Xi'; x)^{\mathsf{mob}\uparrow}$

We now have to determine the set of types for x and *taxi* with respect to contexts Δ' and Ξ'. Their global types are

$$gt(\Delta'; \Xi')(taxi) = \mathsf{amb}[M, C] \quad \text{and} \quad gt(\Delta'; \Xi')(x) = \mathsf{amb}[\,\mathsf{mob}[\{taxi\}, \emptyset], C\,] = A_x$$

Since *taxi* has an empty communication type, its only possible type is $\mathsf{amb}[M, C]$. Therefore,

$$Types_{\perp}(\Delta'; \Xi'; taxi) = \mathsf{amb}[M, C]$$

and (2) holds. Since $gt(\Delta'; \Xi')(x) = \mathsf{var}[\{top\}]$, x may be bound in *top*, where n and m may be communicated. It thus follows that $Ambs(\Delta'; \Xi'; x) = \{n, m\}$. The possible types for x depend on those for n and m, whose global types are

$$gt(\Delta'; \Xi')(n) = \mathsf{amb}[\,\mathsf{mob}[\{top\}, m], \mathsf{com}[\{top\}, \emptyset]\,]$$
$$gt(\Delta'; \Xi')(m) = \mathsf{amb}[\,\mathsf{mob}[\{top, n\}, \emptyset], \mathsf{com}[\{top\}, \emptyset]\,]$$

which we will abbreviate in the following as A_n and A_m, respectively. Both n and m can be sent in *top* where x and some variable represented by the abstract x' may be bound. Therefore

$$Vars(\Delta'; \Xi'; n) = Vars(\Delta'; \Xi'; m) = \{x, \mathsf{x}'\}$$

We then deduce that

$$Types(\Delta'; \Xi'; n) = \{\, A_n, A_n \cup A_x \cup A_{\mathsf{x}'} \,\} \quad \text{and} \quad Types(\Delta'; \Xi'; m) = \{\, A_m, A_m \cup A_x \cup A_{\mathsf{x}'} \,\},$$

where $A_{\mathsf{x}'} = gt(\Delta'; \Xi')(\mathsf{x}') = \mathsf{amb}[\,\mathsf{mob}[\{\mathsf{taxi}'\}, \emptyset], C\,]$. So, we can conclude that the possible types for x are

$$Types(\Delta'; \Xi'; x) = \{\, A_n \cup A_x,\ A_n \cup A_x \cup A_{\mathsf{x}'},\ A_m \cup A_x,\ A_m \cup A_x \cup A_{\mathsf{x}'} \,\},$$

and

$$\begin{aligned} Types_{\perp}(\Delta'; \Xi'; x) &= (A_n \cup A_x) \cap (A_m \cup A_x) = A_x \cup (A_n \cap A_m) \\ &= \mathsf{amb}[\,\mathsf{mob}[\{top,\, taxi\}, \emptyset], \mathsf{com}[\{top\}, \emptyset]\,]. \end{aligned}$$

Therefore, (1) and (3) hold, which concludes the proof of $\Gamma \vdash_{top}^{\Xi;\emptyset} DTaxiServ$. The reader can check that the messages are also well-typed. More precisely, the judgements $\Gamma \vdash_{top}^{\emptyset;\Xi} \langle n \rangle$ and $\Gamma \vdash_{top}^{\emptyset;\Xi} \langle m \rangle$ are both derivable. By the rule (Par) we finally prove

$$\Gamma \vdash_{top}^{\Xi;\emptyset} \langle n \rangle \mid \langle m \rangle \mid DTaxiServ$$

D Results

The main result of this paper is a 'Subject Reduction' theorem for the type systems introduced. Here we illustrate the main lemmas needed to prove subject reduction, and we state the formal theorem. Most of the proofs use the alternate rules with maximum and minimum types.

Lemma 1. *Suppose that $n \notin fn(P) \cup nm(\Gamma, \Xi, \Theta, A)$, $n \neq a$, $an(A) = \emptyset$ and $\mathsf{n} \notin an(\Xi) \cup dom(\Theta)$, then*

- $\Gamma \vdash_a^{\Xi;\Theta,\mathsf{n}:A} P \;\Rightarrow\; \Gamma^{(n:A)}, n : A\{n/\star\} \vdash_a^{\Xi;\Theta\{n/\mathsf{n}\}} P$; *(Weakening)*
- $\Gamma^{(n:A)}, n : A\{n/\star\} \vdash_a^{\Xi;\Theta\{n/\mathsf{n}\}} P \;\Rightarrow\; \Gamma \vdash_a^{\Xi;\Theta,\mathsf{n}:A} P$. *(Strengthening)*

The lemma above is used to show that typing is preserved by scope extrusion.

Lemma 2 (Renaming). *Let σ be an abstract renaming such that $dom(\sigma) = an(\Xi')$ and $im(\sigma) \cap an(\Xi, \Theta) = \emptyset$. Suppose that $an(\Xi) \cap an(\Xi') = \emptyset$, then*

- $\Gamma \vdash_a^{\Theta;\Xi,\Xi'} P \;\Rightarrow \Gamma \vdash_a^{\Theta;\Xi,\Xi'\sigma} P$,
- $\Gamma \vdash_a^{\Xi,\Xi';\Theta} P \;\Rightarrow \Gamma \vdash_a^{\Xi,\Xi'\sigma;\Theta} P$.

The previous lemma states that abstract names may safely be renamed in both local and external abstract contexts. Together with the lemma below it is necessary to prove that typing is preserved by replication.

Lemma 3 (Replication). *Let σ be an abstract renaming such that $dom(\sigma) = an(\Theta')$ and $im(\sigma) \cap an(\Xi, \Theta) = \emptyset$. Suppose that $an(\Theta) \cap an(\Theta') = \emptyset$, then*

$$\Gamma \vdash_a^{\Xi;\Theta,\Theta'} P \;\Rightarrow \Gamma \vdash_a^{\Xi;\Theta,\Theta',\Theta'\sigma} P.$$

As already mentioned, the lemma states that the external abstract context may be safely replicated. This is not the case for local contexts, which are used linearly. The following lemma is sometimes referred to as 'Subject Congruence.'

Lemma 4. *If $\Gamma \vdash_a^{\Xi;\Theta} P$ and $P \equiv Q$, then $\Gamma \vdash_a^{\Xi;\Theta} Q$.*

The proof here proceeds by induction on the definition of the structural congruence, and makes use of the Lemma 1. The lemma below is used for the proof of the 'Substitution Lemma.' The condition about the intersection of B and $A^{\mathsf{com}\uparrow}$ means that n may substitute x. Then, intuitively, the lemma says that the possible types for n are possible types for variable x.

Lemma 5. *Let $A = gt(\Gamma; \Theta)(n)$, and suppose that $B \cap A^{\mathsf{com}\uparrow} \neq \emptyset$, then*

- $Types(\Gamma\{n/x\}; \Theta\{n/x\}; n) \subseteq Types(x : B, \Gamma; \Theta; x)\{n/x\}$,
- $Types(\Gamma\{n/x\}; \Theta\{n/x\}; a) \subseteq Types(x : B, \Gamma; \Theta; a)\{n/x\}$, *for any $a \neq n$.*

Lemma 6 (Substitution Lemma). *If $\Gamma, x : B \vdash_a^{\Xi;\Theta} P$ for $a \in B$, and if for all $A \in Types(\Gamma; \Xi, \Theta; a)$ we have $n \in A^{\mathsf{com}\downarrow}$, then*

$$\Gamma\{n/x\} \vdash_{a\{n/x\}}^{\Xi\{n/x\};\Theta\{n/x\}} P\{n/x\}$$

The following lemma is used to prove that typing is preserved by the reduction (R-Open). It essentially says that if a process P is well-typed at the current location n, and if m is related to n by the conditions of the typing rule (VOpen), then P can safely run in m.

Lemma 7. *Suppose that for any $A \in Types(\Gamma; \Xi, \Theta; n)$ and $A' \in Types(\Gamma; \Xi, \Theta; m)$, we have $A^{\mathsf{mob}} \subseteq A'^{\mathsf{mob}}$ and $A^{\mathsf{com}} = A'^{\mathsf{com}}$. If for any α with $gt(\Gamma; \Xi, \Theta)(\alpha) = B$ we have $n \in B$ iff $m \in B$, then*

$$\Gamma \vdash_n^{\Xi;\Theta} P \;\Rightarrow\; \Gamma \vdash_m^{\Xi;\Theta} P.$$

Abstract contexts may change by reduction. The most obvious illustration is the garbage collection rule: the typing of $(\nu\, n\colon A)\,\mathbf{0}$ requires a local abstract context $\mathsf{n} : A$, whereas $\mathbf{0}$ requires an empty one. Moreover, since abstract contexts are used for the sole purpose of type derivations, they are irrelevant when we are only interested in typeability and type specification. Therefore, the 'Subject Reduction' theorem deals with judgements without abstract contexts. We write $\Gamma \vdash_a P$ if there exist some abstract contexts Ξ and Θ such that $\Gamma \vdash_a^{\Xi;\Theta} P$.

Theorem 2 (Subject Reduction). *If* $\Gamma \vdash_n P$ *and* $P \to Q$, *then* $\Gamma \vdash_n Q$.

hint. Assuming that $\Gamma \vdash_n^{\Xi;\Theta} P$, we proceed by induction on the proof of $P \to Q$. We need to prove the following.

1. If $P \to Q$ is obtained by an axiomatic rule (R-In), (R-Out) or (R-Open), then $\Gamma \vdash_n^{\Xi;\Theta} Q$. The case of the rule (R-Open) is based on Lemma 7.

2. if $P \to Q$ is obtained by an axiomatic rule (R-Garb), $\Xi = \mathsf{a}\colon A, \Xi'$ and $\Gamma \vdash_n^{\Xi';\Theta} Q$.

3. if $P \to Q$ is obtained by an axiomatic rule (R-Rep), then $\Xi = \Xi', \Xi''$ with $an(\Xi') \cap an(\Xi'') = \emptyset$, and there exists an abstract renaming σ such that $dom(\sigma) = an(\Xi')$, $im(\sigma) \cap an(\Xi, \Theta) = \emptyset$ and $\Gamma \vdash_n^{\Xi,\Xi'\sigma;\Theta} Q$. Intuitively, if $\Gamma \vdash_n^{\Xi;\Theta} !R$, then Ξ is used for names created by R and the typing of $R \mid !R$ needs, in addition, a copy of Ξ, that is $\Gamma \vdash_n^{\Xi,\Xi\sigma;\Theta} !R$. Since $!R$ may be a sub-term of P we may only need a copy of a part Ξ' of Ξ. The proof requires Lemma 2 and Lemma 3.

4. if $P \to Q$ is obtained by an axiomatic rule (R-Com), then, there exists x and α such that $\Xi = \mathsf{x}\colon B, \Xi'$ and $\Gamma \vdash_n^{\Xi'\{\alpha/\mathsf{x}\};\Theta} Q$. The proof is based on Lemma 6, and α represents the communicated ambient name. It is an abstract name if the actual communicated name is bound in P.

□