Adjuncts elimination in the static ambient logic

Étienne LOZES [1]

LIP, ENS Lyon – France

Abstract

The Ambient Logic (AL) has been proposed for expressing spatial properties of processes of the Mobile Ambient calculus (MA). Restricting both the calculus and the logic to their static part yields static ambients (SA) and the static ambient logic (SAL), that form a model for queries about semistructured data. SAL also includes the non-standard fresh quantifier ($\mathcal{N}$).

This work adresses the questions of expressiveness and minimality of SAL from the point of view of adjuncts. We define the intensional fragment of the logic (SAL_{int}), the logic without adjuncts, and prove that it captures all the expressiveness of the logic.

We moreover study the question of adjuncts elimination in $\mathrm{SAL}^{\forall}$, where $\mathcal{N}$ quantifier is replaced by the classical $\forall$ quantifier. We conclude with a proof of the minimality of SAL_{int}.

1 Introduction

The Mobile Ambients calculus (MA) [CG98] is a proposal for a new paradigm in the field of concurrency models. Its originality is to set as data the notion of *location*, and as notion of computation the reconfiguration of the hierarchy of locations. The calculus has a spatial part expressing the topology of locations as a labelled unordered tree with binders, and a dynamic part describing the evolution of this topology. The basic connectives for the spatial part are $\mathbf{0}$, defining the empty tree, $a[P]$, defining the tree rooted at a with subtree P, $P \mid Q$ for the tree consisting of the two subtrees P and Q in parallel, and $(\nu n)P$ for the tree P in which the label (or name) n has been hidden.

Type systems are commonly used to express basic requirements on programs. In the case of MA processes, the Ambient Logic, AL [CG00] provides a very flexible descriptive framework. As for a type system, one may ask a process P to match

[1] Email: elozes@ens-lyon.fr

This is a preliminary version. The final version will be published in Electronic Notes in Theoretical Computer Science
URL: www.elsevier.nl/locate/entcs

some specification $\mathcal{A}$, written

$$P \models \mathcal{A}.$$

The AL approach is however much more intensional than in the case of standard type systems. Indeed, all the spatial structure of the calculus is reflected in the logic. For instance, the formula $n[\mathcal{A}]$ is satisfied by processes of the form $n[P]$ with $P \models \mathcal{A}$. AL also handles to the dynamics of computation through the usual $\diamond$ modality. Finally, AL includes *adjunct connectives* for every spatial construct. For instance, the *guarantee* operator

$$\mathcal{A} \triangleright \mathcal{B}$$

specifies that a process is able to satisfy $\mathcal{B}$ whenenever it is put in parallel with any process satisfying $\mathcal{A}$. This connective gives a functional flavour to the logic, in the sense that the formulas may then describe a service offered by the process they refer to. It has been shown that adjuncts, together with the $\diamond$ connective, allow one to express some very intensional properties, and in fact to capture all constructs of the calculus [San01,HLS02].

Leaving out from MA all capabilities, we get rid of the dynamics of the calculus, working with what we call *static ambients*, SA. The logic may then be restricted to its spatial part by forgetting the $\diamond$ connective; we call it the *static ambient logic*, SAL.

SA, associated to SAL, has appeared to be an interesting model for *semistructured data* [CG01a]. Datas are modeled by unordered labelled trees, where the binders may represent pointers [CGG03], and the logic is used at the basis for a language for queries involving such data. For instance, the process

$$(\nu ptr)(Cardelli[Ambients[ptr[text[\mathbf{0}]]]] \mid Gordon[Ambients[ptr[\mathbf{0}]]])$$

is a database containing the two authors Cardelli and Gordon with one copy of their article about Ambients stored at Cardelli's and linked to Gordon's. The query

$$\mathcal{N}ptr.\, ptr® \,(Cardelli[\top] \mid \top)$$

asks whether the database contains some author named Cardelli.

Here $\mathcal{N}n.\mathcal{A}$ is the fresh quantification [GP99]. Intuitively, its meaning is "for almost all names n, $\mathcal{A}$ is true". This quantification is related to α conversion of bound names. This is complementary with the spatial connective $n®\mathcal{A}$ that forces the process to reveal a hidden name by calling it n.

There may be several ways to answer the question "what is SAL able to tell about data"? A first answer can be to study the *separability* of the logic, that is how far the logic can go into distinguishing two datas. This is usually achieved by characterising the logical equivalence, that is the relation $=_L$ relating the datas that satisfy the same formulas. A more refined answer is to characterise completely the set of queries that can be formulated, what we call the *expressiveness* of the logic. For this, one may like to compare the formalism at hand with another, standard,

logic, or to state equivalences in terms of other models for data analysis, such as automata.

The next question is then "what is really needed" for both separate datas and express properties?" For instace, in the case of the classical propositionnal logic, the *nand* connective is known to generate all the expressiveness. In SAL, the intensional connectives surely bring some expressive power. For the adjunct connectives, the situation is not so clear. Some formulas clearly make an unefficient use of ajduncts; for instance, the formula $n[0] \triangleright n[0]$ is equivalent to the adjunct-free formula 0. However, the model-cheking problem for SAL is known to be undecidable [GC03], whereas it is decidable for SAL_{int}, the fragment without adjuncts. This suggests that adjuncts may express non trivial properties, out of the expressive power of SAL_{int}.

This paper study the question of the adjunct elimination in SAL in relation with the nature of the quantification on formulas. The main contribution establishes the adjunct elimination in SAL equiped with fresh quantifier (Theorem 5.4), namely we prove SAL and SAL_{int} to be equally expressive. This shows that the adjuncts do not improve the expressiveness of the logic. In particular, the guarantee operator $\mathcal{A} \triangleright \mathcal{B}$ does not bring extra expressive power.

This result is derived in two steps. We first establish it for the quantifier-free formulas (Theorem 4.4), and then extend it to fresh-quantified formulas by the use of prenex forms (Proposition 5.3). To establish the adjunct elimination on quantifier-free formulas, we first define a notion of intensional bisimilarity, along the lines of [San01], in which we bound the number of test steps. Then, two properties justify the encoding: a property we call *precompactness*, which expresses finiteness of behaviours, and the existence of characteristic formulas for the classes of bounded intensional bisimilarities.

We conclude with two strongly related contributions. First, we prove the absence of adjunct elimination for $\mathrm{SAL}^{\forall}$, that is SAL equiped with classical quantification (Theorem 6.1). Then we establish that SAL_{int} is *minimal* (Theorem 7.1), in the sense that any subfragment of SAL_{int} is less expressive.

Related work.

Out of [Mey], this is, to our knowledge, the first result delimiting completely the expressiveness of a spatial logic. Other works about expressiveness only give some hints; a first hint has been given about the separation power of AL in [San01]. Other examples of expressive formulas of AL are shown in [HLS02], such as formulas for persistence and finiteness.

A compilation result has been derived for a spatial logic for trees without quantification and private names [Mey]. There the target logic includes some new features such as Presburger arithmetic, and the source logic includes a form of Kleene star.

In the present work, the target logic is a sublogic of the original. In this sense, we also address for the first time *minimality* of a spatial logic, that is the indepence

of its connectives.

The setting in which we obtain our encoding is rather different in the dynamic case [HLS02]. There, the presence of adjuncts considerably increases the expressive power of the logic. For instance, $\triangleright$ allows one to construct formulas to characterise processes of the form $\mathsf{open}\, n.P$, and, using the @ connective, we may define a formula to capture processes of the form $\mathsf{out}\, n.P$.

The use of a bounded intensional bisimilarity and the notion of precompactness is original. Intensional bisimilarity plays an important role in the characterisation of the separation power of the logic [San01]. Our proof suggests that it is also a powerful and meaningful concept for the study of expressiveness.

The presence of the $\triangleright$ connective in the logic is crucial for decidability issues. The undecidability of the model-checking of SAL with classical quantification has been firstly established in [CT01]. Quite unexpected decidability results for spatial logics with $\triangleright$ and without quantification were then established in [CYO01] and [CCG03]. [CCG03] is very related to our purpose; roughly, the decidability result of [CCG03] relies on finiteness of *processes*, whereas our encoding exploits finiteness of *observations*. Most recently, the undecidability of the model-checking of SAL has been established [GC03]. This last work study many variations around SAL, derives also decidability results with $\triangleright$ and $\mathcal{W}$, and presents a prenex form result similar to our.

We introduce SA and the logics we use to reason about data in Sec. 2. We prove the adjunct elimination for quantifier-free formulas in Sec. 4, based on the notion of intensional bisimilarity, discussed in Sec. 3. The general result for SAL is then established in Sec. 5, based on prenex forms. We discuss the adjunct elimination for $\mathrm{SAL}^{\forall}$ in Sec. 6, and show minimality of SAL_{int} in Sec. 7; Sec. 8 gives concluding remarks.

2 Background

In all what follows we assume an infinite set $\mathcal{N}$ of names, ranged over by n, m. Tree terms are defined by the following grammar:

$$P \ ::= \ P \mid P \mid n[P] \mid (\nu n)P \mid \mathbf{0}\,.$$

The set $\mathrm{fn}(P) \subset \mathcal{N}$ of free names of P is defined by saying that ν is the only binder on trees. We call *static ambients* tree terms quotiented by the smallest congruence $\equiv$ (called *structural congruence*) such that:

$$\begin{array}{lll} P \mid \mathbf{0} \equiv P & (\nu n)\mathbf{0} \equiv \mathbf{0} & \\ (P \mid Q) \mid R \equiv P \mid (Q \mid R) & (\nu n)\, m[P] \equiv m[(\nu n)P] & (n \neq m) \\ P \mid Q \equiv Q \mid P & (\nu n)P \mid Q \equiv (\nu n)(P \mid Q) & (n \notin \mathrm{fn}(Q)) \end{array}$$

Formulas, ranged over with $\mathcal{A}, \mathcal{B}, \ldots$, are described by the following grammar:

$$\mathcal{A} ::= \mathcal{A} \wedge \mathcal{A} \mid \neg \mathcal{A} \mid \mathcal{V} n.\, \mathcal{A} \mid \mathbf{0} \mid \mathcal{A} \mid \mathcal{A} \mid n[\mathcal{A}] \mid n \circledR \mathcal{A}$$
$$\mid \mathcal{A} \triangleright \mathcal{A} \mid \mathcal{A} @ n \mid \mathcal{A} \oslash n$$

These formulas form *the static ambient logic*, and we call *intensional fragment* the subset of the formulas not using the connectives $\triangleright$, $@$, and $\oslash$ (ajduncts). We note them respectively SAL and SAL_{int}.

We will say that $\mathcal{A}$ is *quantifier-free* if $\mathcal{A}$ does not contain any $\mathcal{V}$ quantification. The set of free names of a formula $\mathcal{A}$, written $\text{fn}(\mathcal{A})$ is the set of names appearing in $\mathcal{A}$ that are not bound by a $\mathcal{V}$ quantification. $\mathcal{A}(n \leftrightarrow n')$ is the formula $\mathcal{A}$ in which names n and n' are swapped.

Definition 2.1 (Satisfaction) *We define the relation* $\models \subset (SA \times \text{SAL})$ *by induction on the formula as follows:*

- $P \models \mathcal{A}_1 \wedge \mathcal{A}_2$ *if* $P \models \mathcal{A}_1$ *and* $P \models \mathcal{A}_2$
- $P \models \neg \mathcal{A}$ *if* $P \not\models \mathcal{A}$
- $P \models \mathcal{V} n.\, \mathcal{A}$ *if* $\forall n' \in \mathcal{N} - (\text{fn}(P) \cup \text{fn}(\mathcal{A}))$, $P \models \mathcal{A}(n \leftrightarrow n')$
- $P \models \mathcal{A}_1 \mid \mathcal{A}_2$ *if there is* P_1, P_2 *s.t.* $P \equiv P_1 \mid P_2$ *and* $P_i \models \mathcal{A}_i$ *for* $i = 1, 2$
- $P \models 0$ *if* $P \equiv \mathbf{0}$
- $P \models n[\mathcal{A}]$ *if there is* P' *such that* $P \equiv n[P']$ *and* $P' \models \mathcal{A}$
- $P \models n \circledR \mathcal{A}$ *if there is* P' *such that* $P \equiv (\nu n)P'$ *and* $P' \models \mathcal{A}$
- $P \models \mathcal{A}_1 \triangleright \mathcal{A}_2$ *if for all* Q *such that* $Q \models \mathcal{A}_1$, $P \mid Q \models \mathcal{A}_2$
- $P \models \mathcal{A} @ n$ *if* $n[P] \models \mathcal{A}$
- $P \models \mathcal{A} \oslash n$ *if* $(\nu n)P \models \mathcal{A}$

We note $\mathcal{A} \dashv\vdash \mathcal{B}$ if for all $P \in SA$, $P \models \mathcal{A}$ iff $P \models \mathcal{B}$. A context is a formula containing a *hole*; if C is a context, $C[\mathcal{A}]$ stands for the formula obtained by replacing the hole with $\mathcal{A}$ in C. The following property stresses a first difference between SAL and the $\forall/\exists$ version of the logic:

Lemma 2.2 *For all* $\mathcal{A}, \mathcal{B}$, *and all context* C, *if* $\mathcal{A} \dashv\vdash \mathcal{B}$, *then* $C[\mathcal{A}] \dashv\vdash C[\mathcal{B}]$.

Remark 2.3

- The formula $\bot$, that no process satisfies, can be defined as $0 \wedge \neg 0$. As e.g. in [CG00], other derived connectors include $\vee$, and $\blacktriangleright$: P satisfies $\mathcal{A} \blacktriangleright \mathcal{B}$ iff there exists Q satisfying $\mathcal{A}$ such that $P \mid Q$ satisfies $\mathcal{B}$.
- If $P \models \mathcal{A}$ and $P \equiv Q$, then $Q \models \mathcal{A}$. Moreover, $\models$ is *equivariant*, that is $P \models \mathcal{A}$ iff $P(n \leftrightarrow n') \models \mathcal{A}(n \leftrightarrow n')$ for any n, n'.
- For any P, there is a characteristic formula (for $\equiv$) $\mathcal{A}_P$, using the same tree representation, such that for all Q, $Q \models \mathcal{A}_P$ iff $Q \equiv P$. In particular, two static ambients are logically equivalent if and only if they are structurally congruent.

3 Intensional bisimilarity

In this section, we define a notion of partial observation over trees corresponding to logical testing with a bound on the formulas' size and on free names. This notion is an incremental version of the intensional bisimilarity presented in [San01]. We then derive two determinant results:

- the congruence of the intensional bisimilarity, which roughly says that SAL_{int} is as separative as SAL; as an important consequence, the bisimilarity is proved to be correct respect to logical equivalence.
- a construction of symbolic sets that represent the classes of bisimilarity by collecting all the necessary information, which will serve for the proofs of next section.

We assume in the remainder some fixed set $N \subset \mathcal{N}$.

3.1 Definition

We now introduce the intensional bisimilarity. Intuitively, $\simeq_{i,N}$ equates processes that may not be distinguished by logical tests involving at most i steps where the names used for the tests are picked in N.

Definition 3.1 (Intensional bisimilarity) *We define the family $(\simeq_{i,N})_{i\in\mathbb{N}}$ of symetric relations over* SA *by induction on i: $\simeq_{0,N} \stackrel{\text{def}}{=} \mathrm{SA} \times \mathrm{SA}$, and for any $i \geq 1$, $\simeq_{i,N}$ is the greatest relation such that if $P \simeq_{i,N} Q$, then the following conditions are verified:*

(i) *if $P \equiv \mathbf{0}$ then $Q \equiv \mathbf{0}$*

(ii) *for all P_1, P_2, if $P \equiv P_1 \mid P_2$ then there is Q_1, Q_2 such that $Q \equiv Q_1 \mid Q_2$ with $P_\epsilon \simeq_{i-1,N} Q_\epsilon$, $\epsilon = 1, 2$.*

(iii) *for all $n \in N$ and for all P', if $P \equiv n[P']$, then there is Q' such that $Q \equiv n[Q']$ and $P' \simeq_{i-1,N} Q'$.*

(iv) *for all $n \in N$ and for all P', if $P \equiv (\nu n)P'$, then there is Q' such that $Q \equiv (\nu n)Q'$ and $P' \simeq_{i-1,N} Q'$.*

Lemma 3.2 *For all i, $\simeq_{i,N}$ is an equivalence relation.*

We shall write $\mathrm{SA}_{/\simeq_{i,N}}$ for the equivalence classes induced by $\simeq_{i,N}$, and range over equivalence classes with C, C_1, C_2.

We may observe that the bisimilarities define a stratification of observations on terms, namely $\simeq_{i',N'} \subseteq \simeq_{i,N}$ for $i \leq i'$ and $N \subseteq N'$. This may be understood in a topological setting. Given a fixed N, we consider the ultrametric distance over models defined by $d(P,Q) = 2^{-i}$ if i is the smallest natural for which $P \not\simeq_{i,N} Q$, and $d(P,Q) = 0$ if $P \simeq_{\omega,N} Q$ where $\simeq_{\omega,N} = \bigcap_{i\in\mathbb{N}} \simeq_{i,N}$. We call it the N-topology. It somehow captures the granularity of the logical observations with respect to their cost.

3.2 Correction

The key step in proving correction of the intensional bisimilarities with respect to the logic is their congruence properties for the connectives admittting an adjunct.

Lemma 3.3 *If $P \simeq_{i,N} Q$, then:*

- *for all R, $P \mid R \simeq_{i,N} Q \mid R$;*
- *for all $n \in \mathcal{N}$, $n[P] \simeq_{i,N} n[Q]$;*
- *for all $n \in N$, $(\nu n)P \simeq_{i,N} (\nu n)Q$.*

Proof. By induction on i. □

Note that the last point cannot be improved: consider $N = \{n\}$, $P \equiv m_1[\mathbf{0}]$, $Q \equiv m_2[\mathbf{0}]$. Then $P \simeq_{2,N} Q$, but $(\nu m_1)P \not\simeq_{2,N} (\nu m_1)Q$. For this reason, $\simeq_{i,N}$ is not a pure congruence.

We note $s(\mathcal{A})$ the size of $\mathcal{A}$, defined as the number of its connectives.

Proposition 3.4 (Correction) *For all P, Q, i such that $P \simeq_{i,N} Q$, for all quantifier free formula $\mathcal{A}$ such that $s(\mathcal{A}) \leq i$ and* $\mathrm{fn}(\mathcal{A}) \subseteq N$,

$$P \models \mathcal{A} \qquad \textit{iff} \qquad Q \models \mathcal{A}.$$

Proof. By induction on $\mathcal{A}$. For the adjuncts, apply the congruence properties of Lemma 3.3, and for the other connectives use the definition of $\simeq_{i,N}$. □

3.3 Signature functions

Definition 3.5 (Signature) *For $i \geq 1$, we set:*

(i) $z_i^N(P) = 0$ *if* $P \equiv \mathbf{0}$, *otherwise* $\neg 0$

(ii) $p_i^N(P) = \{(C_1, C_2) \in (\mathrm{SA}_{/\simeq_{i-1,N}})^2 : P \equiv P_1 \mid P_2 \text{ and } P_i \in C_i\}$

(iii) $a_i^N(P) = [n, C]$ *if there is P' s.t. $P \equiv n[P']$, $n \in N$ and $P \in C$, $C \in \mathrm{SA}_{/\simeq_{i-1,N}}$, otherwise* $a_i^N(P) = \mathsf{noobs}$, *where* noobs *is a special constant.*

(iv) $r_i^N(P) = \{(n, C) \in N \times \mathrm{SA}_{/\simeq_{i-1,N}} : \exists P'.\ P \equiv (\nu n)P' \text{ and } P' \in C\}$

We call signature of P at (i, N) *the quadruplet* $\chi_i^N(P) = [z_i^N(P), p_i^N(P), a_i^N(P), r_i^N(P)]$.

The following lemma says that the signature actually collects all the information that may be obtained from the bisimilarity tests.

Lemma 3.6 *Assume $i \geq 1$. Then $P \simeq_{i,N} Q$ iff $\chi_i^N(P) = \chi_i^N(Q)$.*

4 Adjuncts elimination on quantifier-free formulas

In this section, we show that the quantifier free formulas of SAL have equivalent formulas in SAL_{int}. This result is then extended to all formulas of SAL in the next section.

In all what follows, we will assume N is a finite subset of $\mathcal{N}$; it is intended to bound the free names of the considered formulas. The encoding result is based on two key properties:

- Precompactness of the N-topology. In other words, when i, N are fixed, only a finite number of scenari may be observed.
- Existence of intensional characteristic formulas for the classes of $\simeq_{i,N}$.

Lemma 4.1 *The codomain of χ_i^N is finite.*

Proof. We reason by induction on i. First notice that the codomain of χ_i^N is:

$$\mathbf{codom}\,\chi_i^N \;=\; \{0, \neg 0\} \times (\mathrm{SA}_{/\simeq_{i-1,N}})^2 \times (\{\mathsf{noobs}\} + N \times \mathrm{SA}_{/\simeq_{i-1,N}}) \times (N \times \mathrm{SA}_{/\simeq_{i-1,N}})$$

hence $\mathbf{codom}\,\chi_i^N$ is finite iff $\mathrm{SA}_{/\simeq_{i-1,N}}$ is finite too (here we use that N is finite). For $i = 1$, $\mathrm{SA}_{/\simeq_{0,N}} = \{\mathrm{SA}\}$, hence χ_0^N is finite, and so is $\mathbf{codom}\,\chi_1^N$. For $i \geq 2$, we have by induction $\mathbf{codom}\,\chi_{i-1}^N$ finite. By Lemma 3.6, there is an injection of $\mathrm{SA}_{/\simeq_{i-1,N}}$ into $\mathbf{codom}\,\chi_{i-1}^N$, so $\mathrm{SA}_{/\simeq_{i-1,N}}$ is finite, and so is $\mathbf{codom}\,\chi_i^N$. □

Here is an immediate consequence of Lemma 4.1:

Proposition 4.2 (Precompactness) *For all i, the number of classes of $\simeq_{i,N}$ is finite.*

These results roughly say that there is only a finite amount of information in the determination of a given bisimilarity class. The next result makes it more precise: this information may be collected in a single formula of SAL_{int}.

Proposition 4.3 (Characteristic formulas) *For any $i \in \mathbb{N}$ and for any process P, there is a formula $\mathcal{A}_P^{i,N} \in \mathrm{SAL}_{int}$ such that*

$$\forall Q \qquad Q \models \mathcal{A}_P^{i,N} \qquad \Leftrightarrow \qquad Q \simeq_{i,N} P\,.$$

Proof. By induction on i. For $i = 0$, we may take $\mathcal{A}_P^{i,N} = \top$. Then assume $i \geq 1$, and we have formulas $\mathcal{A}_P^{i-1,N}$ for all P. This obviously gives a characteristic formula $\mathcal{A}_C^{i-1,N}$ for any class C of $\mathrm{SA}_{/\simeq_{i-1,N}}$. Let us consider some fixed P. We set

$$\begin{aligned}
\mathcal{A}_z &= 0 \text{ if } z_i^N(P) = 0, \text{ otherwise } \neg 0\\
\mathcal{A}_p &= \textstyle\bigwedge_{(C_1,C_2)\in p_i^N(P)} \mathcal{A}_{C_1}^{i-1,N} \mid \mathcal{A}_{C_2}^{i-1,N} \;\wedge\; \neg \bigvee_{(C_1,C_2)\notin p_i^N(P)} \mathcal{A}_{C_1}^{i-1,N} \mid \mathcal{A}_{C_2}^{i-1,N}\\
\mathcal{A}_a &= \begin{cases} \bigwedge_{n\in N} \neg\, n[\top] & \text{if } a_i^N(P) = \mathsf{noobs}\\ n[\mathcal{A}_C^{i-1,N}] & \text{if } a_i^N(P) = [n, C] \end{cases}\\
\mathcal{A}_r &= \textstyle\bigwedge_{[n,C]\in r_i^N(P)} n\text{®}\mathcal{A}_C^{i-1,N} \;\wedge\; \neg \bigvee_{[n,C]\notin r_i^N(P)} n\text{®}\mathcal{A}_C^{i-1,N}\\
\mathcal{A}_P^{i,N} &= \mathcal{A}_z \wedge \mathcal{A}_p \wedge \mathcal{A}_a \wedge \mathcal{A}_r
\end{aligned}$$

where the finiteness of the conjunctions and disjunctions is ensured by Lemma 4.1.

Then $Q \models \mathcal{A}_P^{i,N}$ iff $\chi_i^N(Q) = \chi_i^N(P)$, hence the result. □

The precompactness property says that if we bound the granularity of the observations, only finitely many distinct situations may occur. The characteristic formula property says that each of these situations is expressible in the intensional fragment. The idea of the encoding is then just to logically enumerate all these possible situations.

Theorem 4.4 *For all quantifier-free formula* $\mathcal{A} \in \mathrm{SAL}$*, there is a formula* $[\mathcal{A}] \in \mathrm{SAL}_{int}$ *such that*

$$\mathcal{A} \dashv\vdash [\mathcal{A}].$$

Proof. We define $[\mathcal{A}]$ as follows:

$$[\mathcal{A}] \stackrel{\text{def}}{=} \bigvee \mathcal{A}_C^{i,N} \qquad \text{for } C \in \mathrm{SA}_{/\simeq_{i,N}}, C \models \mathcal{A}$$

for $i = s(\mathcal{A})$ and $N = \mathrm{fn}(\mathcal{A})$. The disjunction is finite by Proposition 4.2. $P \models [\mathcal{A}]$ iff there is Q such that $Q \models \mathcal{A}$ and $P \simeq_{i,N} Q$, that is, by Proposition 3.4, $P \models \mathcal{A}$. □

Effectiveness of the encoding:
According to its finiteness, the construction of our proof could seem almost effective. However, this cannot be the case due to an undecidability result for the model-checking problem on SAL[GC03]. This is quite surprising, since it misses only an effective enumeration of the bisimilarity classes to turn the proof in a constructive way. Moreover, such an enumeration exists for SA without name restriction, via testing sets as defined in [CCG03]. This reveals an unexpected richness of SA compared to pure trees.

5 Adjuncts elimination and fresh quantifier

In this section we establish the adjunct elimination for the full SAL. The essential result that entails this extension is the existence of prenex forms for the fresh quantifier. Intuitively, the fresh quantifier may "float" on the formula without changing its meaning.

Proposition 5.1 (Correction of $\rightsquigarrow$) *The term rewriting system* $\rightsquigarrow$ *defined by the rules of Fig. 1 conserves the semantic: for any* $A, B \in \mathrm{SAL}$*, if* $A \rightsquigarrow B$*, then* $\mathcal{A} \dashv\vdash \mathcal{B}$*.*

$$
\begin{array}{lrcll}
(\wedge) & (\mathcal{U}n.\mathcal{A}_1) \wedge \mathcal{A}_2 & \rightsquigarrow & \mathcal{U}n.(\mathcal{A}_1 \wedge \mathcal{A}_2) & (n \notin \mathrm{fn}(\mathcal{A}_2)) \\
(\neg) & \neg\, \mathcal{U}n.\mathcal{A}_1 & \rightsquigarrow & \mathcal{U}n.\neg\, \mathcal{A}_1 & \\
(|) & (\mathcal{U}n.\mathcal{A}_1) \mid \mathcal{A}_2 & \rightsquigarrow & \mathcal{U}n.(\mathcal{A}_1 \mid \mathcal{A}_2) & (n \notin \mathrm{fn}(\mathcal{A}_2)) \\
(\triangleright L) & (\mathcal{U}n.\mathcal{A}_1) \triangleright \mathcal{A}_2 & \rightsquigarrow & \mathcal{U}n.\left((n \circledR \top \wedge \mathcal{A}_1) \triangleright \mathcal{A}_2\right) & (n \notin \mathrm{fn}(\mathcal{A}_2)) \\
(\triangleright R) & \mathcal{A}_1 \triangleright (\mathcal{U}n.\mathcal{A}_2) & \rightsquigarrow & \mathcal{U}n.\left((n \circledR \top \wedge A_1) \triangleright \mathcal{A}_2\right) & (n \notin \mathrm{fn}(\mathcal{A}_1)) \\
(Amb) & m[\mathcal{U}n.\mathcal{A}] & \rightsquigarrow & \mathcal{U}n.\, m[\mathcal{A}] & (m \neq n) \\
(@) & (\mathcal{U}n.\mathcal{A})@m & \rightsquigarrow & \mathcal{U}n.(\mathcal{A}@m) & (m \neq n) \\
(\circledR) & m \circledR \mathcal{U}n.\mathcal{A} & \rightsquigarrow & \mathcal{U}n.\, m \circledR \mathcal{A} & (m \neq n) \\
(\oslash) & (\mathcal{U}n.\mathcal{A}) \oslash m & \rightsquigarrow & \mathcal{U}n.(\mathcal{A} \oslash m) & (m \neq n)
\end{array}
$$

Fig. 1. Term rewriting system on formulas

Proof. (sketched) We only detail the rule $(\triangleright L)$.

$$
\begin{aligned}
& P \models (\mathcal{U}n.\mathcal{A}_1) \triangleright \mathcal{A}_2 \\
\Leftrightarrow\ & \forall Q, \forall n' \notin \mathrm{fn}(\mathcal{A}_1) \cup \mathrm{fn}(Q).\ Q \models \mathcal{A}_1(n \leftrightarrow n') \ \Rightarrow\ P \mid Q \models \mathcal{A}_2 \\
\Leftrightarrow\ & \forall Q, \forall n' \notin \mathrm{fn}(\mathcal{A}_1 \triangleright \mathcal{A}_2) \cup \mathrm{fn}(P \mid Q).\ Q \models \mathcal{A}_1(n \leftrightarrow n') \ \Rightarrow\ P \mid Q \models \mathcal{A}_2 \\
\Leftrightarrow\ & \forall Q, \forall n' \notin \mathrm{fn}(\mathcal{A}_1 \triangleright \mathcal{A}_2) \cup \mathrm{fn}(P \mid Q).\ Q \models \mathcal{A}_1(n \leftrightarrow n') \ \Rightarrow\ P \mid Q \models \mathcal{A}_2(n \leftrightarrow n') \\
\Leftrightarrow\ & \forall n' \notin \mathrm{fn}(\mathcal{A}_1 \triangleright \mathcal{A}_2) \cup \mathrm{fn}(P), \\
& \quad \forall Q.\, n' \notin \mathrm{fn}(Q) \ \Rightarrow\ Q \models \mathcal{A}_1(n \leftrightarrow n') \ \Rightarrow\ P \mid Q \models \mathcal{A}_2(n \leftrightarrow n') \\
\Leftrightarrow\ & P \models \mathcal{U}n.\ (\mathcal{A}_1 \wedge n \circledR \top) \triangleright \mathcal{A}_2
\end{aligned}
$$

□

Remark 5.2 Some of the rules above (such as (Amb), $(\neg)$, and a variant of $(|\ L)$) have already been presented in [CG01b], under the form of equalities. The same result is independantly developped in [GC03].

We say that a formula $\mathcal{A}$ is *wellformed* if every variable bound by $\mathcal{U}$ is distinct from all other (bound and free) variables in $\mathcal{A}$. For such formulas, the side conditions in $\rightsquigarrow$ are always satisfied.

It is easy to see that $\rightsquigarrow$ defines a terminating rewriting system, and that the normal forms of the wellformed formulas are formulas in prenex form. Confluence holds modulo permutation of consecutive $\mathcal{U}$ quantifiers.

Proposition 5.3 (Prenex forms) *For any formula $\mathcal{A}$, there are $\tilde{n}, \mathcal{A}'$ such that $\mathcal{A} \dashv\vdash \mathcal{U}\tilde{n}.\mathcal{A}'$ and $\mathcal{A}'$ is quantifier free.*

This result directly implies the following generalisation of Theorem 4.4:

Theorem 5.4 (Adjunct elimination) *For all formula* $\mathcal{A} \in \mathrm{SAL}$*, there is a formula* $[\mathcal{A}] \in \mathrm{SAL}_{int}$ *such that*

$$\mathcal{A} \dashv\vdash [\mathcal{A}].$$

Proof. There is A' quantifier free and $\tilde{n}$ such that $\mathcal{A} \dashv\vdash \mathcal{N}\tilde{n}.\mathcal{A}'$ by Proposition 5.3. Then by Lemma 2.2 and Theorem 4.4, we may write

$$A \dashv\vdash \mathcal{N}\tilde{n}.A' \dashv\vdash \mathcal{N}\tilde{n}.[A']$$

□

Example 5.5 : We sketch an example to illustrate how SAL_{int} formulas can capture non trivial properties expressed using the adjuncts. Let

$$\mathcal{A} ::= \Big(Hm'.m'[\top] \blacktriangleright (Hn_1.n_1[0] \mid Hn_2.n_2[Hn_3.n_3[0]])\Big) \oslash m@m$$

where $Hn.\mathcal{A}$ (H being the *hidden name quantifier* [CC01]) stands for $\mathcal{N}n.n\circledR\mathcal{A}$. The prenex form of $\mathcal{A}$ is

$$\mathcal{N}m', n_1, n_2, n_3.\ \Big((m'\circledR\top\wedge.m'\circledR m'[\top]) \blacktriangleright (n_1\circledR n_1[0] \mid n_2\circledR n_2[n_3\circledR.n_3[0]])\Big) \oslash m@m$$

Then $P \models \mathcal{A}$ iff there is Q such that

$$(\nu m)\, m[P] \mid (\nu m')\, m'[Q] \equiv (\nu n_1)(\nu n_2)(\nu n_3)(n_1[\mathbf{0}] \mid n_2[n_3[\mathbf{0}]])$$

The only solutions of this equation are $P \equiv \mathbf{0}$ or $P \equiv (\nu n_3)n_3[\mathbf{0}]$. In other words, $\mathcal{A}$ is equivalent to $\mathcal{B} = 0 \vee Hn_3.n_3[0]$.

6 Adjuncts elimination and classical quantifiers

In this section we consider a variant of SAL. Instead of fresh quantified formulas, we consider formulas quantified on names of the form $\forall x.\mathcal{A}$ and $\exists x.\mathcal{A}$ with the natural semantic:

$$P \models \forall x.\mathcal{A} \qquad \text{if} \qquad \forall n \in \mathcal{N}.\ P \models \mathcal{A}\{^n/_x\}$$

Let note $\mathrm{SAL}^{\forall}_{int}$ the intensional fragment with the classical quantification. We ask the question of adjuncts elimination for extensions of this logic. The undecidability result of [CT01] implies that there is no effective adjunct elimination for $\mathrm{SAL}^{\forall}_{int} + \{\triangleright\}$. We establish now a more precise result:

Theorem 6.1 (Adjuncts expressivity in $\mathrm{SAL}^{\forall}_{int}$**)** $\mathrm{SAL}^{\forall}_{int} + \{\triangleright\}$, $\mathrm{SAL}^{\forall}_{int} + \{@\}$ *and* $\mathrm{SAL}^{\forall}_{int} + \{\oslash\}$ *are strictly more expressive than* SAL_{int}.

The proof of this theorem is based on the following observation. In any of the considered extension, this is possible to define a formula $\mathcal{A}$ such that

(1) $$P \models \mathcal{A} \qquad \text{iff} \qquad \sharp\,\mathrm{fn}(P) \leq 1$$

For the $\triangleright$ and @ connectives, we may first encode the formula $n = m$ as $(n[\top] \wedge \neg\, m[\top]) \triangleright \bot$ and $(n[\top])@m$. Then (1) is satisfied by the formula

$$\exists x.\ \forall y.\ (\neg\, y \circledR \top) \rightarrow x = y$$

For the $\oslash$ connective, there is a direct formula satisfying (1):

$$\exists x.\ (\forall y.\ y \circledR \top) \oslash x$$

However, $\mathrm{SAL}^{\forall}_{int}$ cannot bound the number of free names of its model. More precisely,

Proposition 6.2 *There is no formula in* $\mathrm{SAL}^{\forall}_{int}$ *that satisfies (1).*

The proof of this proposition is quite technical and given in appendix.

7 Minimality

In this section, we show minimality w.r.t. expressive power of SAL_{int}. Our result follows from several technical lemmas that are given in appendix.

Theorem 7.1 (Minimality) SAL_{int} *is a minimal logic, that is all fragments of* SAL_{int} *are less expressive.*

Proof (Sketch) We show that for each connective κ, the logic resulting from the removal of κ is stricly less expressive than SAL_{int}. We give an idea of the argument in each case.

- $\kappa = \wedge$: then we may not express $n_1[n_2[0]] \vee n_2[n_1[0]]$.
- $\kappa = \neg$: then we may not express $\neg\, n \circledR \top$, saying that n occurs free. To prove this, we remark that for a formula $\mathcal{A}$ without negation, there is a height h such that for all P, if $P \models \mathcal{A}$ then so does the truncation of P at height h, so we may find a contradiction by considering a process having a deep enough occurrence of n.
- $\kappa = \mathit{\Pi}$: then we may not express $\mathit{\Pi} n.\, n \circledR \neg\, n \circledR \top$: P is a model of this formula iff there is n, P' s.t. $P \equiv (\nu n)P'$ with $n \in \mathrm{fn}(P')$. For $N = \{n_1, \ldots n_r\}$ we consider $P_N = n[n_1[\mathbf{0}] \mid \ldots \mid n_r[\mathbf{0}]]$ for some $n \notin N$. Then for any quantifier free formula $\mathcal{A}$ with $\mathrm{fn}(\mathcal{A}) \subseteq N$, $P \models \mathcal{A}$ iff $(\nu n)P \models \mathcal{A}$.
- $\kappa = 0$: here we assume we take $\top$ instead of 0 as a primitive formula. Then 0 is not expressible. For this, we remark that for any $\mathcal{A}$ without 0 and for $n \notin \mathrm{fn}(A)$, $\mathbf{0} \models \mathcal{A}$ iff $n[\mathbf{0}] \models \mathcal{A}$.
- $\kappa = .\,|\,.$: the separation power is different. For instance, we may not distinguish $n[\mathbf{0}] \mid n[\mathbf{0}]$ from $n[\mathbf{0}] \mid n[\mathbf{0}] \mid n[\mathbf{0}]$.
- $\kappa = n[\,.\,]$: we may not distinguish $n_1[n_2[\mathbf{0}]]$ from $n_2[n_1[\mathbf{0}]]$.

- $\kappa = n\circledR.$: we may not distinguish $(\nu n)n[\mathbf{0}]$ and $(\nu n)n[n[\mathbf{0}]]$.

□

Remark 7.2

- In the proof above, the cases involving the intensional connectives $.|.$, $n[.]$ and $n\circledR.$ are treated by showing that the *separation power* of the logic is reduced. This entails a loss in terms of expressiveness, since equally expressive logics have the same separation power.
- SAL_{int} is minimal in terms of expressiveness, but as far as separation power is concerned, the minimal fragment is $\mathrm{SAL}_{int} - \{И, \neg, \wedge, 0\}$, since for this fragment logical equivalence coincides with intensional bisimilarity.
- Notice that we do not show that SAL_{int} is the *unique* minimal fragment of SAL. This is far from being obvious. For instance, the fragment $\mathrm{SAL} - \{\wedge\}$ is surprisingly quite expressive, as the formula

$$\neg И n.\, n\circledR \neg n\circledR\, (И m_1.\, m_1\circledR И m_2.\, m_2\circledR m_1[m_2[0]]) \oslash n_1 \oslash n_2$$

  shows. This formula is equivalent to $n_1[n_2[0]] \vee n_2[n_1[0]]$, and hence the case $\kappa = \wedge$ in the proof of Theorem 7.1 does not apply here. We do not know the exact expressiveness of this fragment, one could think that it captures any finite set of processes. The interested reader may want to look for a formula for $n_1[0] \vee n_2[n_2[0]]$ in this fragment.

8 Conclusion

We have established the adjuncts elimination property for SAL, a logic for trees with binders including the fresh quantifier $И$. This involves putting a formula in prenex form and then doing the transformation on the quantifier-free formula. The adjunct-free fragment SAL_{int} turns then to be a *minimal* logic.

We established the absence of adjunct elimination for the same logic where $И$ is replaced by the usual $\forall$ quantifier, whatever adjunct is considered. This result, together with the difference of the model-checking treatment on pure trees, illustrates the significant gap existing between both forms of quantification.

Acknowledgement

This work has been supported by the european FET - Global Computing project Profundis, and by the Action Incitative *Méthodes Formelles pour la Mobilité* - CNRS.

I would like to thank M.J. Gabbay for enlightening discussions about Nominal Sets theory. The anonymous referees and G. Ghelli helped me significantly to improve the first version of this presentation. I also want to thank D. Sangiorgi, L. Monteiro, L. Caires, and D. Hirschkoff for their advice all along this work.

References

[CC01] L. Caires and L. Cardelli. A Spatial Logic for Concurrency (Part I). In *Proc. of TACS'01*, LNCS. Springer Verlag, 2001.

[CCG03] C.Calcagno, L. Cardelli, and A. Gordon. Deciding Validity in a Spatial Logic for Trees. In *Proc. of TLDI'03*, pages 62–73. ACM, 2003.

[CG98] L. Cardelli and A. Gordon. Mobile Ambients. In *Proc. of FOSSACS'98*, volume 1378 of *LNCS*, pages 140–155. Springer Verlag, 1998.

[CG00] L. Cardelli and A. Gordon. Anytime, Anywhere, Modal Logics for Mobile Ambients. In *Proc. of POPL'00*, pages 365–377. ACM Press, 2000.

[CG01a] L. Cardelli and G. Ghelli. A Query Language Based on the Ambient Logic. In *Proc. of ESOP'01*, volume 2028 of *LNCS*, pages 1–22. Springer Verlag, 2001. invited paper.

[CG01b] L. Cardelli and A. Gordon. Logical Properties of Name Restriction. In *Proc. of TLCA'01*, volume 2044 of *LNCS*. Springer Verlag, 2001.

[CGG03] L. Cardelli, P. Gardner, and G. Ghelli. Manipulating trees with hidden labels. In *Foundations of Software Science and Computational Structures, 6th International Conference, FOSSACS 2003*, LNCS 2620, pages 216–232. Springer, 2003.

[CT01] W. Charatonik and J-M. Talbot. The Decidability of Model Checking Mobile Ambients. In *Proc. of CSL'01*, LNCS. Springer LNCS, 2001.

[CYO01] C. Calcagno, H. Yang, and P. O'Hearn. Computability and Complexity Results for a Spatial Assertion Language for Data Structures. In *Proceedings of FSTTCS '01*, volume 2245 of *LNCS*. Springer Verlag, 2001.

[GC03] G. Ghelli and G. Conforti. Decidability of freshness, undecidability of revelation. Technical Report TR 03 -11, Università di Pisa, 2003.

[GP99] M. J. Gabbay and A. M. Pitts. A new approach to abstract syntax involving binders. In *14th Annual Symposium on Logic in Computer Science*, pages 214–224. IEEE Computer Society Press, Washington, 1999.

[HLS02] D. Hirschkoff, E. Lozes, and D. Sangiorgi. Separability, Expressiveness and Decidability in the Ambients Logic. In *17th IEEE Symposium on Logic in Computer Science*, pages 423–432. IEEE Computer Society, 2002.

[Mey] C. Meyssonnier. A Logic You Can Count On. In preparation.

[San01] D. Sangiorgi. Extensionality and Intensionality of the Ambient Logic. In *Proc. of 28th POPL*, pages 4–17. ACM Press, 2001.

A Proof of Theorem 7.1 (minimality)

We detail the removal of each connective in the minimality proof for SAL_{int}. Some connectives are coined *'expressive'*, in the sense that removing them hinders the expressive power of the logic, others are *'separative'*, because their removal affects the separation power (and hence expressiveness) of the logic.

A.1 $\wedge$ is expressive

We note $\mathcal{P}_2(\mathcal{N}) = \{\{n_1, n_2\} : n_1 \neq n_2\}$. We note $K_n = \{\{n, m\} : m \neq n\}$. We say that $K \subseteq \mathcal{P}_2(\mathcal{N})$ is cofinite if there is $N \subseteq \mathcal{N}$, N finite, such that for all $n_1, n_2 \notin N$, if $n_1 \neq n_2$ then $\{n_1, n_2\} \in K$. We may remark that K_1, K_2 are cofinite iff $K_1 \cap K_2$ is cofinite, and K is cofinite iff $K - K_n$ is cofinite.

Lemma A.1 *Assume $\mathcal{A}$ is a formula of $\mathrm{SAL}_{int} - \{\wedge\}$ such that $\mathbf{0} \not\models \mathcal{A}$. We set*

$$K_{\mathcal{A}} \stackrel{\text{def}}{=} \{\, \{n_1, n_2\} : n_1 \neq n_2,\ n_1[n_2[\mathbf{0}]] \models \mathcal{A} \text{ and } n_2[n_1[\mathbf{0}]] \models \mathcal{A} \,\}.$$

Then either $K_{\mathcal{A}} = \emptyset$ or $K_{\mathcal{A}}$ is cofinite.

Proof. By induction on $\mathcal{A}$:

- $\mathcal{A} = \forall n.\, \mathcal{A}_1$. Then $\mathbf{0} \not\models \mathcal{A}_1$, and for any n_1, n_2 s.t. $n_1 \neq n, n_2 \neq n$ and $n_1 \neq n_2$, $\{n_1, n_2\} \in K_{\mathcal{A}_1}$ iff $\{n_1, n_2\} \in K_{\mathcal{A}_1}$. That is $K_{\mathcal{A}} - K_n = K_{\mathcal{A}_1} - K_n$.
- $\mathcal{A} = 0$: $\mathbf{0} \models \mathcal{A}$.
- $\mathcal{A} = \neg 0$: then $K_A = \mathcal{P}_2$
- $\mathcal{A} = \mathcal{A}_1 \mid \mathcal{A}_2$: since $\mathbf{0} \not\models \mathcal{A}$, we may assume by symetry that $\mathbf{0} \not\models \mathcal{A}_1$. If also $\mathbf{0} \not\models \mathcal{A}_2$, then $K_{\mathcal{A}} = \emptyset$. Otherwise, $K_{\mathcal{A}} = K_{\mathcal{A}_1}$.
- $\mathcal{A} = \mathcal{A}_1 \parallel \mathcal{A}_2$: since $\mathbf{0} \not\models \mathcal{A}$, $\mathbf{0} \not\models \mathcal{A}_1$ and $\mathbf{0} \not\models \mathcal{A}_2$. then $K_{\mathcal{A}} = K_{\mathcal{A}_1} \cap K_{\mathcal{A}_2}$.
- $\mathcal{A} = n[\mathcal{A}_1]$: then $K_{\mathcal{A}} = \emptyset$.
- $\mathcal{A} = \neg\, n[\mathcal{A}_1]$: then $\mathcal{P}_2(\mathcal{N}) - K_n \subseteq K_{\mathcal{A}}$, so $K_{\mathcal{A}}$ is cofinite.
- $\mathcal{A} = n ® \mathcal{A}_1$: then $\mathbf{0} \not\models \mathcal{A}_1$, and $K_{\mathcal{A}} - K_n = K_{\mathcal{A}_1} - K_n$.
- $\mathcal{A} = \neg\, n ® \mathcal{A}_1$: then $\mathbf{0} \not\models \mathcal{A}_1$, and $K_{\mathcal{A}} - K_n = K_{\neg \mathcal{A}_1} - K_n$.

□

Lemma A.2 *Let n_1, n_2 be two distinct names. Then there is no formula $\mathcal{A} \in \mathrm{SAL}_{int} - \{\wedge\}$ equivalent to $n_1[n_2[0]] \vee n_2[n_1[0]]$.*

Proof. By absurd: if there is such a formula $\mathcal{A}$, then $\mathbf{0} \not\models \mathcal{A}$. Then by Lemma A.1 $\sharp K_{\mathcal{A}} \neq 1$, and the contradiction. □

Remark: Surprisingly, there is a formula in $\mathrm{SAL}_{int} - \{\wedge\}$ equivalent to $n_1[0] \vee n_2[0]$. This is

$$\neg\, n_1 ® \neg\, n_2[0] \ \parallel\ \neg\, n_2 ® \neg\, n_1[0]$$

A.2 $\neg$ is expressive

Definition A.3 We define the truncation at height $h \in \mathbb{N}$ as $t_0(P) = \mathbf{0}$, and

$$t_h((\nu\tilde{n})(n_1[P_1] \mid \ldots \mid n_r[P_r])) \;=\; (\nu\tilde{n})(n_1[t_{h-1}(P_1)] \mid \ldots \mid n_r[t_{h-1}(P_r)]).$$

Note that $\mathrm{fn}(t_h(P)) \subseteq \mathrm{fn}(P)$.

Lemma A.4 *If $\mathcal{A}$ is a formula without $\neg$, $s(\mathcal{A}) \leq h$ and $P \models \mathcal{A}$, then $t_h(P) \models \mathcal{A}$.*

Proof. By induction on $\mathcal{A}$:

- $\mathcal{A} = \mathcal{A}_1 \wedge \mathcal{A}_2$: then by induction $t_h(P) \models \mathcal{A}_1$, $t_h(P) \models \mathcal{A}_2$, so $t_h(P) \models \mathcal{A}_1 \wedge \mathcal{A}_2$.
- $\mathcal{A} = \mathcal{V}n.\mathcal{A}_1$: then there is $n' \notin \mathrm{fn}(P)$ s.t. $P \models \mathcal{A}_1(n \leftrightarrow n')$. By induction $t_h(P) \models \mathcal{A}_1(n \leftrightarrow n')$, $n' \notin \mathrm{fn}(t_h(P))$, so $t_h(P) \models \mathcal{V}n.\mathcal{A}_1$.
- $\mathcal{A} = 0$: then $t_h(P) \equiv P \equiv \mathbf{0}$
- $\mathcal{A} = \mathcal{A}_1 \mid \mathcal{A}_2$: then $P \equiv P_1 \mid P_2$ with $P_\epsilon \models \mathcal{A}_\epsilon$, and by induction $t_h(P_\epsilon) \models \mathcal{A}_\epsilon$, so $t_h(P) \models \mathcal{A}$.
- $\mathcal{A} = n[\mathcal{A}_1]$: then $P \equiv n[P_1]$ and $P_1 \models \mathcal{A}_1$. By induction, $t_{h-1}(P_1) \models \mathcal{A}_1$, and so $t_h(P) \models \mathcal{A}$.
- $\mathcal{A} = n\circledR\mathcal{A}_1$: then $P \equiv (\nu n)P_1$ with $P_1 \models \mathcal{A}_1$. Then by induction $t_h(P_1) \models \mathcal{A}_1$, so $t_h(P) \models \mathcal{A}$.

□

Lemma A.5 *There is no formula $\mathcal{A} \in \mathrm{SAL}_{int} - \{\neg\}$ equivalent to $\neg\, n\circledR\bot$.*

Proof. Suppose $\mathcal{A}$ exists, and take $h = s(A)$. We note $P \equiv m[m[\ldots m[\mathbf{0}]\ldots]]$ and $Q \equiv m[m[\ldots m[n[\mathbf{0}]]\ldots]]$ a nesting of h ambients m, for some $m \neq n$. Then $Q \models \mathcal{A}$, $P \not\models \mathcal{A}$, and $P \equiv t_h(Q)$, which contradicts Lemma A.4 □

A.3 $\mathcal{V}$ is expressive

For $N = \{n_1, \ldots n_r\}$, we set $P^n_N = n[n_1[\mathbf{0}] \mid \ldots \mid n_r[\mathbf{0}]]$.

Lemma A.6 *Assume some finite set of names N and a quantifier free formula $\mathcal{A}$ such that $\mathrm{fn}(\mathcal{A}) \subset N$, and $n \notin N$. Then*

$$P^n_N \models \mathcal{A} \;\; \textit{iff} \;\; (\nu n)P^n_N \models \mathcal{A}$$

Proof. By induction on $\mathcal{A}$:

- the cases $\mathcal{A} = \mathcal{A}_1 \wedge \mathcal{A}_2$, and $\mathcal{A} = \neg\mathcal{A}_1$, are straightforward.
- if $\mathcal{A} = 0$: then none of the two processes satisfies $\mathcal{A}$.
- if $\mathcal{A} = \mathcal{A}_1 \mid \mathcal{A}_2$. Assume first that $P^n_N \models \mathcal{A}$. By symmetry, we may assume $P^n_N \models \mathcal{A}_1$ and $\mathbf{0} \models \mathcal{A}_2$. So $(\nu n)P^n_N \models \mathcal{A}_1$ by induction, and $(\nu n)P^n_N \models \mathcal{A}$. If we assume $(\nu n)P^n_N \models \mathcal{A}$, we may do the same reasoning.
- $\mathcal{A} = m[\mathcal{A}_1]$: none of $P^n_N, (\nu n)P^n_N$ does satisfy $\mathcal{A}$.

- $\mathcal{A} = m\text{®}\mathcal{A}_1$: then $m \in \text{fn}(\mathcal{A}) \subseteq N$, hence none of $P^n_N, (\nu n)P^n_N$ does satisfy $\mathcal{A}$.

□

Lemma A.7 *There is no formula $\mathcal{A} \in \text{SAL}_{int} - \{\mathcal{N}\}$ equivalent to $\mathcal{N}n.\, n\text{®}n\text{®}\bot$.*

Proof. By absurd, let $\mathcal{A}$ be such a quantifier free formula, and $\{n_1, \ldots, n_r\} = \text{fn}(\mathcal{A})$. Then $P^n_N \not\models \mathcal{A}$, so $(\nu n)P \not\models \mathcal{A}$, by Lemma A.6, and the contradiction. □

A.4 0 *is expressive*

In this case, the logic is enriched with $\top$ in order to have a 0-ary connector.

Lemma A.8 *Let $\mathcal{A}$ be a formula without* 0*, and $n \notin \text{fn}(A)$. Then*

$$\mathbf{0} \models \mathcal{A} \text{ iff } n[\mathbf{0}] \models \mathcal{A}$$

Proof. We reason by induction on $\mathcal{A}$

- $\mathcal{A} = \top$, $\mathcal{A} = \mathcal{A}_1 \wedge \mathcal{A}_2$, $\mathcal{A} = \neg\, \mathcal{A}_1$: straightforward.
- $\mathcal{A} = \mathcal{N}m.\mathcal{A}_1$: We assume without loss of generality $m \neq n$. If $\mathbf{0} \models \mathcal{N}m.\mathcal{A}_1$, then $\mathbf{0} \models \mathcal{A}_1$. $n[\mathbf{0}] \models \mathcal{A}_1$ by induction, so $n[\mathbf{0}] \models \mathcal{N}n.\mathcal{A}_1$. Conversely, if $n[\mathbf{0}] \models \mathcal{N}m.\mathcal{A}_1$, then $n[\mathbf{0}] \models \mathcal{A}_1$, so $\mathbf{0} \models \mathcal{A}_1$ by induction, and then $\mathbf{0} \models \mathcal{N}n.\mathcal{A}_1$.
- if $\mathcal{A} = \mathcal{A}_1 \mid \mathcal{A}_2$. Assume first that $\mathbf{0} \models \mathcal{A}_1 \mid \mathcal{A}_2$. Then $\mathbf{0} \models \mathcal{A}_1 \wedge \mathcal{A}_2$, hence by induction $n[\mathbf{0}] \models \mathcal{A}_1$, and $n[\mathbf{0}] \models \mathcal{A}_1 \mid \mathcal{A}_2$. If $\mathbf{0} \not\models \mathcal{A}_1 \mid \mathcal{A}_2$, then we may assume by symmetry that $\mathbf{0} \not\models \mathcal{A}_1$. Assume by absurd that $n[\mathbf{0}] \models \mathcal{A}_1 \mid \mathcal{A}_2$. Then $n[\mathbf{0}] \models \mathcal{A}_1$ and $\mathbf{0} \models \mathcal{A}_2$. By induction $\mathbf{0} \models \mathcal{A}_1$ and the contradiction.
- if $\mathcal{A} = m[\mathcal{A}_1]$. Then $m \neq n$ by hypothesis, and both $\mathbf{0} \not\models \mathcal{A}$ and $n[\mathbf{0}] \not\models \mathcal{A}$.
- if $\mathcal{A} = m\text{®}\mathcal{A}_1$, $m \neq n$ by hypothesis. If $\mathbf{0} \models \mathcal{A}$, then $\mathbf{0} \models \mathcal{A}_1$, and by induction $n[\mathbf{0}] \models \mathcal{A}_1$ and $n[\mathbf{0}] \models \mathcal{A}$. Conversely, if $n[\mathbf{0}] \models \mathcal{A}$, then $n[\mathbf{0}] \models \mathcal{A}_1$, and $\mathbf{0} \models \mathcal{A}_1$ so $\mathbf{0} \models \mathcal{A}$ by induction.

□

Lemma A.9 *There is no formula $\mathcal{A} \in \text{SAL}_{int} - \{0\}$ equivalent to* 0*.*

Proof. By absurd, if $\mathcal{A}$ is such a formula an $n \notin \text{fn}(\mathcal{A})$, then by Lemma A.8, $n[\mathbf{0}] \models \mathcal{A}$ and the contradiction. □

A.5 $|, n[.], n\text{®}$. *are separative*

Lemma A.10 *If $\mathcal{A} \in \text{SAL}_{int} - \{|\}$, then $P_1 = n[\mathbf{0}] \mid n[\mathbf{0}] \models \mathcal{A}$ iff $P_2 = n[\mathbf{0}] \mid n[\mathbf{0}] \mid n[\mathbf{0}] \models \mathcal{A}$.*

Proof. By absurd, suppose there exists a formula $\mathcal{A}$ telling apart P_1 from P_2, take a minimal such $\mathcal{A}$, and reason by case analysis on $\mathcal{A}$.

- the cases $\mathcal{A} = \mathcal{A}_1 \wedge \mathcal{A}_2$, $\mathcal{A} = \neg\, \mathcal{A}_1$ and $\mathcal{A} = \mathcal{N}m\mathcal{A}_1$ are straightforward.
- if $\mathcal{A} = 0$, then none of P_1, P_2 does satisfy $\mathcal{A}$.

- $\mathcal{A} = m\circledR\mathcal{A}_1$: if $m = n$, then none of those processes do satisfy $\mathcal{A}$, otherwise the process satisfying $\mathcal{A}$ does satisfy $\mathcal{A}_1$, and $\mathcal{A}_1$ is a smaller separating formula.
- $\mathcal{A} = m[\mathcal{A}_1]$: none of the two processes do satisfy $\mathcal{A}$.

□

Lemma A.11 *If $\mathcal{A} \in \mathrm{SAL}_{int} - \{n[.]\}$, then for any names n_1, n_2, we set $P_1 = n_1[n_2[\mathbf{0}]]$ and $P_2 = n_2[n_1[\mathbf{0}]]$. Then $P_1 \models \mathcal{A}$ iff $P_2 \models \mathcal{A}$.*

Proof. As above, by absurd and case analysis on a minimal $\mathcal{A}$:

- the cases $\mathcal{A} = \mathcal{A}_1 \wedge \mathcal{A}_2$, $\mathcal{A} = \neg\mathcal{A}_1$ and $\mathcal{A} = \forall m\mathcal{A}_1$ are straightforward.
- if $\mathcal{A} = 0$, then none of P_1, P_2 do satisfy $\mathcal{A}$.
- $\mathcal{A} = \mathcal{A}_1 \mid \mathcal{A}_2$. We may assume by symmetry that $P_1 \models \mathcal{A}$. Also by symmetry, we may assume $P_1 \models \mathcal{A}_1$ and $\mathbf{0} \models \mathcal{A}_2$. If $P_2 \not\models \mathcal{A}$, then $\mathcal{A}_1$ separates P_1 from P_2 and is a smaller formula: contradiction.
- $\mathcal{A} = m\circledR\mathcal{A}_1$: if $m \in \{n_1, n_2\}$, then none of the two processes do satisfy $\mathcal{A}$, otherwise the process satisfying $\mathcal{A}$ also satisfies $\mathcal{A}_1$, and $\mathcal{A}_1$ is a smaller separating formula.

□

Lemma A.12 *Assume $\mathcal{A} \in \mathrm{SAL}_{int} - \{n[.]\}$, We set $P_1 = (\nu n)n[n[\mathbf{0}]]$ and $P_2 = (\nu n)n[\mathbf{0}]$. Then $P_1 \models \mathcal{A}$ iff $P_2 \models \mathcal{A}$.*

Proof. Again, by absurd and case analysis on a minimal $\mathcal{A}$:

- the cases $\mathcal{A} = \mathcal{A}_1 \wedge \mathcal{A}_2$, $\mathcal{A} = \neg\mathcal{A}_1$ and $\mathcal{A} = \forall m\mathcal{A}_1$ are straightforward.
- if $\mathcal{A} = 0$, then none of P_1, P_2 do satisfy $\mathcal{A}$.
- $\mathcal{A} = \mathcal{A}_1 \mid \mathcal{A}_2$. We may assume by symmetry that $P_1 \models \mathcal{A}$. Also by symmetry, we may assume $P_1 \models \mathcal{A}_1$ and $\mathbf{0} \models \mathcal{A}_2$. If $P_2 \not\models \mathcal{A}$, then $\mathcal{A}_1$ separates P_1 from P_2 and is a smaller formula: contradiction.
- $\mathcal{A} = m[\mathcal{A}_1]$: none of P_1, P_2 do satisfy $\mathcal{A}$.

□

B Proof of Proposition 6.2 (∀ quantifier)

In this section, we establish the Proposition 6.2 that is used for the proof of Theorem 6.1. It follows from Lemma B.2, that itself depends on Lemma B.1. Roughly speaking, the aim of this section is to find some sufficient conditions so that substitutions can be operated on formula side and process side without alterating satisfaction.

We call *thread context* a context C of the form

$$C[\,P\,] \;\equiv\; (\nu\tilde{n})\, n_1[\ldots n_k[\,P\,]\ldots]$$

with $\tilde{n} \subseteq \{n_1, \ldots, n_k\}$. We note $n(C) \stackrel{\text{def}}{=} \{n_1, \ldots, n_k\}$ and $d(C) \stackrel{\text{def}}{=} k$. For a formula $\mathcal{A}$, we note $d(\mathcal{A})$ the number of $n[.]$ connectives.

Lemma B.1 *Let $\mathcal{A}$ be a formula of* $\mathrm{SAL}^{\forall}_{int}$*, and C a thread context such that $d(C) > d(\mathcal{A})$. Let n, m be two names such that $\{n,m\} \cap n(C) = \emptyset$, and*

$$P \stackrel{\text{def}}{=} C[\, n[\mathbf{0}] \mid m[\mathbf{0}] \,]$$

Then $P \models \mathcal{A}$ iff $P \models \mathcal{A}\{^n/_m\}$.

Proof. By induction on the size of $\mathcal{A}$:

- the cases $\mathcal{A} = \mathcal{A}_1 \wedge \mathcal{A}_2$, $\mathcal{A} = \neg\, \mathcal{A}_1$, and $\mathcal{A} = \mathbf{0}$ are trivial.
- $\mathcal{A} = \mathcal{A}_1 \mid \mathcal{A}_2$. Assume first $P \models \mathcal{A}$. Since $d(C) \geq 1$, we may assume by symetry that $\mathbf{0} \models \mathcal{A}_2$ and $P \models \mathcal{A}_1$. Then $P \models \mathcal{A}_1\{^n/_m\}$ by induction, and $P \models \mathcal{A}\{^n/_m\}$. The reciproque is the same.
- $\mathcal{A} = a[\mathcal{A}_1]$. Assume first $P \models \mathcal{A}$. Then $C \equiv a[C']$ and $P' \stackrel{\text{def}}{=} C'[n[\mathbf{0}] \mid m[\mathbf{0}]] \models \mathcal{A}_1$. By induction $P' \models \mathcal{A}_1\{^n/_m\}$. Since $\{n,m\} \cap n(C)$, $a \neq m$, so $\mathcal{A}\{^n/_m\} = a[\mathcal{A}_1\{^n/_m\}]$, and $P \models \mathcal{A}\{^n/_m\}$.
  Assume now $P \models \mathcal{A}\{^n/_m\}$. Let $b = a\{^n/_m\}$. Then $C \equiv b[C']$ and $P' \stackrel{\text{def}}{=} C'[n[\mathbf{0}] \mid m[\mathbf{0}]] \models \mathcal{A}_1\{^n/_m\}$. Then $b \in n(C)$, so $b \notin \{m,n\}$, and $b = a$. By induction $P' \models \mathcal{A}_1$, so $P \models b[\mathcal{A}_1] = \mathcal{A}$.
- $\mathcal{A} = a®\mathcal{A}_1$. Assume first $P \models \mathcal{A}$. Then $C \equiv (\nu a)C'$ and $P' \stackrel{\text{def}}{=} C'[n[\mathbf{0}] \mid m[\mathbf{0}]] \models \mathcal{A}_1$. Since n, m are free in P, $a \neq m$ and $a \neq n$. So $\{n,m\} \cap n(C') = \emptyset$, and by induction, $P' \models \mathcal{A}_1\{^n/_m\}$. $\mathcal{A}\{^n/_m\} = a®\mathcal{A}_1\{^n/_m\}$, and $P \models \mathcal{A}\{^n/_m\}$. The reciproque is the same.
- $\mathcal{A} = \forall x.\mathcal{A}_1$. Assume first $P \models \mathcal{A}$. Let take $a \in \mathcal{N}$. Then $P \models \mathcal{A}_1\{^a/_x\}$, and by induction $P \models \mathcal{A}_1\{^a/_x\}\{^n/_m\}$. For $a \neq m$, this is also $P \models \mathcal{A}_1\{^n/_m\}ax$. For $a = m$, this requires a bit more. Consider that $P \models \mathcal{A}_1\{^n/_x\}$. Then $P \models \mathcal{A}_1\{^n/_x\}\{^n/_m\}$ by induction. But $\mathcal{A}_1\{^n/_x\}\{^n/_m\} = (\mathcal{A}_1\{^n/_m\}\{^m/_x\})\{^n/_m\}$, so by induction $P \models \mathcal{A}_1\{^n/_m\}\{^m/_x\}$. Hence $P \models \mathcal{A}_1\{^n/_m\}\{^a/_x\}$ for all a, that is $P \models \forall x.\mathcal{A}_1\{^n/_m\} = \mathcal{A}\{^n/_m\}$.
  Assume now that $P \models \mathcal{A}\{^n/_m\}$. Let take $a \in \mathcal{N}$. Then $P \models \mathcal{A}_1\{^n/_m\}\{^a/_x\}$. If $a \neq m$, this is $P \models \mathcal{A}_1\{^a/_x\}\{^n/_m\}$, so by induction $P \models \mathcal{A}_1\{^a/_x\}$. For $a = m$, consider that $P \models \mathcal{A}_1\{^n/_m\}\{^n/_x\}$, that is $P \models \mathcal{A}_1\{^m/_x\}\{^n/_m\}$, so by induction $P \models \mathcal{A}_1\{^m/_x\}$. Hence $P \models \mathcal{A}_1\{^a/_x\}$ for all a, that is $P \models \mathcal{A}$.

□

Lemma B.2 *Let $\mathcal{A}$ be a formula of* $\mathrm{SAL}^{\forall}_{int}$*, and C a thread context such that $d(C) > d(\mathcal{A})$. Let n, m be two names such that $\{n,m\} \cap n(C) = \emptyset$, and moreover $m \notin \mathrm{fn}(\mathcal{A})$. Let*

$$P_1 \stackrel{\text{def}}{=} C[\, n[\mathbf{0}] \mid m[\mathbf{0}] \,] \qquad \text{and} \qquad P_2 \stackrel{\text{def}}{=} C[\, n[\mathbf{0}] \mid n[\mathbf{0}] \,]$$

If $P_1 \models \mathcal{A}$, then $P_2 \models \mathcal{A}$.

Proof. By induction on the size of $\mathcal{A}$:

- the cases $\mathcal{A} = \mathcal{A}_1 \wedge \mathcal{A}_2$, $\mathcal{A} = \mathcal{A}_1 \vee \mathcal{A}_2$, $\mathcal{A} = \mathbf{0}$ and $\mathcal{A} = \neg\, \mathbf{0}$ are trivial.
- $\mathcal{A} = \mathcal{A}_1 \mid \mathcal{A}_2$. Since $d(C) \geq 1$, we may assume by symetry that $\mathbf{0} \models \mathcal{A}_2$ and $P_1 \models \mathcal{A}_1$. Then $P_2 \models \mathcal{A}_1$ by induction, and $P_2 \models \mathcal{A}$

- $\mathcal{A} = \mathcal{A}_1 \parallel \mathcal{A}_2$. Since $d(C) \geq 1$, $P_1 \models \mathcal{A}_1 \wedge \mathcal{A}_2$, $\mathbf{0} \models \mathcal{A}_1 \wedge \mathcal{A}_2$. By induction, $P_2 \models \mathcal{A}_1 \wedge \mathcal{A}_2$, that is $P_2 \models \mathcal{A}$
- $\mathcal{A} = a[\mathcal{A}_1]$. Then $C \equiv a[C']$ and $C'[n[\mathbf{0}] \mid m[\mathbf{0}]] \models \mathcal{A}_1$. By induction $C'[n[\mathbf{0}] \mid n[\mathbf{0}]] \models \mathcal{A}_1$, that is $P_2 \models \mathcal{A}$.
- $\mathcal{A} = \neg\, a[\mathcal{A}_1]$. Then either C is not of the form $n[C']$, and $P_2 \models \neg\, a[\mathcal{A}_1]$, or $C \equiv n[C']$ but $C'[n[\mathbf{0}] \mid m[\mathbf{0}]] \models \neg\, \mathcal{A}_1$. Then by induction $C'[n[\mathbf{0}] \mid n[\mathbf{0}]] \models \neg\, \mathcal{A}_1$, that is $P_2 \not\models a[\mathcal{A}_1]$.
- $\mathcal{A} = a \circledR \mathcal{A}_1$. Then $C \equiv (\nu a)C'$ and $C'[n[\mathbf{0}] \mid m[\mathbf{0}]] \models \mathcal{A}_1$. Since n, m are free in P, $a \notin \{m, n\}$, so $n(C') \cap \{m, n\} = \emptyset$. Then by induction, $C'[n[\mathbf{0}] \mid n[\mathbf{0}]] \models \mathcal{A}_1$, and $P_2 \models \mathcal{A}$.
- $\mathcal{A} = \neg\, a \circledR \mathcal{A}_1$. Assume first that a is free in P_1. Then $a \neq m$ since $m \notin \mathrm{fn}(\mathcal{A})$ by hypothesis. So a is also free in P_2 and $P_2 \models \mathcal{A}$. Assume now a is fresh for P_1 (and P_2). Let C' be such that $C \equiv (\nu a)C'$. Then $C'[n[\mathbf{0}] \mid n[\mathbf{0}]] \not\models \mathcal{A}_1$, otherwise $C'[n[\mathbf{0}] \mid m[\mathbf{0}]] \models \mathcal{A}_1$ and $P \models \mathcal{A}$. So $P_2 \not\models a \circledR \mathcal{A}_1$.
- $\mathcal{A} = \forall x.\, \mathcal{A}_1$. Let take $a \in \mathcal{N}$. Then $P_1 \models \mathcal{A}_1\{^a/_x\}$, and by induction $P_2 \models \mathcal{A}_1\{^a/_x\}$ for $a \neq m$. Let take some fresh m'. By equivariance, $P_1(m \leftrightarrow m') \models \forall x.\, \mathcal{A}_1$, so $P_1(m \leftrightarrow m') \models \mathcal{A}_1\{^m/_x\}$. Applying induction on P_1 and $\mathcal{A}_1\{^m/_x\}$ for m' instead of m, we have $P_2 \models \mathcal{A}_1\{^m/_x\}$. Hence $P \models \mathcal{A}_1\{^a/_x\}$ for all a, that is $P_2 \models \forall x.\, \mathcal{A}_1$.
- $\mathcal{A} = \exists x.\, \mathcal{A}_1$. Let $a \in \mathcal{N}$ be such that $P_1 \models \mathcal{A}_1\{^a/_x\}$. If $a \neq m$, then we may apply induction on $\mathcal{A}_1\{^a/_x\}$, and $P_2 \models \mathcal{A}_2\{^a/_x\}$, that is $P_2 \models \mathcal{A}$. Otherwise $P_1 \models \mathcal{A}_1\{^m/_x\}$. By Lemma B.1, $P_1 \models \mathcal{A}_1\{^m/_x\}\{^n/_m\} = \mathcal{A}_1\{^n/_x\}\{^n/_m\}$, and again $P_1 \models \mathcal{A}_1\{^n/_x\}$. Then by induction, $P_2 \models \mathcal{A}_1\{^n/_x\}$, that is $P_2 \models \mathcal{A}$.

□

Proof of Proposition 6.2

Proof. Let assume by absurd we have some $\mathcal{A}$ such that

$$P \models \mathcal{A} \qquad \text{iff} \qquad \sharp\,\mathrm{fn}(P) = 1$$

Then let C be the thread context of the form $(\nu a)a[\ldots a[.]\ldots]$, and $d(C) = d(\mathcal{A})+1$. Let m, n be two fresh names. Then $C[n[\mathbf{0}] \mid m[\mathbf{0}]] \models \neg\, \mathcal{A}$ by definition of $\mathcal{A}$, so by Lemma B.2, $C[n[\mathbf{0}] \mid n[\mathbf{0}]] \models \neg\, \mathcal{A}$. Moreover, by definition of $\mathcal{A}$, $C[n[\mathbf{0}] \mid n[\mathbf{0}]] \models \mathcal{A}$, so the contradiction. □