Università degli studi di Udine

A complete axiomatic system for a process-based spatial logic

Original

Availability:
This version is available http://hdl.handle.net/11390/851584 since

Publisher:
Springer verlag

Published
DOI:

Terms of use:
The institutional repository of the University of Udine (http://air.uniud.it) is provided by ARIC services. The aim is to enable open access to all the world.

Publisher copyright

(Article begins on next page)

08 November 2024

The Microsoft Research - University of Trento
Centre for Computational
and Systems Biology

Technical Report CoSBi 21/2008

Towards a Complete Axiomatization for Spatial Logic

Radu Mardare

The Microsoft Research-University of Trento Centre for Computational and Systems Biology, Trento, Italy

mardare@cosbi.eu

Alberto Policriti

Department of Mathematics and Computer Science, University of Udine

policriti@dimi.uniud.it

This is the preliminary version of a paper that will appear in
Proc. of the International Symposium on Mathematical Foundations of Computer Science,
MFCS 2008

Towards a Complete Axiomatization for Spatial Logic

Radu Mardare[1], Alberto Policriti[2,3]

[1]The Microsoft Research-University of Trento, Italy

[2]Department of Mathematics and Computer Science,University of Udine

[3]Applied Genomics Institute, Udine, Italy

September 30, 2009

Abstract

The process-based Spatial Logics are multi-modal logics developed for semantics on Process Algebras and designed to specify concurrent properties of dynamic systems. On the syntactic level, they combine modal operators similar to operators of Hennessy-Milner logic, dynamic logic, arrow logic, relevant logic, or linear logic. This combination generates expressive logics, sometimes undecidable, for which a wide range of applications have been proposed.

In the literature, there exist some sound proof systems for spatial logics, but the problem of completeness against process-algebraic semantics is still open. The main goal of this paper is to identify a sound-complete axiomatization for such a logic. We focus on a particular spatial logic that combines the basic spatial operators with dynamic and classical operators. The semantics is based on a fragment of CCS calculus that embodies the core features of concurrent behaviors. We prove the logic decidable both for satisfiability/validity and mode-checking, and we propose a sound-complete Hilbert-style axiomatic system for it.

1 Introduction

Process algebras [2] are calculi designed for modelling complex systems of *processes*[1] organised in a modular way, which run in a decentralised manner and are able to interact, collaborate and communicate. Starting with Robin Milner's classical work on a *Calculus of Communicating Systems* [17], a plethora of process calculi have been developed and successfully applied to a multitude of issues in concurrent computing, e.g. modelling computer networks, cellular/molecular/chemical networks, and a wide class of problems related to them. This success

[1] In this paradigm, the processes are understood as spatially localised and independently observable units of behaviour and computation (e.g. programs or processors running in parallel).

raises the necessity to define query languages able to express complex properties of systems and, eventually, to develop model-verification techniques. The dual nature of these calculi - algebraical/equational syntax versus coalgebraical operational semantics, makes them appropriate for a modal logic-based approach.

In this context were proposed the process semantics for modal logics, that can be considered as a special case of Kripke semantics: it involves structuring a class of processes as a Kripke model, by endowing it with accessibility relations and then using the standard clauses of Kripke semantics. The most obvious accessibility relations on processes are the ones induced by action transitions $\alpha.P\overset{\alpha}{\textbf{to}}P$, and thus the corresponding (Hennessy-Milner) logic [13] was the first process-based modal logic to be developed. Later, temporal [21], mobile or concurrent features were added [10, 18]. A relatively new type of process logics are *spatial logics* [8, 3], which are particularly tailored for capturing spatial and concurrent properties of processes. Among the various spatial operators we mention: the *parallel operator*[2] $\phi|\psi$ and its adjoint - the *guarantee operator* $\phi \triangleright \psi$; the *location operators* characterize ambient logic[3] [8]; for semantics based on calculi with name passing and name restrictions other specific operators have been proposed, e.g. *placement*, *revelation* and *hiding* operators etc [3]. In addition, most of these logics include transition-based modalities and quantifiers.

The modal operators of spatial logics are similar to modal operators studied in other contexts. The parallel operator, for instance, is just a modal operator of arity 3 that satisfies the axioms of associativity, commutativity and modal distribution, as will be proved latter. Operators such as this have been studied, e.g., in the context of *Arrow Logic* [1] where it entails undecidability for Kripke semantics, as proved in [11]. The parallel operator and the guarantee operator of spatial logics are similar to two operators used in *Relevant* and *Substructural Logics* [22] - the *intentional conjunction* and *relevant implication* respectively. But, as in the case of Arrow Logic, Relevant Logic has a semantics in terms of Kripke structures. Consequently, not many known results can be projected over the process semantics. Some spatial logics are using dynamic operators [12] for expressing the transitions. There are also other relations between spatial logics and well studied modal logics[4].

On the other hand, there are many peculiarities of spatial logics that make them interesting from a modal perspective. For example, the spatial logic we study in this paper allows us to define characteristic formulas for processes. Such a formula identifies a process up to structural congruence, i.e. we have formulas f_P that names a particular state P of the system, thus giving to the logic the expressivity of Hybrid Logics [19]. Another peculiarity is that we can define a universal modality $\circ\phi$ and thus, we can express syntactically meta properties such as validity and satisfiability of a formula. The guarantee operator can be used to translate any satisfiability/validity problem of spatial logic into a model checking problem for the null process, as $\models \phi$ can be proved equivalent with $0 \models \top \triangleright \phi$, [9]. In this way, decidability of satisfiability and validity is directly related with the decidability of model checking. All these peculiarities of spatial logics emerge mainly from the structure of their models, which are not just labelled graphs, but processes with a structure bound by the rigid rules of the operational

[2] A process P has the property $\phi|\psi$, if it can be split into two disjoint parts $P \equiv Q|R$ s.t. Q satisfies ϕ and R satisfies ψ.

[3] Ambient logic is a spatial logic defined over ambient calculus.

[4] See e.g. [8] for a detailed description of the connection between Ambient logic and Linear Logic

semantics of process calculi.

The challenge we take in this paper is to find a sound and complete Hilbert-style axiomatic system for spatial logic that will reveal the nature of the spatial operators, as well as the interrelation between them and the dynamic or classical operators. The axioms we propose are sometimes similar with the axioms of the related modal logics and these similarities are useful in placing the spatial logics in the general context of modal logics. To the best of our knowledge, the problem of completeness for this class of logics has not been approached in the literature, even if the problem of defining sound sequence calculi for them has been considered [6, 8, 4]. Related to static ambient logic, for instance, there exists a sound-complete sequent calculus [6], but its syntax differs from the syntax of ambient logics. It is done for atomic construction of type $P : \phi$ for a process P and a logic formula ϕ, that encodes the satisfiability relation $P \models \phi$ of ambient logic; the sequent rules just rewrite the semantics of ambient logic. In this context, the soundness and completeness are proved as $P \models \phi$ iff $\vdash P : \phi$, result that does not clarify the axiomatics of spatial logics, the syntactic behavior of the spatial operators, or the relation with other logics. Our previous work [14, 15] present some completeness results from a modal perspective, but for only for epistemic versions of spatial logics without the guarantee operator.

A second achievement of the paper is a decidability result that is essential in the completeness proof. The particular spatial logic studied in this paper (that extends the Hennessy-Milner logic with the parallel and guarantee operators) is proved decidable for both satisfiability/validity and model checking against a fragment of CCS calculus that embodies the core features of finite concurrent behaviors. The decidability proof goes on the lines of decidability proofs in [7, 6] and consist in proving the bound model property for the logic. As for the semantics, the same fragment of CCS yields undecidability for other spatial logics, e.g. with a modality encoding communication-based transitions [5].

2 Preliminaries on Process Algebra

In this section we recall a number of basic notions of process algebra, mainly to establish some basic terminology and notations for this paper. We introduce a fragment of CCS calculus that will be latter used as semantics for the logic. The novelty of the section is the *structural bisimulation*, a special relation on processes that will be latter used for proving the bounded model property for the spatial logic.

Definition 2.1 (CCS processes) *Let Σ be a denumerable set of elements called* actions *and $0 \notin \Sigma$ a special object called the* null process. *The* class of CCS processes *is introduced inductively, for arbitrary $\alpha \in \Sigma$, as follows.*

$P := 0 \mid \alpha.P \mid P|P$

We denote by $\mathbb{P}$ the class of CCS processes.

Definition 2.2 (Structural congruence) *The structural congruence is the smallest congruence relation $\equiv \subseteq \mathbb{P} \times \mathbb{P}$ such that $(\mathbb{P}, |, 0)$ is an abelian monoid with respect to $\equiv$, i.e.*

1. $(P|Q)|R \equiv P|(Q|R)$ 2. $P|0 \equiv 0|P \equiv P$ 3. $P|Q \equiv Q|P$

Definition 2.3 (Operational semantics) *Let $\tau \notin \Sigma \cup \mathbb{P}$ and consider a function on Σ that associates to each $\alpha \in \Sigma$ its* complementary action *$\overline{\alpha}$, such that $\overline{\overline{\alpha}} = \alpha$. The operational semantics on $\mathbb{P}$ defines a labeled transition system $\mathbb{T} : \mathbb{P} \to (\Sigma \cup \{\tau\}) \times \mathbb{P}$ by means of the rules in Table 1, where $\mathbb{T}(P) = (\alpha, Q)$ is denoted by $P\overset{\alpha}{\textbf{to}}Q$ for any $\alpha \in \Sigma$, $\mathbb{T}(P) = (\tau, Q)$ is denoted by $P\overset{\tau}{\textbf{to}}Q$, and μ is used to denote arbitrary elements in $\Sigma \cup \{\tau\}$.*

$\alpha.P\overset{\alpha}{\textbf{to}}P$, $\alpha \in \Sigma$ $\alpha.P|\overline{\alpha}.Q\overset{\tau}{\textbf{to}}P|Q$, $\alpha \in \Sigma$

P$\equiv Q$
$P\overset{\mu}{\textbf{to}}P'$ $Q\overset{\mu}{\textbf{to}}P'$, $\mu \in \Sigma \cup \{\tau\}$ $\overset{\mu}{\textbf{Pto}}\, P'$ $P|Q\overset{\mu}{\textbf{to}}P'|Q$, $\mu \in \Sigma \cup \{\tau\}$

Table 1: The transition system

Hereafter, we call a process P *guarded* if $P \equiv \alpha.Q$ for some $\alpha \in \Sigma$ and we use the notation $P^k \overset{def}{=} \underbrace{P|...|P}_{k}$ for $k \leq 1$.

Definition 2.4 *The* set of actions *$Act(P) \subset \Sigma$ of an arbitrary process $P \in \mathbb{P}$ is defined, inductively, as follows.*
$1.Act(0) \overset{def}{=} \emptyset$ $2.Act(\alpha.P) \overset{def}{=} \{\alpha\} \cup Act(P)$ $3.Act(P|Q) \overset{def}{=} Act(P) \cup Act(Q)$.

For a set $\Omega \subseteq \Sigma$ and a pair h, w of nonnegative integers we define the class $\mathbb{P}^{\Omega}_{(h,w)}$ of processes having the actions from Ω and the syntactic trees bound by two dimensions - the *depth* h of the tree and the width w that represents the maximum number of congruent processes that can be found in a node of the tree. $\mathbb{P}^{\Omega}_{(h,w)}$ is introduced inductively on h.
$\mathbb{P}^{\Omega}_{(0,w)} = \{0\}$;
$\mathbb{P}^{\Omega}_{(h+1,w)} = \{(\alpha_1.P_1)^{k_1}|...|(\alpha_i.P_i)^{k_i},$ for $k_j \leq w, \alpha_j \in \Omega, P_j \in \mathbb{P}^{\Omega}_{(h,w)}, \forall j = 1..i\}$.
If $\Omega \subseteq \Sigma$ is a finite set, then $\mathbb{P}^{\Omega}_{(h,w)}$ is a finite set of processes.

2.1 Structural Bisimulations

In this subsection we introduce the *structural bisimulation*, a relation on processes indexed by a subclass $\Omega \subseteq \Sigma$ of actions and by two nonnegative integers h, w. This relation is similar to the pruning relation proposed for trees (static ambients) in [6]. Intuitively, two processes are Ω-structural bisimilar on size (h, w) if they look indistinguishable for an external observer that sees only the actions in Ω, does not following a process for more than h transition steps and cannot distinguish more than w cloned subprocesses of a process.

Definition 2.5 (Ω-Structural Bisimulation) *Let $\Omega \subseteq \Sigma$ and h, w two nonnegative integers. The Ω-structural bisimulation on $\mathbb{P}$ is denoted by $\approx^{\Omega}_{(h,w)}$ and is defined inductively as follows.*
If $P \equiv Q \equiv 0$, then $P \approx^{\Omega}_{(h,w)} Q$;

If $P \not\equiv 0$ and $Q \not\equiv 0$, then
$P \approx^{\Omega}_{(0,w)} Q$ always.
$P \approx^{\Omega}_{(h+1,w)} Q$ iff for any $i \in 1..w$ and any $\alpha \in \Omega$:

- *$P \equiv \alpha.P_1|...|\alpha.P_i|P'$ implies $Q \equiv \alpha.Q_1|...|\alpha.Q_i|Q'$, $P_j \approx^{\Omega}_{(h,w)} Q_j$, $j = 1..i$;*
- *$Q \equiv \alpha.Q_1|...|\alpha.Q_i|Q'$ implies $P \equiv \alpha.P_1|...|\alpha.P_i|P'$, $Q_j \approx^{\Omega}_{(h,w)} P_j$, $j = 1..i$.*

Hereafter we present some results about Ω-structural bisimulation.

[Equivalence] For a set $\Omega \subseteq \Sigma$ and nonnegative integers h, w, $\approx^{\Omega}_{(h,w)}$ is an equivalence relations on $\mathbb{P}$.

[Congruence] Let $\Omega \subseteq \Sigma$ be a set of actions.
1. If $P \approx^{\Omega}_{(h,w)} Q$, then $\alpha.P \approx^{\Omega}_{(h+1,w)} \alpha.Q$.
2. If $P \approx^{\Omega}_{(h,w)} P'$ and $Q \approx^{\Omega}_{(h,w)} Q'$, then $P|Q \approx^{\Omega}_{(h,w)} P'|Q'$.

For nonnegative integers h, h', w, w' we convey to write $(h', w') \leq (h, w)$ iff $h' \leq h$ and $w' \leq w$.

Let $\Omega' \subseteq \Omega \subseteq \Sigma$ and $(h', w') \leq (h, w)$. If $P \approx^{\Omega}_{(h,w)} Q$, then $P \approx^{\Omega'}_{(h',w')} Q$.

[Split] If $P'|P'' \approx^{\Omega}_{(h,w_1+w_2)} Q$ for some $\Omega \subseteq \Sigma$, then there exists $Q, Q' \in \mathbb{P}$ such that $Q \equiv Q'|Q''$ and $P' \approx^{\Omega}_{(h,w_1)} Q'$, $P'' \approx^{\Omega}_{(h,w_2)} Q''$.

[Step-wise propagation] If $P \approx^{\Omega}_{(h,w)} Q$ and $P\overset{\alpha}{\textbf{to}}P'$ for some $\alpha \in \Omega \subseteq \Sigma$, then there exists a transition $Q\overset{\alpha}{\textbf{to}}Q'$ such that $P' \approx^{\Omega}_{(h-1,w-1)} Q'$.

As Σ is a denumerable set, assume a lexicographic order $\ll \subseteq \Sigma \times \Sigma$ on it. Then, any element $\alpha \in \Sigma$ has a successor denoted by $succ(\alpha)$ and any finite subset $\Omega \subset \Sigma$ has a maximum element denoted by $sup(\Omega)$. We define $\Omega^+ = \Omega \cup \{succ(sup(\Omega))\}$.

All the previous results can be used to prove the next theorem. It states that for any finite set Ω of actions and any nonnegative integers h, w, the equivalence relation $\approx^{\Omega}_{(h,w)}$ divides $\mathbb{P}$ in equivalence classes such that each equivalence class has a representative in the set $\mathbb{P}^{\Omega^+}_{(h,w)}$. This set, by Lemma2, is finite. This observation will be the key for proving, latter, the bounded model property.

[Pruning Theorem] For any finite set $\Omega \subseteq \Sigma$, any nonnegative integers h, w and any process $P \in \mathbb{P}$, there exists a process $Q \in \mathbb{P}^{\Omega^+}_{(h,w)}$ such that $P \approx^{\Omega}_{(h,w)} Q$.

3 Spatial Logic

In this section we introduce the spatial logic SL that contains only one atomic proposition[5] 0, a class of dynamic operators $\langle\alpha\rangle$ indexed by a denumerable set $\Sigma \ni \alpha$, the parallel operator and its adjoint together with the Boolean operators.

Definition 3.1 (Syntax of Spatial Logics) *Let Σ be a denumerable alphabet. The class $\mathcal{L}$ of well formed formulas of SL is introduced inductively as follows.*

[5] In spatial logics the symbol 0 it is used both in syntax for representing the atomic proposition and in semantics to represent the null process in CCS.

$$\phi := 0 \mid \neg\phi \mid \phi \wedge \phi \mid \langle\alpha\rangle\phi \mid \phi|\phi \mid \phi \triangleright \phi.$$

Definition 3.2 (Semantics of SL) *The semantics of SL is given by the satisfiability operator, $P \models \phi$ that relates a process $P \in \mathbb{P}$ with the formula $\phi \in \mathcal{L}$, inductively by.*
$P \models 0$ *iff* $P \equiv 0$.
$P \models \neg\phi$ *iff* $P \not\models \phi$.
$P \models \phi \wedge \psi$ *iff* $P \models \phi$ *and* $P \models \psi$.
$P \models \langle\alpha\rangle\phi$ *iff there exists a transition* $P\overset{\alpha}{\textbf{to}}P'$ *and* $P' \models \phi$.
$P \models \phi|\psi$ *iff* $P \equiv Q|R$, $Q \models \phi$ *and* $R \models \psi$.
$P \models \phi \triangleright \psi$ *iff for any* Q, $Q \models \phi$ *implies* $P|Q \models \psi$.

For arbitrary $\phi, \psi \in \mathcal{L}$ and $\alpha \in \Sigma$ we introduce some derived operators[6].

$$\begin{array}{lll}
\top \overset{def}{=} 0 \vee \neg 0 & \bot \overset{def}{=} \neg\top & \phi \parallel \psi \overset{def}{=} \neg(\neg\phi|\neg\psi) \\
\circ\phi \overset{def}{=} (\neg\phi) \triangleright \bot & 1 \overset{def}{=} \neg 0 \wedge (0 \parallel 0) & \alpha.\phi \overset{def}{=} 1 \wedge \langle\alpha\rangle\phi \\
\bullet\phi \overset{def}{=} \neg(\circ\neg\phi) & &
\end{array}$$

The derived operators can be characterized semantically by:
$P \models \top$ always.
$P \models \bot$ never.
$P \models \phi \parallel \psi$ iff $P \equiv P_1|P_2$, then either $P_i, v \models \phi$ or $P_j, v \models \psi$, $\{i, j\} = \{1, 2\}$.
$P \models \circ\phi$ iff for any process Q, $Q \models \phi$.
$P \models \bullet\phi$ iff there exists a process Q, $Q \models \phi$.
$P \models 1$ iff there exists $\alpha \in \Sigma$ and $P \equiv \alpha.Q$.
$P \models \alpha.\phi$ iff there exists $\alpha \in \Sigma$ s.t. $P \equiv \alpha.P'$ and $P' \models \phi$.
Notice, from the semantics, that $\circ$ is a universal modality as the satisfiability of $\circ\phi$ is equivalent with the validity of ϕ, while $\bullet$ is its dual.

Definition 3.3 *A formula $\phi \in \mathcal{L}$ is* satisfiable *if there exists a process $P \in \mathbb{P}$ such that $P \models \phi$. A formula $\phi \in \mathcal{L}$ is* valid *(a* validity*), denoted by $\models \phi$, if for any process $P \in \mathbb{P}$, $P \models \phi$.*

4 Decidability of SL

In what follows we show that satisfiability, validity and model checking are decidable for SL against process semantics. The proof is based on the bounded model property technique which consists in showing that, given a formula $\phi \in \mathcal{L}$, we can identify a finite class of processes bound by the dimension of the formula, $\mathbb{P}_\phi$ such that if ϕ has a model in $\mathbb{P}$, then it has a model in $\mathbb{P}_\phi$. Thus, the satisfiability problem in $\mathbb{P}$ is equivalent with the satisfiability in $\mathbb{P}_\phi$. This result can be further used to prove the decidability of satisfiability. Indeed, as $\mathbb{P}_\phi$ is finite, checking the satisfiability of a formula can be done by investigating, one by one, all the processes in $\mathbb{P}_\phi$.

[6] We also assume all the boolean operators.

Definition 4.1 (Size of a formula) *The* sizes of a formula *of $\mathcal{L}$, denoted by $\phi = (h, w)$, is defined inductively on the structure of a formula. In what follows, suppose that $\phi = (h, w)$ and $\psi = (h', w')$.*
1. $0 \stackrel{def}{=} (1, 1)$. 2. $\neg\phi \stackrel{def}{=} \phi$.
3. $\phi \wedge \psi \stackrel{def}{=} (max(h, h'), max(w, w'))$. 4. $\langle\alpha\rangle\phi \stackrel{def}{=} (h + 1, w + 1)$.
5. $\phi \triangleright \psi \stackrel{def}{=} (max(h, h'), w + w')$. 6. $\phi|\psi \stackrel{def}{=} (max(h, h'), w + w')$.

Definition 4.2 *The set of actions of a formula ϕ, $act(\phi) \subseteq \Sigma$ is given by:*
1. $act(0) \stackrel{def}{=} \emptyset$ 2. $act(\neg\phi) = act(\phi)$
3. $act(\phi \wedge \psi) \stackrel{def}{=} act(\phi) \cup act(\psi)$ 4. $act(\langle\alpha\rangle\phi) \stackrel{def}{=} \{\alpha\} \cup act(\phi)$
5. $act(\phi \triangleright \psi) \stackrel{def}{=} act(\phi) \cup act(\psi)$ 6. $act(\phi|\psi) \stackrel{def}{=} act(\phi) \cup act(\psi)$

The next Lemma states that a formula $\phi \in \mathcal{L}$ expresses a property of a process P up to $\approx_{\phi}^{act(\phi)}$. This means that ϕ expresses a property that involves only its actions and is bounded by its size.

If $P \approx_{\phi}^{act(\phi)} Q$, then $P \models \phi$ iff $Q \models \phi$.

This result guarantees the bounded model property.

Theorem 4.1 (Bound model property) *If $P \models \phi$, then there exists $Q \in \mathbb{P}_{\phi}^{act(\phi)^+}$ such that $Q \models \phi$.*

Proof The result is a direct consequence of Lemma 2.1 and Lemma 4. □

Theorem 4.2 (Decidability) *For SL validity, satisfiability and model checking are decidable against process semantics.*

Proof The decidability of satisfiability derives from the bounded model property. Indeed, if ϕ has a model, by Lemma4.1, it has a model in $\mathbb{P}_{\phi}^{act(\phi)^+}$. As $act(\phi)$ is finite, by Lemma 2, $\mathbb{P}_{\phi}^{act(\phi)^+}$ is finite, hence checking for membership is decidable.

The decidability of validity derives from the fact that ϕ is valid iff $\neg\phi$ is not satisfiable. □

5 Characteristic formulas

In this section we use the peculiarities of $\mathcal{L}$ to define characteristic formulas for processes. Consider the subclass $\overline{\mathcal{F}} \subseteq \mathcal{L}$ of well formed formulas of SL given, for arbitrary $\alpha \in \Sigma$ by $f := 0 \mid \alpha.f \mid f|f$. Let $^* : \overline{\mathcal{F}} \to \overline{\mathcal{F}}$ be the function defined by:
$0^* = 0$; $(\alpha.f)^* = \alpha.f^*$; $(f|0)^* = f^*$; $(f_1|f_2)^* = f_1^*|f_2^*$, for $f_1 \neq 0 \neq f_2$.
Denote by $\mathcal{F} \subseteq \overline{\mathcal{F}}$ the set of fixed points of function * called *proper formulas*, i.e., the set of formulas $f \in \overline{\mathcal{F}}$ s.t. $f^* = f$. For arbitrary positive integers h, w and arbitrary $S \subseteq \Sigma$, let

$$\mathcal{F}_{(h,w)}^{S} = \{f \in \mathcal{F} \mid f \leq (h, w), act(f) \subseteq S\}.$$

Observe that $\mathcal{F} \subseteq \mathcal{L}$ and for a finite set $S \subseteq \Sigma$, $\mathcal{F}^S_{(h,w)}$ is finite. In what follows, we use Greek letters (sometime with indexes) ϕ, ψ, ϕ_1, etc. to denote arbitrary formulas of $\mathcal{L}$ and f, f', f'', f_1, f_2, etc. to denote arbitrary proper formulas of $\mathcal{F}$.

The next Lemma proves that the $\equiv$-equivalence classes of $\mathbb{P}$ can be characterized by formulas of $\mathcal{F}$. For this reason, in what follows, we will use sometime the notation f_P to denote a proper formula $f \in \mathcal{F}$ that characterizes the $\equiv$-equivalence class of $P \in \mathbb{P}$.

1. Let $f \in \mathcal{F}$, $P, Q \in \mathbb{P}$. Then $P \models f$ and $Q \models f$, iff $P \equiv Q$.
2. For any $P \in \mathbb{P}$ there exists $f \in \mathcal{F}$ such that $P \models f$.
3. For any $f \in \mathcal{F}$ there exists $P \in \mathbb{P}$ such that $P \models f$.

Proof The function $[\;] : \mathcal{F} \to \mathbb{P}$ given by the next rules defines the relation between the formulas in $\mathcal{F}$ and the $\equiv$-equivalence classes in $\mathbb{P}$.

$[0] = 0; \qquad [\alpha.f] = \alpha.[f]; \qquad [f_1|f_2] = [f_1]|[f_2].$ □

6 A Hilbert-style axiomatic system of SL

In table 2 is proposed a Hilbert-style axiomatic system for SL. We assume the axioms and the rules of propositional logic. In addition we have axioms and rules that characterize the spatial and dynamic operators and their interrelations. Recall that we use Greek letters to specify arbitrary formulas of $\mathcal{L}$ and f, f_1, f_2 to specify arbitrary proper formulas (of $\mathcal{F}$).

Due to the way the proper formulas are defined, the axioms $(S1) - (S4)$ guarantees that for any formula $f \in \mathcal{F}$ the set $\{(f', f'') \in \mathcal{F} \times \mathcal{F} \mid \; \vdash f \leftrightarrow f'|f''\}$ is finite. This proves that the disjunction in axiom $(S6)$ is finitary.

Observe that the rules $(GR1)$ and $(GR2)$ depicts the adjunction between the two spatial operators $|$ and $\triangleright$.

The condition $\alpha.f, f|f' \in \mathcal{F}^{act(\phi)^+}_{\phi}$ reflects the finite model property and guarantees that (Ind) can be based on a finite number of premises.

Definition 6.1 *A formula $\phi \in \mathcal{L}$ is* provable in SL, *denoted by $\vdash \phi$ if ϕ is an axiom or it can be derived, as a theorem, from the axioms of SL using the rules of SL. A formula $\phi \in \mathcal{L}$ is* consistent in SL *if $\neg\phi$ is not provable in SL.*

All the axioms and the rules of our axiomatic system depict true facts about processes. This is proved by the next soundness theorem.

Theorem 6.1 (Soundness) *The axiomatic system of SL is sound with respect to the process semantics, i.e. if $\vdash \phi$ then $\models \phi$.*

Before continuing with the completeness proof, we list some theorems of SL that will be useful further. Recall that, in what follows, we denote by $f_P \in \mathcal{F}$ any proper formula that characterizes the process P.

[Spatial corollaries] The next assertions are theorems of SL.

1. $\vdash \phi|(\psi \wedge \rho) \to (\phi|\psi) \wedge (\phi|\rho)$
2. If $\vdash \phi \to \rho$ and $\vdash \psi \to \theta$, then $\vdash \phi|\psi \to \rho|\theta$.

Spatial axioms

(S1): $\vdash (\phi|\psi)|\rho \to \phi|(\psi|\rho)$

(S2): $\vdash \phi|0 \leftrightarrow \phi$

(S3): $\vdash \phi|\psi \to \psi|\phi$

(S4): $\vdash \top|\bot \to \bot$

(S5): $\vdash \phi|(\psi \vee \rho) \to (\phi|\psi) \vee (\phi|\rho)$

(S6): $\vdash (f \wedge \phi|\psi) \to \bigvee_{f \leftrightarrow f'|f''} (f' \wedge \phi)|(f'' \wedge \psi)$

Spatial rules

(SR1): If $\vdash \phi \to \psi$ then $\vdash \phi|\rho \to \psi|\rho$

Dynamic axioms

(D1): $\vdash \langle\alpha\rangle\phi|\psi \to \langle\alpha\rangle(\phi|\psi)$

(D2): $\vdash [\alpha](\phi \to \psi) \to ([\alpha]\phi \to [\alpha]\psi)$

(D3): $\vdash 0 \vee \alpha.\top \to [\beta]\bot$, for $\alpha \neq \beta$

(D4): $\vdash \alpha.\phi \to [\alpha]\phi$

Dynamic rules

(DR1): If $\vdash \phi$ then $\vdash [\alpha]\phi$

(DR2): If $\vdash \phi_1 \to [\alpha]\phi_1'$ and $\vdash \phi_2 \to [\alpha]\phi_2'$
then $\vdash \phi_1|\phi_2 \to [\alpha](\phi_1'|\phi_2 \vee \phi_1|\phi_2')$

Guarantee axiom

(G1): $\vdash \circ(f \to \phi) \to \bullet\phi$

Guarantee rules

(GR1): $\vdash \phi_1 \to (\phi_2 \triangleright \psi)$ iff $\vdash \phi_1|\phi_2 \to \psi$

(GR2): $\vdash \phi_1 \to \neg(\phi_2 \triangleright \psi)$ iff $\vdash \bullet(\phi_1|\phi_2 \wedge \neg\psi)$

Induction rule

(Ind): If for any $\alpha.f, f|f' \in \mathcal{F}_{\phi}^{act(\phi)^+}$
$\vdash 0 \to \phi$
$\vdash \circ(f \to \phi) \to \circ(\alpha.f \to \phi)$
$\vdash (\circ(f \to \phi) \wedge \circ(f' \to \phi)) \to \circ(f|f' \to \phi)$
then $\vdash \phi$

Table 2: The axiomatic system of SL

3. If $P \not\equiv Q$, then $\vdash f_P \to \neg f_Q$.
4. If for any Q, R s.t. $P \equiv Q|R$, $\vdash f_Q \to \neg\phi$ or $\vdash f_R \to \neg\psi$, then $\vdash f_P \to \neg(\phi|\psi)$.

[Dynamic corollaries] The next assertions are theorems of SL.

1. If $\vdash \phi \to \psi$, then $\vdash \langle\alpha\rangle\phi \to \langle\alpha\rangle\psi$.
2. If $\vdash \phi \to \psi$, then $\vdash [\alpha]\neg\psi \to [\alpha]\neg\phi$.
3. $\vdash f_P \to [\alpha]\bigvee\{f_Q \mid P \xrightarrow{\alpha} Q\}$.
4. If $\vdash \bigvee\{f_Q \mid P \xrightarrow{\alpha} Q\} \to \phi$, then $\vdash f_P \to [\alpha]\phi$.

[Guarantee corollary] The next assertions are SL-theorems.

1. If $\vdash \bigvee_{f \in \mathcal{F}_{\phi}^{act(\phi)+}} f \to \phi$, then $\vdash \phi$.
2. If $\vdash \phi$, then $\vdash \circ\phi$.

Now we approach the completeness problem. We begin with the next lemma stating that a process P satisfies a property ϕ iff its characteristic formula f_P implies the property ϕ and this implication is a theorem in SL system.

If $P \in \mathbb{P}$ and $f_P \in \mathcal{F}$ characterizes P, then $P \models \phi$ iff $\vdash f_P \to \phi$.

Proof ($\Longrightarrow$:) If $P \models \phi$, then $\vdash f_P \to \phi$. We prove it by induction on the syntactical

structure of ϕ. We show here only the cases that require a more complex analysis.
The case $\phi = \phi_1|\phi_2$**:** $P \models \phi$ iff $P \equiv Q|R$, $Q \models \phi_1$ and $R \models \phi_2$. Using the inductive hypothesis, $\vdash f_Q \rightarrow \phi_1$ and $\vdash f_R \rightarrow \phi_2$. The case 2 of Lemma 6 implies further $\vdash f_Q|f_R \rightarrow \phi_1|\phi_2)$, i.e. $\vdash f_P \rightarrow \phi$.
The case $\phi = \psi \triangleright \rho$**:** $P \models \psi \triangleright \rho$ iff for any process Q, $Q \models \psi$ implies $P|Q \models \rho$. The inductive hypothesis gives that for any Q, $\vdash f_Q \rightarrow \psi$ implies $\vdash f_P|f_Q \rightarrow \rho$. But Rule $(GR1)$ gives the equivalence of $\vdash f_P|f_Q \rightarrow \rho$ and $\vdash f_Q \rightarrow (f_P \triangleright \rho)$. Hence, for any Q, $\vdash f_Q \rightarrow (\phi \rightarrow f_P \triangleright \rho)$. Then, for any Q with $f_Q \in \mathcal{F}^{act(\phi \rightarrow f_P \triangleright \rho)^+}_{\phi \rightarrow f_P \triangleright \rho}$, $\vdash f_Q \rightarrow (\phi \rightarrow f_P \triangleright \rho)$. Hence, $\vdash \bigvee_{f \in \mathcal{F}^{act(\phi \rightarrow f_P \triangleright \rho)^+}_{\phi \rightarrow f_P \triangleright \rho}} f \rightarrow (\phi \rightarrow f_P \triangleright \rho)$ where from, using Lemma 6, $\vdash \phi \rightarrow f_P \triangleright \rho$ that is equivalent with $\vdash f_P \rightarrow \phi \triangleright \rho$.
The case $\phi = \neg(\psi_1|\psi_2)$**:** $P \models \neg(\psi_1|\psi_2)$ means that for any parallel decomposition of $P \equiv Q|R$, $Q \models \neg\psi_1$ or $R \models \neg\psi_2$, i.e., $\vdash f_Q \rightarrow \neg\psi_1$ or $\vdash f_R \rightarrow \neg\psi_2$. Then, the case 4 of Lemma6 gives $\vdash f_P \rightarrow \neg\psi$.
The case $\psi = \neg(\phi_1 \triangleright \phi_2)$**:** $P \models \neg(\phi_1 \triangleright \phi_2)$ is equivalent with $P \not\models \phi_1 \triangleright \phi_2$. Hence, there exists $Q \models \phi_1$ such that $P|Q \models \neg\phi_2$, i.e., $\vdash f_Q \rightarrow \phi_1$ and $\vdash f_P|f_Q \rightarrow \neg\phi_2$. Hence, $\vdash f_P|f_Q \rightarrow (f_P|\phi_1 \wedge \neg\phi_2)$. Further, Lemma 6 implies $\vdash \circ(f_P|f_Q \rightarrow (f_P|\phi_1 \wedge \neg\phi_2))$, Axiom $(G1)$, $\vdash \bullet(f_P|\phi_1 \wedge \neg\phi_2)$ and Rule $(GR2)$, $\vdash f_P \rightarrow \neg(\phi_1 \triangleright \phi_2)$.

($\Longleftarrow$) Let $\vdash f_P \rightarrow \phi$. Suppose that $P \not\models \phi$. Then, $P \models \neg\phi$. Using the reversed implication we obtain $\vdash f_P \rightarrow \neg\phi$, thus, $\vdash f_P \rightarrow \bot$. But $P \models f_P$ which, using the soundness, gives $P \models \bot$ impossible! Hence, $P \models \phi$. □

Using the result of the previous lemma we can prove that consistency implies satisfiability, as stated in the next lemma.

If ϕ is SL-consistent then there exists a process $P \in \mathbb{P}$ such that $P \models \phi$.

Proof Suppose that for any process P we do not have $P \models \phi$, i.e., $P \models \neg\phi$. Using Lemma 6, we obtain $\vdash f_P \rightarrow \neg\phi$, i.e. $\vdash \circ(f_P \rightarrow \neg\phi)$. as this is happening for all processes, implies that for any $f \in \mathcal{F}$ we have $\vdash f \rightarrow \neg\phi$, i.e. $\vdash f \rightarrow \neg\phi$. But then $\vdash 0 \rightarrow \neg\phi$, $\vdash \circ(f \rightarrow \neg\phi) \rightarrow \circ(\alpha.f \rightarrow \neg\phi)$ and $\vdash (\circ(f \rightarrow \neg\phi) \wedge \circ(f' \rightarrow \neg\phi)) \rightarrow \circ(f|f' \rightarrow \neg\phi)$. Further, the rule (Ind) gives $\vdash \neg\phi$ wich contradicts the consistency of ϕ. □

At this point we have all the results needed to prove the completeness of our axiomatic system.

Theorem 6.2 (Completeness) *The axiomatic system of SL is complete with respect to process semantics, i.e. if $\models \phi$ then $\vdash \phi$.*

Proof Suppose that ϕ is a valid formula with respect to our semantics, but ϕ is not provable from our the axiomatic system. Then neither is $\neg\neg\phi$, so, by definition, $\neg\phi$ is SL-consistent. It follows, from Lemma 6, that $\neg\phi$ is satisfiable with respect to process semantics, contradicting the validity of ϕ. □

Consequently, the axiomatic system of SL proposed in Table2 is sound and complete with respect to process semantics. This means that any fact about CCS processes that can be expressed in $\mathcal{L}$ has the properties:

- if it is true, then either it is stated in the axioms or it can be proved from the axioms;
- if it is stated in the axioms or if it can be proved from the axioms, then it true about processes.

These two characteristics of the axiomatic system, the soundness and completeness, present SL as a powerful tool for expressing and analysing properties of CCS processes.

7 Conclusion and future works

The achievements of this paper can be summarized as follows. We identified an interesting multi-modal logic, SL, with semantics on CCS calculus able to express dynamic and concurrent properties of distributed systems. The language of SL is expressive enough to characterize the CCS processes up to structural congruence, quality that reveal for SL an expressivity comparable with the expressivity of hybrid logics. In SL we can also define universal modalities that allow us to express meta properties such as validity and satisfiability. In spite of this level of expressivity, we proved the bounded model property for SL against a fragment of CCS for which other spatial logics are undecidable. The bounded model property entails decidability for satisfiability, validity, and model checking.

The main result of the paper is the sound-complete axiomatic system that we propose for SL. Some of the axioms and rules are similar with axioms and rules known from other modal logics, and this peculiarity can help in better understanding the modal face of the concurrency and in placing spatial logics in the general context of modal logics.

References

[1] J. van Benthem, Language in action. Categories, Lambdas and Dynamic Logic, Elsevier Science Publisher, 1991

[2] J.A. Bergstra, A. Ponse, S.A. Smolka (eds.), Handbook of Process Algebra, North Holland, Elsevier, 2001.

[3] L. Caires and L. Cardelli. A Spatial Logic for Concurrency (Part I), Information and Computation vol. 186/2, 2003

[4] L. Caires and L. Cardelli. A Spatial Logic for Concurrency (Part II), In Proc. of CONCUR'2002, LNCS vol.2421, 2002

[5] L. Caires and E. Lozes, Elimination of Quantifiers and Decidability in Spatial Logics for Concurrency, In Proc. of CONCUR'2004, LNCS vol.3170, 2004

[6] C. Calcagno, L. Cardelli and A. D. Gordon, Deciding validity in a spatial logic for trees, Journal of Functional Programming, Vol. 15, 2005

[7] C.Calcagno, et al. Computability and complexity results for a spatial assertion language for data structures, In Proc. of FSTTCS01, LNCS, vol. 2245, 2001

[8] L. Cardelli and A. D. Gordon. Anytime, Anywhere: Modal Logics for Mobile Ambients, In Proc. 27th ACM Symposium on Principles of Programming Languages, 2000

[9] W. Charatonik, J.M. Talbot, The decidability of model checking mobile ambients, In Proc. of the 15th International Workshop on Computer Science Logic, LNCS vol.2142, 2001

[10] M. Dam, Model checking mobile processes, Information and Computation vol.129(1), 1996

[11] V. Gyuris, Associativity does not imply undecidability without the axiom of Modal Distribution, In M. Marx, et.al eds., Arrow Logic and Multi-Modal Logic, CSLI and FOLLI, 1996

[12] D. Harel et al. Dynamic Logic, MIT Press, 2000

[13] M. Hennessy and R. Milner, Algebraic laws for Nondeterminism and Concurrency, Journal of JACM vol. 32(1), 1985

[14] R. Mardare, Observing distributed computation. A dynamic-Epistemic approach, In Proc. CALCO'07, LNCS vol.4624, 2007

[15] R. Mardare and C. Priami, Decidable extensions of Hennessy-Milner Logic, In Proc. FORTE'06, LNCS vol.4229, 2006

[16] R. Mardare, A. Polocriti, Towards a complete axiomatization for Spatial Logics, TechRep. CoSBi, TR-03-2008, reachable from www.cosbi.eu

[17] R. Milner, A Calculus of Communicating Systems, Springer-Verlag New York, Inc., 1982

[18] R. Milner, J. Parrow and D. Walker, Modal logics for mobile processes, TCS vol.114, 1993

[19] A. Prior, Past, Present and Future. Clarendon Press, Oxford, 1967

[20] D. Sangiorgi, Extensionality and Intensionality of the Ambient Logics, In Proc. of the 28th ACM Annual Symposium on Principles of Programming Languages, 2001

[21] C. Stirling, Modal and temporal properties of processes, Springer-Verlag New York, Inc., 2001

[22] A. Urquhart, Semantics for Relevant Logics, Journal of Symbolic Logic, 37(1), 1972

$M \models \phi|\psi$ iff $M \equiv M'|M''$ and $M' \models \phi$, $M'' \models \psi$

$M \models \phi \triangleright \psi$ iff $M' \models \phi$ implies $M|M' \models \psi$

If agent A "sees" N "taking" the action α, this is expressed by $\langle A : \alpha \rangle$.

$M \models \langle A : \alpha \rangle \phi$ iff $M \equiv N|M'$, $N \overset{\alpha}{\textbf{to}} N'$ and $N'|M'' \models \phi$

If agent A "sees" the submodel N, then its knowledge is described by K_A.

$M \models K_A\phi$ iff $M \equiv N|M'$ and for any M'', $N|M'' \models \phi$

Given a class $\mathfrak{M}$ of models for the logic $\mathcal{L}(At)$ defined for the set At of atomic propositions.

A *refinement* over $\mathfrak{M}$ is a relation $\mathcal{R} \subseteq \mathfrak{M} \times \mathfrak{M}$.

The refinement $\mathcal{R}$ can be used, e.g., to model certain (structural/bio-chemical) modifications (mutations) of a model (individual of a species) $M \in \mathfrak{M}$.

$\mathfrak{M}$ is *robust* for the properties $\Phi \subseteq \mathcal{L}(At)$ against the refinement $\mathcal{R}$ iff

for any $(M, M') \in \mathcal{R}$ and any $\phi \in \Phi$ we have

$M \models \phi$ iff $M' \models \phi$

$\mathfrak{M}$ is *globally robust* against $\mathcal{R}$ if it is robust for $\mathcal{L}(At)$.

Application:

Let $\mathfrak{M}$ be a class of individuals.

Let At be a set of properties that characterize some individuals in $\mathfrak{M}$.

The maximal consistent sets of formulas of $\mathcal{L}(At)$ induces an equivalence relation $\mathcal{R}_0$ over $\mathfrak{M}$. $\mathfrak{M}$ is globally robust against $\mathcal{R}_0$.

The quotients of $\mathcal{R}_0$ over $\mathfrak{M}$ are *species* of $\mathfrak{M}$.

The quotient satisfying At is the *main species*.

The other quotients are *mutants* of the main species.