Elimination of spatial connectives in static spatial logics

Étienne LOZES

LIP, ENS Lyon – France

Abstract

The recent interest for specification on resources yields so-called *spatial logics*, that is specification languages offering new forms of reasoning: the local reasoning through the separation of the resource space into two disjoint subspaces, and the contextual reasoning through hypothetical extension of the resource space.

We consider two resource models and their related logics:

- the Static Ambient model (SA), proposed as an abstraction of semistructured data [5], with the Static Ambient Logic (SAL) that was proposed as a request language, both obtained by restricting the Mobile Ambient calculus [6] and logic [7] to their purely static aspects.
- the memory model and the assertion language of Separation Logic (SL), both defined in [16] for the purpose of the axiomatic semantic of imperative programs manipulating pointers.

We raise the questions of the expressiveness and the minimality of these logics. Our main contribution is a minimalisation technique we may apply for these two logics. We moreover show some restrictions of this technique for the extension $\mathrm{SAL}^{\forall}$ with universal quantification, and we establish the minimality of the adjunct-free fragment (SAL_{int}).

Key words: Spatial logics, Separation logic, Mobile Ambients, Minimality.

1 Introduction

The Mobile Ambients calculus (MA) [6] 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.

Email address: elozes@ens-lyon.fr (Étienne LOZES).

Preprint submitted to Theoretical Computer Science 16 June 2004

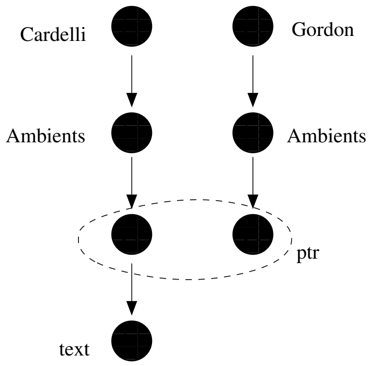

Fig. 1. $(\nu ptr)(Cardelli[Ambients[ptr[text[\mathbf{0}]]]] \,\big|\, Gordon[Ambients[ptr[\mathbf{0}]]])$

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. Leaving out from MA all capabilities, we get rid of the dynamics of the calculus, working with what we call *static ambients*, SA.

Type systems are commonly used to express basic requirements on programs. In the case of SA, the (static) Ambient Logic (SAL) [7] provides a very flexible descriptive framework. Seeing SAL as a request language, one may ask a structure P to match some specification $\mathcal{A}$, written

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

The SAL approach is however much more intensional than it is the case for standard type systems. Indeed, the whole spatial structure of the calculus is reflected in the logic. For instance, the formula $n[\mathcal{A}]$ is satisfied by structures of the form $n[P]$ with $P \models \mathcal{A}$. 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 $\mathcal{B}$ when it is extended by any process satisfying $\mathcal{A}$. SA, associated to SAL, has appeared to be an interesting model for *semistructured data* [5] such as XML documents, due to the underlying tree structure. Data are modelled by unordered labelled trees, where the binders may represent pointers [4], and the logic is used as the basis for a language for queries involving such data. For instance, the process of Fig. 1 represents a database containing the two authors Cardelli and Gordon with one copy of their paper about Ambients stored at Cardelli's and linked to Gordon's. Query

$$\text{И} ptr.\, ptr \circledR\, (Cardelli[\top] \mid \top)$$

asks whether the database contains some author named Cardelli.

Separation Logic [16] is a proposal for a new assertion language in Hoare's approach of imperative programs verification. Indeed, imperative programming languages manipulating pointers allow one to change the value a variable refers to without explicitly mentioning this variable. Such multiple accesses to data make the axiomatic semantics [14] of these programs difficult to handle using classical logic as an assertion language [15]. Separation Logic nicely handles the subtleties of pointer manipulation, providing two new connectives: a separative conjunction $P * Q$ asserting that P and Q hold in separate parts of the memory, and a separating implication $P \mathrel{-\!\!*} Q$ allowing one to introduce 'spatial hypotheses' about the memory. For instance, the judgement

$$\{(x \mapsto -) * ((x \mapsto e) \mathrel{-\!\!*} \phi)\} \;\; x := e \;\; \{\phi\}$$

is the transposition of the classical backward reasoning $\{\phi[e/x]\}\ x := e\ \{\phi\}$ in Hoare logic.

Both specification languages rely on classical logic reasoning extended by two non-standard operations: splitting of the resource space and separated assertions $(|, *)$ on each subspace, and extension of the resource space assuming some hypothesis $(\triangleright, \mathrel{-\!\!*}\ )$. These two aspects are the main novelties of the so-called *spatial logics*. The interest of these connectives has been illustrated in several ways. For Mobile Ambients, it is known that the connective $\triangleright$ coupled with $\Diamond$ can express the action modalities [18], persistence, and other strong properties [13]. For Separation Logic, the proof of an in-place reversal of a list turns out to require complex invariants in the standard classical logic, whereas it has a simple formulation in SL using $*$, as one of the many examples presented in [15].

Although spatial connectives evidently bring a real ease to the formulation of complex properties of the structures, their actual contribution to the expressiveness of the logic is not so clear. For instance, the formula $x \hookrightarrow \mathsf{nil} * y \hookrightarrow \mathsf{nil}$ expresses that both x and y points to nil, but from distinct locations, which can also be expressed as $x \hookrightarrow \mathsf{nil} \wedge y \hookrightarrow \mathsf{nil} \wedge x \neq y$ without requiring $*$; the formula $n[0] \triangleright n[0]$ tells that after extension of the structure adding $n[0]$, one exactly has $n[0]$, which means that the structure was initially empty, hence this formula is equivalent to 0. On the other hand, it has been established for the Mobile Ambient case, i.e in a dynamic setting, that guarantee brings some extra expressive power [13].

This paper studies the contribution of spatial connectives in the expressiveness of static spatial logics. This question is important since spatial connectives introduce a lot of complication from the model-checking point of view. Indeed, separated conjunctions $*$ and $|$ forces to try all the splitting of the structure, which may be costly for wide structures. Even worse, the spatial implications $\mathrel{-\!\!*}$ and $\triangleright$ considerably complicate the model-checking by introducing the need to seek a representative testing set [3,9], when it is not an undecidable problem [3,12]. The expressiveness of spatial connectives is also important from theoretical issues. For instance, the proof of an in-place reversal of a list is derivable, through heavy formulations, in classical Hoare logic as well, and the question is open whether Separation Logic can prove programs on which classical reasoning would fail.

Several kinds of quantification can be taken under consideration for our spatial logics:

- absence of quantification, as it is the case for SL (in this work).
- classical quantification ($\forall, \exists$), which defines the logic $\mathrm{SAL}^{\forall}$.
- fresh quantification [11], ($\reflectbox{N} n.\mathcal{A}$), which is the way SAL handles name generation. This quantification is related to α conversion of bound names. It is complementary to the spatial connective $n \circledR \mathcal{A}$ that forces the process to reveal a hidden name by calling it n.

We establish that the contribution of spatial connectives depends on the forms of quantification supported by the logic.

Indeed, in quantifier-free logics, adjuncts do not increase the expressiveness of the logic (Theorem 4.4). Neither does the separated conjunction ($*$) for SL, since it only expresses separation, so that SL assertions can be translated into a classical logic (Theorem 8.1). In a different way, $|$ brings extra expressiveness to SAL, namely the power of counting, so it cannot be eliminated, and actually the adjunct-free fragment of SAL is minimal (Theorem 7.1). The proof of these elimination results goes through the intensive use of intensional partial equivalences on models; such equivalences are common for the study of the expressiveness of a logic (see [18,13] for spatial logic cases), but were also exploited for decidability issues in [3,9]. 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 partial intensional equivalence.

When classical quantifiers are taken under consideration, more complex properties can be expressed through adjuncts, and they cannot be taken out freely (Theorem 6.1). This difference of nature of the logic was already observed from the decidability aspect [3,10,9], which implied the absence of an effective adjuncts elimination. Our result shows that the adjuncts elimination is impossible even theoretically.

Finally, we establish the quite surprising result that adjuncts elimination is still possible in presence of fresh quantification (Theorem 5.3), essentially due to prenex forms for $\reflectbox{N}$ (Proposition 5.2). This result underlines the fundamental difference between classical quantification and fresh quantification.

Related work. Apart from [17], this is, to our knowledge, the first results studying precisely the expressiveness and minimality of spatial logics. Other works about expressiveness only give some hints. A first result about the separation power of

AL is presented in [18]. Other examples of expressive formulas for AL are shown in [13], such as formulas for persistence and finiteness.

A compilation result has been derived for a spatial logic for trees without quantification and private names [17]. In that work, the target logic includes some new features such as Presburger arithmetic, and the source logic includes a form of Kleene star.

The setting in which we obtain our encoding is rather different in the dynamic case (see [13]). 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 partial intensional equivalence and the notion of precompactness is original. Intensional bisimilarity plays an important role in the characterisation of the separation power of the logic [18]. 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 with respect to decidability issues. The undecidability of the model-checking of SAL with classical quantification has been established in [10]. Quite unexpected decidability results for spatial logics with $\triangleright$ and without quantification were then established in [3] and [9]. These works are closely related to the present study; roughly, the decidability result of [9] relies on finiteness of *processes*, whereas our encoding exploits finiteness of *observations*. For this reason, our approach is more general and cuts out decidability issues. Actually, the undecidability of the model-checking problem for SAL has been recently established [12]. This last work studies many variations around SAL, derives decidability results with $\triangleright$ and И, and presents a prenex form result similar to ours.

Outline. We introduce SA, SAL and its adjunct-free fragment (SAL_{int}) in Sect. 2. We prove adjunct elimination for quantifier-free formulas in Sect. 4, based on the notion of intensional bisimilarity, discussed in Sect. 3. The general result for SAL is then established in Sect. 5, based on prenex forms. We discuss the adjunct elimination for $\mathrm{SAL}^{\forall}$ in Sect. 6, and show minimality of SAL_{int} in Sect. 7; in Sect. 8, we introduce SL and a classical fragment of it (CL), which we prove to be as expressive as SL. Sect. 9 gives concluding remarks.

2 Background

In this section we define the model of static ambients (SA) and its logic SAL. We also define the intensional fragment (SAL_{int}) of SA.

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*) satisfying the axioms of Fig 2. Formulas, ranged

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

Fig. 2. Structural congruence on SA

over with $\mathcal{A}, \mathcal{B}, \ldots$, are defined in Fig 3 . These formulas form *the static ambient*

$$\begin{array}{lr} \mathcal{A} ::= \mathcal{A} \wedge \mathcal{A} \mid \neg\,\mathcal{A} \mid \text{И}n.\,\mathcal{A} \mid 0 \mid \mathcal{A} \mid \mathcal{A} \mid n[\mathcal{A}] \mid n\circledR\mathcal{A} & \text{(intensional fragment)} \\ \mid \mathcal{A} \triangleright \mathcal{A} \mid \mathcal{A}@n \mid \mathcal{A} \oslash n & \text{(adjuncts)} \end{array}$$

Fig. 3. SAL and the intensional fragment SAL_{int}

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

We will say that $\mathcal{A}$ is *quantifier-free* if $\mathcal{A}$ does not contain any И quantification. The set of free names of a formula $\mathcal{A}$, written $\mathrm{fn}(\mathcal{A})$ is the set of names appearing in $\mathcal{A}$ that are not bound by a И 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* $\models\, \subset (SA \times \mathrm{SAL})$ *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* $P \not\models \mathcal{A}$
- $P \models \text{И}n.\,\mathcal{A}$ *if* $\forall n' \in \mathcal{N} - (\mathrm{fn}(P) \cup \mathrm{fn}(\mathcal{A}))$, $P \models \mathcal{A}(n \leftrightarrow n')$
- $P \models \mathcal{A}_1 \mid \mathcal{A}_2$ *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.

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 2.1

- *The formula $\bot$, that no process satisfies, can be defined as $0 \wedge \neg 0$. As e.g. in [7], 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 and the following, we will give a first illustration of our minimalisation method on the case of SAL and SAL_{int}. This minimalisation transforms a formula from a logic to the other; however, it does not proceed as a dictionary, that is we do not show that the connectives from the original logic are some syntactic sugar for some fixed construction in the target logic. The translation actually goes through the exploration of all behaviours a process may have with respect to a formula. Roughly, we translate a formula $\mathcal{A}$ into an exhaustive disjunction

$$\mathcal{A} \quad \rightsquigarrow \quad \bigvee_{C \in \mathrm{Behaviours}(\mathcal{A})} F_C$$

of all the behaviours that lead to the acceptance of $\mathcal{A}$.

The bottleneck of this embedding is to define what are these behaviours. By behaviours, we refer to equivalence classes of some observational equivalence.

In this section, we will hence introduce a notion of partial observation over trees corresponding to logical testing. This model equivalence can be seen as the adapted *game* for this logic (in the sense of Ehrenfreucht-Fraïssé), or as the static *intensional bisimilarity* ([18]). Observations are taken from the logic to which we want to reduce to, in this setting SAL_{int}. Each connective defines a simulation rule in a very natural way. Then we show that this observational equivalence is enough to ensure model equivalence with respect to the logic we want to minimalize, that is SAL (Proposition 3.4) in this setting. We then give a compact representation of the observational equivalence classes as some symbolic sets we call *signatures*.

We will 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 symmetric 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 hold:*

- *if $P \equiv \mathbf{0}$ then $Q \equiv \mathbf{0}$*
- *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 $P_\epsilon \simeq_{i-1,N} Q_\epsilon$, $\epsilon = 1, 2$.*
- *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 $P' \simeq_{i-1,N} Q'$.*
- *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 quotient of SA induced by $\simeq_{i,N}$: it will be ranged over by equivalence classes called 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 admitting 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:*

- $z_i^N(P) = 0$ *if $P \equiv \mathbf{0}$, otherwise* $\neg 0$
- $p_i^N(P) = \{(C_1, C_2) \in (\mathrm{SA}_{/\simeq_{i-1,N}})^2 : P \equiv P_1 \mid P_2$ *and* $P_i \in C_i\}$
- $a_i^N(P) = [n, C]$ *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 $a_i^N(P) =$* noobs*, where* noobs *is a special constant.*
- $r_i^N(P) = \{(n, C) \in N \times \mathrm{SA}_{/\simeq_{i-1,N}} : \exists P'.\ P \equiv (\nu n)P'$ *and* $P' \in C\}$

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

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 behaviours may be observed.
- Existence of intensional characteristic formulas for the classes of $\simeq_{i,N}$.

The first property basically says the following: if we fix some formula $\mathcal{A}$, then we may finitely list all the behaviours a process P may have with respect to $\mathcal{A}$. Then we may tag the ones corresponding to an acceptance and the ones corresponding to a rejection, and from the second property, we may express this by some formula in SAL_{int}.

Here is the proof with more details.

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:

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

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 $\mathbf{codom}\,\chi_i^N$. $\square$

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 only a finite amount of information is needed to capture 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

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

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 $\mathcal{A} \in$ SAL, there is a formula $[\mathcal{A}] \in$ SAL$_{int}$ such that*

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

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

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

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:
Due to its finiteness, the construction of our proof could seem to be effective. However, this cannot be the case due to an undecidability result for the model-checking problem on SAL [12]. This is quite surprising, since only an effective enumeration of the bisimilarity classes is missing to make the proof constructive. Moreover, such an enumeration exists for SA without name restriction, via testing sets as defined in [9]. 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 result we already obtained for quantifier-free formulas easily extends to formulas in prenex forms. So our efforts will focus on establishing the existence of an equivalent formula in prenex form for any formula of SAL. Intuitively, prenex forms can be generated by pulling out the fresh quantifiers. We actually show how to swap the order between a quantifier and another connective without changing the semantic. Except for the $\triangleright$ connective, this turns out to be quite natural.

We present our algorithm as a rewriting system in Fig. 4. The essential result is then

Proposition 5.1 (Correction of $\rightsquigarrow$) *The term rewriting system $\rightsquigarrow$ defined by the rules of Fig. 4 preserves the semantics: for any $\mathcal{A}, \mathcal{B} \in \mathrm{SAL}$, if $\mathcal{A} \rightsquigarrow \mathcal{B}$, then $\mathcal{A} \dashv\vdash \mathcal{B}$.*

$(\wedge)$	$(\text{И}n.\,\mathcal{A}_1) \wedge \mathcal{A}_2 \rightsquigarrow \text{И}n.\,(\mathcal{A}_1 \wedge \mathcal{A}_2)$		$(n \notin \mathrm{fn}(\mathcal{A}_2))$
$(\neg)$	$\neg\, \text{И}n.\,\mathcal{A}_1 \rightsquigarrow \text{И}n.\,\neg\,\mathcal{A}_1$		
$(\vert)$	$(\text{И}n.\,\mathcal{A}_1) \mid \mathcal{A}_2 \rightsquigarrow \text{И}n.\,(\mathcal{A}_1 \mid \mathcal{A}_2)$		$(n \notin \mathrm{fn}(\mathcal{A}_2))$
$(\triangleright L)$	$(\text{И}n.\,\mathcal{A}_1) \triangleright \mathcal{A}_2 \rightsquigarrow \text{И}n.\,\big((n \circledR \top \wedge \mathcal{A}_1) \triangleright \mathcal{A}_2\big)$		$(n \notin \mathrm{fn}(\mathcal{A}_2))$
$(\triangleright R)$	$\mathcal{A}_1 \triangleright (\text{И}n.\,\mathcal{A}_2) \rightsquigarrow \text{И}n.\,\big((n \circledR \top \wedge A_1) \triangleright \mathcal{A}_2\,)$		$(n \notin \mathrm{fn}(\mathcal{A}_1))$
(Amb)	$m[\text{И}n.\,\mathcal{A}] \rightsquigarrow \text{И}n.\,m[\mathcal{A}]$		$(m \neq n)$
$(@)$	$(\text{И}n.\,\mathcal{A})@m \rightsquigarrow \text{И}n.\,(\mathcal{A}@m)$		$(m \neq n)$
$(\circledR)$	$m \circledR \text{И}n.\,\mathcal{A} \rightsquigarrow \text{И}n.\,m \circledR \mathcal{A}$		$(m \neq n)$
$(\oslash)$	$(\text{И}n.\,\mathcal{A}) \oslash m \rightsquigarrow \text{И}n.\,(\mathcal{A} \oslash m)$		$(m \neq n)$

Fig. 4. Term rewriting system for prenexation

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

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

$\square$

Remark 5.1 *Some of the rules above (such as* (Amb), $(\neg\,)$*, and a variant of* $(\mid L)$*) have already been presented in [8], under the form of equalities. The same result is independently developed in [12].*

We say that a formula $\mathcal{A}$ is *well-formed* if every variable bound by И 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 well-formed formulas are formulas in prenex form. Confluence holds modulo permutation of consecutive И quantifiers.

Proposition 5.2 (Prenex forms) *For any formula* $\mathcal{A}$*, there are* $\tilde{n}, \mathcal{A}'$ *such that* $\mathcal{A} \dashv\vdash \text{И}\tilde{n}.\,\mathcal{A}'$ *and* $\mathcal{A}'$ *is quantifier free.*

This result directly implies the following extension of Theorem 4.4:

Theorem 5.3 (Adjunct elimination) *For any 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 $\mathcal{A}'$ quantifier free and $\tilde{n}$ such that $\mathcal{A} \dashv\vdash \text{И}\tilde{n}.\,\mathcal{A}'$ by Proposition 5.2. Then by Lemma 2.2 and Theorem 4.4, we may write

$$\mathcal{A} \ \dashv\vdash\ \text{И}\tilde{n}.\,\mathcal{A}' \ \dashv\vdash\ \text{И}\tilde{n}.\,[\mathcal{A}']\,.$$

$\square$

Example 5.2 *: We show 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 *[1]) stands for $\text{И}n.\, n®\mathcal{A}$. The prenex form of $\mathcal{A}$ is*

$$\text{И}m', n_1, n_2, n_3.\ \Big((m'®\top \wedge .\, m'®m'[\top]) \blacktriangleright (n_1®n_1[0] \mid n_2®n_2[n_3®.\, n_3[0]])\Big)\oslash m@m$$

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 name quantification of the form $\forall x.\mathcal{A}$ and $\exists x.\mathcal{A}$ with the natural semantics:

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

Let us note $\text{SAL}^{\forall}_{int}$ the intensional fragment with classical quantification. We ask the question of adjuncts elimination for extensions of this logic. The undecidability result of [10] implies that there is no effective adjunct elimination for $\text{SAL}^{\forall}_{int} + \{\triangleright\}$. We establish now a more precise result:

Theorem 6.1 (Expressiveness of adjuncts in $\text{SAL}^{\forall}_{int}$) *$\text{SAL}^{\forall}_{int} + \{\triangleright\}$, $\text{SAL}^{\forall}_{int} + \{@\}$ and $\text{SAL}^{\forall}_{int} + \{\oslash\}$ are strictly more expressive than $\text{SAL}^{\forall}_{int}$.*

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

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

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

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

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

$$\exists x.\ (\forall y.\, y®\top) \oslash x$$

We are now interested in proving that such a property cannot be expressed in $\text{SAL}^{\forall}_{int}$. Our approach consists in studying the stability of $\models$ with respect to substitutions. We actually find some particular processes P for which $P \models \mathcal{A}$ is equivalent to $P \models \mathcal{A}\{^n/_m\}$. From this, we deduce processes P such that $P \models \mathcal{A}$ implies $P\{^n/_m\} \models \mathcal{A}$. This last result shows that, on certain conditions, a formula may not observe the action of equating two names in a process, which is contradictory with counting the number of free names.

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 in $\mathcal{A}$.

Lemma 6.2 *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*

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

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 symmetry 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 other direction is proved similarly.
- $\mathcal{A} = a[\mathcal{A}_1]$. 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 other direction is proved similarly.
- $\mathcal{A} = \forall x.\, \mathcal{A}_1$. 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 $P \models \mathcal{A}$.

$\square$

Lemma 6.3 *Let $\mathcal{A}$ be a formula of* $\mathrm{SAL}_{int}^{\forall}$*, 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*

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

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 symmetry 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 6.2, $P_1 \models \mathcal{A}_1\{^m/_x\}\{^n/_m\} = \mathcal{A}_1\{^n/_x\}\{^n/_m\}$, and again $P_1 \models \mathcal{A}_1\{^n/_x\}$. Then by induction, $P_2 \models \mathcal{A}_1\{^n/_x\}$, that is $P_2 \models \mathcal{A}$.

$\square$

This last result implies the desired property about $\mathrm{SAL}_{int}^{\forall}$:

Proposition 6.4 *There is no formula in* $\mathrm{SAL}_{int}^{\forall}$ *that satisfies (1).*

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

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

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 6.3, $C[n[\mathbf{0}] \mid n[\mathbf{0}]] \models \neg\,\mathcal{A}$. Moreover, by definition of $\mathcal{A}$, $C[n[\mathbf{0}] \mid n[\mathbf{0}]] \models \mathcal{A}$, so the contradiction. $\square$

7 Minimality of SAL_{int}

In this section, we show minimality w.r.t. expressive power of SAL_{int}.

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

This result is the consequence of several technical lemmas for each connective. We may distinguish two forms of contribution to the expressiveness of the logic. We will say that a connective κ is *expressive* when there is a property expressed by a formula containing κ that cannot be expressed otherwise. As a consequence, this connective must belong to any minimal fragment. We will also say that a connective κ is *separative* when there exists two models P_1, P_2 and a formula containing κ satisfied by P_1 but not P_2, such that all κ-free formulas equally satisfy P_1 and P_2. Separative connectives are expressive as well, but in a deeper way: removing them, one reduces the separation power of the logic. For SAL_{int}, we will now establish the following classification:

- connectives $.\,|\,.$, $n\circledR.$, and $n[.]$ are separative,
- connectives $0, \wedge, \neg, \text{И}$ are expressive but not separative.

In particular, SAL_{int} is minimal in terms of expressiveness, but as far as separation power is concerned, the minimal fragment is $\mathrm{SAL}_{int} - \{\text{И}, \neg, \wedge, 0\}$, 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.

Example 7.1 *The fragment $\mathrm{SAL} - \{\wedge\}$ is surprisingly quite expressive, as the formula*

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

shows. This formula is equivalent to $n_1[n_2[0]] \vee n_2[n_1[0]]$, and hence the proof of expressiveness of $\wedge$ (see below) must be carried out in a different way. 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.

We establish now that the connectives $. | .$, n®$.$, and $n[.]$ are separative. Intuitively, $|$ carries the ability of SAL_{int} to count, so without this connective it will not be possible to distinguish $n[\mathbf{0}] \mid n[\mathbf{0}]$ from $n[\mathbf{0}] \mid n[\mathbf{0}] \mid n[\mathbf{0}]$; in the same way, $n[.]$ is necessary to separate $n_1[n_2[\mathbf{0}]]$ from $n_2[n_1[\mathbf{0}]]$, and n®$.$ is the only way of specifying properties of hidden names, so it must be required to distinguish $(\nu n)n[\mathbf{0}]$ and $(\nu n)n[n[\mathbf{0}]]$.

Lemma 7.2 *If $\mathcal{A} \in \mathrm{SAL}_{int} - \{|\}$, 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 $\mathcal{A} = Ʉ m\mathcal{A}_1$ are straightforward.
- if $\mathcal{A} = 0$, then none of P_1, P_2 does satisfy $\mathcal{A}$.
- $\mathcal{A} = m$®$\mathcal{A}_1$: 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 7.3 *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 $\mathcal{A} = Ʉ m\mathcal{A}_1$ 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.
- $\mathcal{A} = m$®$\mathcal{A}_1$: 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 7.4 *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 $\mathcal{A} = Ʉ m\mathcal{A}_1$ 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 $\mathcal{A}$.

$\square$

7.2 Expressive connectives

We show that the connectives $\wedge, \neg, \reflectbox{N}, 0$ are expressive. Expressiveness proofs are more subtle than in the separability cases, since the loss of expressiveness is less sensitive. The scheme of the proof that the connective κ is expressive is to find a property (cardinality, stability by substitution, truncation...) common to all set of models corresponding to any formula without κ, and a formula with κ whose set of models does not have this property.

7.2.1 $\wedge$ is expressive

By duality, $\wedge$ expresses disjunction; we will show that the intensional logic may not express the disjunction present in the formula $n_1[n_2[0]] \vee n_2[n_1[0]]$ without the $\wedge$ connective.

Remark 7.2 *The $\wedge$ connective is probably the connective whose expressiveness is the most difficult to characterise. It would be even more difficult if one had to take into account adjuncts. As shown in Example 7.1, we may express the formula $n_1[n_2[0]] \vee n_2[n_1[0]]$ in* SAL $-\{\wedge\}$ *using adjuncts.*

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 7.5 *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 $\mathcal{A}$:

- $\mathcal{A} = \reflectbox{N} n. \mathcal{A}_1$. 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 symmetry 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.
- $\mathcal{A} = n \circledR \mathcal{A}_1$: then $\mathbf{0} \not\models \mathcal{A}_1$, and $K_{\mathcal{A}} - K_n = K_{\mathcal{A}_1} - K_n$.
- $\mathcal{A} = \neg\, n \circledR \mathcal{A}_1$: then $\mathbf{0} \not\models \mathcal{A}_1$, and $K_{\mathcal{A}} - K_n = K_{\neg\, \mathcal{A}_1} - K_n$.

□

Lemma 7.6 *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 7.5 $\sharp K_{\mathcal{A}} \neq 1$, and the contradiction. □

7.2.2 $\neg$ is expressive

$\neg$ enriches the expressive power in several ways; here we consider the property that the name n occurs free, expressed by $\neg\, n \circledR \top$, and show that negation is necessary to express it. 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 an occurrence of n deep enough.

Definition 7.7 *We define the truncation at height $h \in \mathbb{N}$ as $t_0(P) = \mathbf{0}$, and*

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

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

Lemma 7.8 *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 $t_h(P) \models \mathcal{A}_1 \wedge \mathcal{A}_2$.
- $\mathcal{A} = \mathsf{И} n.\, \mathcal{A}_1$: 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 $t_h(P) \models \mathsf{И} n.\, \mathcal{A}_1$.
- $\mathcal{A} = 0$: 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 $t_h(P) \models \mathcal{A}$.

$\square$

Lemma 7.9 *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 7.8 $\square$

7.2.3 И is expressive

И is very useful to deal with an hidden name without making any hypothesis on the free names of processes (which revelation taken alone would do). Here we consider the property of having at least one hidden name, that is the model is congruent to $(\nu n)P'$ with $n \in \mathrm{fn}(P')$. This is expressed by the formula $\text{И}n.\, n \circledR \neg\, n \circledR \top$. For $N = \{n_1, \ldots n_r\}$ we consider $P_N^n = n[n_1[\mathbf{0}] \mid \ldots \mid n_r[\mathbf{0}]]$ for some $n \notin N$.

Lemma 7.10 *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 $\mathcal{A}$.
- $\mathcal{A} = m \circledR \mathcal{A}_1$: then $m \in \mathrm{fn}(\mathcal{A}) \subseteq N$, hence none of $P_N^n, (\nu n)P_N^n$ does satisfy $\mathcal{A}$.

$\square$

Lemma 7.11 *There is no formula* $\mathcal{A} \in \mathrm{SAL}_{int} - \{\text{И}\}$ *equivalent to* $\text{И}n.\, n \circledR n \circledR \bot$.

Proof: By absurd, let $\mathcal{A}$ be such a quantifier free formula, and $\{n_1, \ldots, n_r\} = \mathrm{fn}(\mathcal{A})$. Then $P_N^n \not\models \mathcal{A}$, so $(\nu n)P \not\models \mathcal{A}$, by Lemma 7.10, and the contradiction. $\square$

7.2.4 0 *is expressive*

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 $n \notin \text{fn}(A)$, $\mathbf{0} \models \mathcal{A}$ iff $n[\mathbf{0}] \models \mathcal{A}$.

Lemma 7.12 *Let $\mathcal{A}$ be a formula without* 0*, and $n \notin \text{fn}(A)$. Then*

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

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.
- $\mathcal{A} = И m. \mathcal{A}_1$: We assume without loss of generality $m \neq n$. If $\mathbf{0} \models И m. \mathcal{A}_1$, then $\mathbf{0} \models \mathcal{A}_1$. $n[\mathbf{0}] \models \mathcal{A}_1$ by induction, so $n[\mathbf{0}] \models И n. \mathcal{A}_1$. Conversely, if $n[\mathbf{0}] \models И m. \mathcal{A}_1$, then $n[\mathbf{0}] \models \mathcal{A}_1$, so $\mathbf{0} \models \mathcal{A}_1$ by induction, and then $\mathbf{0} \models И n. \mathcal{A}_1$.
- 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 $\mathcal{A} = m \circledR \mathcal{A}_1$, $m \neq n$ 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 7.13 *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 7.12, $n[\mathbf{0}] \models \mathcal{A}$ and the contradiction. □

8 Separation logic and classical logic

In this section, we give a second illustration of our minimalisation method. We consider the assertion language presented in [3], referred as Separation Logic (SL). SL holds spatial connectives $*$ and $-\!\!*$ similar to $\mid$ and $\triangleright$ in SAL, with a light but significant difference for $*$: the composition requires a compatibility condition $h \perp h'$ that is not always satisfied; in particular, it is not possible to compose two copies of the same structure $(h * h)$. As a consequence, the expressiveness of $*$ is quite restricted and essentially express the separation of resources, which equality already expresses. For this reason, we can establish the elimination of both $*$ and $-\!\!*$. We define a classical fragment CL and prove it to be as expressive as SL.

We assume a countable set Var of variables, ranged over with x, y, and a set Loc of locations such that Loc $\subseteq \mathbb{N}$. Expressions and assertions of SL are defined by the following grammar: We write $\mathsf{v}(P)$ for the set of variables occurring in P. Assertions

$$
\boxed{\begin{aligned}
e &::= x \mid \mathsf{nil} \mid - \\
P &::= (x \mapsto e_1, e_2) \mid x = y \mid \mathsf{emp} \mid \bot \mid P \Rightarrow P \\
&\quad\mid P * P \mid P \mathrel{-\!\!*} P
\end{aligned}}
$$

Fig. 5. Separation logic (SL)

express properties of memory states, modelled as a pair consisting of a store and a heap, as follows:

$$
\begin{aligned}
\mathrm{Val} &\stackrel{\mathrm{def}}{=} \mathrm{Loc} \sqcup \{\mathsf{nil}\} \\
\mathrm{Store} &\stackrel{\mathrm{def}}{=} \mathrm{Var} \to \mathrm{Val} \\
\mathrm{Heap} &\stackrel{\mathrm{def}}{=} \mathrm{Loc} \rightharpoonup_{fin} \mathrm{Val} \\
\mathrm{State} &\stackrel{\mathrm{def}}{=} \mathrm{Stack} \times \mathrm{Heap}
\end{aligned}
$$

where $\rightharpoonup_{fin}$ stands for a partial function with finite domain. We range over stores with s, over heaps with h, and over states with σ. We note $\sigma_1 \bot \sigma_2$ for $s_1 = s_2$ and $dom(h_1) \cap dom(h_2) = \emptyset$, and, when this holds, $\sigma_1 * \sigma_2$ is the state defined by keeping the same store and by setting $h_1 * h_2(x) = h_1(x)$ or $h_2(x)$.

For a value v, we note $v \models_\sigma e$ if either $e = -$, or $v = e = \mathsf{nil}$, or $e = x$ and $v = s(x)$. We then note $(v_1, v_2) \models_\sigma (e_1, e_2)$ if $v_1 \models_\sigma e_1$ and $v_2 \models_\sigma e_2$. The condition for a state σ to match an assertion P, written $\sigma \models P$, is inductively defined as:

$$
\begin{array}{lll}
\sigma \models \bot & \text{never} & \\
\sigma \models (x \mapsto e_1, e_2) & \text{iff} & dom(h) = \{s(x)\} \text{ and} \\
 & & hs(x) \models_\sigma (e_1, e_2) \\
\sigma \models x = e_y & \text{iff} & s(x) = s(y) \\
\sigma \models \mathsf{emp} & \text{iff} & dom(h) = \emptyset \\
\sigma \models P_1 \Rightarrow P_2 & \text{iff} & \sigma \models P_1 \text{ implies } \sigma \models P_2 \\
\sigma \models P_1 * P_2 & \text{iff} & \text{there exist } \sigma_1 \text{ and } \sigma_2 \text{ such that} \\
 & & \sigma = \sigma_1 * \sigma_2;\ \sigma_1 \models P_1 \text{ and } \sigma_2 \models P_2 \\
\sigma \models P_1 \mathrel{-\!\!*} P_2 & \text{iff} & \text{for all } \sigma_1 \text{ such that } \sigma \bot \sigma_1, \\
 & & \sigma_1 \models P_1 \text{ implies } \sigma * \sigma_1 \models P_2
\end{array}
$$

We may define as usual the connectives $\wedge, \vee, \top, \neg, \Leftrightarrow$ in the obvious way. We also introduce two *monotonic*[1] assertions (cf. Fig 6). Any assertion of this form, or of

monotonic assertion	encoding in SL	semantic
$(x \hookrightarrow e_1, e_2)$	$(x \mapsto e_1, e_2) * \top$	$s(x) \in dom(h)$ and $hs(x) \models_\sigma (e_1, e_2)$
$\mathsf{size} \geq n$	$\underbrace{\neg\,\mathsf{emp} * \ldots * \neg\,\mathsf{emp}}_{n \text{ times}}$	$\sharp dom(h) \geq n$

Fig. 6. Monotonic assertions from SL

the form $x = y$ will be said to be *atomic*. In the remainder, we actually take these as primitive, which ensure the encoding of $(x \mapsto e_1, e_2)$ and emp assertions through boolean combinations[2]. We call *classical logic* (CL) the fragment of SL defined by the grammar of Fig 7. We will note $w(P)$ for the maximal n such that $\mathsf{size} \geq n$

$$\boxed{P \;::=\; P \Rightarrow P \mid \bot \mid (x \hookrightarrow e_1, e_2) \mid x = y \mid \mathsf{size} \geq n\,.}$$

Fig. 7. Classical fragment (CL) of SL

is a subassertion of P, and $\mathsf{v}(P)$ for the set of variables of P.

Our main result is the following:

Theorem 8.1 *CL is as expressive as SL, i.e. for all assertion P of SL, there exists a classical assertion P' of CL such that $\models P \Leftrightarrow P'$.*

At the same time, we also prove the following result: the monotonic (indeed atomic) fragment is as separative as the whole language, that is if two states satisfy the same monotonic assertions, then they satisfy the same assertions.

8.2 Proof of the translation

Our proof proceeds in the same way as for SAL: we define an intensional equivalence and prove that it has the precompactness and characteristic formula properties.

Let X be a finite set of variables, and w an integer. We say that two states σ and σ' are intensionally equivalent for X, w, written $\sigma \approx_{X,w} \sigma'$, if for all classical assertion P with $\mathsf{v}(P) \subseteq X$ and $w(P) \leq w$, $\sigma \models P$ iff $\sigma' \models P$.

[1] or *intuitionistic*, using the terminology of [16], that is assertions P such that $\sigma \models P$ implies $\sigma' \models P$ for all $\sigma' \geq \sigma$.

[2] On the contrary, it is not possible to encode $(x \hookrightarrow e_1, e_2)$ and $\mathsf{size} \geq n$ from $(x \mapsto e_1, e_2)$ and emp using only boolean combinations; this point is also discussed in conclusion.

Remarks:

1 This definition amounts to say that σ and σ' satisfy the same atomic classical assertions P with $\mathsf{v}(P) \subseteq X$ and $w(P) \leq w$.
2 Let us write $w(\sigma) = \sharp dom(h)$. Given three natural numbers a, b, w, we write $a =_w b$ if either $a = b$ or $a, b \geq w$. Then for any σ, σ' such that $\sigma \approx_{X,w} \sigma'$, $w(\sigma) =_w w(\sigma')$.
3 Equality assertions $x = y$ only depend on the store. We note $s =_X s'$ if these stores satisfy the same equality assertions with variables in X. Then for any σ, σ' such that $\sigma \approx_{X,w} \sigma'$, $s =_X s'$.
4 Let V be some set of values. We note $v =_V v'$ if either $v = v'$ or $\{v, v'\} \cap V = \emptyset$, and $(v_1, v_2) =_V (v'_1, v'_2)$ if $v_1 =_V v'_1$ and $v_2 =_V v'_2$. Then for any s, h, h' such that $(s, h) \approx_{X,w} (s, h')$, $dom(h) \cap s(X) = dom(h') \cap s(X)$ due to assertions $x \hookrightarrow -, -$, and for all $l \in s(X) \cap dom(h)$, $h(l) =_{s(X)\cup\{\mathsf{nil}\}} h'(l)$ due to assertions $x \hookrightarrow e_1, e_2$.

Let say more about store equivalence. Consider a store s_0 and a state $\sigma = (s, h)$ such that $s_0 =_X s$. Then we may define a new state $\mathsf{shift}_{s_0,X}\sigma$ of store s_0 and heap h' defined such that

- $dom(h) = s_0(s^{-1}(dom(h)) \cap X) \ \cup B$ with B some arbitrary set of locations such that $\sharp dom(h) = \sharp dom(h')$ and $B \cap s_0(X) = \emptyset$.
- for all $l \in dom(h')$, if $l = s_0(x)$ and $hs(x) = (s(y), s(z))$ for some $x, y, z \in X$, $h' s_0(x)$ is set to be $(s_0(y), s_0(z))$, otherwise $h(l)$ is arbitrarily defined out of $s(X)$.

This is easy to check that σ and $\mathsf{shift}_{s_0,X}\sigma$ satisfy the same atomic assertions with variables in X. Moreover, this transformation is compositional, in the sense that $\mathsf{shift}_{s_0,X}(\sigma * \sigma') = \mathsf{shift}_{s_0,X}\sigma * \mathsf{shift}_{s_0,X}\sigma'$. This transformation is not completely deterministic, but assuming that every choice of a "fresh" value is made different at each time and at each call to $\mathsf{shift}_{,X}$, $\sigma \perp \tau$ will imply $\mathsf{shift}_{s_0,X}\sigma \perp \mathsf{shift}_{s_0,X}\tau$. We actually have the following stronger result:

Lemma 8.2 *For all assertions $P \in SL$ with $\mathsf{v}(P) \subseteq X$, $\sigma \models P$ iff $\mathsf{shift}_{s_0,X}\sigma \models P$.*

The proof is straightforward by induction on the assertion P considering previous remarks.

We now recall the equivalence relation defined by Yang in [19] for the decidability proof, and use it to derive the correction of $\approx_{X,w}$.

Definition 8.3 **($\sim_{s,n,X}$[19])** *Given a stack s, a natural number n and a set X of variables, $\sim_{s,n,X}$ is the relation between heaps such that $h \sim_{s,n,X} h'$ iff*

1 $s(X) \cap dom(h) = s(X) \cap dom(h')$;
2 for all $l \in s(X) \cap dom(h)$, $h(l) =_{s(X)} h'(l)$;
3 $\sharp(dom(h) - s(X)) =_n \sharp(dom(h') - s(X))$.

The first step of the correction proof is to factorize $\approx_{X,w}$ in $\sim_{s,n,X}$.

Lemma 8.4 *For any X, w, n such that $n + \sharp X \leq w$, for any $\sigma, \sigma', s, h, h'$ such that $\sigma = (s, h)$, $\sigma \approx_{X,w} \sigma'$, and $\mathsf{shift}_{s,X}\sigma' = (s, h')$, it holds that $h \sim_{s,n,X} h'$.*

Proof: By Lemma 8.2, $(s, h) \approx_{X,w} (s, h')$. Then conditions 1 and 2 in Definition 8.3 holds by Remark 4, so the proof follows from the verification of the condition 3 on the heap size.

Let us assume first that $\sharp(dom(h) - s(X)) < n$; then $\sharp dom(h) = k < n + \sharp X \leq w$, so $\sigma \models P = \mathsf{size} \geq k \wedge \neg\, \mathsf{size} \geq k + 1$, and $w(P) = k + 1 \leq w$. By definition of $\approx_{X,w}$, $\sigma' \models P$, so $\sharp dom(h') = k = \sharp dom(h)$. Moreover, $s(X) \cap dom(h) = s(X) \cap dom(h')$, so finally $\sharp(dom(h) - s(X)) = \sharp(dom(h') - s(X))$.

Let us assume now that $\sharp(dom(h) - s(X)) \geq n$; and set $k = \min(\sharp dom(h), w)$, so that $\sigma \models \mathsf{size} \geq k$, and by definition of $\approx_{X,w}$, $\sigma' \models \mathsf{size} \geq k$. Moreover, $dom(h) \geq n + \sharp(dom(h) \cap s(X))$, and $w \geq n + \sharp X \geq n + \sharp(dom(h) \cap s(X))$, so finally $k \geq n + \sharp(dom(h) \cap s(X))$. This gives $dom(h') \geq k \geq n + \sharp(dom(h') \cap s(X))$ since $s(X) \cap dom(h) = s(X) \cap dom(h')$, i.e. $\sharp(dom(h') - s(X)) \geq n$.

$\sharp dom(h) \geq k \geq n + \sharp(dom(h) \cap s(X))$, where $k = \min(\sharp dom(h), w)$. So $\sigma \models \mathsf{size} \geq k$, and by definition of $\approx_{X,w}$, $\sigma' \models \mathsf{size} \geq k$, so that finally $\sharp dom(h') \geq n + \sharp(dom(h') \cap s(X))$. $\square$

We now recall the correction result obtained by Yang and derive our correction from it. We first recall the notion of formula's size used by Yang:

$$
\begin{array}{lll}
|\, (e \mapsto e_1, e_2)\, | = 1 & |\, e_1 = e_2\, | = 0 & |\, \mathsf{emp}\, | = 1 \\
|\, P \Rightarrow Q\, | = \max(|\, P\,|, |\, Q\,|) & |\, \bot\, | = 0 & \\
|\, P * Q\, | = |\, P\, | + |\, Q\, | & |\, P \mathrel{-\!\!*} Q\, | = |\, Q\, | &
\end{array}
$$

Lemma 8.5 *Take s, h, h', n, X with $h \sim_{s,n,X} h'$. Then for all assertion $P \in SL$ such that $\mathsf{v}(P) \subseteq X$ and $|\, P\, | \leq n$, $(s, h) \models P$ iff $(s, h') \models P$.*

The proof of this result is detailed in [19].

Corollary 8.6 (Correction) *Take σ, σ', w, X with $\sigma \approx_{X,w} \sigma'$. Then for all assertion $P \in SL$ such that $\mathsf{v}(P) \subseteq X$ and $|\, P\, | + \sharp X \leq w$, $\sigma \models P$ iff $\sigma' \models P$.*

Proof: By Lemma 8.4, $h \approx_{s,n,X} h'$ with $\sigma = (s, h)$, $\mathsf{shift}_{s,X}\sigma' = (s, h')$, and $n = w - \sharp X$. Then $\sigma \models P$ implies $\mathsf{shift}_{s,X}\sigma' \models P$ by Lemma 8.5, which implies $\sigma' \models P$ by Lemma 8.2. $\square$

We may now end the proof establishing the properties of precompactness and characteristic formula for $\approx_{X,w}$.

We write $\Phi_{X,w}$ for the set of atomic assertions P such that $\mathsf{v}(P) \subseteq X$ and $w(P) \leq w$. For X finite, $\Phi_{X,w}$ is finite as well. This has two important consequences:

Proposition 8.7 (Precompactness) *For all w and all finite X, $\approx_{X,w}$ has only finitely many classes.*

Proof: A class is represented by a subset $\Phi \subseteq \Phi_{X,w}$ of atomic assertions that are the ones satisfied by any state of the class. So there are less than $2^{\sharp\Phi_{X,w}}$ distinct classes. □

Proposition 8.8 (Characteristic formula) *For all states σ, for all X, w, there is a classical assertion $F_\sigma^{(X,w)}$ such that*

$$\forall \sigma'. \quad \sigma' \models F_\sigma^{(X,w)} \text{ iff } \sigma \approx_{X,w} \sigma' .$$

Proof: Take

$$\bigwedge_{\sigma \models P, P \in \Phi_{X,w}} P \quad \wedge \bigwedge_{\sigma \not\models P, P \in \Phi_{X,w}} \neg P .$$

□

We may now establish Theorem 8.1 noticing that any assertion P of SL is equivalent to the classical assertion:

$$\bigvee_{C \in \mathrm{State}_{/\approx_{X,w}}, C \models P} F_C^{(X,n)} ,$$

where finiteness of this disjunction is ensured by Proposition 8.7.

9 Conclusion

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

We established the absence of adjunct elimination for the same logic where $\reflectbox{\textsf{N}}$ is replaced by the usual $\forall$ quantifier, whichever adjunct is considered. This result, together with the difference w.r.t. decidability of model-checking on pure trees, illustrates the significant gap existing between the two forms of quantification.

Finally, we defined a classical fragment of the Separation Logic, excluding both $*$ and $-\!\!*$, and proved it to be as expressive as the full separation logic. Our approach shows also that all the separative power of the logic lies in the monotonic fragment.

When defining our classical fragment, we had to move from the assertions $x \mapsto e_1, e_2$ and emp to $x \hookrightarrow e_1, e_2$ and $\mathsf{size} \geq n$ in order to capture the $*$ connective; without that, it is probably possible to eliminate only the adjunct. Note that the assertion $(x \mapsto \mathsf{nil}, \mathsf{nil}) \mathrel{-\!\!*} \mathsf{false}$ would be translated in CL as $x \hookrightarrow -, -$, which underlines the importance of the special expression $-$.

In relation to our study, some observations can be made regarding the difference between the И and the $\forall/\exists$ quantification. The existence of prenex forms, the decidability of the model-checking on pure trees, the adjuncts elimination, are properties verified by the logic with the fresh quantifier, whereas they fail for the universal quantifier.

Yang proposed a clever counterexample to the elimination of $\mathrel{-\!\!*}$ in a Separation Logic with quantifiers; this example seems of deeper meaning than the one presented in Sect. 6, but a better understanding of its implications is still lacking. In the same way, we do not know whether $*$ elimination remains true for the assertion language without $\mathrel{-\!\!*}$ and with quantifiers.

The results we obtain for SAL and SL can be adapted to several other substructural logics. However, for the logics including the time modality $\diamond$ [7,1], adjuncts improve the expressiveness of the logic supporting an encoding of action modalities [18,13]. One could think to take them as primitives in the same spirit as for SL, and look for the adjunct elimination. However, even in the case of very elementary concurrent languages, this project is not realisable [2].

Acknowledgements

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, G. Ghelli, and H. Yang helped me significantly to improve the previous versions 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

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

[2] L. Caires and E. Lozes. Elimination of quantifiers and undecidability in spatial logics for concurrency. to appear in CONCUR'04.

[3] 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.

[4] 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.

[5] 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.

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

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

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

[9] 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.

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

[11] 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.

[12] G. Ghelli and G. Conforti. Decidability of freshness, undecidability of revelation. In *Procs. of FOSSACS'04*, march 2004.

[13] 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.

[14] C.A.R. Hoare. An axiomatic basis for computer programming. *Communications of the ACM*, pages 12(10):576–580, october 1969.

[15] J. Reynolds. Intuitionistic reasoning about shared mutable data structure, 2000.

[16] J. Reynolds. Separation logic: a logic for shared mutable data structures - invited paper. In *Proceedings of LICS '02*, 2002.

[17] D. Lugiez S. Dal-Zilio and C. Meyssonnier. A Logic You Can Count On. In *Proc. of POPL'04*, 2004.

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

[19] Hongseok Yang. *Local Reasoning for Stateful programs*. PhD thesis, University of Illinois at Urbana Champaign, 2001.