
**Technical Report CoSBi 03/2006**

# Dynamic Epistemic Spatial Logic

Radu Mardare

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

mardare@cosbi.eu

Corrado Priami

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

priami@cosbi.eu

*This is the preliminary version of a paper that will appear in*
*In Proceedings of International Conference on Formal Methods for Networked and Distributed Systems (FORTE 2006), LNCS 4229, Springer, 2006.*

# Dynamic Epistemic Spatial Logic

Radu Mardare, Corrado Priami
The Microsoft Research-University of Trento, Italy

September 30, 2009

**Abstract**

We propose a new logic for expressing properties of concurrent and distributed systems, Dynamic Epistemic Spatial Logic, as an extension of Hennessy-Milner logic with spatial and epistemic operators. Aiming to provide a completely axiomatized and decidable logic for concurrency, we devise epistemic operators, indexed by processes, to replace the guarantee operator in the classical spatial logics. The knowledge of a process, considered as epistemic agent, is understood as the information, locally available to our process, about the overall-global system/process in which it is an agent/subprocess.
Dynamic Epistemic Spatial Logic supports a semantics based on a fragment of CCS against which the classical spatial logics have been proved to be undecidable. Underpinning on a new congruence relation on processes - the structural bisimulation - we prove the finite model property for our logic, thus concluding on its decidability against the same semantics.
A sound complete Hilbert-style axiomatic system is developed, comprehending the behavior of spatial operators in relation with dynamic/temporal and epistemic ones. Eventually we emphasize on the similarities with the classical axioms and rules of knowledge, that present our logic as an authentic dynamic-epistemic logic.

# 1 Introduction

The development of computer networks came with new paradigms of computation by proposing the *concurrent distributed computing systems*, which are not only sequential, goal-directed, deterministic or hierarchical systems, but represent programs/processors running in parallel and organized in networks of subsystems, each subsystem having its own identity. The subsystems interact, collaborate, communicate and interrupt each other.

Underlying this new paradigm is the assumption that each part of such a system has its own identity, which persists through time. We shall call these parts *agents*. Hence the agents are separate and independently observable units of behavior and computation. They evolve in a given environment, following some primitive rules, their evolution influencing the structure of the whole (multi-agent)

system. The main feature of the agents is their ability to communicate, that is to exchange information inside their environment.

Multi-agent systems are extremely complex. The success in dealing with this complexity depends on the mathematical model we choose to abstract the system. Further we focus on two major paradigms.

## *To be* is *to behave*

The first paradigm is proposed by Process Algebra [3], that abstracts the agents of the system, on the level of their behavior, and using some algebraic calculi and operational semantics [30] describes the evolution of the whole system. Inspired by $\lambda$-calculus and deeply related with the programming languages, this paradigm succeeds in modelling complex computational scenarios. Further, as the behavior of a concurrent system is, mainly, a succession of affine states in (possibly branching) time, was considered the possibility of applying modal (especially temporal) logics for specifying properties of the systems we modelled.

In studying security problems, for example, we may want to be able to specify systems composed by agents that deal with fresh or secret resources. We may want to express properties such as "*the agent has the key*", "*eventually the agent crosses the firewall*" or "*there is always at most one agent here able to decrypt the message*".

In systems biology [10] we need to handle big complex systems having extreme dimensions and variable environments. We need to express properties such as "*somewhere there is a virus*", "*if the virus will meet the macrophage cell then it will be engulfed and eventually destroyed*", or "*the presence of the protein $x$ will stimulate the reaction $X$*", etc.

Hennessy-Milner logic [24] is one of the first modal logics that proposes some modal operators, indexed by actions, to describe the behavior of the systems in CCS. The idea was further developed in combination with temporal operators [31] or applied to other calculi [29, 16, 18]. Latter, Mads Dam introduced a tensor that can express properties of modularity in the system [17], i.e. it can identify subsystems of a system. All these logics are characterized by their *extensional nature*, meaning that they cannot distinguish between processes that behave the same, even if these processes are different.

An increased degree of expressiveness is necessary if we want to specify and to reason about notions such as locations, resources, independence, distribution, connectivity and freshness. The specific applications of mobile computing call for properties that hold at particular locations, and it becomes natural to consider spatial modalities for expressing properties that hold at a certain location, at some locations or at every location. Thus, *Spatial logics* [7, 6, 12] propose, in addition to the modal temporal operators, some modal spatial operators such as the *parallel operator* $\phi|\psi$ (meaning that the current process can be split into a parallel composition $Q|R$ of a process $Q$ satisfying $\phi$ and a process $R$ satisfying $\psi$), and its adjoint - the *guarantee operator* $\phi \triangleright \psi$, or *location operator*[1] $n[\phi]$ (meaning that the current process is an ambient $n[P]$ and the process $P$ satisfies $\phi$), etc. A formula in a spatial logic describes a property of a particular part of the system at a particular time. These spatial

[1]This operator is characteristic for Ambient Logic [12], a special spatial logic developed for Ambient Calculus [11].

modalities have an *intensional flavor*, the properties they express being invariant only for simple spatial rearrangements of the system.

As the main reason for introducing spatial logics was to provide appropriate techniques for specification and model checking concurrent distributed systems, most of the work done in this field points to decidability problems. We briefly present hereafter the (un)decidability results for spatial logics, proved in [8], which motivated our work.

Consider the fragment of CCS generated by the next syntax, where $\mathbb{A}$ is a denumerable set of actions and $\alpha \in \mathbb{A}$:

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

Hereafter this calculus[2] is the object of our paper. We will use $\alpha, \beta$ to range over $\mathbb{A}$ and we will denote by $\mathfrak{P}$ the class of processes.
For it, in [8], were considered two spatial logics:

- $\mathcal{L}_{spat}$ given by the syntax

$$\phi ::= \top \mid 0 \mid \phi_1 \wedge \phi_2 \mid \neg\phi \mid \phi_1|\phi_2 \mid \phi_1 \triangleright \phi_2 \mid \diamond\phi$$

- $\mathcal{L}_{mod}$ given, over an infinite set of variables $X \ni x$, by the syntax

$$\phi ::= \top \mid 0 \mid \phi_1 \wedge \phi_2 \mid \neg\phi \mid \phi_1|\phi_2 \mid \phi_1 \triangleright \phi_2 \mid \diamond\phi \mid \langle x\rangle\phi \mid \exists x.\phi$$

A *valuation* is a mapping from a finite subset of $X$ to $\mathbb{A}$. For any valuation $v$, we write $v\{x \leftarrow \alpha\}$ for the valuation $v'$ such that $v'(x) = \alpha$, and $v'(y) = v(y)$ if $y \neq x$.
The semantics for the two spatial logics, defined by the *satisfaction relation* $P, v \models_M \phi$ where $P$ is a process, $M$ is a set of processes that contains $P$, $\phi$ a formula, and $v$ is a valuation for the free variables of $\phi$, is presented in Table 1.

In [8] it is proved that $\mathcal{L}_{spat}$ can encode $\mathcal{L}_{mod}$, hence they are equally expressive. Then it is proved that model-checking and validity/satisfiability checking for $\mathcal{L}_{spat}$ with respect to this finite fragment of CCS are all undecidable. But $\mathcal{L}_{spat}$ is the core of all Spatial Logics.

Thus it was proved that the basic spatial operators, in combination with temporal operators, generate undecidable logics [8, 14, 13], even against small finite pieces of CCS. This means that we cannot solve most of the problems concerning satisfiability, validity and model checking. The situation is caused, mainly, by the presence of the *guarantee operator*, which acts as a universal quantifier over the class of processes. The reason for introducing such an operator was to have possibility to specify not only local, but global properties of the system. Without it spatial logics are not enough expressive for fulfilling the requirements of relevant applications.

However, some decidable sublogics have been investigated [5, 9, 28, 27] and some model-checking algorithms exist for them. In the light of these results we have two alternatives for avoiding undecidability: either we choose a logic based on a static calculus [9], thus the logic cannot specify properties

[2]We can, additionally, consider an involution on $\mathbb{A}$ that associate to each action $\alpha \in \mathbb{A}$ an action $\overline{\alpha} \in \mathbb{A}$, as usual in CCS, and also to take into consideration the silent action $\tau$. But all these represent just syntactic sugar, irrelevant from the point of view of the logic we discuss.

$P, v \models_M \top$ for any process $P$
$P, v \models_M \neg\phi$ iff $P, v \not\models \phi$
$P, v \models_M \phi \wedge \psi$ iff $P, v \models_M \phi$ and $P, v \models_M \psi$
$P, v \models_M 0$ iff $P \equiv 0$
$P, v \models_M \phi|\psi$ iff $P \equiv Q|R$, $Q, v \models_M \phi$ and $R, v \models_M \psi$
$P, v \models_M \phi \triangleright \psi$ iff for any process $Q, v \models_M \phi$ we have $P|Q, v \models_M \psi$
$P, v \models_M \exists x.\phi$ iff $\exists \alpha \in \mathbb{A}$ such that $P, (v\{x \leftarrow \alpha\}) \models_M \phi$
$P, v \models_M \langle x \rangle \phi$ iff $\exists Q.P \overset{v(x)}{\textbf{to}} Q$ and $Q, v \models_M \phi$

Table 1: Semantics of Spatial Logics

of our system in evolution, or we choose a dynamic calculus, but we have to avoid the use of a guarantee operator [5, 28], hence we can express only local properties of the system. The latter alternative is useful only if our system is an isolated one (there is no upper-system for it) and we have a full description of it. In this sense the possible applications are quite limited. In problems such as those proposed by systems biology, for example, it is not acceptable, as biological systems are almost always subsystems of bigger ones with which they interact. Very often we do not know too much about these upper systems, or we cannot decide how far up we should go with modeling the systems in order to obtain the information we are looking for.

Concluding, though expressive and useful, most of the spatial logics proved to be undecidable, even in the absence of quantifiers. Unlike in static spatial logics, the composition adjunct adds to the expressiveness of the logic, so that adjunct elimination is not possible for dynamic spatial logics, even quantifier-free [8]. To the best of our knowledge, no alternative operator, to replace the guarantee one in order to express global properties and still ensuring decidability, has been studied. We propose further such an alternative.

## To be is to know

The other paradigm of modelling multi-agent systems comes from logics and philosophy: reasoning about systems in terms of knowledge [19]. At the beginning, the interest was to find inherent properties of knowledge and related concepts. More recently, the computer scientists have become increasingly interested in reasoning about knowledge. Within computer science, reasoning about knowledge plays an extremely important role in contemporary theories of (intelligent) agents and it has been proved to be useful in modelling and understanding complex communication-based systems.

In the transition from human agents to (artificial) intelligent agents and latter to the multi-agent system in the most general sense, the meaning of the term *"knowledge"* evolved. It was originally used in its ordinary language meaning: to say that an agent knows a sentence either means that it consciously assents to it, or that it immediately sees it to be true when the question is presented. Latter, in the new interpretation, *the knowledge of the agent* is understood as the sum of actions the

agent may take as a function of its local state in a given environment. Thus the agent knows its *protocol* in a given system. In this context we have an *external* notion of knowledge in the sense that there is no notion of the agent computing his knowledge and no requirement that the agent being able to answer questions based on his knowledge.

*Epistemic/doxastic logics* [19] formalize, in a direct manner, notions of knowledge, or belief, possessed by an agent, or a group of agents, using modalities like $K_A\phi$ - *$A$ knows $\phi$*, $\Box_A\phi$ - *$A$ justifiably believes that $\phi$*, or $Ck\phi$ - *all the agents knows $\phi$ ($\phi$ is a common knowledge)*. These logics supports Kripke-model based semantics, each basic modality being associated with a binary *accessibility relation* in these models. Thus for each epistemic agent $A$ we devise an accessibility relation $\overset{A}{\mathbf{to}}$, called *indistinguishability relation for $A$*, expressing the agent's uncertainty about the current state. The states $s'$ such that $s\overset{A}{\mathbf{to}}s'$ are the epistemic alternatives of $s$ to agent $A$: if the current state is $s$, $A$ thinks that any of the alternatives $s'$ may be the current state. These logics have been extensively studied and applied to multi-agent systems.

Suppose that we have a group consisting of $n$ agents. Then we augment the language of propositional logic by $n$ knowledge operators $K_1, ...K_n$ (one for each agent), and form formulas in the obvious way. A statement like $K_1\phi$ is read *"agent 1 knows $\phi$"*. The state that agent 1 knows that agent 2 knows $\phi$ is formalized by $K_1K_2\phi$. A formula like $K_1\phi \wedge K_1(\phi \rightarrow \psi) \rightarrow K_1\psi$ is interpreted: *"if agent 1 knows $\alpha$ and $\alpha \rightarrow \beta$ then it knows $\beta$"*.

[The language of epistemic logic] Let $\Phi$ be a nonempty, countable set of atomic formulae and $\mathfrak{S} = \{1, ...n\}$ a set of agents. We introduce the language of epistemic logic as the least set $\mathcal{F}^{\mathfrak{S}}$ of formulas such that:

1. $Atom \subseteq \mathcal{F}^{\mathfrak{S}}$
2. if $\phi, \psi \in \mathcal{F}^{\mathfrak{S}}$ then $\phi \wedge \psi \in \mathcal{F}^{\mathfrak{S}}$
3. if $\phi \in \mathcal{F}^{\mathfrak{S}}$ then $\neg\phi \in \mathcal{F}^{\mathfrak{S}}$
4. if $\alpha \in \mathcal{F}^{\mathfrak{S}}$ and $i \in \mathfrak{S}$ then $K_i\phi \in \mathcal{F}^{\mathfrak{S}}$

One approach to defining semantics for epistemic logic is in terms of possible worlds. The intuitive idea behind the possible worlds approach is that an agent can build different models of the world using some suitable language. He usually does not know exactly which one of the models is the right model of the world. However, he does not consider all these models equally possible. Some world models are incompatible with his current information state, so he can exclude these incompatible models from the set of his possible world models. Only a subset of the set of all (logically) possible models are considered possible by the agent.

The set of worlds considered possible by an agent $i$ depends on the "actual world", or the agent's actual state of information. This dependency can be captured formally by introducing a binary relation, say $\mathcal{R}_i$, on the set of possible worlds. To express the idea that for agent $i$, the world $t$ is compatible with his information state when he is in the world $s$, we require that the relation $\mathcal{R}_i$ holds between $s$ and $t$. One says that $t$ is an epistemic alternative to $s$ (for agent $i$). If a sentence $\phi$ is true in all worlds which agent $i$ considers possible then we say that this agent knows $\phi$.

Formally, the concept of models is defined in terms of Kripke structures, as follows:

[Semantics of Epistemic Logic] A model $\mathcal{M}$ for the language $\mathcal{F}^{\mathfrak{S}}$ is a Kripke structure for the agents in $\mathfrak{S}$ over $\Phi$, i.e. is a structure $\mathcal{M} = (S, \pi, (\mathcal{R}_i)_{i\in\mathfrak{S}})$ where

- $S$ is a nonempty set of possible worlds (states)
- $\pi$ is an *interpretation* which associates with each state in $S$ a truth assignment to the primitive propositions in $\Phi$ (i.e. for $s \in S$, $\pi(s) : \Phi \to \{\top, \bot\}$)
- $\mathcal{R}_i$ is a binary relation on $S$ associated to the agent $i \in \mathfrak{S}$

The satisfaction relation $\models$ is defined recursively on $\mathcal{F}^{\mathfrak{S}}$ as follows:

- $\mathcal{M}, s \models p$ iff $\pi(s)(p) = \top$ for any $p \in \Phi$
- $\mathcal{M}, s \models \neg\phi$ iff $\mathcal{M}, s \not\models \phi$
- $\mathcal{M}, s \models \phi \wedge \psi$ iff $\mathcal{M}, s \models \phi$ and $\mathcal{M}, s \models \psi$
- $\mathcal{M}, s \models K_i\phi$ iff for all $t \in S$ such that $s\mathcal{R}_i t$ we have $\mathcal{M}, t \models \phi$

A modal epistemic logic for the agents in $\mathfrak{S}$ is obtained by joining together $n$ modal logics [4], one for each agent in $\mathfrak{S}$. It is usually assumed that the agents are homogeneous, i.e., they can be described by the same logic. So an epistemic logic for $n$ agents consists of $n$ copies of a certain modal logic. Such a system over $\mathfrak{S}$ will be denoted by the same name as the modal system, but with the superscript $\mathfrak{S}$.

[Modal epistemic logic $K^{\mathfrak{S}}$] The modal epistemic logic $K^{\mathfrak{S}}$ is the logic specified by the following axioms and rules of inference, where $i \in \mathfrak{S}$:

**(PC):** All propositional tautologies.
**(K):** $\vdash K_i\phi \wedge K_i(\phi \to \psi) \to K_i\psi$
**(MP):** Modus ponens: if $\vdash \phi$ and $\vdash \phi \to \psi$ then $\vdash \psi$
**(NEC):** Necessity: if $\vdash \phi$ then $\vdash K_i\phi$

Stronger logics can be obtained by adding additional principles, which express the desirable properties of the concept of knowledge, to the basic system $K^{\mathfrak{S}}$. The following properties are often considered:

**(T):** Knowledge axiom: $\vdash K_i\phi \to \phi$
**(D):** Consistency axiom: $\vdash K_i\phi \to \neg K_i\neg\phi$
**(4):** Positive introspection: $\vdash K_i\phi \to K_iK_i\phi$
**(5):** Negative introspection: $\vdash \neg K_i\phi \to K_i\neg K_i\phi$

The formula (T) states that knowledge must be true. In the doxastic logic this axiom is taken to be the major one distinguishing knowledge from belief. For that reason (T) is called the Knowledge Axiom or the Truth Axiom (for knowledge). Systems containing the schema (T) (such as **S4** and **S5**) are then called logics of knowledge, and logics without the schema (T) are called logics of belief.

The property (D), called the Consistency Axiom, requires that agents be consistent in their knowledge: they do not know both a formula and its negation. Generally, (D) is a weaker condition than (T).

The properties (4) and (5) are called positive and negative introspection axioms, respectively. They say that an agent is aware of what he knows and what he does not know. Their converses, i.e.,

the formulae $\vdash K_iK_i\phi \rightarrow K_i\phi$ and $\vdash K_i\neg K_i\phi \rightarrow \neg K_i\phi$, are instances of the schema (T). Taking (4) and (5) together with their converses we have $\vdash K_iK_i\phi \leftrightarrow K_i\phi$ and $\vdash K_i\neg K_i\phi \leftrightarrow \neg K_i\phi$, which allow to reduce multiple knowledge operators to a single (positive or negative) knowledge operator. The commonly used epistemic logics are specified as follows:

- $T^{\mathfrak{S}}$ is $K^{\mathfrak{S}}$ plus (T)
- $S4^{\mathfrak{S}}$ is $T^{\mathfrak{S}}$ plus (4)
- $S5^{\mathfrak{S}}$ is $S4^{\mathfrak{S}}$ plus (5)
- $KD^{\mathfrak{S}}$ is $K^{\mathfrak{S}}$ plus (D)
- $KD4^{\mathfrak{S}}$ is $KD^{\mathfrak{S}}$ plus (4)
- $KD45^{\mathfrak{S}}$ is $KD4^{\mathfrak{S}}$ plus (5)

The following theorem summarizes some completeness and decidability results for modal epistemic logic [15, 25, 21, 22].

[Completeness and decidability of epistemic logics]

1. $K^{\mathfrak{S}}$ describes the class of models with accessibility relations indexed by elements in $\mathfrak{S}$.
2. $T^{\mathfrak{S}}$ describes the class of models with reflexive accessibility relations.
3. $S4^{\mathfrak{S}}$ describes the class of models with reflexive and transitive accessibility relations.
4. $S5^{\mathfrak{S}}$ describes the class of models with equivalence relations as accessibility relations.
5. $KD^{\mathfrak{S}}$ describes the class of models with serial accessibility relations.
6. $KD4^{\mathfrak{S}}$ describes the class of models with serial and transitive accessibility relations.
7. $KD45^{\mathfrak{S}}$ describes the class of models with serial, transitive and Euclidean accessibility relations.
8. $K^{\mathfrak{S}}$, $T^{\mathfrak{S}}$, $S4^{\mathfrak{S}}$, $S5^{\mathfrak{S}}$, $KD^{\mathfrak{S}}$, $KD4^{\mathfrak{S}}$, and $KD45^{\mathfrak{S}}$ are all decidable.

*Dynamic logics* [23] are closer to process calculi, in that they have names for programs (*actions*) and operators to combine them. Accessibility relations are interpreted as transitions induced by programs, and a dynamic modality $[\pi]\phi$ captures the weakest precondition of such a program w.r.t. a given post-specification $\phi$. Modalities in a dynamic logic form an algebraical structure: programs are built using basic program constructors such as *sequential composition* $\pi.\pi'$ or *iteration* $\pi^*$.

By mixing dynamic and epistemic formalisms Dynamic Epistemic Logics have been developed [1, 2, 26, 32, 33, 34], aiming to capture properties of evolving knowledge and of belief-changing actions, such as communication. These logics combine a rich expressivity with low complexity ensuring decidability and complete axiomatizations.

## Our approach

The two paradigms of modelling concurrent distributed systems - the process algebraical paradigm with the epistemic-doxastic one - were developed in parallel, but to our knowledge, there has been no unified paradigm. We propose such a paradigm in this paper, used for constructing a new logic for concurrency completely axiomatized and decidable. The main idea is to combine the features of spatial logics with the epistemic logics thus obtaining a special type of dynamic epistemic logic equipped with spatial operators. We call it Dynamic Epistemic Spatial Logic.

More concretely, our logic extends Hennessy-Milner logic with the parallel operator (hence it is a spatial logic) and epistemic operators. The role of the epistemic operators is to do most of the job of the guarantee operator while maintaining decidability. In our logics the epistemic agents are related (identified) with processes. Thus $K_P\phi$ holds, *the agent related with* $P$ *knows* $\phi$, iff $\phi$ is satisfied by any process having $P$ as subprocess. The intuition is that the agent related with $P$ is an observer inside our system that can see only $P$. So, this epistemic agent cannot differentiate between the global states $P$, $P|Q$ or $P|R$ of the whole system, as in all these states it sees only $P$. Thus its knowledge rests on properties $\phi$ that are satisfied by each of these states (processes). For avoiding unnecessary syntactic sugar we name the epistemic agents by the processes they are related with.

We prove, for Dynamic Epistemic Spatial Logic, the finite model property with respect to the chosen semantics. Thus, we have decidability for satisfiability, validity and model-checking problems.

In proving the finite model property we used a new congruence on processes - *the structural bisimulation*. A conceptually similar congruence has been proposed in [9], but for static processes only. The structural bisimulation is interesting in itself, as it provides a bisimulation-like description of the structural congruence. Informally, it is an approximation of the structural congruence bound by two dimensions: the *height* and the *weight* of a process. The bigger these sizes, the better approximation we obtain. At the limit we find exactly the structural congruence.

For the logic we propose a complete Hilbert-style axiomatic system, which helps in understanding the basic algebraical behavior of the classical process operators. We prove its soundness and completeness with respect to the piece of CCS for which the classic spatial logic has been proved to be undecidable in [8]. Thus, many properties can be syntactically verified and proved. Moreover the interplay of our logical operators allows expression, inside the syntax, of validity and satisfiability for formulas. We also have characteristic formulas able to identify a process (agent) up to structural congruence (cloned copies).

Concluding, the novelty of our logic with respect to the classical spatial logics is the use of the epistemic operators, as alternative to guarantee operator, for expressing global properties while ensuring decidability. The epistemic operators allow to refer directly to agents of our system by mean of their knowledge. An epistemic agent is, thus, an observer that can be placed in different places in our system and has access to partial information. By combining these partial information ("points of view" of different observers) we can specify complex properties of distributed systems.

From the epistemic logics perspective, we propose a new class of epistemic logics by imposing an algebraical structure (CCS-like) on the class of epistemic agents. In this way we may assume compositional and hierarchically organized agents. Thus $P$ and $Q$ are epistemic agents, but also $P|Q$

may be another agent. As they are ontologically related ($P$ and $Q$ are ontological subsidiary of $P|Q$), our logic allows to derive relations between their knowledge and dynamics from their ontological relations. In the classical epistemic logics [19] the agents are assumed to be ontologically independent entities, while our logics accepts dependencies. Other peculiarities of our epistemic logic comes from the fact that we can activate and deactivate agents: thus in a system having the current state described by $\alpha.P$, the agent that sees $P$ is not active, but it might be activated in a future state. Our logic allows also cloned agents. Thus in a system described by $P|Q|P$ we have two clones of the agent seeing $P$. All these features are new for epistemic logics. Thus, we can model simultaneously, as agents in a system, individuals, societies of individuals, societies of societies of individuals, etc and their evolutions.

# 2 On processes

In this chapter we return to CCS and we reconsider the subcalculus for which, in [8] the classical spatial logic was proved undecidable. We will use it further as semantics for our logic. We propose some new concepts that will help the future constructs. One of the most important is a new congruence on processes - *the structural bisimulation*. This relation will be used, further, to prove the finite model property for our logics against the process semantics in combination with the concept of *pruning processes*.

The structural bisimulation is interesting in itself as it provides a bisimulation-like definition for structural congruence. Informally, it is an approximation of the structural congruence bounded by two sizes: the *height* (the depth of the syntactic tree) and the *weight* (the maximum number of bisimilar subprocesses that can be found in a node of the syntactic tree) of a process. The bigger these sizes, the better approximation we obtain. At the limit, for sizes big enough with respect to the sizes of the processes involved, we find exactly the structural congruence. A conceptually similar congruence was proposed in [9] for analyzing trees of location for the static ambient calculus.

On the two sizes defined for processes, *height* and *weight*, we will introduce an effective method to construct, given process $P$, a minimal process $Q$ that has an established size $(h, w)$ and is structurally bisimilar to $P$ on this size. Because, for a small size, the construction is supposed to prune the syntactic tree of $P$, we will call this method *pruning*, and we refer to $Q$ as *the pruned of $P$ on the size* $(h, w)$.

Eventually we will extend the notions of *size*, *structural bisimulation* and *pruning* from processes to classes of processes. We focus our interest on *contexts*, defined as being special classes of processes that contain, in a maximal manner, processes of interest for us (that might model completely or partially our system together with all its subsystems). The contexts will be used, in the next chapters, as the sets of processes on which we will define the satisfiability relation for the logics.

We recall the definition 1 as defining the subcalculus of CCS on which we will focus for the rest of the paper. We will not consider additional features of CCS, such as pairs of names, etc., as we want to avoid all the syntactic sugar that is irrelevant from the point of view of the logic. We might define

an involution on $\mathbb{A}$ and the silent action $\tau$, but all these can be introduced, in our logic, as derived operators.

We call a process $P$ *guarded* iff $P \equiv \alpha.Q$ for $\alpha \in \mathbb{A}$.

We introduce the notation $P^k \stackrel{def}{=} \underbrace{P|...|P}_{k}$, and convey to denote $P^0 \equiv 0$.

[Representativeness modulo structural congruence] By definition, $\equiv$ is a congruence (thence an equivalence relation) over $\mathfrak{P}$. Consequently, we convey to identify processes up to structural congruence, because the structural congruence is the ultimate level of expressivity we want for our logic. Hereafter in the paper, if it is not explicitly otherwise stated, we will speak about processes up to structural congruence.

## 2.1 Size of a process

Further we propose a definition for the *size of a process*, following a similar idea developed in [9] for sizes of trees. The intuition is that the process has a *height* given by the vertical size of its syntactic tree, and a *width* equal to the maximum number of bisimilar subprocesses that can be identified in a node of the syntactic tree.

[Size of a process] We define *the size (height and width) of a process* $P$, denoted by $P$, by:

- $0 \stackrel{def}{=} (0, 0)$
- $P \stackrel{def}{=} (h, w)$ iff
  - $P \equiv (\alpha_1.Q_1)^{k_1}|(\alpha_2.Q_2)^{k_2}|...|(\alpha_j.Q_j)^{k_j}$ and $Q_i = (h_i, w_i)$, $i \in 1..j$
  - $h = 1 + max(h_1, ..., h_k)$, $w = max(k_1, ..., k_j, w_1, ..., w_j)$

where we used $h$ for *height* and $w$ for *width*. We convey to write $(h_1, w_1) \leq (h_2, w_2)$ for $h_1 \leq h_2$ and $w_1 \leq w_2$ and $(h_1, w_1) < (h_2, w_2)$ for $h_1 < h_2$ and $w_1 < w_2$.

Observe that, by construction, the size of a process is unique up to structural congruence. Moreover, if $P = (h, w)$ then for any subprocess $P'$ of $P$ we have $P' \leq (h, w)$.

**Example 2.1** *We show further the size for some processes:*

$$0 = (0,0) \qquad \alpha.0 = (1,1) \qquad \alpha.0|\beta.0 = (1,1)$$
$$\alpha.0|\alpha.0 = (1,2) \qquad \alpha.\alpha.0 = \alpha.\beta.0 = (2,1) \qquad \alpha.(\beta.0|\beta.0) = (2,2)$$

[Size of a set of processes] Let $M \subset \mathfrak{P}$. We write $M = (h, w)$ iff $(h, w) = max\{P \mid P \in M\}$. As the sets of processes may be infinite, not for all of them this definition works, in the sense that some sets may have infinite sizes[3]. For this reason we convey to extend the order, and when $M$ has infinite size, to still write $(h, w) \leq M$ and $(h, w) < M$ for any $(h, w)$.

[3]Such a situation is in the case of the set $\mathcal{M} = \{0, \alpha.0, \alpha.\alpha.0, ..., \alpha....\alpha.0, ...\}$.

## 2.2 Structural bisimulation

In this section we introduce the *structural bisimulation*, a congruence relation on processes bounded by size. It analyzes the behavior of a process focusing on a boundary of its syntactic tree. This relation will be used in the next chapter to prove the finite model property for our logics.

The intuition behind the structural bisimulation is that $P \approx_h^w Q$ ($P$ and $Q$ are structurally bisimilar on size $(h, w)$) iff when we consider for both processes their syntactic trees up to the depth $h$ only (we prune them on the height $h$) and we ignore the presence of more than $w$ parallel bisimilar subprocesses in any node of the syntactic trees (we prune the trees on weight $w$), we obtain syntactic trees depicting two structurally congruent processes.

The relation between the structural bisimulation and the structural congruence is interesting. We will see that the structural bisimulation depicts, step by step, the structural congruence being, in a sense, a bisimulation-like approximation of it on a given size. We will see further how $P \approx_h^w Q$ entails that, if we choose any subprocess of $P$ with the size smaller than $(h, w)$, then there exists a subprocess of $Q$ structurally congruent with it, and vice versa. Now, if the size indexing the structural bisimulation is bigger than the size of the processes, then our relation will describe structurally congruent processes. Moreover, the structural bisimulation is preserved by transitions with the price of decreasing the size.

[Structural bisimulation] Let $P, Q$ be any processes. We define $P \approx_h^w Q$ by:

- $P \approx_0^w Q$ always
- $P \approx_{h+1}^w Q$ iff for any $i \in 1..w$ and any $\alpha \in \mathbb{A}$ we have
  - if $P \equiv \alpha.P_1|...|\alpha.P_i|P'$ then $Q \equiv \alpha.Q_1|...|\alpha.Q_i|Q'$ with $P_j \approx_h^w Q_j$, for $j = 1..i$
  - if $Q \equiv \alpha.Q_1|...|\alpha.Q_i|Q'$ then $P \equiv \alpha.P_1|...|\alpha.P_i|P'$ with $Q_j \approx_h^w P_j$, for $j = 1..i$

**Example 2.2** *Consider the processes*

$$R \equiv \alpha.(\beta.0|\beta.0|\beta.0)|\alpha.\beta.0 \text{ and } S \equiv \alpha.(\beta.0|\beta.0)|\alpha.\beta.\alpha.0$$

*We can verify the requirements of the definition 2.2 and decide that $R \approx_2^2 S$. But $R \not\approx_3^2 S$ because on the depth 2 $R$ has an action $\alpha$ (in figure 1 marked with a dashed arrow) while $S$ does not have it (because the height of $S$ is only 2). Also $R \not\approx_2^3 S$ because $R$ contains only 2 (bisimilar) copies of $\beta.0$ while $S$ contains 3 (the extra one is marked with a dashed arrow). Hence, for any weight bigger than 2 this feature will show the two processes as different. But if we remain on depth 1 we have $R \approx_1^3 S$, as on this deep the two processes have the same number of bisimilar subprocesses, i.e. any of them can perform $\alpha$ in two ways giving, further, processes in the relation $\approx_0^3$. Indeed*

$$R \equiv \alpha R'|\alpha R'', \text{ where } R' \equiv \beta.0|\beta.0|\beta.0 \text{ and } R'' \equiv \beta.0$$
$$S \equiv \alpha.S'|\alpha.S'', \text{ where } S' \equiv \beta.0|\beta.0 \text{ and } S'' \equiv \beta.\alpha.0$$

*By definition, $R' \approx_0^3 S'$ and $R'' \approx_0^3 S''$*

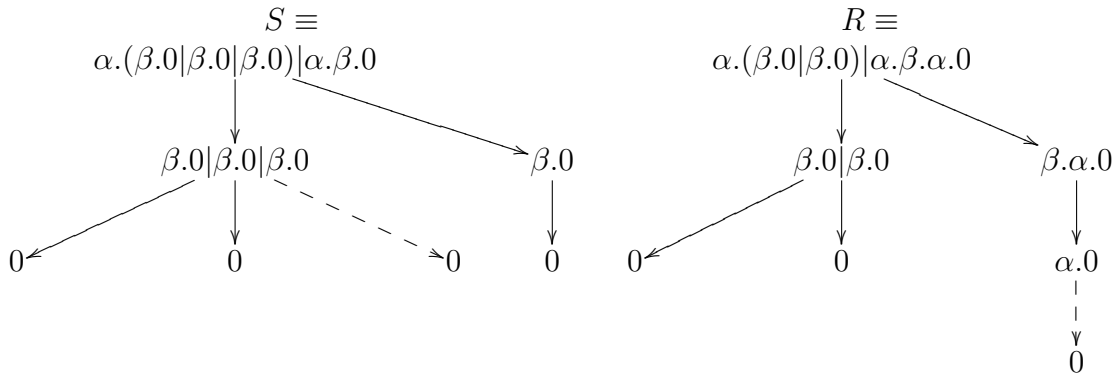


Figure 1: Syntactic trees

We focus further on the properties of the relation $\approx_h^w$. We start by proving that structural bisimulation is a congruence relation.

[Equivalence Relation] The relation $\approx_h^w$ on processes is an equivalence relation.

**Proof** We verify the reflexivity, symmetry and transitivity directly.

**Reflexivity:** $P \approx_h^w P$ - we prove it by induction on $h$

**the case** $h = 0$: we have $P \approx_0^w P$ from the definition 2.2.

**the case** $h + 1$: suppose that $P \equiv \alpha.P_1|...|\alpha.P_i|P'$ for $i \in 1..w$ and some $\alpha \in \mathbb{A}$. The inductive hypotheses gives $P_j \approx_h^w P_j$ for each $j = 1..i$. Further we obtain, by the definition 2.2, that $P \approx_h^w P$.

**Symmetry:** if $P \approx_h^w Q$ then $Q \approx_h^w P$

Suppose that $P \equiv \alpha.P_1|...|\alpha.P_i|P'$ for some $i \in 1..w$ and $\alpha \in \mathbb{A}$ then, by the definition 2.2, exists $Q \equiv \alpha.Q_1|...|\alpha.Q_i|Q'$ with $P_j \approx_{h-1}^w Q_j$ for $j = 1..i$ and vice versa. Similarly, if we start from $Q \equiv \beta.R_1|...|\beta.R_k|R'$ for $k \in 1..w$ and $\beta \in \mathbb{A}$ we obtain $P \equiv \beta.S_1|...|\beta.S_k|S'$ for some $S_j$, with $R_j \approx_{h-1}^w S_j$ for $j = 1..k$ and vice versa. Hence $Q \approx_h^w P$.

**Transitivity:** if $P \approx_h^w Q$ and $Q \approx_h^w R$ then $P \approx_h^w R$ - we prove it by induction on $h$.

**the case** $h = 0$ is trivial, because by the definition 2.2, for any two processes $P, R$ we have $P \approx_0^w R$

**the case** $h + 1$: suppose that $P \equiv \alpha.P_1|...|\alpha.P_i|P'$ for some $i \in 1..w$ and $\alpha \in \mathbb{A}$. Then from $P \approx_h^w Q$ we obtain, by the definition 2.2, that $Q \equiv \alpha.Q_1|...|\alpha.Q_i|Q'$ with $P_j \approx_{h-1}^w Q_j$ for $j = 1..i$ and vice versa. Further, because $Q \approx_h^w R$, we obtain that $R \equiv \alpha.R_1|...|\alpha.R_i|R'$ with $Q_j \approx_{h-1}^w R_j$ for $j = 1..i$ and vice versa.

As $P_j \approx_{h-1}^w Q_j$ and $Q_j \approx_{h-1}^w R_j$ for $j = 1..i$, we obtain, using the inductive hypothesis that $P_j \approx_{h-1}^w R_j$ for $j = 1..i$.

Hence, for $P \equiv \alpha.P_1|...|\alpha.P_i|P'$, some $i \in 1..w$ and $\alpha \in \mathbb{A}$ we have that $R \equiv \alpha.R_1|...|\alpha.R_i|R'$ with $Q_j \approx_{h-1}^w R_j$ for $j = 1..i$ and vice versa. This entails $P \approx_h^w R$. □

If $P \approx_h^w Q$ and $Q \equiv R$ then $P \approx_h^w R$.

**Proof** Suppose that $P \equiv \alpha.P_1|...|\alpha.P_i|P'$ for some $i \in 1..w$ and $\alpha \in \mathbb{A}$. As $P \approx_h^w Q$, we obtain $Q \equiv \alpha.Q_1|...|\alpha.Q_i|Q'$ with $P_j \approx_{h-1}^w Q_j$ for $j = 1..i$ and vice versa. But $Q \equiv R$, so $R \equiv \alpha.Q_1|...|\alpha.Q_i|Q'$ with $P_j \approx_{h-1}^w Q_j$ for $j = 1..i$ and vice versa. Hence $P \approx_h^w R$. □

[Antimonotonicity] If $P \approx_h^w Q$ and $(h', w') \leq (h, w)$ then $P \approx_{h'}^{w'} Q$.

**Proof** We prove it by induction on $h$.

**The case** $h = 0$ is trivial, as $(h', w') \leq (0, w)$ gives $h' = 0$ and for any processes $P, Q$ we have $P \approx_0^w Q$.

**The case** $h + 1$ in the context of the inductive hypothesis:
Suppose that $P \approx_{h+1}^w Q$ and $(h', w') \leq (h + 1, w)$.
If $h' = 0$ we are, again, in a trivial case as for any two processes $P, Q$ we have $P \approx_0^w Q$.
If $h' = h'' + 1$ then consider any $i \in 1..w'$, and any $\alpha \in \mathbb{A}$ such that $P \equiv \alpha.P_1|...|\alpha.P_i|P'$. Because $i \leq w' \leq w$, and as $P \approx_{h+1}^w Q$, we have $Q \equiv \alpha.Q_1|...|\alpha_i.Q_i|Q'$ with $P_j \approx_h^w Q_j$, for $j = 1..i$. A similar argument can de developed if we start the analysis from $Q$.
But $(h'', w') \leq (h, w)$, so we can use the inductive hypothesis that gives $P_j \approx_{h'',w'} Q_j$ for $j = 1..i$.
Hence $P \approx_{h''+1}^{w'} Q$, that is, $P \approx_{h'}^{w'} Q$ q.e.d. □

[Congruence] The following holds:

1. if $P \approx_h^w Q$ then $\alpha.P \approx_{h+1}^w \alpha.Q$
2. if $P \approx_h^w P'$ and $Q \approx_h^w Q'$ then $P|Q \approx_h^w P'|Q'$

**Proof** 1.: Suppose that $P \approx_h^w Q$. Because $\alpha.P$ is guarded, it cannot be represented as $P \equiv \alpha.P'|P''$ for $P'' \not\equiv 0$. The same about $\alpha.Q$. But this observation, together with $P \approx_h^w Q$ gives, in the light of definition 2.2, $\alpha.P \approx_{h+1}^w \alpha.Q$.

2.: We prove it by induction on $h$.
**If** $h = 0$ then the conclusion is immediate.
**For** $h+1$, suppose that $P \approx_{h+1}^w P'$ and $Q \approx_{h+1}^w Q'$; then consider any $i = 1..w$, $\alpha$ and $R_j$ for $j = 1..i$ such that

$$P|Q \equiv \alpha.R_1|...|\alpha.R_i|R_{i+1}$$

Suppose, without loss of generality, that $R_j$ are ordered in such a way that there exist $k \in 1..i$, $P'', Q''$ such that

$$\begin{gathered} P \equiv \alpha.R_1|...|\alpha.R_k|P'' \\ Q \equiv \alpha.R_{k+1}|...|\alpha.R_i|Q'' \\ R_{i+1} \equiv P''|Q'' \end{gathered}$$

Because $k \in 1..w$, from $P \approx_{h+1}^w P'$ we have $P' \equiv \alpha.P'_1|...|\alpha.P'_k|P_0$ such that $R_j \approx_h^w P'_j$ for $j = 1..k$.
Similarly, from $Q \approx_{h+1}^w Q'$ we have $Q' \equiv \alpha.Q'_{k+1}|...|\alpha.Q'_i|Q_0$ such that $Rj \approx_h^w Q'_j$ for $j = (k+1)..i$.
Hence, we have

$$P'|Q' \equiv \alpha.P'_1|...|\alpha.P'_k|\alpha.Q'_{k+1}|...|\alpha.Q'_i|P_0|Q_0$$

As $R_j \approx_h^w P'_j$ for $j = 1..k$ and $R_j \approx_h^w Q'_j$ for $j = (k+1)..i$, and because a similar argument starting from $P'|Q'$ is possible, we proved that $P|Q \approx_{h+1}^w P'|Q'$. □

[Inversion] If $P'|P'' \approx_h^{w_1+w_2} Q$ then exists $Q', Q''$ such that $Q \equiv Q'|Q''$ and $P' \approx_h^{w_1} Q'$, $P'' \approx_h^{w_2} Q''$.

**Proof** Let $w = w_1 + w_2$. We prove the theorem by induction on $h$:

**The case** $h = 0$**:** is trivial.

**The case** $h + 1$**:** Suppose that $P'|P'' \approx_{h+1}^w Q$.

Consider the following definition: a process $P$ is in $(h, w)$-*normal form* if whenever $P \equiv \alpha_1.P_1|\alpha_2.P_2|P_3$ and $P_1 \approx_h^w P_2$ then $P_1 \equiv P_2$. Note that $P \approx_{h+1}^w \alpha_1.P_1|\alpha_2.P_1|P_3$. This shows that for any $P$ and any $(h, w)$ we can find a $P_0$ such that $P_0$ is in $(h, w)$-normal form and $P \approx_{h+1}^w P_0$.

Now, we can suppose, without loosing generality, that[4]:

$$P' \equiv (\alpha_1.P_1)^{k'_1}|...|(\alpha_n.P_n)^{k'_n}$$
$$P'' \equiv (\alpha_1.P_1)^{k''_1}|...|(\alpha_n.P_n)^{k''_n}$$
$$Q \equiv (\alpha_1.P_1)^{l_1}|...|(\alpha_n.P_n)^{l_n}$$

For each $i \in 1..n$ we split $l_i = l'_i + l''_i$ in order to obtain a splitting of $Q$. We define the splitting of $l_i$ such that $(\alpha_i.P_i)^{k'_i} \approx_{h+1,w_1} (\alpha_i.P_i)^{l'_i}$ and $(\alpha_i.P_i)^{k''_i} \approx_{h+1,w_2} (\alpha_i.P_i)^{l''_i}$. We do this as follows:

- if $k'_i + k''_i < w_1 + w_2$ then $P'|P'' \approx_{h+1}^w Q$ implies $l_i = k'_i + k''_i$, so we can choose $l'_i = k'_i$ and $l''_i = k''_i$.
- if $k'_i + k''_i \geq w_1 + w_2$ then $P'|P'' \approx_{h+1}^w Q$ implies $l_i \geq w_1 + w_2$. We meet the following subcases:
  - $k'_i \geq w_1$ and $k''_i \geq w_2$. We choose $l'_i = w_1$ and $l''_i = l_i - w_1$ (note that as $l_i \geq w_1 + w_2$, we have $l''_i \geq w_2$).
  - $k'_i < w_1$, then we must have $k''_i \geq w_2$. We choose $l'_i = k'_i$ and $l''_i = l_i - k'_i$. So $l''_i \geq w_2$ as $l_i \geq w_1 + w_2$ and $l'_i < w_1$.
  - $k''_i < w_2$ is similar with the previous one. We choose $l''_i = k''_i$ and $l'_i = l_i - k''_i$.

Now for $Q' \equiv (\alpha_1.P_1)^{l'_1}|...|(\alpha_n.P_n)^{l'_n}$ and $Q'' \equiv (\alpha_1.P_1)^{l''_1}|...|(\alpha_n.P_n)^{l''_n}$ the theorem is verified by repeatedly using theorem 2.2. □

The next theorems point out the relation between the structural bisimulation and the structural congruence. We will prove that for a well-chosen boundary, which depends on the processes involved, the structural bisimulation guarantees the structural congruence. $P \approx_h^w Q$ entails that if we choose any subprocess of $P$ having the size smaller than $(h, w)$, we will find a subprocess of $Q$ structurally congruent with it, and vice versa. Now, if the size indexing the structural bisimulation is bigger than

[4]Else we can replace $P', P''$ with $(h+1, w)$-related processes having the same $(h, w)$-normal forms

the size of the processes, then our relation will describe structurally congruent processes. We also prove that the structural bisimulation is preserved by transitions with the price of decreasing the size.

If $P \leq (h, w)$ and $P' \leq (h, w)$ then $P \approx_h^w P'$ iff $P \equiv P'$.

**Proof** $P \equiv P'$ implies $P \approx_h^w P'$, because by reflexivity $P \approx_h^w P$ and then we can apply theorem 2.2.

We prove further that $P \approx_h^w P'$ implies $P \equiv P'$. We'll do it by induction on $h$.

**The case** $h = 0$**:** $P \leq (0, w)$ and $P' \leq (0, w)$ means $P \equiv 0$ and $P' \equiv 0$, hence $P \equiv P'$.

**The case** $h + 1$**:** suppose that $P \leq (h + 1, w)$, $P' \leq (h + 1, w)$ and $P \approx_{h+1}^w P'$. We can suppose, without loosing generality, that

$$P \equiv (\alpha_1.Q_1)^{k_1}|...|(\alpha_n.Q_n)^{k_n}$$
$$P' \equiv (\alpha_1.Q_1)^{l_1}|...|(\alpha_n.Q_n)^{l_n}$$

where for $i \neq j$, $\alpha_i.Q_i \not\equiv \alpha_j.Q_j$. Obviously, as $P \leq (h + 1, w)$ and $P' \leq (h + 1, w)$ we have $k_i \leq w$ and $l_i \leq w$.

We show that $k_i \leq l_i$. If $k_i = 0$ then, obviously, $k_i \leq l_i$. If $k_i \neq 0$ then $P \equiv (\alpha_i.Q_i)^{k_i}|P_i$ and $P \approx_{h+1}^w P'$ provides that $P' \equiv \alpha_i.Q_1''|...\alpha_i.Q_{k_i}''|R$ with $Q_i \approx_h^w Q_j''$ for $j = 1..k_i$. By construction, $Q_i \leq ((h + 1) - 1, w) = (h, w)$ and $Q_j'' \leq ((h + 1) - 1, w) = (h, w)$. So, we can apply the inductive hypothesis that provides $Q_i \equiv Q_j''$ for $j = 1..i$. Hence $P' \equiv (\alpha_i.Q_i)^{k_i}|R$ that gives $k_i \leq l_i$.

With a symmetrical argument we can prove that $l_i \leq k_i$ that gives $k_i = l_i$ and, finally, $P \equiv P'$. □

If $P \approx_h^w Q$ and $P < (h, w)$ then $P \equiv Q$.

**Proof** Suppose that $P = (h', w')$ and $P \equiv (\alpha_1.P_1)^{k_1}|...|(\alpha_n.P_n)^{k_n}$ with $\alpha_i.P_i \not\equiv \alpha_j.P_j$ for $i \neq j$. Obviously we have $k_i \leq w' < w$.

We prove the theorem by induction on $h$. The first case is $h = 1$ (because $h > h'$).

**The case** $h = 1$**:** we have $h' = 0$ that gives $P \equiv 0$. Further $0 \approx_1^w Q$ gives $Q \equiv 0$, because else $Q \equiv \alpha.Q'|Q''$ asks for $0 \equiv \alpha.P'|P''$ - impossible. Hence $P \equiv Q \equiv 0$.

**The case** $h + 1$**:** as $P \equiv (\alpha_i.P_i)^{k_i}|P^+$, $P \approx_h^w Q$ and $k_i < w$, we obtain that $Q \equiv \alpha_i.R_1|...|\alpha_i.R_{k_i}|R^+$ with $P_i \approx_{h-1}^w R_j$ for any $j = 1..k_i$.

But $P_i \approx_{h-1}^w R_j$ allows us to use the inductive hypothesis, because $P_i \leq (h' - 1, w') < (h - 1, w)$, that gives $P_i \equiv R_j$ for any $j = 1..k_i$. Hence $Q \equiv (\alpha_i.P_i)^{k_i}|R^+$ and this is sustained for each $i = 1..n$. As $\alpha_i.P_i \not\equiv \alpha_j.P_j$ for $i \neq j$, we derive $Q \equiv (\alpha_1.P_1)^{k_1}|...|(\alpha_n.P_n)^{k_n}|R$.

We prove now that $R \equiv 0$. Suppose that $R \equiv (\alpha.R')|R''$. Then $Q \equiv \alpha.R'|R^-$, and as $P \approx_h^w Q$, we obtain that there is an $i = 1..n$ such that $\alpha = \alpha_i$ and $R' \approx_{h-1,w} P_i$.

Because $P_i \leq (h' - 1, w') < (h - 1, w)$, we can use the inductive hypothesis and obtain $R' \equiv P_i$. Therefore $R \equiv \alpha_i.P_i|R''$, that gives further

$$Q \equiv (\alpha_1.P_1)^{k_1}|...(\alpha_{i-1}.P_{i-1})^{k_{(i-1)}}|(\alpha_i.P_i)^{k_i+1}|(\alpha_{i+1}.P_{i+1})^{k_{(i+1)}}|...|(\alpha_n.P_n)^{k_n}|R$$

So, we can consider $Q \equiv (\alpha_i.P_i)^{k_i+1}|Q^+$. Because $P \approx_h^w Q$ and $k_i + 1 \leq w' + 1 \leq w$, we obtain that $P \equiv \alpha_i.P_1'|...|\alpha_i.P_{k_i+1}'|P'$ with $P_j' \approx_{h-1}^w P_i$ for any $j = 1..k_i + 1$.

But $P_i \leq (h'-1, w') < (h-1, w)$, consequently we can use the inductive hypothesis and obtain $P'_j \equiv P_i$ for any $j = 1..k_i + 1$.
Hence $P \equiv (\alpha_i.P_i)^{k_i+1}|P''$ which is impossible because we supposed that $P \equiv (\alpha_1.P_1)^{k_1}|...|(\alpha_n.P_n)^{k_n}$ with $\alpha_i.P_i \not\equiv \alpha_j.P_j$ for $i \neq j$.

Concluding, $R \equiv 0$ and $Q \equiv (\alpha_1.P_1)^{k_1}|...|(\alpha_n.P_n)^{k_n}$, i.e. $Q \equiv P$. □

If $P \equiv R|P'$, $P \approx_h^w Q$ and $R < (h, w)$ then
$Q \equiv R|Q'$.

**Proof** Suppose that $R = (h', w') < (h, w)$. Because $P \equiv R|P'$ and $P \approx_h^w Q$, using theorem 2.2, we obtain that exists $Q_1, Q_2$ such that $Q \equiv Q_1|Q_2$ and $R \approx_h^{w'+1} Q_1$ and $P' \approx_h^{w-(w'+1)} Q_2$. Further, as $R \approx_h^{w'+1} Q_1$ and $R = (h', w') < (h, w' + 1)$ we obtain, by using theorem 2.2, that $Q_1 \equiv R$, hence $Q \equiv R|Q_2$. □

Let $P \approx_h^w Q$. If $P \equiv \alpha.P'|P''$ then $Q \equiv \alpha.Q'|Q''$ and $P'|P'' \approx_{h-1}^{w-1} Q'|Q''$

**Proof** As $P \approx_h^w Q$ and $P \equiv \alpha.P'|P''$, we obtain that, indeed, $Q \equiv \alpha.Q'|Q''$ with $P' \approx_{h-1}^w Q'$. We will prove that $P'|P'' \approx_{h-1}^{w-1} Q'|Q''$. Consider any $i = 1..w-1$ and $\beta \in \mathbb{A}$ such that:

$$P'|P'' \equiv \beta.P_1|...|\beta.P_i|P^\star \tag{1}$$

We can suppose, without loos of generality that for some $k \leq i$ we have

$$P' \equiv \beta.P_1|...|\beta.P_k|P^+$$
$$P'' \equiv \beta.P_{k+1}|...|\beta.P_i|P^-$$
$$P^\star \equiv P^+|P^-$$

Because $P' \approx_{h-1}^w Q'$ and $k \leq i \leq w-1$, we obtain that $Q' \equiv \beta.Q_1|...|\beta.Q_k|Q^+$ with $P_j \approx_{h-2}^w Q_j$ for $j = 1..k$. Further we distinguish two cases:

- if $\alpha \neq \beta$ then we have

  $$P \equiv \beta.P_{k+1}|...|\beta.P_i|(P^-|\alpha.P')$$

  and because $P \approx_h^w Q$, we obtain

  $$Q \equiv \beta.R_{k+1}|...|\beta.R_i|R^\star \text{ with } R_j \approx_{h-1}^w P_j \text{ for } j = k+1..i$$

  But $Q \equiv \alpha.Q'|Q''$ and because $\alpha \neq \beta$, we obtain $Q'' \equiv \beta.R_{k+1}|...|\beta.R_i|R^+$ that gives us in the end

  $$Q'|Q'' \equiv \beta.Q_1|...|\beta.Q_k|\beta.R_{k+1}|...|\beta.R_i|(R^+|Q^+)$$

with $P_j \approx^w_{h-2} Q_j$ for $j = 1..k$ (hence $P_j \approx^{w-1}_{h-2} Q_j$) and $P_j \approx^w_{h-1} R_j$ for $j = k+1..i$ (hence $P_j \approx^{w-1}_{h-2} R_j$).

- if $\alpha = \beta$ then we have

$$P \equiv \alpha.P_{k+1}|...|\alpha.P_i|\alpha.P'|P^-$$

and as $P \approx^w_h Q$ and $i \leq w-1$, we obtain

$$Q \equiv \alpha.R_{k+1}|...|\alpha.R_i|\alpha.R'|R^\star$$

with $R_j \approx^w_{h-1} P_j$ for $j = k+1..i$ and $R' \approx^w_{h-1} P'$. Because $P' \approx^w_{h-1} Q'$ and $\approx^w_h$ is an equivalence relation, we can suppose that $R' \equiv Q'$ (Indeed, if $\alpha.Q'$ is a subprocess of $R^\star$ then we can just substitute $R'$ with $Q'$; if $\alpha.Q' \equiv \alpha.R_s$, then $Q' \approx^w_{h-1} P_s$ and as $Q' \approx^w_{h-1} P'$ and $P' \approx^w_{h-1} R'$ we derive $R' \approx^w_{h-1} P_s$ and $Q' \approx^w_{h-1} P'$, so we can consider this correspondence). So

$$Q \equiv \alpha.R_{k+1}|...|\alpha.R_i|\alpha.Q'|R^\star$$

that gives

$$Q'' \equiv \alpha.R_{k+1}|...|\alpha.R_i|R^\star$$

which entails further

$$Q'|Q'' \equiv \alpha.Q_1|...|\alpha.Q_k|\alpha.R_{k+1}|...|\alpha.R_i|(R^\star|Q^+)$$

with $P_j \approx^w_{h-2} Q_j$ for $j = 1..k$ (hence $P_j \approx^{w-1}_{h-2} Q_j$) and $P_j \approx^w_{h-1} R_j$ for $j = k+1..i$ (hence $P_j \approx^{w-1}_{h-2} R_j$).

All these prove that $P'|P'' \approx^{w-1}_{h-1} Q'|Q''$ (as we can develop a symmetric argument starting in (1) with $Q|Q'$). □

[Behavioral simulation] Let $P \approx^w_h Q$. If $P \xrightarrow{\alpha} P'$ then exists a transition $Q \xrightarrow{\alpha} Q'$ such that $P' \approx^{w-1}_{h-1} Q'$.

**Proof** If $P \xrightarrow{\alpha} P'$ then $P \equiv \alpha.R'|R''$ and $P' \equiv R'|R''$. But $P \approx^w_h Q$ gives, using theorem 2.2 that $Q \equiv \alpha.S'|S''$ and $R'|R'' \approx^{w-1}_{h-1} S'|S''$. And because $Q \xrightarrow{\alpha} S'|S''$, we can take $Q' \equiv S'|S''$. □

## 2.3 Bound pruning processes

In this subsection we prove the bound pruning theorem, stating that for a given process $P$ and a given size $(h, w)$, we can always find a process $Q$ having the size at most equal with $(h, w)$ such that $P \approx_h^w Q$. Moreover, in the proof of the theorem we will present a method for constructing such a process from $P$, by pruning its syntactic tree to the given size.

[Bound pruning theorem] For any process $P \in \mathfrak{P}$ and any $(h, w)$ exists a process $Q \in \mathfrak{P}$ with $P \approx_h^w Q$ and $Q \leq (h, w)$.

**Proof** We describe the construction[5] of $Q$ by induction on $h$.

**For** $h = 0$**:** we just take $Q \equiv 0$, because $P \approx_0^w Q$ and $0 = (0, 0)$.

**For** $h + 1$**:** suppose that $P \equiv \alpha_1.P_1|...|\alpha_n.P_n$.

Let $P_i'$ be the result of pruning $P_i$ by $(h, w)$ (we use the inductive step of construction) and $P' \equiv \alpha_1.P_1'|...|\alpha_n.P_n'$. As for any $i = 1..n$ we have $P_i \approx_h^w P_i'$ (by the inductive hypothesis), we obtain, using theorem 2.2, that $\alpha_i.P_i \approx_{h+1}^w \alpha_i.P_i'$ and further $P \approx_{h+1}^w P'$.

Consider the canonical representation of $P' \equiv (\beta_1.Q_1)^{k_1}|...|(\beta_m.Q_m)^{k_m}$.

Let $l_i = min(k_i, w)$ for $i = 1..m$. Then we define $Q \equiv (\beta_1.Q_1)^{l_1}|...|(\beta_m.Q_m)^{l_m}$. Obviously $Q \approx_{h+1}^w P'$ and as $P \approx_{h+1}^w P'$, we obtain $P \approx_{h+1}^w Q$. By construction, $Q \leq (h + 1, w)$. □

[Bound pruning processes] For a process $P$ and for a tuple $(h, w)$ we denote by $P_{(h,w)}$ the process obtained by pruning $P$ to the size $(h, w)$ by the method described in the proof of theorem 2.3.

**Example 2.3** *Consider the process* $P \equiv \alpha.(\ \beta.(\gamma.0|\gamma.0|\gamma.0) \mid \beta.\gamma.0\ ) \mid \alpha.\beta.\gamma.0$.
*Observe that* $P = (3, 3)$*, hence* $P_{(3,3)} \equiv P$*. For constructing* $P_{(3,2)}$ *we have to prune the syntactic tree of* $P$ *such that to not exist, in any node, more than two bisimilar branches. Hence* $P_{(3,2)} = \alpha.(\ \beta.(\gamma.0|\gamma.0) \mid \beta.\gamma.0) \mid \alpha.\beta.\gamma.0$
*If we want to prune* $P$ *on the size* $(3, 1)$*, we have to prune its syntactic tree such that, in any node, there are no bisimilar branches. The result is* $P_{(3,1)} = \alpha.\beta.\gamma.0$.
*For pruning* $P$ *on the size* $(2, 2)$*, we have to prune all the nodes on depth* $2$ *and in the new tree we have to let, in any node, a maximum of two bisimilar branches. As a result of these modifications, we obtain* $P_{(2,2)} = \alpha.(\beta.0|\beta.0) \mid \alpha.\beta.0$*. Going further we obtain the smaller processes* $P_{(0,0)} = 0$*,* $P_{(1,1)} = \alpha.0$*,* $P_{(1,2)} = \alpha.0|\alpha.0$*,* $P_{(2,1)} = \alpha.\beta.0$.

If $P \equiv Q$ then $P_{(h,w)} \equiv Q_{(h,w)}$.

**Proof** Because a process is unique up to structural congruence, the result can be derived trivially, following the construction in the proof of theorem 2.3. □

$P \leq (h, w)$ iff $P_{(h,w)} \equiv P$.

**Proof** ($\Rightarrow$) If $P \leq (h, w)$, then, by construction, $P_{(h,w)} \leq (h, w)$ and $P \approx_h^w P_{(h,w)}$, we can use theorem 2.2 and obtain $P_{(h,w)} \equiv P$.

($\Leftarrow$) Suppose that $P_{(h,w)} \equiv P$. Suppose, in addition that $P > (h, w)$. By construction, $P_{(h,w)} \leq (h, w)$, hence $P_{(h,w)} \leq (h, w) < P$, i.e. $P_{(h,w)} \neq P$. But this is impossible, because the size of a process is unique up to structural congruence, see remark 2.1. □

[5] This construction is not necessarily unique.

## 2.4 Substitutions

For the future constructs is also useful to introduce the substitutions of actions in a process. [The set of actions of a process] We define $Act(P) \subset \mathbb{A}$, inductively by:

1. $Act(0) \stackrel{def}{=} \emptyset$ 2. $Act(\alpha.P) \stackrel{def}{=} \{\alpha\} \cup Act(P)$ 3. $Act(P|Q) \stackrel{def}{=} Act(P) \cup Act(Q)$ For a set $M \subset \mathfrak{P}$ of processes we define $Act(M) \stackrel{def}{=} \bigcup_{P \in M} Act(P)$.

We will define further the set of all processes having a size smaller than a given tuple $(h, w)$ and the actions in a set $A \subset \mathbb{A}$, and we will prove that for the fragment of CCS we considered they are finitely many (modulo $\equiv$).

Let $A \subset \mathbb{A}$. We define

$$\mathfrak{P}^A_{(h,w)} \stackrel{def}{=} \{P \in \mathfrak{P} \mid Act(P) \subset A,\ P \leq (h, w)\}$$

If $A \subset \mathbb{A}$ is finite, then $\mathfrak{P}^A_{(h,w)}$ is finite[6].

**Proof** We will prove more, that if we denote by $n = (w+1)^{card(A)}$, then

$$card(\mathfrak{P}^A_{(h,w)}) = \begin{cases} 1 & \text{if } h = 0 \\ \underbrace{n^{n^{\cdots^n}}}_{h} & \text{if } h \neq 0 \end{cases}$$

We prove this by induction on $h$.

**The case** $h = 0$**:** we have $Q = (0, w)$ iff $Q \equiv 0$, so $\mathfrak{P}^A_{(0,w)} = \{0\}$ and $card(\mathfrak{P}^A_{(0,w)}) = 1$.

**The case** $h = 1$**:** let $Q \in \mathfrak{P}_{(1,w)}$. Then

$$Q \equiv (\alpha_1.Q_1)^{k_1}|...|(\alpha_s.Q_s)^{k_s} \text{ with } Q_i \in \mathfrak{P}^A_{(0,w)} \text{ and } \alpha_i.Q_i \not\equiv \alpha_j.Q_j \text{ for } i \neq j.$$

But $Q_i \in \mathfrak{P}^A_{(0,w)}$ means $Q_i \equiv 0$, hence

$$Q \equiv (\alpha_1.0)^{k_1}|...|(\alpha_s.0)^{k_s}$$

Since $Q \leq (1, w)$ we obtain that $k_i \leq w$. The number of guarded processes $\alpha.0$ with $\alpha \in A$ is $card(A)$ and since $k_i \in 0..w$, the number of processes in $\mathfrak{P}^A_{(1,w)}$ is $(w+1)^{card(A)} = n^1$.

**The case** $h + 1$**:** let $Q \in \mathfrak{P}^A_{(h+1,w)}$. Then

$$Q \equiv (\alpha_1.Q_1)^{k_1}|...|(\alpha_s.Q_s)^{k_s} \text{ with } Q_i \in \mathfrak{P}^A_{(h,w)} \text{ and } \alpha_i.Q_i \not\equiv \alpha_j.Q_j \text{ for } i \neq j.$$

Since $Q \leq (h+1, w)$ we obtain that $k_i \leq w$. The number of guarded processes $\alpha.R$ with $\alpha \in A$ and $R \in \mathfrak{P}^A_{(h,w)}$ is $card(A) \times card(\mathfrak{P}^A_{(h,w)})$ and since $k_i \in 0..w$, the number of processes in $\mathfrak{P}^A_{(h+1,w)}$ is $(w+1)^{card(A) \times card(\mathfrak{P}^A_{(h,w)})} = ((w+1)^{card(A)})^{card(\mathfrak{P}^A_{(h,w)})} = n^{card(\mathfrak{P}^A_{(h,w)})}$. But the inductive hypothesis gives $card(\mathfrak{P}^A_{(h,w)}) = \underbrace{n^{n^{\cdots^n}}}_{h}$, so $card(\mathfrak{P}^A_{(h+1,w)}) = \underbrace{n^{n^{\cdots^n}}}_{h+1}$. □

[6]We count the processes up to structural congruence.

[Action substitution] We call *action substitution* any function $\sigma : \mathbb{A}\mathbf{to}\mathbb{A}$. We extend it further, syntactically, from actions to processes, $\sigma : \mathfrak{P}\mathbf{to}\mathfrak{P}$, by

$$\sigma(P) = \begin{cases} 0 & \text{if } P \equiv 0 \\ \sigma(Q)|\sigma(R) & \text{if } P \equiv Q|R \\ \sigma(\gamma).\sigma(R) & \text{if } P \equiv \gamma.R \end{cases}$$

We extend $\sigma$ for sets of processes $M \subset \mathfrak{P}$ by $\sigma(M) \stackrel{def}{=} \{\sigma(P) \mid P \in M\}$.
For short, we will denote, sometimes, $\sigma(P)$ by $P^\sigma$ and $\sigma(M)$ by $M^\sigma$.

Observe that $P \equiv Q$ entails $Act(P) = Act(Q)$ and $P^\sigma \equiv Q^\sigma$.

Let $\sigma$ be a substitution. We define the *subject of* $\sigma$, $sub(\sigma)$ and the *object of* $\sigma$, $obj(\sigma)$, by:

$$sub(\sigma) \stackrel{def}{=} \{\alpha \in \mathbb{A} \mid \sigma(\alpha) \neq \alpha\}$$

$$obj(\sigma) \stackrel{def}{=} \{\beta \in \mathbb{A} \mid \beta \neq \alpha,\ \sigma(\alpha) = \beta\}$$

If $sub(\sigma) \cap Act(P) = \emptyset$ then $\sigma(P) \equiv P$.

**Proof** We prove it by induction on $P$.

**The case** $P \equiv 0$**:** by definition, $\sigma(0) \equiv 0$.

**The case** $P \equiv \alpha.Q$**:** $\sigma(P) \equiv \sigma(\alpha).\sigma(Q)$. But $\alpha \in Act(P)$, and because $Act(P) \cap sub(\sigma) = \emptyset$, we obtain $\alpha \notin sub(\sigma)$, hence $\sigma(\alpha) = \alpha$. But then $\sigma(P) \equiv \alpha.\sigma(Q)$. Further $Act(Q) \subset Act(P)$, i.e. $Act(Q) \cap sub(\sigma) = \emptyset$ and we can apply the inductive hypothesis that provides $\sigma(Q) \equiv Q$, so $\sigma(P) \equiv \alpha.Q$, q.e.d.

**The case** $P \equiv Q|R$**:** $\sigma(P) \equiv \sigma(Q)|\sigma(R)$. But $Act(Q), Act(R) \subset Act(P)$, hence $Act(Q) \cap sub(\sigma) = Act(R) \cap sub(\sigma) = \emptyset$. Hence we can apply the inductive hypothesis that provides $\sigma(Q) \equiv Q$ and $\sigma(R) \equiv R$, thus $\sigma(P) \equiv Q|R \equiv P$. □

If $obj(\sigma) \cap Act(P) = \emptyset$ then $\sigma(Q) \equiv P$ implies $Q \equiv P$.

**Proof** We prove it by induction on $P$.

**If** $P \equiv 0$**:** if $Q \not\equiv 0$ then $Q \equiv \alpha.Q'|Q''$, thus $\sigma(Q) \equiv \sigma(\alpha).\sigma(Q')|\sigma(Q'') \not\equiv 0$. Impossible.

**If** $P \not\equiv 0$**:** Suppose that

$$P \equiv \alpha_1.P_1|...|\alpha_n.P_n$$

and

$$Q \equiv \beta_1.Q_1|...|\beta_m.Q_m$$

Then $\sigma(Q) \equiv \sigma(\beta_1).\sigma(Q_1)|...|\sigma(\beta_m).\sigma(Q_m)$ and

$$\alpha_1.P_1|...|\alpha_n.P_n \equiv \sigma(\beta_1).\sigma(Q_1)|...|\sigma(\beta_m).\sigma(Q_m)$$

But then $m = n$ and for each $i = 1..n$ there exists $j = 1..n$ such that $\alpha_i.P_i \equiv \sigma(\beta_j).\sigma(Q_j)$, thus $\alpha_i = \sigma(\beta_j)$. But from $obj(\sigma) \cap Act(P) = \emptyset$ we derive $\sigma(\beta_j) = \beta_j = \alpha_i$. Further, from

$\alpha_i.P_i \equiv \sigma(\beta_j).\sigma(Q_j)$ we infer $P_i \equiv \sigma(Q_j)$, and since $Act(P_i) \subset Act(P)$, we can use the inductive hypothesis and derive $P_i \equiv Q_j$. Thus $P \equiv Q$. □

If $\sigma(P) \equiv Q|R$ then there exist processes $Q', R'$ such that $P \equiv Q'|R'$, with $\sigma(Q') \equiv Q$ and $\sigma(R') \equiv R$.

**Proof** Suppose that $P \equiv \alpha_1.P_1|...|\alpha_n.P_n$. Then

$$\sigma(P) \equiv \sigma(\alpha_1).\sigma(P_1)|...|\sigma(\alpha_n).\sigma(P_n) \equiv Q|R$$

We can suppose, without loosing generality, that

$$Q \equiv \sigma(\alpha_1).\sigma(P_1)|...|\sigma(\alpha_i).\sigma(P_i)$$

$$R \equiv \sigma(\alpha_{i+1}).\sigma(P_{i+1})|...|\sigma(\alpha_n).\sigma(P_n)$$

Then we can define $Q' \equiv \alpha_1.P_1|...|\alpha_i.P_i$ and $R' \equiv \alpha_{i+1}.P_{i+1}|...|\alpha_n.P_n$. □

If $P \not\equiv R|Q$ and $obj(\sigma) \cap Act(R) = \emptyset$, then $\sigma(P) \not\equiv R|S$.

**Proof** Suppose that $\sigma(P) \equiv R|S$ for some $S$. Then, by the theorem 2.4, there exists $R', S'$ such that $P \equiv S'|R'$ and $\sigma(R') \equiv R$, $\sigma(S') \equiv S$. But because $obj(\sigma) \cap Act(R) = \emptyset$ and $\sigma(R') \equiv R$, we derive, applying the theorem 2.4, that $R' \equiv R$, hence $P \equiv R|S'$. But this contradicts the hypothesis of the theorem. So, there is no $S$ such that $\sigma(P) \equiv R|S$. □

# 3 Contexts

In this section we introduce *the contexts*, sets of processes that will be used to evaluate formulas of our logics. The intuition is that a *context* $\mathcal{M}$ is a (possibly infinite) set of processes that contains, in a maximal manner, any process representing a possible state of our system or of a subsystem of our system. Hence if a process belongs to a context then any process obtained by pruning its syntactic tree, in any way[7], should belong to the context, as it might represent a subsystem. For the same reason, the context should be also closed to transitions.

It is useful in this point to define some operations on sets of processes.

For any sets of processes $M, N \subset \mathfrak{P}$ and any $\alpha \in \mathbb{A}$ we define:

$\alpha.M \stackrel{def}{=} \{\alpha.P \mid P \in M\}$ $\qquad$ $M|N \stackrel{def}{=} \{P|Q \mid P \in M, Q \in N\}$

As we speak about processes up to structural congruence, the parallel operator on sets of processes will be commutative, associative and will have $\{0\}$ as null.

We associate further to each process $P$ the set $\pi(P)$ of all processes obtained by pruning, in the most general way, the syntactic tree of $P$.

[7]We do not refer here on bound pruning only, but on any possible pruning of the syntactic tree.

For $P \in \mathfrak{P}$ we define[8] $\pi(P) \subset \mathfrak{P}$ inductively by:

1. $\pi(0) \stackrel{def}{=} \{0\}$ 2. $\pi(\alpha.P) \stackrel{def}{=} \{0\} \cup \alpha.\pi(P)$ 3. $\pi(P|Q) \stackrel{def}{=} \pi(P)|\pi(Q)$

We extend the definition of $\pi$ to sets of processes $M \subset \mathfrak{P}$ by $\pi(M) \stackrel{def}{=} \bigcup_{P \in M} \pi(P)$.

The next assertions hold:

1. $P \in \pi(P)$ 2. $0 \in \pi(P)$ 3. $P \in \pi(P|Q)$ 4. $P_{(h,w)} \in \pi(P)$

**Proof** 1. We prove it by induction on $P$

- if $P \equiv 0$ then $\pi(P) = \{0\} \ni 0 \equiv P$
- if $P \equiv \alpha.Q$ then $\pi(P) = \{0\} \cup \alpha.\pi(Q)$. But the inductive hypothesis gives $Q \in \pi(Q)$, hence $\alpha.Q \in \alpha.\pi(Q) \subset \pi(P)$.
- if $P \equiv Q|R$ then $\pi(P) = \pi(Q)|\pi(R)$. The inductive hypothesis provide $Q \in \pi(Q)$ and $R \in \pi(R)$, hence $P \equiv Q|R \in \pi(Q)|\pi(R) = \pi(P)$.

2. We prove it by induction on $P$.

- if $P \equiv 0$ we have, by definition, $\pi(P) = \{0\} \ni 0$
- if $P \equiv \alpha.Q$ then $\pi(P) = \{0\} \cup \alpha.\pi(Q) \ni 0$.
- if $P \equiv Q|R$ then $\pi(P) = \pi(Q)|\pi(R)$. The inductive hypothesis provide $0 \in \pi(Q)$ and $0 \in \pi(R)$, hence $0 \equiv 0|0 \in \pi(Q)|\pi(R) = \pi(P)$.

3. We have $\pi(P|Q) = \pi(P)|\pi(Q)$. But $P \in \pi(P)$ and $0 \in \pi(Q)$, hence $P \equiv P|0 \in \pi(P)|\pi(Q) = \pi(P|Q)$.

4. We prove the theorem by induction on the structure of $P$.

- if $P \equiv 0$: we have $P_{(h,w)} \equiv 0 \in \{0\} = \pi(P)$ for any $(h, w)$.
- if $P \equiv \alpha.Q$: we distinguish two more cases:
  if $w = 0$ then $P_{(h,0)} \equiv 0 \in \pi(P)$
  if $w \neq 0$ then $(\alpha.Q)_{(h,w)} \equiv \alpha.Q_{(h-1,w)}$ by the construction of the adjusted processes. If we apply the inductive hypothesis we obtain that $Q_{(h-1,w)} \in \pi(Q)$, hence $(\alpha.Q)_{(h,w)} \in \alpha.\pi(Q) \subset \pi(P)$.
- if $P \equiv (\alpha.Q)^k$: we have $P_{(h,w)} \equiv (\alpha.Q_{(h-1,w)})^l$ where $l = min(k, w)$, by the construction of the adjusted processes. The inductive hypothesis gives $Q_{(h-1,w)} \in \pi(Q)$, hence $\alpha.Q_{(h-1,w)} \in \alpha.\pi(Q) \subset \pi(\alpha.Q)$. But because $0 \in \pi(\alpha.Q)$ and

$$P_{(h,w)} \equiv \underbrace{\alpha.Q_{(h-1,w)}|...|\alpha.Q_{(h-1,w)}}_{l} \,|\, \underbrace{0|...|0}_{k-l}$$

[8] We consider also $\pi(P)$ defined up to structural congruence.

we obtain

$$P_{(h,w)} \in \underbrace{\pi(\alpha.Q)|...|\pi(\alpha.Q)}_{k} = \pi(P)$$

- if $P \equiv (\alpha_1.P_1)^{k_1}|...|(\alpha_n.P_n)^{k_n}$ with $n \geq 2$: we split it in two subprocesses $Q \equiv (\alpha_1.P_1)^{k_1}|...|(\alpha_i.P_i)^{k_i}$ and $R \equiv (\alpha_{i+1}.P_{i+1})^{k_{i+1}}|...|(\alpha_n.P_n)^{k_n}$. By the way we split the process $P$ we will have $P_{(h,w)} \equiv Q_{(h,w)}|R_{(h,w)}$ and using the inductive hypothesis on $Q$ and $R$ we derive $P_{(h,w)} \equiv Q_{(h,w)}|R_{(h,w)} \in \pi(Q)|\pi(R) = \pi(P)$.

□

1. $Act(\pi(P)) \subseteq Act(P)$ 2. If $P$**to**$Q$ then $Act(Q) \subseteq Act(P)$.

**Proof** 1. We prove it by induction on $P$.
**if** $P \equiv 0$ **then** $Act(\pi(P)) = Act(\emptyset) = \emptyset \subseteq Act(P)$.
**if** $P \equiv \alpha.Q$ **then** $Act(\pi(P)) = Act(\{0\} \cup \alpha.\pi(Q)) = Act(\alpha.\pi(Q)) = \{\alpha\} \cup Act(\pi(Q))$. By inductive hypothesis, $Act(\pi(Q)) \subseteq Act(Q)$, hence $Act(\pi(P)) \subseteq \{\alpha\} \cup Act(Q) = Act(P)$.
**if** $P \equiv Q|R$ **then** $Act(\pi(P)) = Act(\pi(Q)|\pi(R)) = Act(\pi(Q)) \cup Act(\pi(R))$. Using the inductive hypothesis, $Act(\pi(Q)) \subseteq Act(Q)$ and $Act(\pi(R)) \subseteq Act(R)$, hence $Act(\pi(P)) \subseteq Act(Q) \cup Act(R) = Act(Q|R) = Act(P)$.
2. If $P$**to**$Q$ then $P \equiv \alpha.Q_1|Q_2$ and $Q \equiv Q_1|Q_2$. Then $Act(Q) = Act(Q_1) \cup Act(Q_2) \subseteq \{\alpha\} \cup Act(Q_1) \cup Act(Q_2) = Act(P)$. □

$\pi(\pi(P)) = \pi(P)$.

**Proof** We prove it by induction on $P$.
**The case** $P \equiv 0$**:** $\pi(\pi(0)) = \pi(\{0\}) = \pi(0)$
**The case** $P \equiv \alpha.Q$**:** $\pi(\pi(\alpha.Q)) = \pi(\{0\} \cup \alpha.\pi(Q)) = \pi(0) \cup \pi(\alpha.\pi(Q)) = \{0\} \cup \alpha.\pi(\pi(Q))$. Now we can use the inductive hypothesis and we obtain $\pi(\pi(Q)) = \pi(Q)$. Hence $\pi(\pi(\alpha.Q)) = \{0\} \cup \alpha.\pi(Q) = \pi(\alpha.Q) = \pi(P)$.
**The case** $P \equiv Q|R$**:** $\pi(\pi(P)) = \pi(\pi(Q|R)) = \pi(\pi(Q)|\pi(R)) = \pi(\pi(Q))|\pi(\pi(R))$. Now we ca apply the inductive hypothesis on $Q$ and $R$ and obtain $\pi(\pi(P)) = \pi(Q)|\pi(R) = \pi(Q|R) = \pi(P)$. □

If $Q \in \pi(P)$ then $\pi(Q) \subset \pi(P)$.

**Proof** $Q \in \pi(P)$ implies $\pi(Q) \subset \pi(\pi(P))$, and applying the theorem 3, we obtain $\pi(Q) \subset \pi(P)$. □

If $\sigma$ is a substitution, then $\pi(\sigma(P)) = \sigma(\pi(P))$.

**Proof** We prove it by induction on $P$.
**The case** $P \equiv 0$**:** $\pi(\sigma(P)) = \pi(0) = \{0\} = \sigma(\{0\}) = \sigma(\pi(P))$.

**The case** $P \equiv \alpha.Q$**:** $\pi(\sigma(P)) = \pi(\sigma(\alpha).\sigma(Q)) = \{0\} \cup \sigma(\alpha).\pi(\sigma(Q))$. But the inductive hypothesis gives $\pi(\sigma(Q)) = \sigma(\pi(Q))$, hence

$$\pi(\sigma(P)) = \{0\} \cup \sigma(\alpha).\sigma(\pi(Q))$$

from the other side, $\sigma(\pi(P)) = \sigma(\{0\} \cup \alpha.\pi(Q)) = \{0\} \cup \sigma(\alpha).\sigma(\pi(Q))$.
**The case** $P \equiv Q|R$**:** $\pi(\sigma(Q|R)) = \pi(\sigma(Q)|\sigma(R)) = \pi(sigma(Q))|\pi(\sigma(R))$. But the inductive hypothesis gives $\pi(\sigma(Q)) = \sigma(\pi(Q))$ and $\pi(\sigma(R)) = \sigma(\pi(R))$. Hence $\pi(\sigma(P)) = \sigma(\pi(Q))|\sigma(\pi(R)) = \sigma(\pi(Q)|\pi(R)) = \sigma(\pi(P))$. □

These being proved, we can propose the definition of context:
[Context] *A context* is a nonempty set $\mathcal{M} \subseteq \mathfrak{P}$ of processes such that

- if $P \in \mathcal{M}$ and $P \longrightarrow P'$ then $P' \in \mathcal{M}$
- if $P \in \mathcal{M}$ then $\pi(P) \subset \mathcal{M}$

If $\mathcal{M}$ is a context and $\sigma$ a substitution, then $\mathcal{M}^\sigma$ is a context.
**Proof** Let $P \in \mathcal{M}^\sigma$. Then it exists a process $Q \in \mathcal{M}$ such that $\sigma(Q) \equiv P$. Then $\pi(P) = \pi(\sigma(Q))$, and using theorem 3 we derive $\pi(P) = \sigma(\pi(Q))$. But $Q \in \mathcal{M}$ implies $\pi(Q) \subset \mathcal{M}$, thus $\sigma(\pi(Q)) \subset \mathcal{M}^\sigma$. Then $\pi(P) \subset \mathcal{M}^\sigma$.
Let $P \in \mathcal{M}^\sigma$ and $P$**to**$P'$. Then it exists $Q \in \mathcal{M}$ such that $\sigma(Q) \equiv P$. Suppose that

$$Q \equiv \alpha_1.Q_1|...|\alpha_k.Q_k$$

then

$$P \equiv \sigma(Q) \equiv \sigma(\alpha_1).\sigma(Q_1)|...|\sigma(\alpha_k).\sigma(Q_k)$$

But then $P$**to**$P'$ gives that it exists $i = 1..k$ such that

$$P' \equiv \sigma(\alpha_1).\sigma(Q_1)|...|\sigma(\alpha_{i-1}).\sigma(Q_{i-1}) \mid \sigma(Q_i) \mid \sigma(\alpha_{i+1}).\sigma(Q_{i+1})|...|\sigma(\alpha_k).\sigma(Q_k)$$

and if we define

$$Q' \equiv \alpha_1.Q_1|...|\alpha_{i-1}.Q_{i-1} \mid Q_i \mid \alpha_{i+1}.Q_{i+1}|...|\alpha_k.Q_k$$

we obtain $Q$**to**$Q'$ (i.e. $Q' \in \mathcal{M}$) and $\sigma(Q') \equiv P'$. Hence $P' \in \mathcal{M}^\sigma$. □

Observe that, due to the closure clauses in definition 3, we can consider the possibility to define systems of generators for a context, as a class of processes that, using the rules in definition 3 can generate the full context.

[System of generators for a context] We say that the set $M \subset \mathfrak{P}$ is a system of generators for the context $\mathcal{M}$ if $\mathcal{M}$ is the smallest context that contains $M$. We denote this by $\overline{M} = \mathcal{M}$.

If $M \in \mathfrak{P}$ is a finite set of processes, then $\overline{M}$ is a finite context.

**Proof** Trivial. □

## 3.1 Structural bisimulation on contexts

We extend the definitions of structural bisimulation from processes to contexts. This will allow us to prove the *context pruning theorem*, a result similar to the bound pruning theorem proved for processes.

[Structural bisimulation over contexts] Let $\mathcal{M}, \mathcal{N}$ be two contexts. We write $\mathcal{M} \approx_h^w \mathcal{N}$ iff

1. for any $P \in \mathcal{M}$ there is a $Q \in \mathcal{N}$ with $P \approx_h^w Q$
2. for any $Q \in \mathcal{N}$ there is a $P \in \mathcal{M}$ with $P \approx_h^w Q$

We convey to write $(\mathcal{M}, P) \approx_h^w (\mathcal{N}, Q)$ for the case when $P \in \mathcal{M}$, $Q \in \mathcal{N}$, $P \approx_h^w Q$ and $\mathcal{M} \approx_h^w \mathcal{N}$.

[Antimonotonicity over contexts] If $\mathcal{M} \approx_h^w \mathcal{N}$ and $(h', w') \leq (h, w)$ then $\mathcal{M} \approx_{h'}^{w'} \mathcal{N}$.

**Proof** For any process $P \in \mathcal{M}$ there exists a process $Q \in \mathcal{N}$ such that $P \approx_h^w Q$ and using theorem 2.2 we obtain $P \approx_{h'}^{w'} Q$. And the same if we start from a process $Q \in N$. These proves that $\mathcal{M} \approx_{h'}^{w'} \mathcal{N}$. □

## 3.2 Pruning contexts

As for processes, we can define the pruning of a context $\mathcal{M}$ as the context generated by the set of pruned processes of $\mathcal{M}$, taken as system of generators.

[Pruning contexts] For any context $\mathcal{M}$ and any $(h, w)$ we define

$$\mathcal{M}_{(h,w)} \stackrel{def}{=} \overline{\{P_{(h,w)} \mid P \in \mathcal{M}\}}$$

For any context $\mathcal{M}$, and any size $(h, w)$ we have $\mathcal{M}_{(h,w)} \approx_w^h \mathcal{M}$.

**Proof** Denote by

$$M = \{P_{(h,w)} \mid P \in \mathcal{M}\}$$

Let $P \in \mathcal{M}$. Then it exists a process $Q \in \mathcal{M}_{(h,w)}$, more exactly $Q \equiv P_{(h,w)}$ such that $P \approx_w^h Q$.
Let $Q \in \mathcal{M}_{(h,w)}$. Since $\overline{M}$ is the smallest context containing $M$, and because, by construction, $M \subseteq \mathcal{M}$ we derive that $\overline{M} \subseteq \mathcal{M}$. Hence, for any process $Q \in \overline{M}$ there is a process $P \in \mathcal{M}$, more exactly $P \equiv Q$ such that $P \approx_w^h Q$ (since $P \equiv Q$ implies $P \approx_w^h Q$). □

For any context $\mathcal{M}$ and any size $(h, w)$ we have $Act(\mathcal{M}_{(h,w)}) \subseteq Act(\mathcal{M})$.

**Proof** As $P_{(h,w)} \in \pi(P)$ for any process $P \in \mathcal{M}$ and any $(h, w)$, by theorem 3, we obtain, by applying theorem 3, $Act(P_{(h,w)}) \subseteq Act(\mathcal{M})$, hence $Act(\{P_{(h,w)} \mid P \in \mathcal{M}\}) \subseteq Act(\mathcal{M})$. Further applying again theorem 3, we trivially derive the desired result. □

Let $A \subset \mathbb{A}$. We denote by $\mathfrak{M}_{(h,w)}^A$ the set of all contexts generated by systems with the size at most $(h, w)$ and the actions in $A$:

$$\mathfrak{M}_{(h,w)}^A \stackrel{def}{=} \{\overline{M} \subset \mathfrak{P} \mid Act(M) \subseteq A,\ M \leq (h, w)\}$$

If $A \subset \mathbb{A}$ is a finite set of actions, then the following hold:

1. If $\mathcal{M} \in \mathfrak{M}^A_{(h,w)}$ then $\mathcal{M}$ is a finite context.

2. $\mathfrak{M}^A_{(h,w)}$ is finite.

**Proof** 1.: If $\mathcal{M} \in \mathfrak{M}^A_{(h,w)}$ then $\mathcal{M} = \overline{M}$, $M \leq (h, w)$ and $Act(M) \subset A$. Thus $M \subset \mathfrak{P}^A_{(h,w)}$. But $\mathfrak{P}^A_{(h,w)}$ is finite, by theorem 2.4. Thus, by theorem 3, $\overline{M} = \mathcal{M}$ is a finite context.

2.: As $\mathfrak{P}^A_{(h,w)}$ is finite by theorem 2.4, the set of its subsets is finite, and as all the elements of $\mathfrak{M}^A_{(h,w)}$ are generated by subsets of $\mathfrak{P}^A_{(h,w)}$, we obtain that $\mathfrak{M}^A_{(h,w)}$ is finite. □

[Pruning theorem] Let $\mathcal{M}$ be a context. Then for any $(h, w)$ there is a context $\mathcal{N} \in \mathfrak{M}^{Act(\mathcal{M})}_{(h,w)}$ such that $\mathcal{M} \approx^w_h \mathcal{N}$.

**Proof** The context $\mathcal{N} = \mathcal{M}_{(h,w)}$ fulfills the requirements of the theorem, by construction. Indeed, it is a context, and it is generated by the set $N = \{P_{(h,w)} \mid P \in \mathcal{M}\}$. Moreover $N \leq (h, w)$ and, by theorem 3.2, $Act(\mathcal{M}_{(h,w)}) \subseteq Act(\mathcal{M})$. Hence $\mathcal{N} \in \mathfrak{M}^{Act(\mathcal{M})}_{(h,w)}$. □

# 4 Dynamic Epistemic Spatial Logic

In this section we introduce Dynamic Epistemic Spatial Logic, $\mathcal{L}^{\mathfrak{S}}_{DES}$, which extends Hennessy-Milner logic with the parallel operator and epistemic operators. The intuition is to define the knowledge of the process $P$ in the context $\mathcal{M}$ as the common properties of the processes in $\mathcal{M}$ that contain $P$ as subprocess. If we think to the epistemic agent as to an observer that can see only the process $P$, then its knowledge about any state of global system concerns only $P$. Thus, for it, the global states $P|Q$ and $P|R$ looks indistinguishable. Hence the knowledge implies a kind of universal quantifier over $\mathcal{M}$, since $K_P\phi$, if is satisfied by a process $P|Q$, then it is satisfied by any process $P|R \in \mathcal{M}$. We find this enough for expressing most of the properties considered in the spatial logic literature, which required the use of the guarantee operator.

By using the *structural bisimulation* and *pruning method*, we will prove the finite model property for $\mathcal{L}^{\mathfrak{S}}_{DES}$ in relation to the semantics we considered. Consequently, we obtain decidability for satisfiability/validity and model checking.

For $\mathcal{L}^{\mathfrak{S}}_{DES}$ we will develop a Hilbert-style axiomatic system that will be proved to be sound and complete with respect to process semantics. Thus we identify the main axioms and rules that regularize the behavior of the classical, spatial, dynamic and epistemic logical operators. We will stress the similarities between our axioms and the classical axioms of epistemic logic, and we will prove some meaningful theorems.

Combined with the decidability, the properties of soundness and completeness make our logic a useful tool in analyzing complex multi-agent systems.

To introduce epistemic operators into our syntax we need to specify, for the beginning, the *epistemic agents*. As in classic epistemic logic, we may start with a class of agents, each agent pointing to a predefined subsystem (subprocess) of the system we consider. In this respect, we should consider quite a large class of agents, also for the processes that are not active in the current state but might be activated in future.

Hence for a system containing an agent associated with the process $\alpha.P|Q$, we might want to have also agents associated with $\alpha.P$, $P$, $P|Q$ and $Q$ respectively.

To avoid a syntax that is too complex, we decided to identify the agents with the processes they represent. Hence, in our logic the class of epistemic agents is just a subclass of $\mathfrak{P}$. We will call this class *signature*, as it contains processes that will be part of the syntax as indexes of the epistemic agents. To denote the signature of our logic we will use the symbol $\mathfrak{S}$.

[Signature] *A signature over* $\mathfrak{P}$ is a set of processes $\mathfrak{S} \subset \mathfrak{P}$, hereafter called *epistemic agents*, satisfying the conditions:

- if $P|Q \in \mathfrak{S}$ then $P, Q \in \mathfrak{S}$
- if $P \in \mathfrak{S}$ and $P \longrightarrow Q$, then $Q \in \mathfrak{S}$

Observe that, by the previous definition, any signature $\mathfrak{S}$ contains $0$.

## 4.1 Syntax of $\mathcal{L}^{\mathfrak{S}}_{DES}$

[Syntax of $\mathcal{L}^{\mathfrak{S}}_{DES}$] Let $\mathfrak{S}$ be a signature over $\mathfrak{P}$. We define the language of Dynamic Epistemic Spatial Logic over $\mathfrak{S}$, $\mathcal{F}^{\mathfrak{S}}_{DES}$, by the following grammar:

$$\phi := \ 0 \mid \top \mid \neg\phi \mid \phi \wedge \phi \mid \phi|\phi \mid \langle\alpha\rangle\phi \mid K_Q\phi$$

where $Q \in \mathfrak{S}$ and $\alpha \in \mathbb{A}$.

Anticipating the semantics, we will outline here the intuition that motivates the choice of the formulas. Mainly it is similar to that of Hennessy-Milner and spatial logics.

The formula $0$ is meant to characterize any process structurally congruent with $0$ (and only these) in any context, expressing *"there is no activity here"*. It should not be confused with "*false*".[9]

$\top$ will be satisfied by any process in any context.

The reason for introducing the parallel operator $\phi|\psi$ is that we want to be able to express, as in other spatial logics, the situation in which our system is composed by two parallel subsystems, one satisfying $\phi$ and the other satisfying $\psi$.

The dynamic-like operator $\langle\alpha\rangle\phi$ is meant to be used, as in Hennessy-Milner logic, to speak about the transitions of our system. It expresses *"the system may perform the action $\alpha$ thus meeting a state described by $\phi$"*.

We associate to each process $P \in \mathfrak{S}$ an epistemic operator $K_P\phi$ meaning *the agent (process) $P$ knows $\phi$*. Obviously, for our agents the notion of knowledge is different than in the standard

[9] We insist on this aspect as some syntaxes of classical logic use $0$ for denoting *false*. This is not our intention. We use $\bot$ to denote *false*.

approaches to intelligent agents, in the sense that we do not expect our agents to answer questions concerning their knowledge or to compute it. The knowledge of the agent $P$ in a context $\mathcal{M}$ is strictly related to the spectrum of actions $P$ can perform in this environment.

In our approach an inactive agent does not have a knowledge. This is an expected fact, as an inactive agent does not exist. Indeed, approaching systems from the point of view of behavior, *to be* is *to behave*. This aspect is new for the class of epistemic logic where, always, all the agents exist and know at least the tautologies.

[Derived operators] In addition we introduce some derived operators:

1. $\bot \stackrel{def}{=} \neg\top$
2. $\phi \vee \psi \stackrel{def}{=} \neg((\neg\phi) \wedge (\neg\psi))$
3. $\phi \rightarrow \psi \stackrel{def}{=} (\neg\phi) \vee \psi$
4. $[\alpha]\phi \stackrel{def}{=} \neg(\langle\alpha\rangle(\neg\phi))$
5. $1 \stackrel{def}{=} \neg((\neg 0) \mid (\neg 0))$
6. $\langle !\alpha\rangle\psi \stackrel{def}{=} (\langle\alpha\rangle\psi) \wedge 1$
7. $\widetilde{K}_Q\phi \stackrel{def}{=} \neg K_Q \neg\phi$

We could also introduce, for each action $\alpha$, a derived operator[10] $\langle\alpha, \overline{\alpha}\rangle$ to express communication by $\alpha$, supposing that we have defined an involution $co : \mathbb{A} \longrightarrow \mathbb{A}$ which associates to each action $\alpha$ its co-action $\overline{\alpha}$:

$$\langle\alpha, \overline{\alpha}\rangle\phi \stackrel{def}{=} \bigvee_{\phi \leftrightarrow \phi_1|\phi_2} \langle\alpha\rangle\phi_1 | \langle\overline{\alpha}\rangle\phi_2$$

$\bot$ will be used to express the inconsistent behavior of the system. For this reason no process, in any context, will satisfy $\bot$.

The dynamic-like operator $[\alpha]\phi$, the dual operator of $\langle\alpha\rangle\phi$, expresses the situation where either the system cannot perform $\alpha$, or if the system can perform $\alpha$ then any future state that can be reached by performing $\alpha$ can be described by $\phi$.

The formula $1$ is meant to describe the situation in which the system cannot be decomposed into two non-trivial subsystems. $1$ can describe also the trivial system $0$.

The formula $\langle !\alpha\rangle\psi$ expresses a process guarded by $\alpha$, which, after consuming $\alpha$, will satisfy $\psi$.

We convey that the precedence order of the operators in the syntax of $\mathcal{L}^{\mathfrak{S}}_{DES}$ is $\neg,\ K_Q,\ \langle\alpha\rangle,\ |, \wedge, \vee, \rightarrow$ where $\neg$ has precedence over all the other operators.

## 4.2 Process semantics

A formula of $\mathcal{F}^{\mathfrak{S}}_{DES}$ will be evaluated to processes in a given context, by mean of a satisfaction relation $\mathcal{M}, P \models \phi$.

[Models and satisfaction] A model of $\mathcal{L}^{\mathfrak{S}}_{DES}$ is a context $\mathcal{M}$ for which we define the satisfaction relation, for $P \in \mathcal{M}$, as follows:

$\mathcal{M}, P \models \top$ always

$\mathcal{M}, P \models 0$ iff $P \equiv 0$

[10] The disjunction is considered up to logically-equivalent decompositions $\phi \leftrightarrow \phi_1|\phi_2$ that ensures the use of a finitary formula.

$\mathcal{M}, P \models \neg\phi$ iff $\mathcal{M}, P \not\models \phi$
$\mathcal{M}, P \models \phi \wedge \psi$ iff $\mathcal{M}, P \models \phi$ and $\mathcal{M}, P \models \psi$
$\mathcal{M}, P \models \phi|\psi$ iff $P \equiv Q|R$ and $\mathcal{M}, Q \models \phi$, $\mathcal{M}, R \models \psi$
$\mathcal{M}, P \models \langle\alpha\rangle\phi$ iff there exists a transition $P \xrightarrow{\alpha} P'$ and $\mathcal{M}, P' \models \phi$
$\mathcal{M}, P \models K_Q\phi$ iff $P \equiv Q|R$ and $\forall Q|R' \in \mathcal{M}$ we have $\mathcal{M}, Q|R' \models \phi$

Then the semantics of the derived operators will be:

$\mathcal{M}, P \models [\alpha]\phi$ iff for any $P' \in \mathcal{M}$ such that $P \xrightarrow{\alpha} P'$ (if any), $\mathcal{M}, P' \models \phi$
$\mathcal{M}, P \models 1$ iff $P \equiv 0$ or $P \equiv \alpha.Q$ ($P$ is null or guarded)
$\mathcal{M}, P \models \langle!\alpha\rangle\phi$ iff $P \equiv \alpha.Q$ and $\mathcal{M}, Q \models \phi$
$\mathcal{M}, P \models \widetilde{K}_Q\phi$ iff either $P \not\equiv Q|R$ for any $R$, or it exists $Q|S \in \mathcal{M}$ such that $\mathcal{M}, Q|S \models \phi$

Remark the interesting semantics of the operators $K_0$ and $\widetilde{K}_0$:

$\mathcal{M}, P \models K_0\phi$ iff for any $Q \in \mathcal{M}$ we have $\mathcal{M}, Q \models \phi$
$\mathcal{M}, P \models \widetilde{K}_0\phi$ iff it exists a process $Q \in \mathcal{M}$ such that $\mathcal{M}, Q \models \phi$

If a process $P \in \mathcal{M}$ satisfies $K_0\phi$ then $\phi$ is valid in $\mathcal{M}$ (the same about $K_0\phi$) and vice versa. Hence we can encode, in the syntax, the validity with respect to a given context.

If a process $P \in \mathcal{M}$ satisfies $\widetilde{K}_0\phi$ (then all the processes in $\mathcal{M}$ satisfy $\widetilde{K}_0\phi$) then it exists a process $Q \in \mathcal{M}$ that satisfies $\phi$ and vice versa. Hence $\widetilde{K}_0\phi$ provides a way to encode the satisfiability with respect to a given model.

In the end of this section we recall some classic definitions.

We call a formula $\phi \in \mathcal{F}^{\mathfrak{S}}_{DES}$ *satisfiable* if there exists a context $\mathcal{M}$ and a process $P \in \mathcal{M}$ such that $\mathcal{M}, P \models \phi$.

We call a formula $\phi \in \mathcal{F}^{\mathfrak{S}}_{DES}$ *validity* if for any context $\mathcal{M}$ and any process $P \in \mathcal{M}$ we have $\mathcal{M}, P \models \phi$. In such a situation we write $\models \phi$.

Given a context $\mathcal{M}$, we denote by $\mathcal{M} \models \phi$ the situation when for any $P \in \mathcal{M}$ we have $\mathcal{M}, P \models \phi$.

$\phi$ is satisfiable iff $\neg\phi$ is not a validity, and vice versa, $\phi$ is a validity iff $\neg\phi$ is not satisfiable.

## 4.3 Finite model property and decidability

Now we prove the finite model property for our logic that will entail the decidability against the process semantics. To prove the finite model property means to prove that it exists, for a formula $\phi$, a finite class $C_\phi$ of couples $(\mathcal{M}, P)$ with $\mathcal{M}$ context and $P \in \mathcal{M}$ such that if $\phi$ is satisfiable then, necessarily, an element $(\mathcal{M}, P) \in C_\phi$ exists such that $\mathcal{M}, P \models \phi$. Anticipating, we define a size for $\phi$; then we prove that if $\mathcal{M}, P \models \phi$ then substituting, by $\sigma$, all the actions in $\mathcal{M}$ (and implicitly in $P$) that are not in the syntax of $\phi$ (as indexes of dynamic operators) by a fixed action with the same property, and then pruning $\mathcal{M}^\sigma$ and $P^\sigma$ to the size of $\phi$ we will obtain a couple $(\mathcal{N}, Q)$ such that $\mathcal{N}, Q \models \phi$. The fixed action of substitution can be chosen as the successor[11] of the maximum action of $\phi$, which is unique. Hence $\mathcal{N} \in \mathfrak{M}^A_{(h,w)}$ where $(h, w)$ is the size of $\phi$ and $A$ is the set of actions of

[11] We consider defined, on the class of actions $\mathbb{A}$, a lexicographical order.

$\phi$ augmented with the successor of its maximum, thus $A$ is finite. But then theorem 3.2 ensures that the set of pairs $(\mathcal{N}, Q)$, with this property, is finite.

[Size of a formula] We define *the sizes of a formula*, $\phi$ (*height* and *width*), inductively on $\mathcal{F}^{\mathfrak{S}}_{DES}$, by:

1. $0 = \top \stackrel{def}{=} (0,0)$ 2. $\neg\phi \stackrel{def}{=} \phi$

and supposing that $\phi = (h, w)$, $\psi = (h', w')$ and $R = (h_R, w_R)$ we define further:

3. $\phi \wedge \psi \stackrel{def}{=} (max(h, h'), max(w, w'))$ 4. $\phi|\psi \stackrel{def}{=} (max(h, h'), w + w')$
5. $\langle\alpha\rangle\phi \stackrel{def}{=} (1 + h, 1 + w)$ 6. $K_R\phi \stackrel{def}{=} (1 + max(h, h_R), 1 + max(w, w_R))$

The next theorem states that $\phi$ is *"sensitive"* via satisfaction only up to size $\phi$. In other words, the relation $\mathcal{M}, P \models \phi$ is conserved by substituting the couple $(M, P)$ with any other couple $(N, P)$ structurally bisimilar to it at the size $\phi$.

[Extending the structural bisimulation] We write $(\mathcal{M}, P) \approx^w_h (\mathcal{N}, Q)$ for the case when $P \in \mathcal{M}$, $Q \in \mathcal{N}$, $P \approx^w_h Q$ and $\mathcal{M} \approx^w_h \mathcal{N}$.

If $\phi = (h, w)$, $\mathcal{M}, P \models \phi$ and $(\mathcal{M}, P) \approx^w_h (\mathcal{N}, Q)$ then $\mathcal{N}, Q \models \phi$.

**Proof** We prove it by induction on the syntactical structure of $\phi$.

- **The case** $\phi = 0$**:** $\phi = (1, 1)$.
  $\mathcal{M}, P \models 0$ implies $P \equiv 0$.
  As $P \approx^1_1 Q$ we should have $Q \equiv 0$ as well, because else $Q \equiv \alpha.Q'|Q''$ asks for $P \equiv \alpha.P'|P''$ for some $P', P''$, but this is impossible because $P \equiv 0$.
  So $Q \equiv 0 \in \mathcal{N}$ and we have $\mathcal{N}, Q \models 0$, q.e.d.

- **The case** $\phi = \top$**:** is a trivial case as $\mathcal{N}, Q \models \top$ always.

- **The case** $\phi = \phi_1 \wedge \phi_2$**:** denote by $(h_i, w_i) = \phi_i$ for $i = 1, 2$. Then we have $\phi = (max(h_1, h_2), max(w_1, w_2)$
  $\mathcal{M}, P \models \phi$ is equivalent with $\mathcal{M}, P \models \phi_1$ and $\mathcal{M}, P \models \phi_2$.
  Because $(\mathcal{M}, P) \approx^{max(w_1,w_2)}_{max(h_1,h_2)} (\mathcal{N}, Q)$ we obtain, by using theorem 3.1, that $(\mathcal{M}, P) \approx^{w_1}_{h_1} (\mathcal{N}, Q)$ and $(\mathcal{M}, P) \approx^{w_2}_{h_2} (\mathcal{N}, Q)$.
  Now $(\mathcal{M}, P) \approx^{w_1}_{h_1} (\mathcal{N}, Q)$ and $\mathcal{M}, P \models \phi_1$ give, by inductive hypothesis, $\mathcal{N}, Q \models \phi_1$, while $(\mathcal{M}, P) \approx^{w_2}_{h_2} (\mathcal{N}, Q)$ and $\mathcal{M}, P \models \phi_2$ give, by inductive hypothesis $\mathcal{N}, Q \models \phi_2$.
  Hence $\mathcal{N}, Q \models \phi_1 \wedge \phi_2$, q.e.d.

- **The case** $\phi = \neg\phi'$**:** $\phi = \phi' = (h, w)$.
  We have $\mathcal{M}, P \models \neg\phi'$ and $(\mathcal{M}, P) \approx^w_h (\mathcal{N}, Q)$.
  If $\mathcal{N}, Q \not\models \neg\phi'$, then $\mathcal{N}, Q \models \neg\neg\phi'$, i.e. $\mathcal{N}, Q \models \phi'$.
  Because $(\mathcal{M}, P) \approx^w_h (\mathcal{N}, Q)$ and $\mathcal{N}, Q \models \phi'$, the inductive hypothesis gives that $\mathcal{M}, P \models \phi'$, which combined with $\mathcal{M}, P \models \neg\phi'$ gives $\mathcal{M}, P \models \bot$ - impossible. Hence $\mathcal{N}, Q \models \neg\phi'$.

- **The case** $\phi = \phi_1|\phi_2$**:** suppose that $\phi_i = (h_i, w_i)$ for $i = 1, 2$. Then $\phi = (max(h_1, h_2), w_1+w_2)$.

  Further, $\mathcal{M}, P \models \phi_1|\phi_2$ requires $P \equiv P_1|P_2$, with $\mathcal{M}, P_1 \models \phi_1$ and $\mathcal{M}, P_2 \models \phi_2$.

  As $(\mathcal{M}, P) \approx^{w_1+w_2}_{max(h_1,h_2)} (\mathcal{N}, Q)$ we obtain $P \approx^{w_1+w_2}_{max(h_1,h_2)} Q$. Than, from $P \equiv P_1|P_2$, using theorem 2.2, we obtain $Q \equiv Q_1|Q_2$ and $P_i \approx^{w_i}_{max(h_1,h_2)} Q_i$ for $i = 1, 2$. Hence, using theorem 3.1,
  $(\mathcal{M}, P_i) \approx^{w_i}_{max(h_1,h_2)} (\mathcal{N}, Q_i)$. Further, using again theorem 3.1, we obtain $(\mathcal{M}, P_i) \approx^{w_i}_{h_i}$ $(\mathcal{N}, Q_i)$, and using the inductive hypothesis,
  $\mathcal{N}, Q_1 \models \phi_1$ and $\mathcal{N}, Q_2 \models \phi_2$. Hence $\mathcal{N}, Q \models \phi$.

- **The case** $\phi = \langle\alpha\rangle\phi'$**:** suppose that $\phi' = (h', w')$. We have $\langle\alpha\rangle\phi' = (1 + h', 1 + w')$.

  $\mathcal{M}, P \models \langle\alpha\rangle\phi'$ means that $P \xrightarrow{\alpha} P'$ and $\mathcal{M}, P' \models \phi'$.

  Now $(\mathcal{M}, P) \approx^{1+w'}_{1+h'} (\mathcal{N}, Q)$ gives $P \approx^{1+w'}_{1+h'} Q$, and using theorem 2.2, we obtain that $Q \xrightarrow{\alpha} Q'$ and $P' \approx^{w'}_{h'} Q'$.

  But $(\mathcal{M}, P) \approx^{1+w'}_{1+h'} (\mathcal{N}, Q)$ gives also $\mathcal{M} \approx^{w'+1}_{h'+1} \mathcal{N}$, so using theorem 3.1, $\mathcal{M} \approx^{w'}_{h'} \mathcal{N}$. Hence $(\mathcal{M}, P') \approx^{w'}_{h'} (\mathcal{N}, Q')$.

  Now from $\mathcal{M}, P' \models \phi'$ and $(\mathcal{M}, P') \approx^{w'}_{h'} (\mathcal{N}, Q')$, we obtain, by using the inductive hypothesis, that $\mathcal{N}, Q' \models \phi'$, and as $Q \xrightarrow{\alpha} Q'$, we obtain further that $\mathcal{N}, Q \models \phi$.

- **The case** $\phi = K_R\phi'$ **with** $R \in \mathfrak{S}$**:** suppose that $\phi' = (h', w')$ and $R = (h_R, w_R)$.

  Then $K_R\phi' = (1 + max(h', h_R), 1 + max(w', w_R))$.

  Now $\mathcal{M}, P \models K_R\phi'$ gives $P \equiv R|P'$ and for any $R|S \in \mathcal{M}$ we have $\mathcal{M}, R|S \models \phi'$.

  As $(\mathcal{M}, P) \approx^{1+max(w',w_R)}_{1+max(h',h_R)} (\mathcal{N}, Q)$ then $P \approx^{1+max(w',w_R)}_{1+max(h',h_R)} Q$ and because $P \equiv R|P'$ and $R = (h_R, w_R) < (1+max(h', h_R), 1+max(w', w_R))$, we obtain, using theorem 2.2, that $Q \equiv R|Q'$.

  Let $R|S' \in \mathcal{N}$ be an arbitrary process. Because $\mathcal{M} \approx^{1+max(w',w_R)}_{1+max(h',h_R)} \mathcal{N}$ we obtain that exists a process $P'' \in \mathcal{M}$ such that $P'' \approx^{1+max(w',w_R)}_{1+max(h',h_R)} R|S'$. But $R < (1+max(h', h_R), 1+max(w', w_R))$, so, using theorem 2.2, $P'' \equiv R|S''$.

  Then $\mathcal{M}, R|S'' \models \phi'$, as $\mathcal{M}, R|S \models \phi'$ for any $R|S \in \mathcal{M}$.

  From the other side, $(\mathcal{M}, P) \approx^{1+max(w',w_R)}_{1+max(h',h_R)} (\mathcal{N}, Q)$ gives, using theorem 3.1, $(\mathcal{M}, P) \approx^{w'}_{h'}$ $(\mathcal{N}, Q)$ where from we obtain $\mathcal{M} \approx^{w'}_{h'} \mathcal{N}$.

  Also $R|S'' \approx^{1+max(w',w_R)}_{1+max(h',h_R)} R|S'$ gives $R|S'' \approx^{w'}_{h'} R|S'$, i.e. $(\mathcal{M}, R|S'') \approx^{w'}_{h'} (\mathcal{N}, R|S')$.

  Now $\mathcal{M}, R|S'' \models \phi'$ and $(\mathcal{M}, R|S'') \approx^{w'}_{h'} (\mathcal{N}, R|S')$ give, using the inductive hypothesis, that $\mathcal{N}, R|S' \models \phi'$.

  Concluding, we obtained that $Q \equiv R|Q'$ and for any $R|S' \in \mathcal{N}$ we have $\mathcal{N}, R|S' \models \phi'$. These two give $\mathcal{N}, Q \models K_R\phi'$ q.e.d.

□

Now, using this lemma, we conclude that if a process, in a context, satisfies $\phi$ then by pruning the process and the context on the size $\phi$, we still have satisfiability for $\phi$.

If $\mathcal{M}, P \models \phi$ then $\mathcal{M}_\phi, P_\phi \models \phi$.

**Proof** Let $\phi = (h, w)$. By contexts pruning theorem 3.2, we have $\mathcal{M} \approx^h_w \mathcal{M}_{(h,w)}$. By process pruning theorem 2.3, we have $P \approx^h_w P_{(h,w)}$ and $P_{(h,w)} \in \mathcal{M}_{(h,w)}$. Hence $(\mathcal{M}, P) \approx^h_w (\mathcal{M}_{(h,w)}, P_{(h,w)})$. Further lemma 4.3 establishes $\mathcal{M}_{(h,w)}, P_{(h,w)} \models \phi$ q.e.d. □

[The set of actions of a formula] We define the set of actions of a formula $\phi$, $act(\phi) \subset \mathbb{A}$, inductively by:

1. $act(0) \stackrel{def}{=} \emptyset$ 3. $act(\phi \wedge \psi) = act(\phi|\psi) \stackrel{def}{=} act(\phi) \cup act(\psi)$ 5. $act(K_R\phi) \stackrel{def}{=} Act(R) \cup act(\phi)$
2. $act(\top) \stackrel{def}{=} \emptyset$ 4. $act(\neg\phi) = act(\phi)$ 6. $act(\langle\alpha\rangle\phi) \stackrel{def}{=} \{\alpha\} \cup act(\phi)$

The next result states that a formula $\phi$ does not reflect properties that involves more then the actions in its syntax. Thus if $\mathcal{M}, P \models \phi$ then any substitution $\sigma$ having the elements of $act(\phi)$ as fix points preserves the satisfaction relation, i.e. $\mathcal{M}^\sigma, P^\sigma \models \phi$.

If $\mathcal{M}, P \models \phi$ and $\sigma$ is a substitution with $act(\sigma) \bigcap act(\phi) = \emptyset$ then $\mathcal{M}^\sigma, P^\sigma \models \phi$.

**Proof** We prove, simultaneously, by induction on $\phi$, that

1. if $\mathcal{M}, P \models \phi$ then $\sigma(\mathcal{M}), \sigma(P) \models \phi$
2. if $\mathcal{M}, P \not\models \phi$ then $\sigma(\mathcal{M}), \sigma(P) \not\models \phi$

**The case $\phi = 0$:**

1. $\mathcal{M}, P \models 0$ iff $P \equiv 0$. Then $\sigma(P) \equiv 0$ and $\sigma(\mathcal{M}), \sigma(0) \models 0$ q.e.d.
2. $\mathcal{M}, P \not\models 0$ iff $P \not\equiv 0$, iff $\sigma(P) \not\equiv 0$. Hence $\sigma(\mathcal{M}), \sigma(P) \not\models 0$.

**The case $\phi = \top$:**

1. $\mathcal{M}, P \models \top$ implies $\sigma(\mathcal{M}), \sigma(P) \models \top$, because this is happening for any context and process.
2. $\mathcal{M}, P \not\models \top$ is an impossible case.

**The case $\phi = \psi_1 \wedge \psi_2$:**

1. $\mathcal{M}, P \models \psi_1 \wedge \psi_2$ implies that $\mathcal{M}, P \models \psi_1$ and $\mathcal{M}, P \models \psi_2$. Because $act(\sigma) \cap act(\phi) = \emptyset$ we derive that $act(\sigma) \cap act(\psi_1) = \emptyset$ and $act(\sigma) \cap act(\psi_2) = \emptyset$. Further, applying the inductive hypothesis, we obtain $\mathcal{M}^\sigma, P^\sigma \models \psi_1$ and $\mathcal{M}^\sigma, P^\sigma \models \psi_2$ that implies $\mathcal{M}^\sigma, P^\sigma \models \psi_1 \wedge \psi_2$.

2. $\mathcal{M}, P \not\models \psi_1 \wedge \psi_2$ implies that $\mathcal{M}, P \not\models \psi_1$ or $\mathcal{M}, P \not\models \psi_2$. But, as argued before, $act(\sigma) \cap act(\psi_1) = \emptyset$ and $act(\sigma) \cap act(\psi_2) = \emptyset$, hence we can apply the inductive hypothesis that entails $\mathcal{M}^\sigma, P^\sigma \not\models \psi_1$ or $\mathcal{M}^\sigma, P^\sigma \not\models \psi_2$. Thus $\mathcal{M}^\sigma, P^\sigma \not\models \psi_1 \wedge \psi_2$.

**The case $\phi = \neg\psi$:**

1. $\mathcal{M}, P \models \neg\psi$ is equivalent with $\mathcal{M}, P \not\models \psi$ and because $act(\sigma) \cap act(\phi) = \emptyset$ guarantees that $act(\sigma) \cap act(\psi) = \emptyset$, we ca apply the inductive hypothesis and we obtain $\sigma(\mathcal{M}), \sigma(P) \not\models \psi$ which is equivalent with $\sigma(\mathcal{M}), \sigma(P) \models \neg\psi$.

2. $\mathcal{M}, P \not\models \neg\psi$ is equivalent with $\mathcal{M}, P \models \psi$ and applying the inductive hypothesis, $\sigma(\mathcal{M}), \sigma(P) \models \psi$, i.e. $\sigma(\mathcal{M}), \sigma(P) \not\models \neg\psi$.

**The case $\phi = \psi_1|\psi_2$:**

1. $\mathcal{M}, P \models \psi_1|\psi_2$ implies that $P \equiv Q|R$, $\mathcal{M}, Q \models \psi_1$ and $\mathcal{M}, R \models \psi_2$. As $act(\sigma) \cap act(\phi) = \emptyset$ we have $act(\sigma) \cap act(\psi_1) = \emptyset$ and $act(\sigma) \cap act(\psi_2) = \emptyset$. Then we can apply the inductive hypothesis and obtain $\sigma(\mathcal{M}), \sigma(Q) \models \psi_1$ and $\sigma(\mathcal{M}), \sigma(R) \models \psi_2$. But $\sigma(P) \equiv \sigma(Q)|\sigma(R)$, hence $\sigma(\mathcal{M}), \sigma(P) \models \phi$.

2. $\mathcal{M}, P \not\models \psi_1|\psi_2$ implies that for any decomposition $P \equiv Q|R$ we have either $\mathcal{M}, Q \not\models \psi_1$ or $\mathcal{M}, R \not\models \psi_2$. But, as before, from $act(\sigma) \cap act(\phi) = \emptyset$ guarantees that $act(\sigma) \cap act(\psi_1) = \emptyset$ and $act(\sigma) \cap act(\psi_2) = \emptyset$. Hence, we can apply the inductive hypothesis and consequently, for any decomposition $P \equiv Q|R$ we have either $\sigma(\mathcal{M}), \sigma(Q) \not\models \psi_1$ or $\sigma(\mathcal{M}), \sigma(R) \not\models \psi_2$.
Consider any arbitrary decomposition $\sigma(P) \equiv P'|P''$. By theorem 2.4, there exists $P \equiv Q|R$ such that $\sigma(Q) \equiv P'$ and $\sigma(R) \equiv P''$. Thus either $\sigma(\mathcal{M}), P' \not\models \psi_1$ or $\sigma(\mathcal{M}), P'' \not\models \psi_2$. Hence $\sigma(\mathcal{M}), \sigma(P) \not\models \psi_1|\psi_2$.

**The case $\phi = \langle\gamma\rangle\psi$:**

1. $\mathcal{M}, P \models \langle\gamma\rangle\psi$ means that there is a transition $P\overset{\gamma}{\mathbf{to}}Q$ and $\mathcal{M}, Q \models \psi$. Because $act(\sigma) \cap act(\langle\gamma\rangle\psi) = \emptyset$ implies $act(\sigma) \cap act(\psi) = \emptyset$. We can apply the inductive hypothesis and derive $\sigma(\mathcal{M}), \sigma(Q) \models \psi$. As $P\overset{\gamma}{\mathbf{to}}Q$ we have $P \equiv \gamma.P'|P''$ and $Q \equiv P'|P''$. This mean that $\sigma(P) \equiv \sigma(\gamma).\sigma(P')|\sigma(P'')$. Now $act(\sigma) \cap act(\langle\gamma\rangle\psi) = \emptyset$ ensures that $\sigma(\gamma) = \gamma$. So $\sigma(P) \equiv \gamma.\sigma(P')|\sigma(P'')$ and $\sigma(Q) \equiv \sigma(P')|\sigma(P'')$. Hence $\sigma(P)\overset{\gamma}{\mathbf{to}}\sigma(Q)$. Now because $\sigma(\mathcal{M}), \sigma(Q) \models \psi$, we derive $\sigma(\mathcal{M}), \sigma(P) \models \langle\gamma\rangle\psi$.

2. $\mathcal{M}, P \not\models \langle\gamma\rangle\psi$ implies one of two cases: either there is no transition of $P$ by $\gamma$, or there is such a transition and for any transition $P\overset{\gamma}{\mathbf{to}}Q$ we have $\mathcal{M}, Q \not\models \psi$.
If there is no transition of $P$ by $\gamma$ then $P \equiv \alpha_1.P_1|...|\alpha_k.P_k$ with $\alpha_i \neq \gamma$ for each $i \neq 1..k$. Because $\sigma(P) \equiv \sigma(\alpha_1).\sigma(P_1)|...|\sigma(\alpha_k).\sigma(P_k)$, and because $\gamma \neq \alpha_i$, and $\gamma \notin act(\sigma)$, we can state that $\gamma \neq \sigma(\alpha_i)$, hence $\sigma(P)$ cannot perform a transition by $\gamma$. Thus $\sigma(\mathcal{M}), \sigma(P) \not\models \langle\gamma\rangle\psi$.
If there are transitions of $P$ by $\gamma$, and for any such a transition $P\overset{\gamma}{\mathbf{to}}Q$ we have $\mathcal{M}, Q \not\models \psi$:

then, because from $act(\sigma) \cap act(\langle\gamma\rangle\psi) = \emptyset$ we can derive $act(\sigma) \cap act(\psi) = \emptyset$, the inductive hypothesis can be applied and we obtain $\sigma(\mathcal{M}), \sigma(Q) \not\models \psi$. But because $\gamma \notin act(\sigma)$ we obtain $\sigma(\gamma) = \gamma$ and $\sigma(P) \overset{\gamma}{\mathbf{to}} \sigma(Q)$. Hence $\sigma(\mathcal{M}), \sigma(P) \not\models \langle\gamma\rangle\psi$.

**The case** $\phi = K_R\psi$**:**

1. $\mathcal{M}, P \models K_R\psi$ implies $P \equiv R|S$ and for any $R|S' \in \mathcal{M}$ we have $\mathcal{M}, R|S' \models \psi$. From $act(\sigma) \cap act(\phi) = \emptyset$ we derive $act(\sigma) \cap act(\psi) = \emptyset$ and $act(\sigma) \cap Act(R) = \emptyset$. So, we can apply the inductive hypothesis that gives $\mathcal{M}^\sigma, \sigma(R|S') \models \psi$ and, because $\sigma(R) \equiv R$, $M^\sigma, R|\sigma(S') \models \psi$.
   Consider an arbitrary process $R|S'' \in \mathcal{M}^\sigma$. There exists a process $Q \in \mathcal{M}$ such that $\sigma(Q) \equiv R|S''$. Thus, by theorem 2.4, $Q \equiv R'|S'''$ with $\sigma(R') = R$ and $\sigma(S''') = S''$. But $Act(R) \cap act(\sigma) = \emptyset$ implies $Act(R) \cap obj(\sigma) = \emptyset$, so applying the theorem 2.4, we derive $R \equiv R'$. Thus $Q \equiv R|S'''$ and because $\mathcal{M}^\sigma, R|\sigma(S') \models \psi$ for any $S'$, we derive $\mathcal{M}^\sigma, R|S'' \models \psi$.
   Because $R|S'' \in \mathcal{M}^\sigma$ was arbitrarily chosen, and because $\sigma(P) = \sigma(R|S) = R|\sigma(S)$, we obtain $\mathcal{M}^\sigma, P^\sigma \models K_R\psi$.

2. $\mathcal{M}, P \not\models K_R\psi$ implies that either $P \not\equiv R|S$ for any $S$, or $P \equiv R|S$ for some $S$ and there exists a process $R|S' \in \mathcal{M}$ such that $\mathcal{M}, R|S' \not\models \psi$.
   If $P \not\equiv R|P'$, because $act(\sigma) \cap Act(R) = \emptyset$ implies $obj(\sigma) \cap Act(R) = \emptyset$ we derive, by theorem 2.4, that $\sigma(P) \not\equiv R|S$ for any $S$. Hence, we can state that $\mathcal{M}^\sigma, P^\sigma \not\models K_R\psi$.
   If $P \equiv R|S$ for some $S$ and there exists a process $R|S' \in \mathcal{M}$ such that $\mathcal{M}, R|S' \not\models \psi$, then the inductive hypothesis gives $\mathcal{M}^\sigma, \sigma(R)|\sigma(S') \not\models \psi$. But $\sigma(R)|\sigma(S') \equiv R|\sigma(S')$, and $\sigma(P) \equiv R|\sigma(S)$ thus $\sigma(\mathcal{M}), R|\sigma(S') \not\models \psi$ implies $\sigma(\mathcal{M}), \sigma(P) \not\models K_R\psi$.

□

We suppose to have defined on $\mathbb{A}$ a lexicographical order $\ll$. So, for a finite set $A \subset \mathbb{A}$ we can identify a maximal element that is unique. Hence the successor of this element is unique as well. We convey to denote by $A_+$ the set obtained by adding to $A$ the successor of its maximal element.

[Finite model property]

$$\text{If } \mathcal{M}, P \models \phi \text{ then } \exists \mathcal{N} \in \mathfrak{M}_\phi^{act(\phi)_+} \text{ and } Q \in \mathcal{N} \text{ such that } \mathcal{N}, Q \models \phi$$

**Proof** Consider the substitution $\sigma$ that maps all the actions $\alpha \in \mathbb{A} \setminus act(\phi)$ in the successor of the maximum element of $act(\phi)$ (it exists as $act(\phi)$ is finite). Obviously $act(\sigma) \cap act(\phi) = \emptyset$, hence, using theorem 4.3 we obtain $\mathcal{M}^\sigma, P^\sigma \models \phi$. Further we take $\mathcal{N} = \mathcal{M}^\sigma_{(h,w)} \in \mathfrak{M}^{act(\phi)^+}_{(h,w)}$ and $Q = P^\sigma_{(h,w)} \in \mathcal{M}^{act(\phi)^+}_{(h,w)}$, and theorem 4.3 proves the finite model property. □

Because $act(\phi)$ is finite implying $act(\phi)_+$ finite, we apply theorem 3.2 ensuring that $\mathfrak{M}_\phi^{act(\phi)_+}$ is finite and any context $\mathcal{M} \in \mathfrak{M}_\phi^{act(\phi)_+}$ is finite as well. Thus we obtain the finite model property for our

logic. A consequence of theorem 4.3 is the decidability for satisfiability, validity and model checking against the process semantics.

[Decidability] For $\mathcal{L}^{\mathfrak{S}}_{DES}$ validity, satisfiability and model checking are decidable against the process semantics.

## 4.4 Axioms of $\mathcal{L}^{\mathfrak{S}}_{DES}$

Now we propose a Hilbert-style axiomatic system for Dynamic Epistemic Spatial Logic, $\mathcal{L}^{\mathfrak{S}}_{DES}$. The system will be constructed in top of the classical propositional logic. Hence all the *axioms and rules of propositional logic* are available. In addition we will have a class of *spatial axioms and rules* that describes, mainly, the behavior of the parallel operator, a class of *dynamic axioms and rules* regarding the behavior of the dynamic operators, and a class of *epistemic axioms and rules* focusing on the behavior of epistemic operators. In the next subsections we will prove that the system is sound and complete with respect to process semantics.

We begin by defining, inductively on processes, some special classes of formulas that, will be proved further, characterize processes and finite contexts.

[Characteristic formulas for processes] We define a class of formulas $(c_P)_{P\in\mathfrak{P}}$, indexed by ($\equiv$-equivalence classes of) processes, as follows:

1. $c_0 \stackrel{def}{=} 0$ 2. $c_{P|Q} \stackrel{def}{=} c_P|c_Q$ 3. $c_{\alpha.P} \stackrel{def}{=} \langle !\alpha\rangle c_P$

[Characteristic formulas for contexts] If $\mathcal{M}$ is a finite context, we define its *characteristic formula* by:

$$c_{\mathcal{M}} = K_0(\bigvee_{Q\in\mathcal{M}} c_Q) \wedge (\bigwedge_{Q\in\mathcal{M}} \widetilde{K}_0 c_Q) \tag{2}$$

### Spatial axioms

$\vdash \top|\bot \rightarrow \bot$
$\vdash \phi|0 \leftrightarrow \phi$
$\vdash \phi|\psi \rightarrow \psi|\phi$
$\vdash (\phi|\psi)|\rho \rightarrow \phi|(\psi|\rho)$
$\vdash \phi|(\psi \vee \rho) \rightarrow (\phi|\psi) \vee (\phi|\rho)$
$\vdash (c_P \wedge \phi|\psi) \rightarrow \bigvee_{P\equiv Q|R}(c_Q \wedge \phi)|(c_R \wedge \psi)$

### Spatial rules

If $\vdash \phi \rightarrow \psi$ then $\vdash \phi|\rho \rightarrow \psi|\rho$

Axiom E4.4 states the propagation of the inconsistency from a subsystem to the upper system.

Axioms E4.4, E4.4 and E4.4 depict the structure of abelian monoid projected by the parallel operator on the class of processes.

Concerning axiom E4.4, observe that the disjunction involved has a finite number of terms, as we considered the processes up to structural congruence level. The theorem states that if system has a property expressed by parallel composition of specifications, then it must have two parallel complementary subsystems, each of them satisfying one of the specifications.

Rule $E_R$4.4 states a monotony property for the parallel operator.

## Dynamic axioms

$\vdash \langle\alpha\rangle\phi|\psi \rightarrow \langle\alpha\rangle(\phi|\psi)$

$\vdash [\alpha](\phi \rightarrow \psi) \rightarrow ([\alpha]\phi \rightarrow [a]\psi)$

$\vdash 0 \rightarrow [\alpha]\bot$

If $\beta \neq \alpha_i$ for $i = 1..n$ then $\vdash \langle!\alpha_1\rangle\top|...|\langle!\alpha_n\rangle\top \rightarrow [\beta]\bot$

$\vdash \langle!\alpha\rangle\phi \rightarrow [\alpha]\phi$

## Dynamic rules

If $\vdash \phi$ then $\vdash [\alpha]\phi$

If $\vdash \phi \rightarrow [\alpha]\phi'$ and $\vdash \psi \rightarrow [\alpha]\psi'$ then $\vdash \phi|\psi \rightarrow [\alpha](\phi'|\psi \vee \phi|\psi')$.

If $\vdash \bigvee_{\mathcal{M}\in\mathfrak{M}_\phi^{act(\phi)_+}} c_{\mathcal{M}} \rightarrow \phi$ then $\vdash \phi$.

The first dynamic axiom, axiom E4.4, presents a domain extrusion property for the dynamic operator. It expresses the fact that if an active subsystem of a bigger system performs the action $\alpha$, then the bigger system performs it as a whole.

Axiom E4.4 is just the (K)-axiom for the dynamic operator.

Axiom E4.4 states that an inactive system cannot perform any action.

Given a complex process that can be exhaustively decomposed in $n$ parallel subprocesses, each of them being able to perform one action only, $\alpha_i$, for $i = 1..n$, axiom E4.4 ensures us that the entire system, as a whole, cannot perform another action $\beta \neq \alpha_i$ for $i = 1..n$.

Recalling that the operator $\langle!\alpha\rangle$ describes processes guarded by $\alpha$, axiom E4.4 states that a system described by a guarded process can perform one and only one action, the guarding one.

Rule $E_R$4.4 is the classic necessity rule used for the dynamic operator.

Rule $E_R$4.4 is, in a sense, a counterpart of axiom E4.4 establishing the action of the operator $[\alpha]$ in relation to the parallel operator.

Rule $E_R$4.4 comes as a consequence of the finite model property and provides a rule that characterizes, in a finite manner, the validity of a formula. Observe that the disjunction in the first part of the rule has a finite number of terms.

# Epistemic axioms

If $P \in \mathfrak{S}$ then $\vdash K_P\top \leftrightarrow c_P|\top$
$\vdash K_Q\phi \wedge K_Q(\phi \rightarrow \psi) \rightarrow K_Q\psi$
$\vdash K_Q\phi \rightarrow \phi$
$\vdash K_Q\phi \rightarrow K_QK_Q\phi$.
$\vdash K_Q\top \rightarrow (\neg K_Q\phi \rightarrow K_Q\neg K_Q\phi)$
$\vdash K_Q\phi \leftrightarrow (K_Q\top \wedge K_0(K_Q\top \rightarrow \phi))$
$\vdash K_0\phi \wedge \psi|\rho \rightarrow (K_0\phi \wedge \psi)|(K_0\phi \wedge \rho)$
$\vdash K_0\phi \rightarrow [\alpha]K_0\phi$
$\vdash K_0\phi \rightarrow (K_Q\top \rightarrow K_QK_0\phi)$

# Epistemic rules

If $\vdash \phi$ then $\vdash K_Q\top \rightarrow K_Q\phi$.

If $\mathcal{M} \ni P$ is a finite context and $\vdash c_{\mathcal{M}} \wedge c_P \rightarrow K_0\phi$ then $\vdash c_{\mathcal{M}} \rightarrow \phi$.

Axiom E4.4 states the equivalence between *to be active* and *to know* for the epistemic agents. Indeed $\mathcal{M}, Q \models K_P\top$ means exactly $P$ is an active subsystem of $Q$ and nothing more. The same can be expressed by $\mathcal{M}, Q \models c_P|\top$.

Axiom E4.4 is the classical (K)-axiom stating that our epistemic operator is a normal one. This is an expected axiom as all the epistemic logics have it.

The same remark on axiom E4.4 which is just the axiom (T) - necessity axiom, for the epistemic operator.

Also axiom E4.4 is well known in epistemic logics. It states that our epistemic agents satisfy *the positive introspection property*, i.e. if $P$ knows something then it knows that it knows that thing.

Axiom E4.4 states a variant of the *negative introspection*, saying that if an agent $P$ is active and if it doesn't know $\phi$, then it knows that it doesn't know $\phi$. The novelty in our axiom is the precondition $K_P\top$ of the negative introspection. This precondition guarantees that the agent really exists, i.e. it is active. Such a precondition does not appear in the other epistemic logics for the reason that, in those cases, the agents exists always and they knows, always, at least the tautologies.

Axiom E4.4 provides a full description of the $K_Q$ operator by means of $K_0$ and $K_Q\top$. As, by axiom E4.4, $K_Q\top$ can be expressed by the epistemic operators, our system might be reduced to one epistemic operator only, $K_0$. We leave for future work the analysis of minimality for our axiomatic system. For the moment we consider it interesting to have all these epistemic operators that provide links with the rest of epistemic logics.

Axioms E4.4, E4.4 and E4.4 present $K_0\phi$ as a syntactic encryption of validity, stating that once $K_0\phi$ can be stated for a real system, it will be propagated to all the levels of it.

Rule $E_R$4.4 states that any active agent knows all the tautologies. As in the case of the negative introspection, we deal with a well known epistemic rule, widely spread in epistemic logics, but our rules work under the assumption that the agent is active.

Also rule $E_R4.4$ depicts the fact that $K_0\phi$ is an encoding of the validity in a given context.

## 4.5 The soundness of $\mathcal{L}^{\mathfrak{S}}_{DES}$ against the process semantics

In this section we will motivate the choice of the axioms by proving the soundness of our system with respect to process semantics. In this way we will prove that everything expressed by our axioms and rules about the process semantics is correct and, in conclusion, using our system, we can derive only theorems that can be meaningfully interpreted.

[Process-Soundness] The system $\mathcal{L}^{\mathfrak{S}}_{DES}$ is sound against the process semantics.

**Proof** The soundness of $\mathcal{L}^{\mathfrak{S}}_{DES}$ will be sustained by the soundness of all spatial, dynamic and epistemic axioms and rules. □

### Soundness of the spatial axioms and rules

We start with proving the soundness of the spatial axioms and rules.

[Soundness of axiom E4.4] $\models \top|\bot \rightarrow \bot$

**Proof** Suppose that it exists a context $\mathcal{M}$ and a process $P \in \mathcal{M}$ such that $\mathcal{M}, P \models \top|\bot$. Then $P \equiv Q|R$ with $\mathcal{M}, Q \models \top$ and $\mathcal{M}, R \models \bot$; i.e. $\mathcal{M}, R \not\models \top$. But this is not possible. Hence, there is no context $\mathcal{M}$ and process $P \in \mathcal{M}$ such that $\mathcal{M}, P \models \top|\bot$, i.e. for any context $\mathcal{M}$ and any process $P \in \mathcal{M}$ we have $\mathcal{M}, P \models \neg(\top|\bot)$, i.e. $\mathcal{M}, P \models \top|\bot \rightarrow \bot$. □

[Soundness of axiom E4.4] $\models \phi|0 \leftrightarrow \phi$.

**Proof** $\mathcal{M}, P \models \phi|0$ iff $P \equiv Q|R$, $\mathcal{M}, Q \models \phi$ and $\mathcal{M}, R \models 0$. Then $R \equiv 0$, so $P \equiv Q$, hence $\mathcal{M}, P \models \phi$.
If $\mathcal{M}, P \models \phi$, because $\mathcal{M}, 0 \models 0$ and $P \equiv P|0 \in \mathcal{M}$ we obtain that $\mathcal{M}, P \models \phi|0$. □

[Soundness of axiom E4.4] $\models \phi|\psi \rightarrow \psi|\phi$.

**Proof** $\mathcal{M}, P \models \phi|\psi$ means that $P \equiv Q|R$, $\mathcal{M}, Q \models \phi$ and $\mathcal{M}, R \models \psi$. But $P \equiv R|Q \in \mathcal{M}$, hence $\mathcal{M}, P \models \psi|\phi$. □

[Soundness of axiom E4.4] $\models (\phi|\psi)|\rho \rightarrow \phi|(\psi|\rho)$.

**Proof** $\mathcal{M}, P \models (\phi|\psi)|\rho$ implies that $P \equiv Q|R$, $\mathcal{M}, Q \models \phi|\psi$ and $\mathcal{M}, R \models \rho$. Then $Q \equiv S|V$ with $\mathcal{M}, S \models \phi$ and $\mathcal{M}, V \models \psi$. But $P \equiv (S|V)|R \equiv S|(V|R)$, where $\mathcal{M}, S \models \phi$ and $\mathcal{M}, V|R \models \psi|\rho$. Hence $\mathcal{M}, P \models \phi|(\psi|\rho)$. □

[Soundness of axiom E4.4] $\models \phi|(\psi \vee \rho) \rightarrow (\phi|\psi) \vee (\phi|\rho)$

**Proof** $\mathcal{M}, P \models \phi|(\psi \vee \rho)$ means that $P \equiv Q|R$, $\mathcal{M}, P \models \phi$ and $\mathcal{M}, R \models \psi \vee \rho$, i.e. $\mathcal{M}, R \models \psi$ or $\mathcal{M}, R \models \rho$. Hence $\mathcal{M}, P \models \phi|\psi$ or $\mathcal{M}, P \models \phi|\rho$. So $\mathcal{M}, P \models (\phi|\psi) \vee (\phi|\rho)$. □

On this point we have enough information to prove two expected results: first that $c_P$ is, indeed, satisfied by the process $P$ and second, that the formula $c_P$ is satisfied by the whole $\equiv$-equivalence class of $P$. These results will be useful in proving the rest of the soundness lemmas.

If $P \in \mathcal{M}$, then $\mathcal{M}, P \models c_P$.

**Proof** We prove it by induction on the structure of the process $P$.
**The case** $P \equiv 0$**:** $\mathcal{M}, 0 \models c_0$, because $0 \in \mathcal{M}$, $c_0 = 0$ and $\mathcal{M}, 0 \models 0$.
**The case** $P \equiv Q|R$**:** we have $Q, R \in \mathcal{M}$ and $c_P = c_Q|c_R$. By the inductive hypothesis $\mathcal{M}, Q \models c_Q$ and $\mathcal{M}, R \models c_R$, so $\mathcal{M}, Q|R \models c_Q|c_R$. Hence $\mathcal{M}, P \models c_P$.
**The case** $P \equiv \alpha.Q$**:** we have $P \xrightarrow{\alpha} Q$, hence $Q \in \mathcal{M}$. Moreover, $c_P = \langle\alpha\rangle c_Q \wedge 1$. By the inductive hypothesis $\mathcal{M}, Q \models c_Q$. Because $P \xrightarrow{\alpha} Q$, we obtain $\mathcal{M}, P \models \langle\alpha\rangle c_Q$, and because $P \equiv \alpha.Q$ is a guarded process, we have also $\mathcal{M}, P \models 1$. Hence $\mathcal{M}, P \models c_P$. □

$\mathcal{M}, P \models c_Q$ iff $P \equiv Q$.

**Proof** ($\Leftarrow$) We prove it by verifying that $\mathcal{M}, P \models c_Q$ for any $P, Q$ involved in the equivalence rules.

- if $P = R|S$ and $Q = S|R$, we have $\mathcal{M}, R|S \models c_R|c_S$ and using the soundness of axiom E4.4, we obtain $\mathcal{M}, R|S \models c_S|c_R$, i.e. $\mathcal{M}, P \models c_Q$
- if $P = (R|S)|U$ and $Q = R|(S|U)$ we have $\mathcal{M}, P \models (c_R|c_S)|c_U$. Using the soundness of axiom E4.4, we obtain $\mathcal{M}, P \models c_Q$. Similarly $\mathcal{M}, Q \models c_P$, using the soundness of axioms E4.4 and E4.4.
- if $P = Q|0$ then $\mathcal{M}, P \models c_Q|0$, i.e., by using the soundness of axiom E4.4, $\mathcal{M}, P \models c_Q$. Similarly reverse, form $\mathcal{M}, Q \models c_Q$ we derive, by using the soundness of axiom E4.4, $\mathcal{M}, Q \models c_Q|0$, i.e. $\mathcal{M}, Q \models c_P$.
- if $P = P'|R$ and $Q = Q'|R$ with $P' \equiv Q'$ and $\mathcal{M}, P' \models c_{Q'}$, because $\mathcal{M}, R \models c_R$, we obtain that $\mathcal{M}, P \models c_{Q'}|c_R$, i.e. $\mathcal{M}, P \models c_Q$.
- if $P = \alpha.P'$ and $Q = \alpha.Q'$ with $P' \equiv Q'$ and $\mathcal{M}, P' \models c_{Q'}$, as $P \xrightarrow{\alpha} P'$, then $\mathcal{M}, P \models \langle\alpha\rangle c_{Q'}$. But $\mathcal{M}, P \models 1$, because $P$ is a guarded process, hence $\mathcal{M}, P \models \langle\alpha\rangle c_{Q'} \wedge 1$, i.e. $\mathcal{M}, P \models c_Q$.

($\Rightarrow$) We prove the implication in this sense by induction on the structure of $Q$.

- if $Q \equiv 0$, then $\mathcal{M}, P \models c_0$, means $\mathcal{M}, P \models 0$. Hence $P \equiv 0$.
- if $Q \equiv R|S$ then $\mathcal{M}, P \models c_Q$ is equivalent with $\mathcal{M}, P \models c_R|c_S$. So $P \equiv U|V$, $\mathcal{M}, U \models c_R$ and $\mathcal{M}, V \models c_S$. By the inductive hypothesis we obtain that $U \equiv R$ and $V \equiv S$. Hence $P \equiv Q$.
- if $Q \equiv \alpha.R$, then $\mathcal{M}, P \models c_Q$ is equivalent with $\mathcal{M}, P \models \langle\alpha\rangle c_R \wedge 1$. So $P \xrightarrow{\alpha} P'$ with $\mathcal{M}, P' \models c_R$. By the inductive hypothesis, $P' \equiv R$. And because $\mathcal{M}, P \models 1$ we obtain that $P \equiv \alpha.R$, i.e. $P \equiv Q$.

□

[Soundness of axiom E4.4] $\models (c_P \wedge \phi|\psi) \rightarrow \bigvee_{P\equiv Q|R}(c_Q \wedge \phi)|(c_R \wedge \psi)$

**Proof** Suppose that $\mathcal{M}, S \models c_P \wedge \phi|\psi$. Then $S \equiv P$ (by theorem 4.5) and $S \equiv S_1|S_2$ with $\mathcal{M}, S_1 \models \phi$ and $\mathcal{M}, S_2 \models \psi$.
But $\mathcal{M}, S_1 \models c_{S_1}$ and $\mathcal{M}, S_2 \models c_{S_2}$, by theorem 4.5.
Hence $\mathcal{M}, S_1 \models \phi \wedge c_{S_1}$ and $\mathcal{M}, S_2 \models \psi \wedge c_{S_2}$.
And because $P \equiv S \equiv S_1|S_2$, we obtain $\mathcal{M}, P \models (\phi \wedge c_{S_1})|(\psi \wedge c_{S_2})$, hence $\mathcal{M}, P \models \bigvee_{P\equiv Q|R}(c_Q \wedge \phi)|(c_R \wedge \psi)$, q.e.d. □

[Soundness of rule E$_R$4.4] If $\models \phi \rightarrow \psi$ then $\models \phi|\rho \rightarrow \psi|\rho$

**Proof** If $\mathcal{M}, P \models \phi|\rho$ then $P \equiv Q|R$, $\mathcal{M}, Q \models \phi$ and $\mathcal{M}, R \models \rho$. But from the hypothesis, $\mathcal{M}, Q \models \phi \rightarrow \psi$, hence $\mathcal{M}, Q \models \psi$. Then $\mathcal{M}, P \models \psi|\rho$, so $\models \phi|\rho \rightarrow \psi|\rho$. □

## Soundness of the dynamic axioms and rules

We prove now the soundness for the class of dynamic axioms and rules.

[Soundness of axiom E4.4] $\models \langle\alpha\rangle\phi|\psi \rightarrow \langle\alpha\rangle(\phi|\psi)$.

**Proof** If $\mathcal{M}, P \models \langle\alpha\rangle\phi|\psi$, then $P \equiv R|S$, $\mathcal{M}, R \models \langle\alpha\rangle\phi$ and $\mathcal{M}, S \models \psi$. So $\exists R \xrightarrow{\alpha} R'$ and $\mathcal{M}, R' \models \phi$. So $\exists P \equiv R|S \xrightarrow{\alpha} P' \equiv R'|S$ and $\mathcal{M}, P' \models \phi|\psi$. Hence $\mathcal{M}, P \models \langle\alpha\rangle(\phi|\psi)$. □

[Soundness of axiom E4.4] $\models [\alpha](\phi \rightarrow \psi) \rightarrow ([\alpha]\phi \rightarrow [\alpha]\psi)$

**Proof** Let $\mathcal{M}, P \models [\alpha](\phi \rightarrow \psi)$ and $\mathcal{M}, P \models [\alpha]\phi$. If there is no $P'$ such that $P \xrightarrow{\alpha} P'$, then $\mathcal{M}, P \models [\alpha]\psi$. Suppose that exists such $P'$. Then for any such $P'$ we have $\mathcal{M}, P' \models \phi \rightarrow \psi$ and $\mathcal{M}, P' \models \phi$. Hence $\mathcal{M}, P' \models \psi$, i.e. $\mathcal{M}, P \models [\alpha]\psi$. □

[Soundness of axiom E4.4] $\models 0 \rightarrow [\alpha]\bot$

**Proof** If $\mathcal{M}, P \models 0$ then $P \equiv 0$ and there is no transition $0 \xrightarrow{\alpha} P'$, hence $\mathcal{M}, P \not\models \langle\alpha\rangle\top$, i.e. $\mathcal{M}, P \models [\alpha]\bot$. □

[Soundness of axiom E4.4]

$$\text{If } \beta \neq \alpha_i \text{ for } i = 1..n, \text{ then } \models \langle!\alpha_1\rangle\top|...|\langle!\alpha_n\rangle\top \rightarrow [\beta]\bot$$

**Proof** Suppose that $\mathcal{M}, P \models \langle!\alpha_1\rangle\top|...|\langle!\alpha_n\rangle\top$. Then necessarily $P \equiv \alpha_1.P_1|...|\alpha_n.P_n$. But if $\alpha_i \neq \beta$ for $i = 1..n$, there is no transition

$$\alpha_1.P_1|...|\alpha_n.P_n \xrightarrow{\beta} P'$$

hence $\mathcal{M}, P \not\models \langle\beta\rangle\top$, i.e. $\mathcal{M}, P \models [\beta]\bot$. □

[Soundness of axiom E4.4] $\models \langle !\alpha\rangle\phi \rightarrow [\alpha]\phi$

**Proof** Suppose that $\mathcal{M}, P \models \langle !\alpha\rangle\phi$, then $\mathcal{M}, P \models 1$ and $\mathcal{M}, P \models \langle\alpha\rangle\phi$. Then necessarily $P \equiv \alpha.P'$ and $\mathcal{M}, P' \models \phi$. But there is only one reduction that $P$ can do, $P \xrightarrow{\alpha} P'$. So, for any reduction $P \xrightarrow{\alpha} P''$ (because there is only one), we have $\mathcal{M}, P'' \models \phi$, i.e. $\mathcal{M}, P \models [\alpha]\phi$ □

[Soundness of rule $E_R$4.4] If $\models \phi$ then $\models [\alpha]\phi$.

**Proof** Let $\mathcal{M}$ be a context and $P \in \mathcal{M}$ a process. If there is no $P'$ such that $P \xrightarrow{\alpha} P'$, then $\mathcal{M}, P \models [\alpha]\phi$. Suppose that exists such $P'$ (obviously $P' \in \mathcal{M}$). Then for any such $P'$ we have $\mathcal{M}, P' \models \phi$, due to the hypothesis $\models \phi$. Hence $\mathcal{M}, P \models [\alpha]\phi$. □

[Soundness of rule $E_R$4.4]

$$\text{If } \models \phi \rightarrow [\alpha]\phi' \text{ and } \models \psi \rightarrow [\alpha]\psi' \text{ then } \models \phi|\psi \rightarrow [\alpha](\phi'|\psi \vee \phi|\psi')$$

**Proof** Suppose that $\mathcal{M}, P \models \phi|\psi$, then $P \equiv Q|R$, $\mathcal{M}, Q \models \phi$ and $\mathcal{M}, R \models \psi$. Because $\models \phi \rightarrow [\alpha]\phi'$ and $\models \psi \rightarrow [\alpha]\psi'$, we derive $\mathcal{M}, Q \models [\alpha]\phi'$ and $\mathcal{M}, R \models [\alpha]\psi'$. We analyze some cases:

- if $P$ cannot perform a transition by $\alpha$, then $\mathcal{M}, P \models [\alpha]\bot$, and using the soundness of axiom E4.4 and rule $E_R$4.4 we derive

  $$\models [\alpha]\bot \rightarrow [\alpha](\phi'|\psi \vee \phi|\psi')$$

  hence, we obtain in the end $\mathcal{M}, P \models [\alpha](\phi'|\psi \vee \phi|\psi')$.

- if $Q \overset{\alpha}{\textbf{to}} Q'$ and $R$ cannot perform a transition by $\alpha$, then $Q|R \overset{\alpha}{\textbf{to}} Q'|R$ and the transitions of $P \equiv Q|R$ by $\alpha$ have always this form.
  But $\mathcal{M}, Q \models [\alpha]\phi'$, so for any such $Q'$ we have $\mathcal{M}, Q' \models \phi'$, thus $\mathcal{M}, Q'|R \models \phi'|\psi$, i.e. $\mathcal{M}, Q'|R \models (\phi'|\psi \vee \phi|\psi')$.
  Hence for any transition $P \overset{\alpha}{\textbf{to}} P'$ we have $\mathcal{M}, P' \models (\phi'|\psi \vee \phi|\psi')$. In conclusion, $\mathcal{M}, P \models [\alpha](\phi'|\psi \vee \phi|\psi')$.

- if $Q$ cannot perform a transition by $\alpha$ and $R \overset{\alpha}{\textbf{to}} R'$, similarly as in the previous case, we can derive $\mathcal{M}, P \models [\alpha](\phi'|\psi \vee \phi|\psi')$.

- if $Q \overset{\alpha}{\textbf{to}} Q'$ and $R \overset{\alpha}{\textbf{to}} R'$ then $P \overset{\alpha}{\textbf{to}} P'$ has either the form $Q|R \overset{\alpha}{\textbf{to}} Q'|R$ or $Q|R \overset{\alpha}{\textbf{to}} Q|R'$. But $\mathcal{M}, Q'|R \models \phi'|\psi$, hence $\mathcal{M}, Q'|R \models (\phi'|\psi \vee \phi|\psi')$ and $\mathcal{M}, Q|R' \models \phi|\psi'$, hence $\mathcal{M}, Q|R' \models (\phi'|\psi \vee \phi|\psi')$.
  Thus, for any transition $P \overset{\alpha}{\textbf{to}} P'$ we have $\mathcal{M}, P' \models (\phi'|\psi \vee \phi|\psi')$, i.e. $\mathcal{M}, P \models [\alpha](\phi'|\psi \vee \phi|\psi')$.

So, in any case $\mathcal{M}, P \models [\alpha](\phi'|\psi \vee \phi|\psi')$, that concludes the proof. □

[Soundness of rule $E_R$4.4] If $\models \bigvee_{\mathcal{M} \in \mathfrak{M}_\phi^{act(\phi)_+}} c_{\mathcal{M}} \rightarrow \phi$ then $\models \phi$.

**Proof** Suppose that $\models \bigvee_{\mathcal{M}\in\mathfrak{M}_\phi^{act(\phi)_+}} c_\mathcal{M} \rightarrow \phi$ but it exists a model $\mathcal{N}$ and a process $Q \in \mathcal{N}$ with $\mathcal{N}, Q \not\models \phi$. Then $\mathcal{N}, Q \models \neg\phi$.
Further, using the finite model property, theorem 4.3, we obtain that it exists a context $\mathcal{N}' \in \mathfrak{M}_\phi^{act(\phi)+}$ and a process $R \in \mathcal{N}'$ with $\mathcal{N}', R \models \neg\phi$.
But $\phi = \neg\phi$, and $act(\phi) = act(\neg\phi)$ so it exists a context $\mathcal{N}' \in \mathfrak{M}_\phi^{act(\phi)_+}$ and a process $R \in \mathcal{N}'$ with $\mathcal{N}', R \models \neg\phi$. Because $\mathcal{N}', R \models c_{\mathcal{N}'}$, we derive $\mathcal{N}', R \models \bigvee_{\mathcal{M}\in\mathfrak{M}_\phi^{act(\phi)_+}} c_\mathcal{M}$.
But $\models \bigvee_{\mathcal{M}\in\mathfrak{M}_\phi^{act(\phi)_+}} c_\mathcal{M} \rightarrow \phi$ implies $\mathcal{N}', R \models \bigvee_{\mathcal{M}\in\mathfrak{M}_\phi^{act(\phi)_+}} c_\mathcal{M} \rightarrow \phi$, hence $\mathcal{N}', R \models \phi$.
As we also have $\mathcal{N}', R \models \neg\phi$, we obtain $\mathcal{N}', R \models \bot$ - impossible!
Then, for any model $\mathcal{N}$ and any process $P \in \mathcal{N}$ we have $\mathcal{N}, P \models \phi$, i.e. $\models \phi$.

□

## Soundness of the epistemic axioms and rules

Hereafter we prove the soundness for the epistemic axioms and rules.

[Soundness of axiom E4.4] If $Q \in \mathfrak{S}$ then $\models c_Q|\top \leftrightarrow K_Q\top$

**Proof** If $\mathcal{M}, P \models c_Q|\top$ then $P \equiv R|S$, with $\mathcal{M}, S \models c_Q$. Then theorem 4.6 gives $S \equiv Q$, hence $P \equiv Q|R$. And because for any $Q|R' \in \mathcal{M}$ we have $\mathcal{M}, Q|R' \models \top$, we derive $\mathcal{M}, P \models K_Q\top$.
Suppose now the reverse, i.e. that $\mathcal{M}, P \models K_Q\top$. Then $P \equiv Q|R$. But $\mathcal{M}, P \models c_P$, hence $\mathcal{M}, P \models c_Q|c_R$.
Because $\models c_Q \rightarrow \top$, using the soundness of rule $E_R$4.4, we derive $\models c_Q|c_R \rightarrow c_Q|\top$ from where we conclude that $\mathcal{M}, P \models c_Q|\top$. □

[Soundness of axiom E4.4] $\models K_Q\phi \wedge K_Q(\phi \rightarrow \psi) \rightarrow K_Q\psi$

**Proof** Suppose that $\mathcal{M}, P \models K_Q\phi$ and that $\mathcal{M}, P \models K_Q(\phi \rightarrow \psi)$. Then $P \equiv Q|R$ and for any $S$ such that $S|Q \in \mathcal{M}$ we have $\mathcal{M}, S|Q \models \phi$ and $\mathcal{M}, Q|S \models \phi \rightarrow \psi$. Hence for any such $Q|S$ we have $\mathcal{M}, Q|S \models \psi$ and because $P \equiv Q|R$ we obtain that $\mathcal{M}, P \models K_Q\psi$. □

[Soundness of axiom E4.4] $\models K_Q\phi \rightarrow \phi$.

**Proof** If $\mathcal{M}, P \models K_Q\phi$ then $P \equiv Q|R$ and for any $Q|S \in \mathcal{M}$ we have $\mathcal{M}, Q|S \models \phi$, i.e. $\mathcal{M}, Q|R \models \phi$, so $\mathcal{M}, P \models \phi$. □

[Soundness of axiom E4.4] $\models K_Q\phi \rightarrow K_QK_Q\phi$.

**Proof** Suppose that $\mathcal{M}, P \models K_Q\phi$, then $P \equiv Q|R$ and for any $Q|S \in \mathcal{M}$ we have $\mathcal{M}, Q|S \models \phi$. Let $Q|S' \in \mathcal{M}$ be arbitrarily chosen. As for any $Q|S \in \mathcal{M}$ we have $\mathcal{M}, Q|S \models \phi$, we derive that $\mathcal{M}, Q|S' \models K_Q\phi$. But $Q|S'$ has been arbitrarily chosen, so for any $Q|S \in \mathcal{M}$ we have $\mathcal{M}, Q|S \models K_Q\phi$, and because $P \equiv Q|R$ we obtain $\mathcal{M}, P \models K_QK_Q\phi$. □

[Soundness of axiom E4.4] $\models K_Q\top \rightarrow (\neg K_Q\phi \rightarrow K_Q\neg K_Q\phi)$

**Proof** Suppose that $\mathcal{M}, P \models K_Q\top$ and $\mathcal{M}, P \models \neg K_Q\phi$. Then $P \equiv Q|R$ and $\exists S$ such that $\mathcal{M}, S|Q \models \neg\phi$. But then for any $U$ such that $U|Q \in \mathcal{M}$ we have $\mathcal{M}, U|Q \models \neg K_Q\phi$. Hence $\mathcal{M}, P \models K_Q\neg K_Q\phi$. □

[Soundness of axiom E4.4] $\models K_Q\phi \leftrightarrow (K_Q\top \wedge K_0(K_Q\top \rightarrow \phi))$

**Proof** Suppose that $\mathcal{M}, P \models K_Q\phi$. Then $P \equiv Q|R$ and for any $Q|S \in \mathcal{M}$ we have $\mathcal{M}, Q|S \models \phi$. From $P \equiv Q|R$, because for any $Q|S \in \mathcal{M}$ we have $\mathcal{M}, Q|S \models \top$, we derive $\mathcal{M}, P \models K_Q\top$. Consider now an arbitrary process $S \in \mathcal{M}$. If $\mathcal{M}, S \not\models K_Q\top$, then $\mathcal{M}, S \models K_Q\top \rightarrow \phi$.
If $\mathcal{M}, S \models K_Q\top$ we derive that $S \equiv Q|S'$, hence $\mathcal{M}, S \models \phi$.
So, for an arbitrarily chosen $S \in \mathcal{M}$ we have $\mathcal{M}, S \models K_Q\top \rightarrow \phi$.
Because $P \equiv P|0$ and for any process $S \equiv S|0 \in \mathcal{M}$ we have
$\mathcal{M}, S \models K_Q\top \rightarrow \phi$, we derive that $\mathcal{M}, P \models K_0(K_Q\top \rightarrow \phi)$. Hence $\models K_Q\phi \rightarrow (K_Q\top \wedge K_0(K_Q\top \rightarrow \phi))$.

Suppose now that $\mathcal{M}, P \models K_Q\top \wedge K_0(K_Q\top \rightarrow \phi)$. From $\mathcal{M}, P \models K_Q\top$ we derive $P \equiv Q|R$. Because $\mathcal{M}, P \models K_0(K_Q\top \rightarrow \phi)$, we obtain that for any process $S \in \mathcal{M}$ we have $\mathcal{M}, S \models K_Q\top \rightarrow \phi$. Hence, for any process $S|Q \in \mathcal{M}$ we have $\mathcal{M}, S|Q \models \phi$ (because $\mathcal{M}, S|Q \models K_Q\top$). And because $P \equiv Q|R$, we derive $\mathcal{M}, P \models K_Q\phi$. □

[Soundness of axiom E4.4] $\models K_0\phi \wedge \psi|\rho \rightarrow (K_0\phi \wedge \psi)|(K_0\phi \wedge \rho)$

**Proof** Suppose that $\mathcal{M}, P \models K_0\phi \wedge \psi|\rho$ then $\mathcal{M}, P \models K_0\phi$ and $\mathcal{M}, P \models \psi|\rho$.
$\mathcal{M}, P \models K_0\phi$ gives that for any $R \in \mathcal{M}$ we have $\mathcal{M}, R \models \phi$.
$\mathcal{M}, P \models \psi|\rho$ gives that $P \equiv P'|P''$ and $\mathcal{M}, P' \models \psi$, $\mathcal{M}, P'' \models \rho$. Because $P', P'' \in \mathcal{M}$ and because for any $R \in \mathcal{M}$, $\mathcal{M}, R \models \phi$ we derive that $\mathcal{M}, P' \models K_0\phi$ and $\mathcal{M}, P'' \models K_0\phi$.
Hence $\mathcal{M}, P' \models \psi \wedge K_0\phi$ and $\mathcal{M}, P'' \models \rho \wedge K_0\phi$. As $P \equiv P'|P''$, we obtain further $\mathcal{M}, P \models (K_0\phi \wedge \psi)|(K_0\phi \wedge \rho)$. □

[Soundness of axiom E4.4] $\models K_0\phi \rightarrow [\alpha]K_0\phi$

**Proof** Suppose that $\mathcal{M}, P \models K_0\phi$, then for any $R \in \mathcal{M}$ we have
$\mathcal{M}, R \models \phi$.
If $P$ cannot perform a transition by $\alpha$, we have $\mathcal{M}, P \models [\alpha]K_0\phi$.
If $P$ can perform such transitions, then for any $P \overset{\alpha}{\textbf{to}} P'$ we have
$\mathcal{M}, P' \models K_0\phi$ (as for any $R \in \mathcal{M}$ we have $\mathcal{M}, R \models \phi$). This means $\mathcal{M}, P \models [\alpha]K_0\phi$. □

[Soundness of axiom E4.4] $\models K_0\phi \rightarrow (K_Q\top \rightarrow K_QK_0\phi)$

**Proof** Suppose that $\mathcal{M}, P \models K_0\phi$ and $\mathcal{M}, P \models K_Q\top$.
$\mathcal{M}, P \models K_0\phi$ gives that for any $R \in \mathcal{M}$ we have $\mathcal{M}, R \models \phi$.
$\mathcal{M}, P \models K_Q\top$ means that $P \equiv Q|S$. Because for any $R \in \mathcal{M}$ we have $\mathcal{M}, R \models \phi$, we obtain that for any $Q|S' \in \mathcal{M}$ we have $\mathcal{M}, Q|S' \models K_0\phi$, and because $P \equiv Q|S$ we obtain $\mathcal{M}, P \models K_QK_0\phi$. □

[Soundness of rule $E_R$4.4] If $\models \phi$ then $\models K_Q\top \rightarrow K_Q\phi$

**Proof** If $\models \phi$ then for any context $\mathcal{M}$ and any process $P \in \mathcal{M}$ we have $\mathcal{M}, P \models \phi$. Suppose now that $\mathcal{M}, P \models K_Q\top$. Then $P \equiv Q|R$. Because $\mathcal{M}, S \models \phi$ for each $S \in \mathcal{M}$, we derive that for any $S|Q \in \mathcal{M}$ we have $\mathcal{M}, S|Q \models \phi$. Hence $\mathcal{M}, P \models K_Q\phi$. □

[Soundness of rule E$_R$4.4]

$$\text{If } \mathcal{M} \ni P \text{ is a finite context and } \models c_{\mathcal{M}} \wedge c_P \rightarrow K_0\phi \text{ then } \models c_M \rightarrow \phi$$

**Proof** Suppose that $\models c_{\mathcal{M}} \wedge c_P \rightarrow K_0\phi$ and $\mathcal{N}$ is an arbitrary context with $Q \in \mathcal{N}$.
If $\mathcal{N}, Q \not\models c_{\mathcal{M}}$ then $\mathcal{N}, Q \models c_{\mathcal{M}} \rightarrow \phi$.
If $\mathcal{N}, Q \models c_{\mathcal{M}}$, then $\mathcal{N} = \mathcal{M}$. Further $\mathcal{M}, P \models c_P \wedge c_{\mathcal{M}}$ gives $\mathcal{M}, P \models K_0\phi$, i.e. for each $S|0 \equiv S \in \mathcal{M}$ we have $\mathcal{M}, S \models \phi$. Now, because $\mathcal{N} = \mathcal{M}$ and $Q \in \mathcal{M}$ we obtain $\mathcal{N}, Q \models \phi$. Hence, also in this case $\mathcal{N}, Q \models c_M \rightarrow \phi$. Thus $\models c_{\mathcal{M}} \rightarrow \phi$. □

Hence we have a sound system and all the theorems that can be proved with it are sound results with respect to process semantics.

## 4.6 Characteristic formulas

In this subsection we use the peculiarities of the dynamic and epistemic operators to prove that the characteristic formulas for processes and for finite contexts introduced before can identify the processes and the finite contexts respectively.

We begin by restating some relevant results, proved before, in order to offer to the reader a full picture of the problem.

$\mathcal{M}, P \models c_P$.

**Proof** It has been proved as theorem 4.5. □

$\mathcal{M}, P \models c_Q$ iff $P \equiv Q$.

**Proof** It has been proved as theorem 4.5. □

The next theorems show that $c_P$ could provide a syntactic characterization of the process $P$, stating that the conjunction of two such formulas, $c_P$ and $c_Q$, is inconsistent if the indexes are not structurally congruent, and respectively that two structurally congruent indexes generate logical equivalent formulas.

If $P \not\equiv Q$ then $\vdash c_P \rightarrow \neg c_Q$.

**Proof** We prove it by induction on $P$.

- **the case** $P \equiv 0$**:** as $P \not\equiv Q$ we obtain that $Q \equiv \alpha.R|S$. So $c_Q = \langle\alpha\rangle c_R \wedge 1|c_S$ that implies, using theorem 4.7, $\vdash c_Q \rightarrow \langle\alpha\rangle c_R|c_S$, and applying axiom E4.4, $\vdash c_Q \rightarrow \langle\alpha\rangle(c_R|c_S)$.
  But $\vdash c_R|c_S \rightarrow \top$ and applying theorem 4.8, we obtain
  $\vdash \langle\alpha\rangle(c_R|c_S) \rightarrow \langle\alpha\rangle\top$.
  Hence, $\vdash c_Q \rightarrow \langle\alpha\rangle\top$. Then $\vdash \neg\langle\alpha\rangle\top \rightarrow \neg c_Q$.
  Axiom E4.4 gives $\vdash 0 \rightarrow \neg\langle\alpha\rangle\top$ hence, in the end, $\vdash 0 \rightarrow \neg c_Q$, i.e. $\vdash c_P \rightarrow \neg c_Q$.

- **the case** $P \equiv P'|P''$**:** we have $c_P = c_{P'}|c_{P''}$. Because $P \not\equiv Q$, we obtain that for any decomposition $Q \equiv Q'|Q''$ we have either $P' \not\equiv Q'$ or $P'' \not\equiv Q''$. Using the inductive hypothesis, we derive that either $\vdash c_{Q'} \rightarrow \neg c_{P'}$ or $\vdash c_{Q''} \rightarrow \neg c_{P''}$. Because this is happening for any decomposition of $Q$, we can apply theorem 4.7 and we obtain
$\vdash c_Q \rightarrow \neg(c_{P'}|c_{P''})$, i.e. $\vdash c_Q \rightarrow \neg c_P$. Hence $\vdash c_P \rightarrow \neg c_Q$.

- **the case** $P \equiv \alpha.P'$**:** $c_P = 1 \wedge \langle\alpha\rangle c_{P'}$, so $\vdash c_P \rightarrow 1 \wedge \langle\alpha\rangle\top$.
But axiom E4.4 gives $\vdash \langle\alpha\rangle\top \wedge 1 \rightarrow \neg\langle\beta\rangle\top$ for any $\beta \neq \alpha$.
Hence, for any $\beta \neq \alpha$ we have $\vdash c_P \rightarrow \neg\langle\beta\rangle\top$.

  - if $Q \equiv 0$ we already proved that $\vdash c_Q \rightarrow \neg c_P$ (because $P \not\equiv 0$), so $\vdash c_P \rightarrow \neg c_Q$
  - if $Q \equiv \beta.Q'|Q''$ for some $\beta \neq \alpha$, then $\vdash c_Q \rightarrow \langle\beta\rangle\top$, hence $\vdash \neg\langle\beta\rangle\top \rightarrow \neg c_Q$. But we proved that $\vdash c_P \rightarrow \neg\langle\beta\rangle\top$. Hence $\vdash c_P \rightarrow \neg c_Q$.
  - if $Q \equiv \alpha.Q_1|...|\alpha.Q_k$ for $k > 1$, then $\vdash c_Q \rightarrow \neg 0|\neg 0$ (as $\vdash 0 \rightarrow \neg c_{\alpha.Q_1}$ and $\vdash 0 \rightarrow \neg c_{\alpha.Q_2|...|\alpha.Q_k}$). Then $\vdash c_Q \rightarrow \neg 1$, i.e.
$\vdash 1 \rightarrow \neg c_Q$. But $\vdash c_P \rightarrow 1$. Hence $\vdash c_P \rightarrow \neg c_Q$.
  - if $Q \equiv \alpha Q'$: then $P \not\equiv Q$ gives $P' \not\equiv Q'$. For this case we can use the inductive hypothesis and we obtain $\vdash c_{Q'} \rightarrow \neg c_{P'}$. Further, applying theorem 4.8, we obtain $\vdash [\alpha]c_{P'} \rightarrow [\alpha]\neg c'_Q$, i.e.
$\vdash [\alpha]c_{P'} \rightarrow \neg\langle\alpha\rangle c_{Q'}$ that gives, because $c_Q = 1 \wedge \langle\alpha\rangle c_{Q'}$,
$\vdash [\alpha]c_{P'} \rightarrow \neg c_Q$.
Now, using axiom E4.4, $\vdash 1 \wedge \langle\alpha\rangle c_{P'} \rightarrow [\alpha]c_{P'}$, so $\vdash c_P \rightarrow [\alpha]c_{P'}$, and, combining it with the previous result, we derive $\vdash c_P \rightarrow \neg c_Q$.

□

If $P \equiv Q$ then $\vdash c_P \leftrightarrow c_Q$.
**Proof** We prove it verifying the congruence rules:

- if $P = R|S$ and $Q = S|R$ then $\vdash c_R|c_S \leftrightarrow c_S|c_R$ from theorem 4.7, i.e. $\vdash c_P \leftrightarrow c_Q$

- if $P = (R|S)|U$ and $Q = R|(S|U)$ then theorem 4.7 we have
$\vdash (c_R|c_S)|c_U \leftrightarrow c_R|(c_S|c_U)$, i.e. $\vdash c_P \leftrightarrow c_Q$

- if $P = Q|0$ then axiom E4.4 gives $\vdash c_Q|0 \leftrightarrow c_Q$, i.e. $\vdash c_P \leftrightarrow c_Q$.

- if $P = P'|R$ and $Q = Q'|R$ with $P' \equiv Q'$ and $\vdash c_{P'} \leftrightarrow c_{Q'}$ then rule E$_R$4.4 gives $\vdash c_{P'}|c_R \leftrightarrow c_{Q'}|c_R$. Hence $\vdash c_P \leftrightarrow c_Q$.

- if $P = \alpha.P'$ and $Q = \alpha.Q'$ with $P' \equiv Q'$ and $\vdash c_{P'} \leftrightarrow c_{Q'}$ then theorem 4.8 gives $\vdash \langle\alpha\rangle c_{P'} \leftrightarrow \langle\alpha\rangle c_{Q'}$, so $\vdash (\langle\alpha\rangle c_{P'} \wedge 1) \leftrightarrow (\langle\alpha\rangle c_{Q'} \wedge 1)$. Hence $\vdash c_P \leftrightarrow c_Q$.

□

We prove now that the intuition behind the definition of characteristic formulas for contexts is correct and, indeed, $c_{\mathcal{M}}$ can be used to characterize $\mathcal{M}$.

If $\mathcal{M}$ is a finite context and $P \in \mathcal{M}$ then $\mathcal{M}, P \models c_{\mathcal{M}}$.

**Proof** Obviously $\mathcal{M}, P \models c_P$, hence $\mathcal{M}, P \models \bigvee_{Q \in \mathcal{M}} c_Q$.
Similarly, for any $R \in \mathcal{M}$ we have $\mathcal{M}, R \models \bigvee_{Q \in \mathcal{M}} c_Q$, and because $R \equiv R|0$ and $P \equiv P|0$, we derive $\mathcal{M}, P \models K_0(\bigvee_{Q \in \mathcal{M}} c_Q)$.
As for any $R \in \mathcal{M}$ there exists a process $U \in \mathcal{M}$ (more exactly $U = R$) such that $\mathcal{M}, U \models c_R$, we obtain that for each $R \in \mathcal{M}$ we have
$\mathcal{M}, P \models \widetilde{K}_0 c_R$, hence $\mathcal{M}, P \models \bigwedge_{Q \in \mathcal{M}} \widetilde{K}_0 c_Q$. □

If $\mathcal{M}$ is a finite context and $P \in \mathcal{M}$ then

$$\mathcal{M}, P \models c_{\mathcal{M}} \wedge c_P$$

If $\mathcal{M}, P \models c_{\mathcal{N}}$ then $\mathcal{N} = \mathcal{M}$.

**Proof** Suppose that $\mathcal{M}, P \models c_{\mathcal{N}}$, then $\mathcal{M}, P \models K_0(\bigvee_{Q \in \mathcal{N}} c_Q)$, i.e. for any $R \in \mathcal{M}$ we have $\mathcal{M}, R \models \bigvee_{Q \in \mathcal{N}} c_Q$. Hence, for any $R \in \mathcal{M}$ there exists a process $Q \in \mathcal{N}$ with $\mathcal{M}, R \models c_Q$, or equivalently, $R \equiv Q$.
Now $\mathcal{M}, P \models \bigwedge_{Q \in \mathcal{N}} \widetilde{K}_0 c_Q$ gives that for any $Q \in \mathcal{N}$ we have
$\mathcal{M}, P \models \widetilde{K}_0 c_Q$, i.e. there exists a process $R \in \mathcal{M}$ such that $\mathcal{M}, R \models c_Q$, or equivalently, $R \equiv Q$.
Hence, we proved that for any $R \in \mathcal{M}$ there exists $Q \in \mathcal{N}$ such that $R \equiv Q$, and for any $Q \in \mathcal{N}$ there exists $R \in \mathcal{M}$ such that $R \equiv Q$. Because we identify processes up to structural congruence, we decide that $M = N$. □

## 4.7 Theorems of $\mathcal{L}_{DES}^{\mathfrak{S}}$

In this section we will derive some theorems for $\mathcal{L}_{DES}^{\mathfrak{S}}$. As, by soundness, the theorems specify *"facts"* about processes, we will try to interpret the nontrivial ones.

### Spatial results

We start with the results that can be proved on the basis of the spatial theorems and rules only. They reflect the behavior of the parallel operator in relation to the operators of the classical logic.

$\vdash \top|\top \leftrightarrow \top$

**Proof** Obviously $\vdash \top|\top \rightarrow \top$. As $\vdash 0 \rightarrow \top$, using rule $\mathrm{E}_R$4.4, we obtain $\vdash \top|0 \rightarrow \top|\top$. Further axiom E4.4 gives us $\vdash \top \rightarrow \top|\top$. □

If $\vdash \phi$ then $\vdash \theta|\rho \rightarrow \phi|\rho$

**Proof** Because $\vdash \phi$ implies $\vdash \theta \rightarrow \phi$, using rule $E_R$4.4 we obtain the result. □

$\vdash \phi|\psi \leftrightarrow \psi|\phi$

**Proof** We use axiom E4.4 in both directions. □

$\vdash (\phi|\psi)|\rho \leftrightarrow \phi|(\psi|\rho)$

**Proof** We use axiom E4.4 and theorem 4.7. □

$\vdash \phi|(\psi \vee \rho) \leftrightarrow (\phi|\psi) \vee (\phi|\rho)$

**Proof** $\vdash \psi \rightarrow \psi \vee \rho$ so, using rule $E_R$4.4, $\vdash \phi|\psi \rightarrow \phi|(\psi \vee \rho)$. Similarly, $\vdash \phi|\rho \rightarrow \phi|(\psi \vee \rho)$. Hence $\vdash (\phi|\psi) \vee (\phi|\rho) \rightarrow \phi|(\psi \vee \rho)$. The other direction is stated by axiom E4.4. □

$\vdash \phi|(\psi \wedge \rho) \rightarrow (\phi|\psi) \wedge (\phi|\rho)$

**Proof** Because $\vdash \psi \wedge \rho \rightarrow \psi$, by applying rule $E_R$4.4, we have $\vdash \phi|(\psi \wedge \rho) \rightarrow \phi|\psi$. Similarly $\vdash \phi|(\psi \wedge \rho) \rightarrow \phi|\rho$. □

The next result proves a strong version of monotonicity of the parallel composition.

If $\vdash \phi \rightarrow \rho$ and $\vdash \psi \rightarrow \theta$ then $\vdash \phi|\psi \rightarrow \rho|\theta$.

**Proof** If $\vdash \phi \rightarrow \rho$ then rule $E_R$4.4 gives us $\vdash \phi|\psi \rightarrow \rho|\psi$. If $\vdash \psi \rightarrow \theta$, then the same rule gives $\vdash \rho|\psi \rightarrow \rho|\theta$. Hence $\vdash \phi|\psi \rightarrow \rho|\theta$. □

The next result speaks about the negative parallel decomposition of a specification. It states that, given two specifications, $\phi$ and $\psi$, if considering any parallel decomposition of our system (process) $P \equiv Q|R$, we obtain that either $Q$ doesn't satisfy $\phi$ or $R$ doesn't satisfy $\psi$, then our system $P$ does not satisfy the parallel composition of the two specifications, $\phi|\psi$.

If for any decomposition $P \equiv Q|R$ we have $\vdash c_Q \rightarrow \neg\phi$ or $\vdash c_R \rightarrow \neg\psi$ then $\vdash c_P \rightarrow \neg(\phi|\psi)$.

**Proof** $\vdash c_Q \rightarrow \neg\phi$ is equivalent with $\vdash c_Q \wedge \phi \rightarrow \bot$ and because $\vdash c_R \wedge \psi \rightarrow \top$, we obtain, by theorem 4.7 $\vdash (c_Q \wedge \phi)|(c_R \wedge \psi) \rightarrow \bot|\top$. And using axiom E4.4, we derive

$$\vdash (c_Q \wedge \phi)|(c_R \wedge \psi) \rightarrow \bot$$

Similarly, from $\vdash c_R \rightarrow \neg\psi$ we can derive

$$\vdash (c_Q \wedge \phi)|(c_R \wedge \psi) \rightarrow \bot$$

Hence, the hypothesis of the theorem says that for any decomposition $P \equiv Q|R$ we have $\vdash (c_Q \wedge \phi)|(c_R \wedge \psi) \rightarrow \bot$, i.e.

$$\vdash \bigvee_{P \equiv Q|R} (c_Q \wedge \phi)|(c_R \wedge \psi) \rightarrow \bot$$

But axiom E4.4 gives

$$\vdash (c_P \wedge \phi|\psi) \rightarrow \bigvee_{P \equiv Q|R} (c_Q \wedge \phi)|(c_R \wedge \psi)$$

hence

$$\vdash (c_P \wedge \phi|\psi) \rightarrow \bot, \ i.e. \ \vdash c_P \rightarrow \neg(\phi|\psi).$$

□

Related to the same topic of the relation between negation and the parallel operator, observe that the negation is not distributive with respect to parallel. This is the reason why, in the previous theorem, we had to ask in the premises that the condition $\vdash c_Q \rightarrow \neg\phi$ or $\vdash c_R \rightarrow \neg\psi$ be fulfilled by all the possible decompositions of $P$. If only a decomposition $P \equiv Q|R$ exists such that $\vdash c_Q \rightarrow \neg\phi$ or $\vdash c_R \rightarrow \neg\psi$, this is not enough to derive $\mathcal{M}, P \models \neg(\phi|\psi)$. Indeed suppose that $\mathcal{M}, Q \models \phi$ but $\mathcal{M}, Q \not\models \psi$ and $\mathcal{M}, R \models \psi$ but $\mathcal{M}, R \not\models \phi$. Then from $\mathcal{M}, Q \models \phi$ and $\mathcal{M}, R \models \psi$ we derive $\mathcal{M}, P \models \phi|\psi$. It is not the case that, from the additional information $\mathcal{M}, Q \not\models \psi$ and $\mathcal{M}, R \not\models \phi$, $\mathcal{M}, P \models \neg(\phi|\psi)$ to be derived. All we can derive from the unused information is that $\mathcal{M}, P \models \neg\phi|\neg\psi$, which does not contradict $\mathcal{M}, P \models \phi|\psi$.

## 4.8 Dynamic results

Now we focus of the theorems that derive from the class of dynamic axioms and rules. Remark the *modal behaviors* of the dynamic operators.

The next result states the monotonicity of the diamond operator.

[Monotonicity] If $\vdash \phi \rightarrow \psi$ then $\vdash \langle\alpha\rangle\phi \rightarrow \langle\alpha\rangle\psi$.

**Proof** $\vdash \phi \rightarrow \psi$ implies $\vdash \neg\psi \rightarrow \neg\phi$. Using rule $E_R$4.4 we obtain $\vdash [\alpha](\neg\psi \rightarrow \neg\phi)$ and axiom E4.4 gives $\vdash [\alpha]\neg\psi \rightarrow [\alpha]\neg\phi$. This is equivalent with $\vdash \neg\langle\alpha\rangle\psi \rightarrow \neg\langle\alpha\rangle\phi$, i.e. $\vdash \langle\alpha\rangle\phi \rightarrow \langle\alpha\rangle\psi$. □

If $\vdash \phi \rightarrow \psi$ then $\vdash [\alpha]\neg\psi \rightarrow [\alpha]\neg\phi$.

**Proof** If $\vdash \phi \rightarrow \psi$ then, by theorem 4.8, $\vdash \langle\alpha\rangle\phi \rightarrow \langle\alpha\rangle\psi$, hence $\vdash \neg\langle\alpha\rangle\psi \rightarrow \neg\langle\alpha\rangle\phi$, that gives $\vdash [\alpha]\neg\psi \rightarrow [\alpha]\neg\phi$. □

The next theorems confirm the intuition that the formulas $c_P$, in their interrelations, mimic the transitions of the processes (the dynamic operators mimic the transition labeled by the action it has as index).

If $P$ cannot do any transition by $\alpha$ then $\vdash c_P \rightarrow [\alpha]\bot$.

**Proof** We prove it by induction on the structure of $P$.

**The case** $P \equiv 0$**:** axiom E4.4 implies $\vdash 0 \rightarrow [\alpha]\bot$ which proves this case, because $c_0 = 0$.

**The case** $P \equiv \alpha_1.P_1|...|\alpha_n.P_n$**:** as $P$ cannot perform $\alpha$ we have $\alpha \neq \alpha_i$ for $i = 1..n$. We have $c_P = (\langle\alpha_1\rangle c_{P_1} \wedge 1)|...|(\langle\alpha_n\rangle c_{P_n} \wedge 1)$. From $\vdash c_{P_i} \rightarrow \top$ we derive, using theorem 4.8, $\vdash (\langle\alpha_i\rangle c_{P_i} \wedge 1) \rightarrow$

$(\langle\alpha_i\rangle\top \wedge 1)$. Further, we apply theorem 4.7 and obtain $\vdash c_P \to (\langle\alpha_1\rangle\top \wedge 1)|...|(\langle\alpha_n\rangle\top \wedge 1)$. Axiom E4.4 gives that for $\alpha \neq \alpha_i$, $\vdash (\langle\alpha_1\rangle\top \wedge 1)|...|(\langle\alpha_n\rangle\top \wedge 1) \to [\alpha]\bot$. Hence $\vdash c_P \to [\alpha]\bot$. □

$\vdash c_P \to [\alpha]\bigvee\{c_Q \mid P \xrightarrow{\alpha} Q\}$

**Proof** We prove it by induction on $P$.

**The case $P \not\equiv \alpha.P'|P''$ for some $P', P''$:** then $P$ cannot preform a transition by $\alpha$, hence, by theorem 4.8, $\vdash c_P \to [\alpha]\bot$. But
$\vdash \neg\bigvee\{c_Q \mid P \xrightarrow{\alpha} Q\} \to \top$, and using theorem 4.8, we derive

$$\vdash [\alpha]\bot \to [\alpha]\bigvee\{c_Q \mid P \xrightarrow{\alpha} Q\}$$

Combining this with $\vdash c_P \to [\alpha]\bot$, we derive

$$\vdash c_P \to [\alpha]\bigvee\{c_Q \mid P \xrightarrow{\alpha} Q\}$$

**The case $P \equiv \alpha.P'$:** then $\{c_Q \mid P \xrightarrow{\alpha} Q\} = \{c_{P'}\}$ and $c_P = \langle\alpha\rangle c_{P'} \wedge 1$. Applying axiom E4.4 we obtain $\vdash c_P \to [\alpha]c_{P'}$. Hence

$$\vdash c_P \to [\alpha]\bigvee\{c_Q \mid P \xrightarrow{\alpha} Q\}$$

**The case $P \equiv \alpha.P'|P''$ with $P'' \not\equiv 0$:** we apply the inductive hypothesis to $\alpha.P'$ and $P''$ respectively, and we obtain

$$\vdash c_{\alpha.P'} \to [\alpha]\bigvee\{c_{Q'} \mid \alpha.P' \xrightarrow{\alpha} Q'\}$$

and

$$\vdash c_{P''} \to [\alpha]\bigvee\{c_{Q''} \mid P'' \xrightarrow{\alpha} Q''\}$$

We apply rule $E_R$4.4 and obtain

$$\vdash c_P \to [\alpha](c_{\alpha.P'}|\bigvee\{c_{Q''} \mid P'' \xrightarrow{\alpha} Q''\} \vee \bigvee\{c_{Q'} \mid \alpha.P' \xrightarrow{\alpha} Q'\}|c_{P''})$$

Using theorem 4.7, we obtain this result equivalent with

$$\vdash c_P \to [\alpha]\bigvee\{c_Q \mid P \xrightarrow{\alpha} Q\}$$

□

If $\vdash \bigvee\{c_Q \mid P \xrightarrow{\alpha} Q\} \to \phi$ then $\vdash c_P \to [\alpha]\phi$

**Proof** If $\vdash \bigvee\{c_Q \mid P \xrightarrow{\alpha} Q\} \to \phi$ then rule $E_R$4.4 gives

$$\vdash [\alpha](\bigvee\{c_Q \mid P \xrightarrow{\alpha} Q\} \to \phi)$$

and further axiom E4.4 gives $\vdash [\alpha]\bigvee\{c_Q \mid P \xrightarrow{\alpha} Q\} \to [\alpha]\phi$. But theorem 4.8 gives $\vdash c_P \to [\alpha]\bigvee\{c_Q \mid P \xrightarrow{\alpha} Q\}$, hence $\vdash c_P \to [\alpha]\phi$. □

## Epistemic results

We begin by stating that $0$ is always an active agent: it always performs its *"inactivity"* expressed by $0. \vdash K_0\top$.

**Proof** Trivial consequence of axiom E4.4 and axiom E4.4. □

The next result states that an agent knows something only if it is active. Hence *to know* implies *to be*.

$\vdash K_P\phi \to K_P\top$.

**Proof** Trivial consequence of axiom E4.4. □

Further we prove another obvious property of knowledge: if $Q$ knows $\phi$ and $Q$ knows $\psi$, this is equivalent with $Q$ knows $\phi \wedge \psi$.

$\vdash K_Q\phi \wedge K_Q\psi \leftrightarrow K_Q(\phi \wedge \psi)$

**Proof** $\vdash \phi \to (\psi \to (\phi \wedge \psi))$. Using rule $E_R$4.4, we obtain

$$\vdash K_Q\top \to K_Q[\phi \to (\psi \to (\phi \wedge \psi))]$$

We apply axiom E4.4 twice, and obtain

$$\vdash K_Q\top \to [K_Q\phi \to (K_Q\psi \to K_Q(\phi \wedge \psi))]$$

i.e.

$$\vdash K_Q\top \wedge K_Q\phi \to [K_Q\psi \to K_Q(\phi \wedge \psi)]$$

But $\vdash K_Q\phi \to K_Q\top$, hence $\vdash K_Q\phi \to [K_Q\psi \to K_Q(\phi \wedge \psi)]$, i.e.

$$\vdash K_Q\phi \wedge K_Q\psi \to K_Q(\phi \wedge \psi)$$

Reverse, we apply rule $E_R$4.4 to $\vdash \phi \wedge \psi \to \psi$ and then axiom E4.4, and obtain $\vdash K_Q\top \to (K_Q(\phi \wedge \psi) \to K_Q\phi)$. But $\vdash K_Q(\phi \wedge \psi) \to K_Q\top$, hence $\vdash K_Q(\phi \wedge \psi) \to K_Q\phi$.
Similarly $\vdash K_Q(\phi \wedge \psi) \to K_Q\psi$. □

The knowledge is redundant and introspective: if $Q$ knows $\phi$ this is equivalent with the fact that $Q$ knows that $Q$ knows $\phi$.

$\vdash K_QK_Q\phi \leftrightarrow K_Q\phi$.

**Proof** Axiom E4.4 gives $\vdash K_Q\phi \to K_QK_Q\phi$, and axiom E4.4 gives $\vdash K_QK_Q\phi \to K_Q\phi$. □

[Monotonicity of knowledge]

$$\text{If } \vdash \phi \to \psi \text{ then } \vdash K_P\phi \to K_P\psi$$

**Proof** Because $\vdash \phi \rightarrow \psi$, we can use rule $E_R$4.4 and obtain
$\vdash K_P\top \rightarrow K_P(\phi \rightarrow \psi)$. But theorem 4.8 gives $\vdash K_P\phi \rightarrow K_P\top$, hence $\vdash K_P\phi \rightarrow K_P(\phi \rightarrow \psi)$ where from we derive

$$\vdash K_P\phi \rightarrow (K_P\phi \wedge K_P(\phi \rightarrow \psi))$$

This entails, using axiom E4.4, $\vdash K_P\phi \rightarrow K_P\psi$. □

The existence of an agent entails the existence of its active sub-agents, as proved further. This is a knowledge-like description of the ontological topology of agents. It relies on *to be* is *to know*.

$\vdash K_{P|Q}\top \rightarrow K_P\top$.

**Proof** Axiom E4.4 gives $\vdash K_{P|Q}\top \leftrightarrow c_P|c_Q|\top$ and $\vdash K_P\top \leftrightarrow c_P|\top$. But $\vdash c_Q \rightarrow \top$ and applying rule $E_R$4.4, we obtain $\vdash c_P|c_Q|\top \rightarrow c_P|\top$. Hence $\vdash K_{P|Q}\top \rightarrow K_P\top$. □

The knowledge of an agent is consistent: if it knows $\neg\phi$ (it knows that $\phi$ is false) then it cannot know $\phi$ as well. This is proved in the next two theorems.

$\vdash K_Q\neg\phi \rightarrow \neg K_Q\phi$.

**Proof** Axiom E4.4 gives $\vdash K_Q\neg\phi \rightarrow \neg\phi$ and $\vdash K_Q\phi \rightarrow \phi$. The last is equivalent with $\vdash \neg\phi \rightarrow \neg K_Q\phi$, and combined with the first entails $\vdash K_Q\neg\phi \rightarrow \neg K_Q\phi$. □

[Consistency theorem] $\vdash K_Q\phi \rightarrow \neg K_Q\neg\phi$.

**Proof** By using the negative form of theorem 4.8 □

In the next four theorems we will focus on the knowledge of the agent $0$. It represents *"the most ignorant"* agent in $\mathcal{M}$ in the sense that if it knows something then everybody else knows it as well. This property might be exploited in the sense that what $0$ knows is a validity in $\mathcal{M}$. And the dual of knowledge operator applied to $0$ gives the satisfiability in $\mathcal{M}$.

$\vdash K_0\phi \rightarrow (K_Q\top \rightarrow K_Q\phi)$

**Proof** Axioms E4.4 gives $\vdash K_0\phi \rightarrow \phi$ and applying the monotonicity of knowledge, $\vdash K_QK_0\phi \rightarrow K_Q\phi$.
Now axiom E4.4 provides $\vdash K_0\phi \wedge K_Q\top \rightarrow K_QK_0\phi$. Thus $\vdash K_0\phi \wedge K_Q\top \rightarrow K_Q\phi$, that is equivalent with $\vdash K_0\phi \rightarrow (K_Q\top \rightarrow K_Q\phi)$. □

$\vdash \widetilde{K}_0\phi \leftrightarrow K_0\widetilde{K}_0\phi$

**Proof** By definition, we have $\vdash \widetilde{K}_0\phi \leftrightarrow \neg K_0\neg\phi$, and because $\vdash K_0\top$, we derive $\vdash \widetilde{K}_0\phi \rightarrow (\neg K_0\neg\phi \wedge K_0\top)$.
But axiom E4.4 entails $\vdash (\neg K_0\neg\phi \wedge K_0\top) \rightarrow K_0\neg K_0\neg\phi$, i.e.

$$\vdash (\neg K_0\neg\phi \wedge K_0\top) \rightarrow K_0\widetilde{K}_0\phi$$

Hence $\vdash \widetilde{K}_0\phi \rightarrow K_0\widetilde{K}_0\phi$.
We have also $\vdash K_0\widetilde{K}_0\phi \rightarrow \widetilde{K}_0\phi$, by applying axiom E4.4. □

$\vdash \widetilde{K}_0\phi \wedge \psi | \rho \rightarrow (\widetilde{K}_0\phi \wedge \psi) | (\widetilde{K}_0\phi \wedge \rho)$

**Proof** Axiom E4.4 instantiated with $\phi = \widetilde{K}_0\phi$ gives

$$\vdash K_0\widetilde{K}_0\phi \wedge \psi | \rho \rightarrow (K_0\widetilde{K}_0\phi \wedge \psi) | (K_0\widetilde{K}_0\phi \wedge \rho)$$

Further, using theorem 4.8, we obtain the wanted result. □

$\vdash \widetilde{K}_0\phi \rightarrow [\alpha]\widetilde{K}_0\phi$

**Proof** Axiom E4.4 instantiated with $\phi = \widetilde{K}_0\phi$ gives

$$\vdash K_0\widetilde{K}_0\phi \rightarrow [\alpha]K_0\widetilde{K}_0\phi$$

Further, using theorem 4.8, we obtain the wanted result. □

$\vdash \widetilde{K}_0\phi \rightarrow (K_Q\top \rightarrow K_Q\widetilde{K}_0\phi)$

**Proof** Axiom E4.4 instantiated with $\phi = \widetilde{K}_0\phi$ gives

$$\vdash K_0\widetilde{K}_0\phi \rightarrow (K_Q\top \rightarrow K_QK_0\widetilde{K}_0\phi)$$

Further, using theorem 4.8, we obtain the wanted result. □

## Theorems referring to contexts

In this section we focus on results that involve the characteristic formulas of finite contexts. We try to show, in this way, how sensitive our system is with respect to contexts. Further, these results will be used in proving the completeness for $\mathcal{L}^{\mathfrak{S}}_{DES}$.

If $\mathcal{M}$ is a finite context and $R \notin \mathcal{M}$ then $\vdash c_{\mathcal{M}} \rightarrow \neg c_R$.

**Proof** Because $c_{\mathcal{M}} = K_0(\bigvee_{P\in\mathcal{M}} c_P) \wedge (\bigwedge_{P\in\mathcal{M}} \widetilde{K}_0 c_P)$ we derive that

$$\vdash c_{\mathcal{M}} \rightarrow K_0(\bigvee_{P\in\mathcal{M}} c_P)$$

But from axiom E4.4 $\vdash K_0(\bigvee_{P\in\mathcal{M}} c_P) \rightarrow \bigvee_{P\in\mathcal{M}} c_P$, so $\vdash c_{\mathcal{M}} \rightarrow \bigvee_{P\in\mathcal{M}} c_P$. Further theorem 4.6 gives $\vdash c_P \rightarrow \neg c_R$ (as $R \notin \mathcal{M}$ and $P \in \mathcal{M}$ implies $R \not\equiv P$) which implies $\vdash \bigvee_{P\in\mathcal{M}} c_P \rightarrow \neg c_R$. But we proved that $\vdash c_{\mathcal{M}} \rightarrow \bigvee_{P\in\mathcal{M}} c_P$. Hence $\vdash c_{\mathcal{M}} \rightarrow \neg c_R$. □

If $\mathcal{M}$ is a finite context then

$$\vdash (c_{\mathcal{M}} \wedge \phi | \psi) \rightarrow (c_{\mathcal{M}} \wedge \phi) | (c_{\mathcal{M}} \wedge \psi)$$

**Proof** Observe that, by applying axiom E4.4, we obtain

$$\vdash (K_0\theta_1 \wedge \widetilde{K}_0\theta_2 \wedge \widetilde{K}_0\theta_3) \wedge \phi|\psi \rightarrow (\widetilde{K}_0\theta_2 \wedge \widetilde{K}_0\theta_3) \wedge (K_0\theta_1 \wedge \phi)|(K_0\theta_1 \wedge \psi) \tag{3}$$

If, further, we apply theorem 4.8 once, we obtain

$$\begin{array}{c}\vdash (\widetilde{K}_0\theta_3 \wedge \widetilde{K}_0\theta_2) \wedge (K_0\theta_1 \wedge \phi)|(K_0\theta_1 \wedge \psi) \rightarrow \\ \widetilde{K}_0\theta_3 \wedge (\widetilde{K}_0\theta_2 \wedge K_0\theta_1 \wedge \phi)|(\widetilde{K}_0\theta_2 \wedge K_0\theta_1 \wedge \psi)\end{array}$$

Hence

$$\vdash (K_0\theta_1 \wedge \widetilde{K}_0\theta_2 \wedge \widetilde{K}_0\theta_3) \wedge \phi|\psi \rightarrow \widetilde{K}_0\theta_3 \wedge (\widetilde{K}_0\theta_2 \wedge K_0\theta_1 \wedge \phi)|(\widetilde{K}_0\theta_2 \wedge K_0\theta_1 \wedge \psi)$$

If we apply again theorem 4.8 we obtain

$$\begin{array}{c}\vdash \widetilde{K}_0\theta_3 \wedge (\widetilde{K}_0\theta_2 \wedge K_0\theta_1 \wedge \phi)|(\widetilde{K}_0\theta_2 \wedge K_0\theta_1 \wedge \psi) \rightarrow \\ (\widetilde{K}_0\theta_3 \wedge \widetilde{K}_0\theta_2 \wedge K_0\theta_1 \wedge \phi)|(\widetilde{K}_0\theta_3 \wedge \widetilde{K}_0\theta_2 \wedge K_0\theta_1 \wedge \psi)\end{array}$$

hence

$$\begin{array}{c}\vdash (K_0\theta_1 \wedge \widetilde{K}_0\theta_2 \wedge \widetilde{K}_0\theta_3) \wedge \phi|\psi \rightarrow \\ (\widetilde{K}_0\theta_3 \wedge \widetilde{K}_0\theta_2 \wedge K_0\theta_1 \wedge \phi)|(\widetilde{K}_0\theta_3 \wedge \widetilde{K}_0\theta_2 \wedge K_0\theta_1 \wedge \psi)\end{array}$$

Because $c_{\mathcal{M}} = K_0(\bigvee_{Q\in\mathcal{M}} c_Q) \wedge (\bigwedge_{Q\in\mathcal{M}} \widetilde{K}_0 c_Q)$, we can use the same idea, applying theorem 4.8 once for each process in $\mathcal{M}$ (being finite) and we obtain

$$\vdash (c_{\mathcal{M}} \wedge \phi|\psi) \rightarrow (c_{\mathcal{M}} \wedge \phi)|(c_{\mathcal{M}} \wedge \psi)$$

□

If $\mathcal{M}$ is a finite context then $\vdash (c_{\mathcal{M}} \wedge \phi|\psi) \rightarrow (c_{\mathcal{M}} \wedge \phi)|\psi$

**Proof** From the previous theorem, 4.8, we have

$$\vdash (c_{\mathcal{M}} \wedge \phi|\psi) \rightarrow (c_{\mathcal{M}} \wedge \phi)|(c_{\mathcal{M}} \wedge \psi)$$

Theorem 4.7 gives

$$(c_{\mathcal{M}} \wedge \phi)|(c_{\mathcal{M}} \wedge \psi) \rightarrow ((c_{\mathcal{M}} \wedge \phi)|c_{\mathcal{M}}) \wedge ((c_{\mathcal{M}} \wedge \phi)|\psi))$$

Hence $\vdash (c_{\mathcal{M}} \wedge \phi|\psi) \rightarrow (c_{\mathcal{M}} \wedge \phi)|\psi$. □

If $\mathcal{M}$ is a finite context then $\vdash c_{\mathcal{M}} \rightarrow [\alpha]c_{\mathcal{M}}$

**Proof** Observe that, by applying axiom E4.4, we obtain

$$\vdash K_0\theta_1 \wedge \widetilde{K}_0\theta_2 \wedge \widetilde{K}_0\theta_3 \rightarrow (\widetilde{K}_0\theta_2 \wedge \widetilde{K}_0\theta_3) \wedge [\alpha]K_0\theta_1$$

If, further, we apply theorem 4.8 once, we obtain

$$\vdash (\widetilde{K}_0\theta_3 \wedge \widetilde{K}_0\theta_2) \wedge [\alpha]K_0\theta_1 \rightarrow \widetilde{K}_0\theta_3 \wedge [\alpha]\widetilde{K}_0\theta_2 \wedge [\alpha]K_0\theta_1,\ i.e.$$

$$\vdash (\widetilde{K}_0\theta_3 \wedge \widetilde{K}_0\theta_2) \wedge [\alpha]K_0\theta_1 \rightarrow \widetilde{K}_0\theta_3 \wedge [\alpha](\widetilde{K}_0\theta_2 \wedge K_0\theta_1)$$

Hence

$$\vdash (K_0\theta_1 \wedge \widetilde{K}_0\theta_2 \wedge \widetilde{K}_0\theta_3) \rightarrow \widetilde{K}_0\theta_3 \wedge [\alpha](\widetilde{K}_0\theta_2 \wedge K_0\theta_1)$$

If we apply again theorem 4.8 we obtain

$$\vdash \widetilde{K}_0\theta_3 \wedge [a](\widetilde{K}_0\theta_2 \wedge K_0\theta_1) \rightarrow [\alpha](\widetilde{K}_0\theta_3 \wedge \widetilde{K}_0\theta_2 \wedge K_0\theta_1)$$

hence

$$\vdash (K_0\theta_1 \wedge \widetilde{K}_0\theta_2 \wedge \widetilde{K}_0\theta_3) \rightarrow [\alpha](\widetilde{K}_0\theta_3 \wedge \widetilde{K}_0\theta_2 \wedge K_0\theta_1)$$

As $c_{\mathcal{M}} = K_0(\bigvee_{Q\in\mathcal{M}} c_Q) \wedge (\bigwedge_{Q\in\mathcal{M}} \widetilde{K}_0 c_Q)$, we can use the same idea, applying theorem 4.8 once for each process in $\mathcal{M}$ (being finite) and we obtain

$$\vdash c_{\mathcal{M}} \rightarrow [\alpha]c_{\mathcal{M}}$$

□

If $\mathcal{M}$ is a finite context then $\vdash c_{\mathcal{M}} \rightarrow (K_Q\top \rightarrow K_Q c_{\mathcal{M}})$

**Proof** Observe that, by applying axiom E4.4, we obtain

$$\vdash K_0\theta_1 \wedge \widetilde{K}_0\theta_2 \wedge \widetilde{K}_0\theta_3 \rightarrow (\widetilde{K}_0\theta_2 \wedge \widetilde{K}_0\theta_3) \wedge (K_Q\top \rightarrow K_Q K_0\theta_1)$$

If, further, we apply theorem 4.8 once, we obtain

$$\vdash (\widetilde{K}_0\theta_3 \wedge \widetilde{K}_0\theta_2) \wedge (K_Q\top \rightarrow K_Q K_0\theta_1) \rightarrow$$
$$\widetilde{K}_0\theta_3 \wedge (K_Q\top \rightarrow K_Q\widetilde{K}_0\theta_2) \wedge (K_Q\top \rightarrow K_Q K_0\theta_1),\ i.e.$$

$$\vdash (\widetilde{K}_0\theta_3 \wedge \widetilde{K}_0\theta_2) \wedge (K_Q\top \rightarrow K_Q K_0\theta_1) \rightarrow \widetilde{K}_0\theta_3 \wedge (K_Q\top \rightarrow (K_Q\widetilde{K}_0\theta_2 \wedge K_Q K_0\theta_1))$$

i.e., using 4.8,

$$\vdash (\widetilde{K}_0\theta_3 \wedge \widetilde{K}_0\theta_2) \wedge (K_Q\top \rightarrow K_Q K_0\theta_1) \rightarrow \widetilde{K}_0\theta_3 \wedge (K_Q\top \rightarrow K_Q(\widetilde{K}_0\theta_2 \wedge K_0\theta_1))$$

Hence

$$\vdash (K_0\theta_1 \wedge \widetilde{K}_0\theta_2 \wedge \widetilde{K}_0\theta_3) \rightarrow \widetilde{K}_0\theta_3 \wedge (K_Q\top \rightarrow K_Q(\widetilde{K}_0\theta_2 \wedge K_0\theta_1))$$

If we apply again the theorems 4.8 and 4.8 we obtain

$$\vdash [\widetilde{K}_0\theta_3 \wedge (K_Q\top \rightarrow K_Q(\widetilde{K}_0\theta_2 \wedge K_0\theta_1))] \rightarrow [K_Q\top \rightarrow K_Q(\widetilde{K}_0\theta_3 \wedge \widetilde{K}_0\theta_2 \wedge K_0\theta_1)]$$

hence

$$\vdash (K_0\theta_1 \wedge \widetilde{K}_0\theta_2 \wedge \widetilde{K}_0\theta_3) \rightarrow [K_Q\top \rightarrow K_Q(\widetilde{K}_0\theta_3 \wedge \widetilde{K}_0\theta_2 \wedge K_0\theta_1)]$$

Because $c_{\mathcal{M}} = K_0(\bigvee_{Q\in\mathcal{M}} c_Q) \wedge (\bigwedge_{Q\in\mathcal{M}} \widetilde{K}_0 c_Q)$, we can use the same idea, applying theorem 4.8 once for each process in $\mathcal{M}$ (being finite) and we obtain

$$\vdash c_{\mathcal{M}} \rightarrow (K_Q\top \rightarrow K_Q c_{\mathcal{M}})$$

□

Now we prove a context sensitive version of rule $E_R$4.4.

If $\mathcal{M}$ is a finite context and $\vdash c_{\mathcal{M}} \rightarrow (\phi \rightarrow \psi)$ then $\vdash c_{\mathcal{M}} \rightarrow (\phi|\rho \rightarrow \psi|\rho)$.

**Proof** $\vdash c_{\mathcal{M}} \rightarrow (\phi \rightarrow \psi)$ implies $\vdash (c_{\mathcal{M}} \wedge \phi) \rightarrow \psi$ where we apply rule $E_R$4.4 and obtain $\vdash (c_{\mathcal{M}} \wedge \phi)|\rho \rightarrow \psi|\rho$. But theorem 4.8 gives $\vdash (c_{\mathcal{M}} \wedge \phi|\rho) \rightarrow (c_{\mathcal{M}} \wedge \phi)|\rho$. Combining these two results we obtain
$\vdash (c_{\mathcal{M}} \wedge \phi|\rho) \rightarrow \psi|\rho$, i.e. $\vdash c_{\mathcal{M}} \rightarrow (\phi|\rho \rightarrow \psi|\rho)$. □

A context-sensitive version of theorem 4.7 is also available.

If for a finite context $\mathcal{M} \ni P$ and any decomposition $P \equiv Q|R$ we have

$$\vdash c_{\mathcal{M}} \rightarrow (c_Q \rightarrow \neg\phi) \; or \; \vdash c_{\mathcal{M}} \rightarrow (c_R \rightarrow \neg\psi) \; then \; \vdash c_{\mathcal{M}} \rightarrow (c_P \rightarrow \neg(\phi|\psi)).$$

**Proof** If $\vdash c_{\mathcal{M}} \rightarrow (c_Q \rightarrow \neg\phi)$ then we have, equivalently, $\vdash c_{\mathcal{M}} \wedge c_Q \rightarrow \neg\phi$, i.e. $\vdash c_Q \rightarrow (c_{\mathcal{M}} \rightarrow \neg\phi)$, hence $\vdash c_Q \rightarrow \neg(c_{\mathcal{M}} \wedge \phi)$.
Similarly $\vdash c_{\mathcal{M}} \rightarrow (c_R \rightarrow \neg\psi)$ gives $\vdash c_R \rightarrow \neg(c_{\mathcal{M}} \wedge \psi)$.

Hence the hypothesis of the theorem can be rewritten as: for any decomposition $P \equiv Q|R$ we have

$$\vdash c_Q \rightarrow \neg(c_{\mathcal{M}} \wedge \phi) \; or \; \vdash c_R \rightarrow \neg(c_{\mathcal{M}} \wedge \psi).$$

Then we can apply theorem 4.7 and we obtain

$$\vdash c_P \rightarrow \neg((c_{\mathcal{M}} \wedge \phi)|(c_{\mathcal{M}} \wedge \psi)) \tag{4}$$

But theorem 4.8 entails $\vdash c_{\mathcal{M}} \wedge \phi|\psi \rightarrow (c_{\mathcal{M}} \wedge \phi)|(c_{\mathcal{M}} \wedge \psi)$, hence $\vdash \neg((c_{\mathcal{M}} \wedge \phi)|(c_{\mathcal{M}} \wedge \psi)) \rightarrow \neg(c_{\mathcal{M}} \wedge \phi|\psi)$, and applying this result to (4), we obtain

$$\vdash c_P \rightarrow \neg(c_{\mathcal{M}} \wedge \phi|\psi) \; that \; is \; equivalent \; with \; \vdash c_{\mathcal{M}} \rightarrow (c_P \rightarrow \neg(\phi|\psi))$$

□

Further we prove a context-sensitive version of rule $E_R$4.4.

If $\vdash c_{\mathcal{M}} \rightarrow \phi$ then $\vdash c_{\mathcal{M}} \rightarrow [\alpha]\phi$.

**Proof** If we apply rule $E_R4.4$ to $\vdash c_{\mathcal{M}} \rightarrow \phi$ we obtain $\vdash [\alpha](c_{\mathcal{M}} \rightarrow \phi)$. But axiom E4.4 gives $\vdash [\alpha](c_{\mathcal{M}} \rightarrow \phi) \rightarrow ([\alpha]c_{\mathcal{M}} \rightarrow [\alpha]\phi)$, hence $\vdash [\alpha]c_{\mathcal{M}} \rightarrow [\alpha]\phi$. Theorem 4.8 proves that $\vdash c_{\mathcal{M}} \rightarrow [\alpha]c_{\mathcal{M}}$ which gives further $\vdash c_{\mathcal{M}} \rightarrow [\alpha]\phi$. □

The next result is a context-sensitive variant of rule $E_R4.4$.

If $\vdash c_{\mathcal{M}} \rightarrow \phi$ then $\vdash c_{\mathcal{M}} \rightarrow (K_Q\top \rightarrow K_Q\phi)$.

**Proof** If we apply rule $E_R4.4$ to $\vdash c_{\mathcal{M}} \rightarrow \phi$, we obtain

$$\vdash K_Q\top \rightarrow K_Q(c_{\mathcal{M}} \rightarrow \phi)$$

But axiom E4.4 gives further $\vdash K_Q(c_{\mathcal{M}} \rightarrow \phi) \rightarrow (K_Qc_{\mathcal{M}} \rightarrow K_Q\phi)$. Hence $\vdash K_Q\top \wedge K_Qc_{\mathcal{M}} \rightarrow K_Q\phi$ that is equivalent with

$$\vdash K_Qc_{\mathcal{M}} \rightarrow (K_Q\top \rightarrow K_Q\phi)$$

Now, theorem 4.8 ensures that $\vdash c_{\mathcal{M}} \rightarrow (K_Q\top \rightarrow K_Qc_{\mathcal{M}})$.
Hence $\vdash c_{\mathcal{M}} \rightarrow (K_Q\top \rightarrow K_Q\phi)$. □

If $\vdash c_{\mathcal{M}} \rightarrow (K_Q\psi \rightarrow \phi)$ then $\vdash c_{\mathcal{M}} \rightarrow (K_Q\psi \rightarrow K_Q\phi)$.

**Proof** We apply theorem 4.8 to $\vdash c_{\mathcal{M}} \rightarrow (K_Q\psi \rightarrow \phi)$ and we obtain
$\vdash c_{\mathcal{M}} \rightarrow (K_Q\top \rightarrow K_Q(K_Q\psi \rightarrow \phi))$, i.e. $\vdash (c_{\mathcal{M}} \wedge K_Q\top) \rightarrow K_Q(K_Q\psi \rightarrow \phi)$.
But axiom E4.4 gives $\vdash K_Q(K_Q\psi \rightarrow \phi) \rightarrow (K_QK_Q\psi \rightarrow K_Q\phi)$. Now if we use theorem 4.8 we obtain further

$$\vdash K_Q(K_Q\psi \rightarrow \phi) \rightarrow (K_Q\psi \rightarrow K_Q\phi)$$

All these proved that $\vdash (c_{\mathcal{M}} \wedge K_Q\top) \rightarrow (K_Q\psi \rightarrow K_Q\phi)$, i.e.

$$\vdash c_{\mathcal{M}} \rightarrow (K_Q\top \rightarrow (K_Q\psi \rightarrow K_Q\phi))$$

which is equivalent with $\vdash c_{\mathcal{M}} \rightarrow (K_Q\top \wedge K_Q\psi \rightarrow K_Q\phi)$.
Theorem 4.8 proved that $\vdash K_Q\psi \rightarrow K_Q\top$, result which, combined with the previous one, gives further $\vdash c_{\mathcal{M}} \rightarrow (K_Q\psi \rightarrow K_Q\phi)$. □

If $Q|R \in \mathcal{M}$ then $\vdash c_{\mathcal{M}} \rightarrow (c_Q|c_R \rightarrow \neg\phi)$ implies $\vdash c_{\mathcal{M}} \rightarrow \neg K_Q\phi$.

**Proof** Because $\vdash c_R \rightarrow \top$, rule $E_R4.4$ gives $\vdash c_Q|c_R \rightarrow c_Q|\top$ that gives further $\vdash c_{\mathcal{M}} \rightarrow (c_Q|c_R \rightarrow c_Q|\top)$. Combining this result with the hypothesis of the theorem, $\vdash c_{\mathcal{M}} \rightarrow (c_Q|c_R \rightarrow \neg\phi)$, we obtain

$$\vdash (c_{\mathcal{M}} \wedge c_Q|c_R) \rightarrow (c_Q|\top \wedge \neg\phi), \text{ i.e. } \vdash c_{\mathcal{M}} \rightarrow (c_Q|c_R \rightarrow (c_Q|\top \wedge \neg\phi))$$

But $\vdash (c_Q|\top \wedge \neg\phi) \leftrightarrow \neg(c_Q|\top \rightarrow \phi)$, hence

$$\vdash c_{\mathcal{M}} \rightarrow (c_Q|c_R \rightarrow \neg(c_Q|\top \rightarrow \phi)) \tag{5}$$

Axiom E4.4 ensure that $\vdash K_0(c_Q|\top \to \phi) \to (c_Q|\top \to \phi)$ or, equivalently, $\vdash \neg(c_Q|\top \to \phi) \to \neg K_0(c_Q|\top \to \phi)$, that, used in (5) gives

$$\vdash c_{\mathcal{M}} \to (c_Q|c_R \to \neg K_0(c_Q|\top \to \phi)) \tag{6}$$

But theorem 4.8 gives $\vdash K_0\top$, that can be used in (6) providing

$$\vdash c_{\mathcal{M}} \to (c_Q|c_R \to (K_0\top \wedge \neg K_0(c_Q|\top \to \phi))) \tag{7}$$

The negative introspection, axiom E4.4, infers

$$\vdash (K_0\top \wedge \neg K_0(c_Q|\top \to \phi)) \to K_0\neg K_0(c_Q|\top \to \phi) \tag{8}$$

Combining (7) and (8) we obtain

$$\vdash c_{\mathcal{M}} \to (c_Q|c_R \to K_0\neg K_0(c_Q|\top \to \phi)) \tag{9}$$

But (9) is equivalent with $\vdash (c_{\mathcal{M}} \wedge c_Q|c_R) \to K_0\neg K_0(c_Q|\top \to \phi)$, and because $Q|R \in \mathcal{M}$, we can apply rule $\mathrm{E}_R$4.4 and obtain

$$\vdash c_{\mathcal{M}} \to \neg K_0(K_Q\top \to \phi) \tag{10}$$

But from axiom E4.4 we derive $\vdash K_Q\phi \to K_0(K_Q\top \to \phi)$, hence

$$\vdash \neg K_0(K_Q\top \to \phi) \to \neg K_Q\phi \tag{11}$$

Combining (10) with (11) we obtain $\vdash c_{\mathcal{M}} \to \neg K_Q\phi$, q.e.d. □

The next result is a context-sensitive version of theorem 4.7.

If $\vdash c_{\mathcal{M}} \to (\phi \to \psi)$ and $\vdash c_{\mathcal{M}} \to (\rho \to \theta)$ then $\vdash c_{\mathcal{M}} \to (\phi|\rho \to \psi|\theta)$.

**Proof** To $\vdash c_{\mathcal{M}} \to (\phi \to \psi)$ we can apply theorem 4.8 and we obtain $\vdash c_{\mathcal{M}} \to (\phi|\rho \to \psi|\rho)$, i.e. $\vdash (c_{\mathcal{M}} \wedge \phi|\rho) \to \psi|\rho$ which implies

$$\vdash (c_{\mathcal{M}} \wedge \phi|\rho) \to (c_{\mathcal{M}} \wedge \psi|\rho) \tag{12}$$

The same theorem 4.8 can be applied to $\vdash c_{\mathcal{M}} \to (\rho \to \theta)$ giving $\vdash c_{\mathcal{M}} \to (\psi|\rho \to \psi|\theta)$, i.e.

$$\vdash (c_{\mathcal{M}} \wedge \psi|\rho) \to \psi|\theta \tag{13}$$

Further, combining (12) and (13) we derive $\vdash (c_{\mathcal{M}} \wedge \phi|\psi) \to \psi|\theta$, hence $\vdash c_{\mathcal{M}} \to (\phi|\psi \to \psi|\theta)$. □

We prove further a contextual version of theorem 4.8.

If $\vdash c_{\mathcal{M}} \to (\phi \to \psi)$ then $\vdash c_{\mathcal{M}} \to (\langle\alpha\rangle\phi \to \langle\alpha\rangle\psi)$.

**Proof** $\vdash c_{\mathcal{M}} \to (\phi \to \psi)$ implies $\vdash c_{\mathcal{M}} \to (\neg\psi \to \neg\phi)$ where, applying theorem 4.8, we obtain $\vdash c_{\mathcal{M}} \to [\alpha](\neg\psi \to \neg\phi)$. But axiom E4.4 gives $\vdash [\alpha](\neg\psi \to \neg\phi) \to ([\alpha]\neg\psi \to [\alpha]\neg\phi)$. Hence $\vdash$

$c_{\mathcal{M}} \to ([\alpha]\neg\psi \to [\alpha]\neg\phi)$, i.e. $\vdash c_{\mathcal{M}} \to (\neg\langle\alpha\rangle\psi \to \neg\langle\alpha\rangle\phi)$. Concluding, $\vdash c_{\mathcal{M}} \to (\langle\alpha\rangle\phi \to \langle\alpha\rangle\psi)$. □

The next result is a variant of theorem 4.8, but sensitive to the context.

$$\text{If } \vdash c_{\mathcal{M}} \to (\bigvee\{c_Q \mid P \xrightarrow{\alpha} Q\} \to \phi) \text{ then } \vdash c_{\mathcal{M}} \to (c_P \to [\alpha]\phi)$$

**Proof** If $\vdash c_{\mathcal{M}} \to (\bigvee\{c_Q \mid P \xrightarrow{\alpha} Q\} \to \phi)$ then theorem 4.8 gives $\vdash c_{\mathcal{M}} \to [\alpha](\bigvee\{c_Q \mid P \xrightarrow{\alpha} Q\} \to \phi)$ and further axiom E4.4 gives

$$\vdash c_{\mathcal{M}} \to ([\alpha]\bigvee\{c_Q \mid P \xrightarrow{\alpha} Q\} \to [\alpha]\phi)$$

But theorem 4.8 gives

$$\vdash c_P \to [\alpha]\bigvee\{c_Q \mid P \xrightarrow{\alpha} Q\}$$

hence $\vdash c_{\mathcal{M}} \wedge c_P \to [\alpha]\phi$, i.e. $\vdash c_{\mathcal{M}} \to (c_P \to [\alpha]\phi)$. □

## 4.9 Completeness of $\mathcal{L}^{\mathfrak{S}}_{DES}$ against process semantics

Now we will prove the completeness of $\mathcal{L}^{\mathfrak{S}}_{DES}$ with respect to process semantics. We recall that completeness ensures that everything that can be derived in the semantics can be proved in the syntax. In this way we have the possibility to syntactically verify properties.

In the context of a decidable system, as ours is, the completeness provides a powerful tool for making predictions on the evolution of the system we analyze. Indeed, knowing the state of our system, we can characterize it syntactically. And because any other state can be characterized, we can project our problem into the syntax and verify its satisfiability. Hence if our system can reach that state, we will obtain that the formula is satisfiable and the method will provide also a minimal model that satisfies it. Thus we made a prediction without investigating (simulating) the full evolution of the system that might cause, sometimes, unsolvable computational problems (usually the time is branching generating exponential complexity).

We start by proving a lemma that provides a syntactic characterization of the satisfiability. The intuition is that, because $c_P$ and $c_{\mathcal{M}}$ are characteristic formulas, we should have an equivalence between $\mathcal{M}, P \models \phi$ and $\vdash c_{\mathcal{M}} \wedge c_P \to \phi$ (of course for finite contexts) as both can be read as *the process $P$ in the context $\mathcal{M}$ has the property $\phi$*.

If $\mathcal{M}$ is a finite context then $\mathcal{M}, P \models \phi$ iff $\vdash c_{\mathcal{M}} \wedge c_P \to \phi$.

**Proof** ($\Longrightarrow$) We prove it by induction on the syntactical structure of $\phi$.

- **The case $\phi = 0$:** $\mathcal{M}, P \models 0$ implies $P \equiv 0$. But $c_0 = 0$ and $\vdash 0 \to 0$, hence $\vdash 0 \wedge c_{\mathcal{M}} \to 0$. This gives $\vdash c_{\mathcal{M}} \wedge c_P \to \phi$.
- **The case $\phi = \top$:** we have always $\mathcal{M}, P \models \top$ and $\vdash c_P \wedge c_{\mathcal{M}} \to \top$, hence $\vdash c_P \wedge c_{\mathcal{M}} \to \phi$.

- **The case $\phi = \phi_1 \wedge \phi_2$:** $\mathcal{M}, P \models \phi$ iff $\mathcal{M}, P \models \phi_1$ and $\mathcal{M}, P \models \phi_2$.
Further, using the inductive hypothesis, we obtain $\vdash c_{\mathcal{M}} \wedge c_P \rightarrow \phi_1$ and $\vdash c_{\mathcal{M}} \wedge c_P \rightarrow \phi_2$.
Hence $\vdash c_{\mathcal{M}} \wedge c_P \rightarrow (\phi_1 \wedge \phi_2)$, i.e. $\vdash c_{\mathcal{M}} \wedge c_P \rightarrow \phi$.

- **The case $\phi = \phi_1 | \phi_2$:** $\mathcal{M}, P \models \phi$ iff $P \equiv Q|R$, $\mathcal{M}, Q \models \phi_1$ and $\mathcal{M}, R \models \phi_2$.
Using the inductive hypothesis,
$\vdash c_{\mathcal{M}} \wedge c_Q \rightarrow \phi_1$ and $\vdash c_{\mathcal{M}} \wedge c_R \rightarrow \phi_2$, i.e.
$\vdash c_{\mathcal{M}} \rightarrow (c_Q \rightarrow \phi_1)$ and $\vdash c_{\mathcal{M}} \rightarrow (c_R \rightarrow \phi_2)$.
Hence, using theorem 4.8 we obtain $\vdash c_{\mathcal{M}} \rightarrow (c_Q | c_R \rightarrow \phi_1 | \phi_2)$, i.e. $\vdash c_{\mathcal{M}} \wedge c_P \rightarrow \phi$.

- **The case $\phi = K_Q \top$:** $\mathcal{M}, P \models K_Q \top$ iff $P \equiv Q|R$, iff $c_P = c_Q | c_R$.
Using rule $E_R$4.4 we obtain $\vdash c_Q | c_R \rightarrow c_Q | \top$, further using axiom E4.4 $\vdash c_Q | c_R \rightarrow K_Q \top$, i.e. $\vdash c_P \rightarrow K_Q \top$. Hence $\vdash c_{\mathcal{M}} \wedge c_P \rightarrow \phi$.

- **The case $\phi = K_Q \psi$:** $\mathcal{M}, P \models K_Q \psi$, and because $\vdash K_Q \psi \rightarrow K_Q \top$ (by theorem 4.8), using the soundness, we obtain that $\mathcal{M}, P \models K_Q \top$. Now, we apply the previous case that gives

$$\vdash c_{\mathcal{M}} \wedge c_P \rightarrow K_Q \top \tag{14}$$

$\mathcal{M}, P \models K_Q \psi$ is equivalent with $P \equiv Q|R$ and for any $Q|S \in \mathcal{M}$ we have $\mathcal{M}, Q|S \models \psi$. Then the inductive hypothesis gives

$$\text{for any } Q|S \in \mathcal{M} \text{ we have } \vdash (c_{\mathcal{M}} \wedge c_Q | c_S) \rightarrow \psi \tag{15}$$

Consider now a process $Q|S \notin \mathcal{M}$. Because $\mathcal{M}$ is finite, we apply theorem 4.8 and obtain $\vdash c_{\mathcal{M}} \rightarrow \neg(c_Q | c_S)$ or equivalent,
$\vdash c_{\mathcal{M}} \wedge (c_Q | c_S) \rightarrow \bot$. But $\vdash \bot \rightarrow \psi$, hence

$$\text{for any } Q|S \notin \mathcal{M} \text{ we have } \vdash (c_{\mathcal{M}} \wedge c_Q | c_S) \rightarrow \psi \tag{16}$$

Now (15) and (16) together give

$$\text{for any } S \in \mathcal{M} \text{ we have } \vdash (c_{\mathcal{M}} \wedge c_Q | c_S) \rightarrow \psi \tag{17}$$

i.e., using theorem 4.7,

$$\vdash (c_{\mathcal{M}} \wedge c_Q | \bigvee_{S \in \mathcal{M}} c_S) \rightarrow \psi \tag{18}$$

But

$$\vdash K_0(\bigvee_{S \in \mathcal{M}} c_S) \rightarrow \bigvee_{S \in \mathcal{M}} c_S, \ hence \ \vdash c_{\mathcal{M}} \rightarrow \bigvee_{S \in \mathcal{M}} c_S$$

Now, we can apply rule $E_R$4.4 and obtain

$$\vdash c_Q | c_{\mathcal{M}} \rightarrow c_Q | \bigvee_{S \in \mathcal{M}} c_S, \ hence \ \vdash (c_Q | c_{\mathcal{M}} \wedge c_{\mathcal{M}}) \rightarrow (c_Q | \bigvee_{S \in \mathcal{M}} c_S \wedge c_{\mathcal{M}})$$

In this point, using (18) we obtain

$$\vdash (c_Q|c_{\mathcal{M}} \wedge c_{\mathcal{M}}) \rightarrow \psi \tag{19}$$

We have $\vdash c_{\mathcal{M}} \rightarrow (\top \rightarrow c_{\mathcal{M}})$ and $\vdash c_{\mathcal{M}} \rightarrow (c_Q \rightarrow c_Q)$ where from, applying theorem 4.8, we can derive $\vdash c_{\mathcal{M}} \rightarrow (c_Q|\top \rightarrow c_Q|c_{\mathcal{M}})$, i.e. $\vdash c_M \wedge c_Q|\top \rightarrow c_Q|c_{\mathcal{M}}$ and further

$$\vdash (c_M \wedge c_Q|\top) \rightarrow (c_{\mathcal{M}} \wedge c_Q|c_{\mathcal{M}})$$

Using this result together with (19), we obtain further

$$\vdash (c_M \wedge c_Q|\top) \rightarrow \psi,\ i.e.\ \vdash c_M \rightarrow (c_Q|\top \rightarrow \psi)$$

where we can apply axiom E4.4 that gives

$$\vdash c_{\mathcal{M}} \rightarrow (K_Q\top \rightarrow \psi)$$

applying theorem 4.8, we obtain

$$\vdash c_{\mathcal{M}} \rightarrow (K_Q\top \rightarrow K_Q\psi),\ i.e.\ \vdash (c_{\mathcal{M}} \wedge K_Q\top) \rightarrow K_Q\psi \tag{20}$$

But (14) gives

$$\vdash c_{\mathcal{M}} \wedge c_P \rightarrow K_Q\top \text{ where from } \vdash (c_{\mathcal{M}} \wedge c_P) \rightarrow (c_{\mathcal{M}} \wedge K_Q\top)$$

and using this in (20),

$$\vdash (c_{\mathcal{M}} \wedge c_P) \rightarrow K_Q\psi\ i.e.\ \vdash (c_{\mathcal{M}} \wedge c_P) \rightarrow \phi.$$

- **The case $\phi = \langle\alpha\rangle\psi$:** $\mathcal{M}, P \models \langle\alpha\rangle\psi$ means that exists $P' \in \mathcal{M}$ such that $P \xrightarrow{\alpha} P'$ and $\mathcal{M}, P' \models \psi$. Then the inductive hypothesis gives

$$\vdash c_{\mathcal{M}} \wedge c_{P'} \rightarrow \psi$$

$P \xrightarrow{\alpha} P'$ means that $P \equiv \alpha.R|S$ and $P' \equiv R|S$, so $c_P = (\langle\alpha\rangle c_R \wedge 1)|c_S$ and $c_{P'} = c_R|c_S$. So $\vdash c_{\mathcal{M}} \wedge c_R|c_S \rightarrow \psi$, i.e. $\vdash c_{\mathcal{M}} \rightarrow (c_R|c_S \rightarrow \psi)$ and using theorem 4.8

$$\vdash c_{\mathcal{M}} \rightarrow (\langle\alpha\rangle(c_R|c_S) \rightarrow \langle\alpha\rangle\psi) \tag{21}$$

theorem 4.7 gives $\vdash c_P \rightarrow \langle\alpha\rangle c_R|c_S \wedge 1|c_S$, hence

$$\vdash c_P \rightarrow \langle\alpha\rangle c_R|c_S \tag{22}$$

Axiom E4.4 gives

$$\vdash \langle\alpha\rangle c_R|c_S \rightarrow \langle\alpha\rangle(c_R|c_S) \tag{23}$$

Hence, from (21), (22) and (23) we derive

$$\vdash c_{\mathcal{M}} \rightarrow (c_P \rightarrow \langle\alpha\rangle\psi),\ i.e.\ \vdash (c_{\mathcal{M}} \wedge c_P) \rightarrow \langle\alpha\rangle\psi$$

- **The case** $\phi = \neg\psi$**:** we argue by induction on the syntactical structure of $\psi$.

  - **the subcase** $\psi = 0$**:** $\mathcal{M}, P \models \neg 0$ means that $P \not\equiv 0$. Then we can apply theorem 4.6 and obtain $\vdash c_P \rightarrow \neg 0$.
    So $\vdash c_{\mathcal{M}} \wedge c_P \rightarrow \neg 0$.
  - **the subcase** $\psi = \top$**:** is an impossible one as we cannot have $\mathcal{M}, P \models \bot$.
  - **the subcase** $\psi = \psi_1 \wedge \psi_2$**:** $\mathcal{M}, P \models \neg(\psi_1 \wedge \psi_2)$ is equivalent with $\mathcal{M}, P \models \neg\psi_1 \vee \neg\psi_2$, i.e. $\mathcal{M}, P \models \neg\psi_1$ or $\mathcal{M}, P \models \neg\psi_2$. By the inductive hypothesis, $\vdash c_{\mathcal{M}} \wedge c_P \rightarrow \neg\psi_1$ or $\vdash c_{\mathcal{M}} \wedge c_P \rightarrow \neg\psi_2$, where from we obtain $\vdash c_{\mathcal{M}} \wedge c_P \rightarrow \psi$
  - **the subcase** $\psi = \neg\psi_1$**:** $\mathcal{M}, P \models \neg\psi$ is equivalent with $\mathcal{M}, P \models \neg\neg\psi_1$, i.e. $\mathcal{M}, P \models \psi_1$ where we can use the inductive hypothesis $\vdash c_{\mathcal{M}} \wedge c_P \rightarrow \psi_1$ which is equivalent with $\vdash c_{\mathcal{M}} \wedge c_P \rightarrow \phi$.
  - **the subcase** $\psi = \psi_1|\psi_2$**:** $\mathcal{M}, P \models \neg(\psi_1|\psi_2)$ means that for any parallel decomposition of $P \equiv Q|R$, $\mathcal{M}, Q \models \neg\psi_1$ or $\mathcal{M}, R \models \neg\psi_2$. These imply, using the inductive hypothesis, that for any decomposition $P \equiv Q|R$ we have

    $$\vdash c_{\mathcal{M}} \rightarrow (c_Q \rightarrow \neg\psi_1) \; or \; \vdash c_{\mathcal{M}} \rightarrow (c_R \rightarrow \neg\psi_2)$$

    then we can apply theorem 4.8 that gives

    $$\vdash c_{\mathcal{M}} \wedge c_P \rightarrow \neg\psi.$$

  - **the subcase** $\psi = K_0\psi_1$**:** $\mathcal{M}, P \models \neg K_0\psi_1$ means $\exists R \in \mathcal{M}$ such that $\mathcal{M}, R \models \neg\psi_1$. Using the inductive hypothesis,
    $\vdash c_{\mathcal{M}} \wedge c_R \rightarrow \neg\psi_1$, i.e. $\vdash c_{\mathcal{M}} \rightarrow (c_R|c_0 \rightarrow \neg\psi_1)$. Now theorem 4.8 gives $\vdash c_{\mathcal{M}} \rightarrow \neg K_0\psi_1$, hence $\vdash c_{\mathcal{M}} \wedge c_P \rightarrow \neg K_0\psi_1$.
  - **the subcase** $\psi = K_Q\psi_1$**,** $Q \not\equiv 0$**:** we distinguish two cases
    - **the sub-subcase** $\psi_1 = \top$**:** $\mathcal{M}, P \models \neg K_Q\top$ implies that $Q$ is not a subprocess of $P$. Then for any $R \in \mathcal{M}$ we have $P \not\equiv Q|R$. Then theorem 4.6 gives us $\vdash c_{Q|R} \rightarrow \neg c_P$, i.e. $\vdash c_Q|c_R \rightarrow \neg c_P$. From here we can infer

      $$\vdash c_Q| \bigvee_{S \in \mathcal{M}} c_S \rightarrow \neg c_P \tag{24}$$

      But

      $$\vdash K_0(\bigvee_{S \in \mathcal{M}} c_S) \rightarrow \bigvee_{S \in \mathcal{M}} c_S, \; hence \; \vdash c_{\mathcal{M}} \rightarrow \bigvee_{S \in \mathcal{M}} c_S$$

      Now, we can apply rule $E_R$4.4 and obtain

      $$\vdash c_Q|c_{\mathcal{M}} \rightarrow c_Q| \bigvee_{S \in \mathcal{M}} c_S$$

In this point, using (24) we obtain

$$\vdash c_Q|c_{\mathcal{M}} \rightarrow \neg c_P \tag{25}$$

We have $\vdash c_{\mathcal{M}} \rightarrow (\top \rightarrow c_{\mathcal{M}})$ and $\vdash c_{\mathcal{M}} \rightarrow (c_Q \rightarrow c_Q)$ where from, applying theorem 4.8, we can derive $\vdash c_{\mathcal{M}} \rightarrow (c_Q|\top \rightarrow c_Q|c_{\mathcal{M}})$, i.e. $\vdash c_M \wedge c_Q|\top \rightarrow c_Q|c_{\mathcal{M}}$ Using this result together with (25), we obtain further

$$\vdash (c_M \wedge c_Q|\top) \rightarrow \neg c_P, \ i.e. \ \vdash c_M \wedge c_P \rightarrow \neg(c_Q|\top)$$

and axiom E4.4 gives

$$\vdash c_{\mathcal{M}} \wedge c_P \rightarrow \neg K_Q \top.$$

∗ **the sub-subcase** $\psi_1 \neq \top$**:** we distinguish two more cases $\mathcal{M}, P \models \neg K_Q \top$ and $\mathcal{M}, P \models K_Q \top$.

· **if** $\mathcal{M}, P \models \neg K_Q \psi_1$ and $\mathcal{M}, P \models \neg K_Q \top$, we have
$\vdash c_{\mathcal{M}} \wedge c_P \rightarrow \neg K_Q \top$ (proved before). Moreover, because $\vdash K_Q \psi_1 \rightarrow K_Q \top$ (theorem 4.8) we have
$\vdash \neg K_Q \top \rightarrow \neg K_Q \psi_1$ which gives $\vdash c_{\mathcal{M}} \wedge c_P \rightarrow \neg K_Q \psi_1$.

· **if** $\mathcal{M}, P \models \neg K_Q \psi_1$ and $\mathcal{M}, P \models K_Q \top$, $\exists Q|S \in \mathcal{M}$ with $\mathcal{M}, S|Q \models \neg \psi_1$. Using the inductive hypothesis we obtain $\vdash c_{\mathcal{M}} \rightarrow (c_S|c_Q \rightarrow \neg \psi_1)$ and from theorem 4.8 that $\vdash c_{\mathcal{M}} \rightarrow \neg K_Q \psi_1$. Hence $\vdash c_{\mathcal{M}} \wedge c_P \rightarrow \neg K_Q \psi_1$.

– **the subcase** $\psi = \langle \alpha \rangle \psi_1$**:** $\mathcal{M}, P \models \neg \langle \alpha \rangle \psi_1$ is equivalent with $\mathcal{M}, P \models [\alpha] \neg \psi_1$.
If there is a process $Q \in \mathcal{M}$ such that $P \xrightarrow{\alpha} Q$, then for any $Q \in \mathcal{M}$ such that $P \xrightarrow{\alpha} Q$ we have $\mathcal{M}, Q \models \neg \psi_1$. Using the inductive hypothesis we obtain that for any $Q \in \mathcal{M}$ such that $P \xrightarrow{\alpha} Q$ we have $\vdash c_{\mathcal{M}} \wedge c_Q \rightarrow \neg \psi_1$, i.e.

$$\vdash c_{\mathcal{M}} \wedge \bigvee \{c_Q \mid P \xrightarrow{\alpha} Q\} \rightarrow \neg \psi_1$$

or equivalently

$$\vdash c_{\mathcal{M}} \rightarrow (\bigvee \{c_Q \mid P \xrightarrow{\alpha} Q\} \rightarrow \neg \psi_1)$$

Using theorem 4.8, we obtain $\vdash c_{\mathcal{M}} \wedge c_P \rightarrow [\alpha] \neg \psi_1$.
If there is no process $Q \in \mathcal{M}$ such that $P \overset{\alpha}{\textbf{to}} Q$ then theorem 4.8 gives $\vdash c_P \rightarrow [\alpha] \bot$. But $\vdash \psi_1 \rightarrow \top$, hence $\vdash [\alpha] \bot \rightarrow [\alpha] \neg \psi_1$. So, also in this case we have $\vdash c_{\mathcal{M}} \wedge c_P \rightarrow [\alpha] \neg \psi_1$.

($\Longleftarrow$) Let $\vdash c_{\mathcal{M}} \wedge c_P \rightarrow \phi$. Suppose that $\mathcal{M}, P \not\models \phi$. Then $\mathcal{M}, P \models \neg \phi$. Using the reversed implication we obtain $\vdash c_{\mathcal{M}} \wedge c_P \rightarrow \neg \phi$, thus
$\vdash c_{\mathcal{M}} \wedge c_P \rightarrow \bot$. But from corollary 4.6 we have $\mathcal{M}, P \models c_{\mathcal{M}} \wedge c_P$ which, using the soundness, gives $\mathcal{M}, P \models \bot$ impossible!
Hence $\mathcal{M}, P \models \phi$. □

We recall the definitions of provability, consistency, satisfiability and validity.

[Provability and consistency] We say that a formula $\phi \in \mathcal{F}_{DES}^{\mathfrak{S}}$ is *provable in* $\mathcal{L}_{DES}^{\mathfrak{S}}$ (or $\mathcal{L}_{DES}^{\mathfrak{S}}$-*provable* for short), if $\phi$ can be derived, as a theorem, using the axioms and the rules of $\mathcal{L}_{DES}^{\mathfrak{S}}$. We denote this by $\vdash \phi$.
We say that a formula $\phi \in \mathcal{F}_{DES}^{\mathfrak{S}}$ is *consistent in* $\mathcal{L}_{DES}^{\mathfrak{S}}$ (or $\mathcal{L}_{DES}^{\mathfrak{S}}$-*consistent* for short) if $\neg\phi$ is not $\mathcal{L}_{DES}^{\mathfrak{S}}$-provable.

[Satisfiability and validity] We call a formula $\phi \in \mathcal{F}_{DES}^{\mathfrak{S}}$ *satisfiable* if there exists a context $\mathcal{M}$ and a process $P \in \mathcal{M}$ such that $\mathcal{M}, P \models \phi$.
We call a formula $\phi \in \mathcal{F}_{DES}^{\mathfrak{S}}$ *validity* if for any context $\mathcal{M}$ and any process $P \in \mathcal{M}$ we have $\mathcal{M}, P \models \phi$. In such a situation we write $\models \phi$.
Given a context $\mathcal{M}$, we denote by $\mathcal{M} \models \phi$ the situation when for any $P \in \mathcal{M}$ we have $\mathcal{M}, P \models \phi$.

$\phi$ is satisfiable iff $\neg\phi$ is not a validity, and vice versa, $\phi$ is a validity iff $\neg\phi$ is not satisfiable.

If $\phi$ is $\mathcal{L}_{DES}^{\mathfrak{S}}$-consistent then exists a context $\mathcal{M}$ and a process $P \in \mathcal{M}$ such that $\mathcal{M}, P \models \phi$.

**Proof** Suppose that for any context $\mathcal{M}$ and any process $P \in \mathcal{M}$ we do not have $\mathcal{M}, P \models \phi$, i.e. we have $\mathcal{M}, P \models \neg\phi$. Hence, for any finite context $\mathcal{M}$ and any process $P \in \mathcal{M}$ we have $\mathcal{M}, P \models \neg\phi$. Using lemma 4.9, we obtain $\vdash c_{\mathcal{M}} \wedge c_P \rightarrow \neg\phi$. Hence $\vdash c_{\mathcal{M}} \wedge \bigvee_{P \in \mathcal{M}} c_P \rightarrow \neg\phi$. But $\vdash c_{\mathcal{M}} \rightarrow \bigvee_{P \in \mathcal{M}} c_P$ which, combined with the previous result, implies $\vdash c_{\mathcal{M}} \rightarrow \neg\phi$.
Thus for each finite context $\mathcal{M}$ we have $\vdash c_{\mathcal{M}} \rightarrow \neg\phi$. But then for each context $\mathcal{M} \in \mathfrak{M}_{\neg\phi}^{act(\neg\phi)_+}$ we have $\vdash c_{\mathcal{M}} \rightarrow \neg\phi$. As $\mathfrak{M}_{\neg\phi}^{act(\neg\phi)_+}$ is finite, we can infer further $\vdash \bigvee_{\mathcal{M} \in \mathfrak{M}_{\neg\phi}^{act(\neg\phi)_+}} c_{\mathcal{M}} \rightarrow \neg\phi$. Now, applying rule $E_R$4.4, we obtain $\vdash \neg\phi$. This contradicts with the hypothesis of consistency of $\phi$. Hence, it exists a context $\mathcal{M}$ and a process $P \in \mathcal{M}$ such that $\mathcal{M}, P \models \phi$. □

[Completeness] The $\mathcal{L}_{DES}^{\mathfrak{S}}$ system is complete with respect to process semantics.

**Proof** Suppose that $\phi$ is a valid formula with respect to our semantics, but $\phi$ is not provable in the system $\mathcal{L}_{DES}^{\mathfrak{S}}$. Then neither is $\neg\neg\phi$, so, by definition, $\neg\phi$ is $\mathcal{L}_{DES}^{\mathfrak{S}}$-consistent. It follows, from lemma 4.9, that $\neg\phi$ is satisfiable with respect to process semantics, contradicting the validity of $\phi$. □

# 5 Concluding remarks

In this paper we developed Dynamic Epistemic Spatial Logic, $\mathcal{L}_{DES}^{\mathfrak{S}}$, which extends Hennessy-Milner logic with the parallel operator and with epistemic operators. The lasts are meant to express global properties over contexts. We propose these operators as alternative to the guarantee operator of the classical spatial logics, in order to obtaining a logic adequately expressive and decidable.

Obviously Dynamic Epistemic Spatial Logic is more expressive than guarantee-free Dynamic Spatial Logic as the first can express global properties. Still our logic is less expressive than the classic spatial logic. Indeed, using the guarantee operator and the characteristic formulas, we can express our epistemic operators in classic spatial logic, while guarantee operator cannot be expressed by using our logic:

$$K_Q\phi \stackrel{def}{=} c_Q|\top \wedge \ (\neg(c_Q|\top \rightarrow \phi) \triangleright \bot)$$

Still, as remarked in section 4.2, validity and satisfiability in a model can be expressed in our syntax. Combining this feature with the possibility to characterize processes and finite contexts, we may argue on utility of our logic in most of the CCS-like applications for which classic spatial logic was proposed.

In the context of decidability, our sound and complete Hilbert-style axiomatic system provides a powerful tool for making predictions on the evolution of the concurrent distributed systems. Knowing the current state or a sub-state of a system, we can characterize it syntactically. And because any other state can be characterized, we can project any prediction-like problem into the syntax and verify its satisfiability. Hence if the system we considered can reach the state we check, we will obtain that the formula is satisfiable and this method will provide also a minimal model. Thus we can make predictions without investigating (simulating) the full evolution of the system that might cause, sometimes, unsolvable computational problems (usually the time is branching generating exponential complexity).

The axioms and rules considered are very similar to the classical axioms and rules in epistemic logic, and some derivable theorems state meaningful properties of epistemic agents. All these relates our logic with the classical epistemic/doxastic logics and focus the specifications on external observers as epistemic agents. This interpretation is consistent with the spirit of process algebras.

Further researches are to be considered such as adding a Gabbay-Pitts operator [20] for specify new names and adding location operators. Challenging will be also the perspective of adding recursion in semantics.

**Acknowledgements.** We thank to Alexandru Baltag for contributing with valuable comments, since the beginning, on the construction of this logic. Thanks also to Luca Cardelli for comments and related discussions. The name *structural bisimulation* was suggested to us by Gordon Plotkin.

# References

[1] A. Baltag and L.S. Moss. Logics for epistemic programs. *Synthese (: Special Section: Knowledge, Rationality and Action).Editors: J. Symons, J. Hintikka. Special Section Editor: W. van der Hoek. Springer Science+Business Media B.V. ISSN: 0039-7857*, 139 (2):165–224, 2004.

[2] A. Baltag, L.S. Moss, and S. Solecki. The logic of public announcements. common knowledge and private suspicions. *CWI Technical Report SEN-R9922*, 1999.

[3] J. A. Bergstra. *Handbook of Process Algebra*. Elsevier Science Inc., New York, NY, USA, 2001.

[4] Patrick Blackburn, Maarten de Rijke, and Yde Venema. *Modal logic*. Cambridge University Press, New York, NY, USA, 2001.

[5] Luis Caires. Behavioral and spatial properties in a logic for the pi-calculus. *In Igor Walukiwicz, editor, Proc. of Foundations of Software Science and Computation Structures2004, Lecture Notes in Computer Science, Springer-Verlag*, vol:2987, 2004.

[6] Luis Caires and Luca Cardelli. A spatial logic for concurrency (part ii). *In Proceedings of CONCUR'2002, Lecture Notes in Computer Science, Springer-Verlag*, vol:2421, 2002.

[7] Luis Caires and Luca Cardelli. A spatial logic for concurrency (part i). *Information and Computation*, Vol: 186/2:194–235, November 2003.

[8] Luis Caires and Etienne Lozes. Elimination of quantifiers and decidability in spatial logics for concurrency. *In Proceedings of CONCUR'2004, Lecture Notes in Computer Science, Springer-Verlag*, vol:3170, 2004.

[9] Cristiano Calcagno, Luca Cardelli, and Andrew D. Gordon. Deciding validity in a spatial logic for trees. *In Proceedings of the ACM Workshop on Types in Language Design and Implementation*, pages 62–73, 2003.

[10] Luca Cardelli. Bioware languages. *In: Andrew Herbert, Karen Sprck Jones (Eds.): Computer Systems: Theory, Technology, and Applications - A Tribute to Roger Needham, Monographs in Computer Science. Springer*, ISBN 0-387-20170-X.:59–65., 2004.

[11] Luca Cardelli and Andrew D. Gordon. Mobile ambients. In *Foundations of Software Science and Computation Structures: First International Conference, FOSSACS '98*. Springer-Verlag, Berlin Germany, 1998.

[12] Luca Cardelli and Andrew D. Gordon. Ambient logic. *To appear in Mathematical Structures in Computer Science*, 2003.

[13] Witold Charatonik, Andrew D. Gordon, and Jean-Marc Talbot. Finite-control mobile ambients. In *ESOP '02: Proceedings of the 11th European Symposium on Programming Languages and Systems*, pages 295–313. Springer-Verlag, 2002.

[14] Witold Charatonik and Jean-Marc Talbot. The decidability of model checking mobile ambients. *Proceedings of the 15th Annual Conference of the European Association for Computer Science Logic, Springer-Verlag*, 2142 of Lecture Notes in Computer Science:339–354, 2001.

[15] B. Chellas. *Modal logic. An introduction*, volume Cambridge UP, Cambridge. 1980.

[16] M. Dam. Proof systems for $\pi$-calculus. *In de Queiroz, editor, Logic for Concurrency and Synchronisation, Studies in Logic and Computation. Oxford University Press. To appear.*

[17] M. Dam. Relevance logic and concurrent composition. *In Proceedings of Third Annual Symposium on Logic in Computer Science, Edinburgh, Scotland, July 1988. IEEE Computer Society.*, pages 178–185.

[18] M. Dam. Model checking mobile processes. *Information and Computation*, vol:129(1):35–51, 1996.

[19] Ronald Fagin, Joseph Y. Halpern, Yoram Moses, and Moshe Y. Vardi. *Reasoning about Knowledge*. MIT Press, 1995.

[20] M. Gabbay and A. Pitts. A new approach to abstract syntax involving binders. *To appear in Formal Aspects of Computing*.

[21] R. Goldblatt. *Logics of time and computation*, volume CSLI, Stanford. 1987.

[22] J. Y. Halpern and Y. Moses. A guide to completeness and complexity for modal logics of knowledge and belief. *Artificial Intelligence*, 54:319–379, 1992.

[23] D Harel, D. Kozen, and J. Tiuryn. *Dynamic Logic*. MIT Press, 2000.

[24] M. Hennessy and R. Milner. Algebraic laws for nondeterminism and concurrency. *JACM*, vol: 32(1):137–161, 1985.

[25] G. E. Hughes and M. J. Cresswell. *A new introduction to modal logic*, volume Routledge, London. 1996.

[26] W. Groeneveld J. Gerbrandy. Reasoning about information change. *Journal of Logic, Language and Information*, 6:146–169, 1997.

[27] R. Mardare and C. Priami. A logical approach to security in the context of ambient calculus. *ENTCS*, vol. 99, 2004.

[28] R. Mardare, C. Priami, P. Quaglia, and A. Vagin. Model checking biological systems described using ambient calculus. *Proceedings of CMSB04, Lecture Notes in BioInformatics. Berlin: Springer-Verlag*, 3082: 3:85– 10, 2005.

[29] R. Milner, J. Parrow, and D. Walker. Modal logics for mobile processes. *Theoretical Computer Science*, vol:114:149–171, 1993.

[30] Gordon D. Plotkin. A structural approach to operational semantics. *Technical Report FN-19, DAIMI, Department of Computer Science, University of Aarhus, Aarhus, Denmark*, 43, September 1981.

[31] Colin Stirling. *Modal and temporal properties of processes*. Springer-Verlag New York, Inc., New York, NY, USA, 2001.

[32] J. F. A. K. van Benthem. Games in dynamic epistemic logic. *Bulletin of Economic Research, Los Altos*, 53(4):219–248, 2001.

[33] J. F. A. K. van Benthem. Logic for information update. *In Proceedings of TARK01, Los Altos*, 2001.

[34] H. van Ditmarsch. Knowledge games. *Bulletin of Economic Research*, 53(4):249–273, 2001.