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

Technical Report CoSBi 02/2007

Dynamic-Epistemic reasoning on distributed systems

Radu Mardare

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

mardare@cosbi.eu

This is the preliminary version of a paper that will appear in
In Proceedings of the second Conference on Algebra and Coalgebra in Computer Science (CALCO2007), LNCS 4624, Springer, 2007.

Dynamic-Epistemic reasoning on distributed systems

Radu Mardare

The Microsoft Research-University of Trento, Italy

September 30, 2009

Abstract

We propose a new logic designed for modelling and reasoning about information flow and information exchange between spatially located (but potentially mobile), interconnected *agents* witnessing a distributed computation. This is a major problem in the field of distributed systems, covering many different issues, with potential applications from Computer Science and Economy to Chemistry and Systems Biology.

Underpinning on the dual algebraical-coalgebraical characteristics of process calculi, we design a decidable and completely axiomatizad logic that combines the process-algebraical/equational and the modal/coequational features and is developed for process-algebraical semantics. The construction is done by mixing operators from dynamic and epistemic logics with operators from spatial logics for distributed and mobile systems.

1 Introduction

Observation is fast becoming an important topic in computer science. In which manner can observation (in the broad sense of the word) influence the way of computing? In which way can the partial information available to an external observer of a computational system be used in deriving knowledge about the overall complete system? We will approach these problems by developing a logic designed to handle (partial) information flow and information exchange between external observers (agents) of a distributed system.

In the context of distributed computation, a concurrent computational system can be thought of as being composed of a number of *modules*, i.e. spatially localized and independently observable units of behavior and computation (e.g. programs or processors running in parallel), organized in networks of subsystems and being able to interact, collaborate, communicate and interrupt each other. Moreover, with the development of mobile computation, modules (subsystems) are able to move across networks. We shall consider *agents* - *external observers* of the modules. As an external observer, an agent witnesses the global computation and interacts with the whole system only by means of its module. Thus it derives its knowledge about the overall system from the observed behavior of its subsystem and from epistemic reasoning on the knowledge (and reactions) of other agents witnessing the same computational process (possibly from a different perspective). The mobility of modules allows agents to even "penetrate" inside other modules, either “legally” (i.e. with the proper authorizations) or “illegally” (by taking advantage of some security failures).

In this context, one has to face issues concerning control over information and its flow (specifications of when agents can acquire, communicate and protect truthful, relevant, preferably exclusive information), and hence issues of privacy, secrecy, belief, trust, authentication etc; all these in the context of concurrent computation. The general problem approached in this paper has thus to do with modelling and reasoning about information flow and information exchange between spatially located (but potentially mobile), interconnected *agents*. This is a major problem in the field of distributed systems, covering many different issues, with potential applications: in Secure Communication (checking secrecy and authentication for given communication protocols), in Debugging and Performance analysis (checking for the cause of errors or of high computational costs in a system where we can control only some modules), in Artificial Intelligence (endowing artificial agents with good and flexible tools to reason about their changing environment and about each other), in designing and improving strategies for knowledge acquisition over complex networks (such as the Internet), etc.

Lately, in experimental sciences, such as Systems Biology or Bio-Chemistry, the possibility has been considered to construct tools for analysing and simulating bio-systems *in silico*. The approach is based on the partial information we have about the live systems (obtained from *in vivo* experiments). We are just external observers of a bio-system and we observe only a subpart of it (which we consider essential with respect to the problem we want to approach). It is not realistic to suppose that we will ever have complete information about a live system [**?**]. From this partial information we want to understand the behavior of the system and to design a method to control it. Hence, the success of our approach depends on our ability to manipulate partial information and to extract knowledge from it.

In approaching this problem we have chosen the process-algebraical representation of (mobile) distributed system and we developed a logic of information flow for process-algebraical semantics. Taking process calculi as semantics is theoretically challenging due to their dual algebraical/coalgebraical nature. While the algebraical features of processes are naturally approached in equational fashion (that reflects, on logical level, the program constructors), the coalgebraical features (intrinsically related to transition systems via the denotational and the operational semantics of process calculi) ask for a modal/coequational treatment. The modal approach is also needed for developing the epistemic reasoning.

Consequently, our paper combines two logical paradigms to information flow in distributed systems: *dynamic-epistemic (and doxastic) logics* [20, 15, 18], semantically based on epistemic-doxastic Kripke models; and the spatial logics for concurrency [8, 9, 10], for which the semantics is usually given in terms of process algebra. The intention is to develop and study a decidable and completely axiomatized process-based multimodal logic able to capture the complexity of the process-algebraical semantics.

Finally, we are interested in using this tool for the general task of modelling and classifying various types of information exchanges in distributed settings, and more specifically for the concrete task of reasoning about, verifying and designing communication protocols in an open, mobile environment.

2 Using partial information

In this section we will show how, playing with partial information about a system, we can derive properties of the whole system. For this we reconsider a variant of the muddy children puzzle [15] adapted for our paradigm.

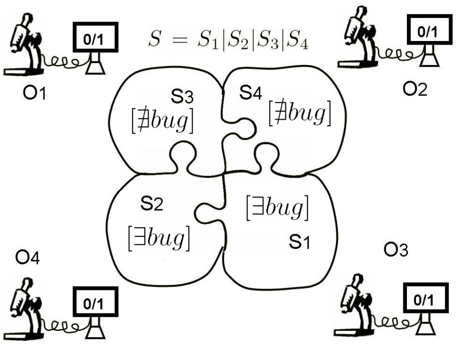

Figure 1: The system S

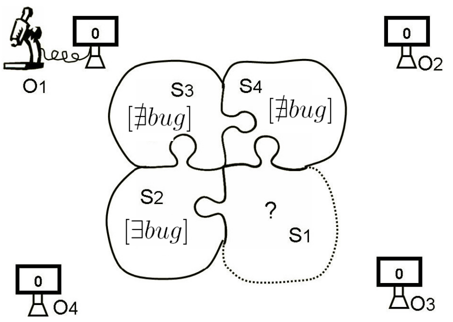

Figure 2: The perspective of O_1

Consider a computational system S composed by four disjoint modules S_1, S_2, S_3 and S_4 running in parallel (Figure 1). Syntactically, we describe this situation using the parallel operator $S = S_1|S_2|S_3|S_4$. Each module is characterized by the presence/absence of a "bug" that might generate undesirable behavior. Suppose, in addition, that the system is analyzed by four observers, each observer having access to a subpart of S. Thus, observer O_1 can see the subsystem $S_2|S_3|S_4$, O_2 the subsystem $S_3|S_4|S_1$, O_3 can see the subsystem $S_4|S_1|S_2$ and observer O_4 sees $S_1|S_2|S_3$. Each observer has a display used for making public announcements.

The observers know that each module of the system S might contain a bug and that the system contains at least one bug. Each observer tries to compute the exact number of them and their positions in the system. In doing this the observers do not communicate but they make public announcements concerning their knowledge about the system. Thus, each observer displays 0 until it knows the exact number and positions of the bugs in the system, at which point it switches to 1. In addition, the observers are synchronized by a clock that counts each step of computation. After each "tic" the observer has to evaluate its knowledge and to decide if its display remains on 0 or switches to 1. Thus, each observer computes information about the whole system by using the partial information it possesses and by evaluating the knowledge of the other observers (by reading their displays). If an observer is able to decide the correct number of bugs and their exact positions in the system, then it succeeded to do this with a lower cost than the cost of fully investigating the system. Hereafter we show that such a deduction is possible.

Consider that the real state of the system is the one in Figure 1. And suppose that we can control only the observer O_1. As O_1 sees the subsystem $S_2|S_3|S_4$, it sees a bug in subsystem S_2 and no bugs in S_3 and S_4 (Figure **??** represents the perspective of O_1). But it does not know if the system S_1 contains a bug or not. For O_1 both situations are equally possible. Hence, after the first round of computation the display of O_1 remains 0. Concerning observer O_2, it sees a bug in S_1, but it does not know if there is one also in S_2, thus, after the first round, it will show 0 too.

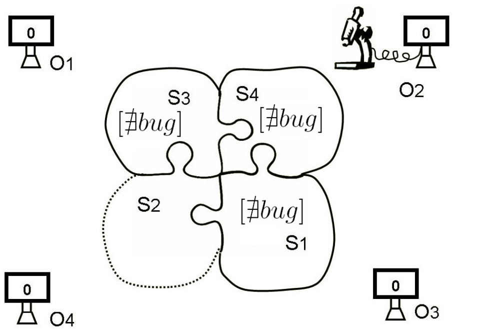

Figure 3: A hypothetical perspective of O_2

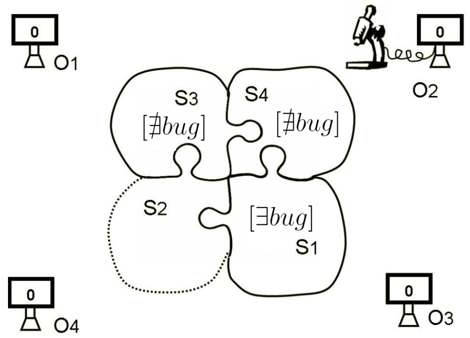

Figure 4: The real perspective of O_2

The second round of computation starts. O_1 has seen that, after the first round, the observer O_2 has not succeeded in understanding the situation (as O_2 shows 0 on its display). If the system S_1 does not contain a bug then, in the first round, O_2 would have seen no bugs (Figure **??**). O_2 also knows that there is at least one bug in the system. Hence, if this was the case, O_2 had enough information to decide, in the first round, that the only bug of the system is in S_2. Consequently, 1 had to appear on its display. But this was not the case. This means that what O_2 observed was the situation presented in Figure **??**. Therefore, O_1 is able to decide that the real situation of the system is the one with a bug in S_1 and it will display 1. The example works similarly in more complex situations.

Observe the advantages of this analysis: using only the partial information available to O_1 and judging the behavior of the other observers, we were able to compute the real configuration of the system. The observers do not exchange information about S, but only about their level of understanding S. The rest can be computed. If each subsystem is very complex then the complete information about the system can be larger than an observer can store or manipulate. Note also that the observers do not need a central unit for organizing their information. Each observer organizes its own information and makes public announcements about its level of knowledge. They work simultaneously in a distributed network and, only playing with their partial information about S and with the information about the state of the network, they are able to derive overall properties of the system.

3 The main problem and alternative approaches

We can consider even more complex examples where the system itself evolves while it is observed and where the agents can also interact with the system as a response to their level of knowledge about it. In such a case we can identify two parallel levels of the model. On one level we have the evolution of the system and, in each state of the system, there is a second level - the evolution of the knowledge of the agents with respect to the system. As underlined in [2] it is difficult to collapse the two in one Kripke-style semantics.

There are three kinds of modal logics of relevance to our subject: *epistemic/doxastic logics* [20, 15], *dynamic logics* [18] and *spatial logics* [9, 8]. The usual semantics for the first two is in terms of Kripke models, while the third was developed as a logic for concurrent processes, with semantics given in terms of process calculi.

3.1 Kripke-model based logics

Epistemic/doxastic logics [15] 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 that ϕ) or $\Box_A\phi$ (A justifiably believes that ϕ). In the models of these logics each basic modality is associated to a binary *"accessibility"* relation interpreted as an *"indistinguishability"* relation $\overset{A}{\textbf{to}}$ for each agent A. It expresses the agent's uncertainty about the current state. The states s' such that $s\overset{A}{\textbf{to}}s'$ 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 multiagent systems.

Dynamic logics [18] are closer to process calculi, in that they have names for "programs", or "actions", and ways 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 ϕ. Modalities in a dynamic logic form an algebraic structure: programs are built using basic program constructors such as $\pi.\pi'$ (sequential composition) or π^* (iteration), etc.

Dynamic Epistemic Logics. By combining the dynamic and epistemic formalisms a class of logics have been developed [2, 3, 17, 4, 14] for specifying properties of evolving knowledge and beliefs in dynamic systems. The high level of expressivity reaches here a low complexity (decidability and complete axiomatizations). Further, all these approaches have been generalized by the so called *Logics of Epistemic Programs* [2, 3]. These are based on the concept of *"epistemic programs"* - models for informational changes, providing a representation of the inherent epistemic features of a program (what is happening, what does each agent "think" is happening, what does it think the others think etc). In this approach the uncertainties about the current action of the system are also modelled as Kripke models. So, an epistemic program is essentially just an epistemic Kripke model, but whose elements are now interpreted as "actions". Each action σ has attached a precondition σ_0, telling us when σ can be executed. To see how an epistemic program changes an epistemic situation, [1] proposes a binary operation, taking "static" models (i.e. epistemic Kripke models of possible input states) and "dynamic" models (i.e. epistemic programs) and returning other static models (of possible output states). The operation associates to each pair (s, σ) of a state and an action an input state s', provided the action's precondition σ_0 is satisfied by the state s.

3.2 Process logics

In modeling parallel distributed (and mobile) systems process algebra imposes itself as a malleable tool useful in many applications. In this paradigm, typically, one considers various operations with processes, corresponding to known program constructors: sequential composition $\alpha.P$, various notions of parallel composition $P|P'$ (some of which involve communication), replication $!P$ etc. These calculi are also adapted to deal with mobility, i.e. changes affecting the communication network (redirecting communication channels, creating new ones, sending not just information, but the processes themselves, over channels). Further, for specifying properties of distributed systems different types of logics have been developed for semantics based on process calculi.

Process Logics. Process semantics for modal logics can be considered as a special case of Kripke semantics, since it involves structuring a class of processes as a Kripke model, by endowing it with accessibility relations, and then using the standard clauses of Kripke semantics. The most obvious accessibility relations on processes are the ones induced by action transitions $\alpha.P$, and thus the corresponding (Hennessy- Milner) logic [19] was the first process-based modal logic that was developed. Later, temporal, mobile and concurrent features have been added [32, 13, 29].

Spatial logics. A relatively new type of process logics are spatial logics [8, 9, 10], which are particularly tailored for reasoning about mobility and security, since they capture spatial properties of processes, i.e. properties which depend on location. Informally, these are properties such as *"the agent has gone away"*, *"eventually the agent crosses the firewall"*, *"somewhere there is a virus"* etc. Among the various spatial operators we mention: the *parallel operator* $\phi|\psi$ and its adjoint - the *guarantee operator* $\phi \triangleright \psi$; operators designed for expressing the *"new name features"* that are central in security - *revelation* and *hiding operators*, inspired by the Gabbay-Pitts quantifier [16]. In addition, most of these logics include temporal modalities and quantifiers. Though expressive and useful, most spatial logics proved to be undecidable, even in the absence of quantifiers.

4 A unified paradigm

In this paper we will collapse the two paradigms and propose a unified one. We give a spatial interpretation of epistemic modalities in CCS: if we associate to each "agent" A the process P describing the behavior of the module observed by A, then the agent observing a process (possibly running in parallel with many other processes) *"knows"* only the activity and actions of its own process. *"Knowledge"* is thus identified with "information (about the overall, global process) that is locally available (to an agent observing a subprocess)". In effect, this organizes any class $\mathcal{M}$ of processes (thought of as "states") as an epistemic Kripke model, with indistinguishability relations $\overset{A}{\textbf{to}}$ for each agent A observing the subprocess P, given by: $P|P'\overset{A}{\textbf{to}}P|P''$ for any P', P''. Since these are equivalence relations, we obtain a notion of "(truthful) knowledge". The resulting Kripke modality, $K_A\phi$, read the agent A knows ϕ, holds at a given state (process) R iff the process P is active (as a subprocess) at R and property ϕ holds in any context in which P is active.

We capture a very simplified analogue of the above notion of *"appearance of an action to an agent"* by stating that an agent A can *"see"* only the actions of the process P it observes. To make this precise, we need to keep track of which actions are executed by which module, by defining "signed" transitions of the form $Q \overset{A:\alpha}{\textbf{to}} R$ whenever $Q \equiv P|S$, $R \equiv P'|S$ and $P\overset{\alpha}{\textbf{to}}P'$. The corresponding dynamic modalities are of the form $[A : \alpha]\phi$, exhibiting the agent A doing/witnessing the action α.

The resulting logic is completely axiomatizable and decidable. The Hilbert-style axiomatics we propose for it presents our logic as an authentic dynamic-epistemic logic. The classical axioms of knowledge will be present in our system.

Unlike in standard dynamic-epistemic logic, our agents are now structured: the process algebraical structure defined on the modules of the system can be projected on the ontology of agents. Thus we can have the agent $A_1|A_2$ which is the agent seeing the process $P_1|P_2$, where the agent A_1 sees P_1 and the agent A_2 sees P_2. In this way the knowledge of the agent $A_1|A_2$ contains the common knowledge of A_1 and of A_2 together with all the properties that derive from the fact that P_1 and P_2 runs in parallel. Similarly we might speak of the agent $\alpha.A$ as the agent seeing the process $\alpha.P$ when A is an agent seeing P. This algebraical structure on the level of ontology of agents is relevant in many applications and there is no trivial way to mimic it using classical epistemic logics.

5 On processes

In this section we introduce a fragment of CCS [27] calculus that is representative for process algebra being "the core" of most of the process calculi. This fragment will be used further as semantics for our logic. For the proofs of the results presented in this section and for additional results on the subject, the reader is referred to [25, 23, 24].

5.1 CCS processes

Definition 5.1 (Processes) *Let $\mathbb{A}$ be a denumerable signature. The syntax of the calculus is given by a grammar with one non-terminal symbol P and the productions*

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

where $\alpha \in \mathbb{A}$. We denote by $\mathbb{P}$ the language generated by this grammar. We call the elements of $\mathbb{A}$ (basic) actions *and the objects in* $\mathbb{P}$ processes.

Definition 5.2 (Structural congruence) *Let $\equiv \subseteq \mathfrak{P} \times \mathfrak{P}$ be the smallest equivalence relation defined on $\mathbb{P}$ such that*

1. $(\mathbb{P}, |, 0)$ *is a commutative monoid with respect to $\equiv$;*

2. *$\equiv$ is a congruence on the syntax of $\mathbb{P}$, i.e. if $P', P'' \in \mathbb{P}$ such that $P' \equiv P''$ then $\alpha.P' \equiv \alpha.P''$ and $P'|P \equiv P''|P$ for any $P \in \mathbb{P}$ and $\alpha \in \mathbb{A}$.*

Definition 5.3 *We call a process P* guarded *iff $P \equiv \alpha.Q$ for $\alpha \in \mathbb{A}$. We denote $P^0 \overset{def}{=} 0$ and $P^k \overset{def}{=} \underbrace{P|...|P}_{k}$.*

Definition 5.4 (Labelled transition system) *We consider on $\mathfrak{P}$ the labelled transition system*[1] *$\mathfrak{P}\textbf{\textit{to}}\mathbb{A} \times \mathfrak{P}$ defined by the next rules.*

$$\alpha.P\overset{\alpha}{\textbf{\textit{to}}}P \qquad\qquad P{\equiv}\ Q$$
$$P\overset{\alpha}{\textbf{\textit{to}}}P'\ Q\overset{\alpha}{\textbf{\textit{to}}}P' \qquad\qquad P\overset{\alpha}{\textbf{\textit{to}}}P'\ P|Q\overset{\alpha}{\textbf{\textit{to}}}P'|Q$$

Definition 5.5 (Extended transition system) *We write $P \xrightarrow{Q:\alpha} P'$ whenever $P \equiv Q|R$, $P' \equiv Q'|R$ and $Q \xrightarrow{\alpha} Q'$. We call this* composed transition *and its label $(Q : \alpha)$* composed action. *We consider the set $\mathbb{A}^*$ of all basic and complex actions. Hereafter we use a to range over $\mathbb{A}^*$, while α will be used to refer to arbitrary objects of $\mathbb{A}$.*
We extend the transition system previously defined to $\mathfrak{P}\textbf{\textit{to}}\mathbb{A}^* \times \mathfrak{P}$ that includes the composed transitions.

Definition 5.6 *We call a process P* guarded *iff $P \equiv \alpha.Q$ for $\alpha \in \mathbb{A}$.*
We introduce the notation $P^k \overset{def}{=} \underbrace{P|...|P}_{k}$, 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.

5.2 Size of a process

Definition 5.7 *We define, inductively, the* size $P = (h, w)$ *(*height *and* width*) of a process P:*

1. $0 \overset{def}{=} (0, 0)$
2. $P \overset{def}{=} (h, w)$ *iff $P = (\alpha_1.Q_1)^{k_1}|...|(\alpha_j.Q_j)^{k_j}$,*

for $Q_i = (h_i, w_i)$ and $h = 1 + max(h_1, .., h_k)$, $w = max(k_1, .., k_j, w_1, .., w_j)$.
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 $w_1 < w_2$.

The intuition is that the size of a process is given by the depth of its syntactic tree and by the maximum number of bisimilar processes that can be found in a node of the syntactic tree. Observe that, by construction, the size of a process is unique up to structural congruence.

[1] We did not consider the communication transition as, on the logical level, we can express it as a composition of dynamic operators.

Example 5.1 *The size for some processes:*
1. $0 = (0, 0)$ 4. $\alpha.0|\alpha.0 = (1, 2)$
2. $\alpha.0 = (1, 1)$ 5. $\alpha.\alpha.0 = \alpha.\beta.0 = (2, 1)$
3. $\alpha.0|\beta.0 = (1, 1)$ 6. $\alpha.(\beta.0|\beta.0) = (2, 2)$

Definition 5.8 *For a set $M \subset \mathbb{P}$ we define*[2] $M \overset{def}{=} max\{P \mid P \in M\}$.

5.3 Structural bisimulation

Hereafter we introduce the *structural bisimulation*, a relation on processes that is an approximation of the structural congruence defined on size. It analyzes the behavior of a process focusing on a boundary of its syntactic tree. This relation is similar with the pruning relation proposed in [6] for the syntactic trees of ambient calculus.

Definition 5.9 (Structural bisimulation) *Let $P, Q \in \mathbb{P}$. We define $P \approx_h^w Q$ by:*
$P \approx_0^w Q$ always
$P \approx_{h+1}^w Q$ iff $\forall i \in 1..w$ and $\forall \alpha \in \mathbb{A}$ 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 5.2 *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 5.9 and decide that $R \approx_2^2 S$. But $R \not\approx_3^2 S$ because on the depth 2 R has an action α (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 α 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 $R'' \approx_0^3 S''$

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

Theorem 5.1 (Equivalence Relation) *The relation $\approx_h^w$ on processes is an equivalence relation.*

[2] Observe that not any set of processes has a size, as for an infinite set it might be not possible to have the maximum required. However we accept the definition and we will use it only where it is well-defined.

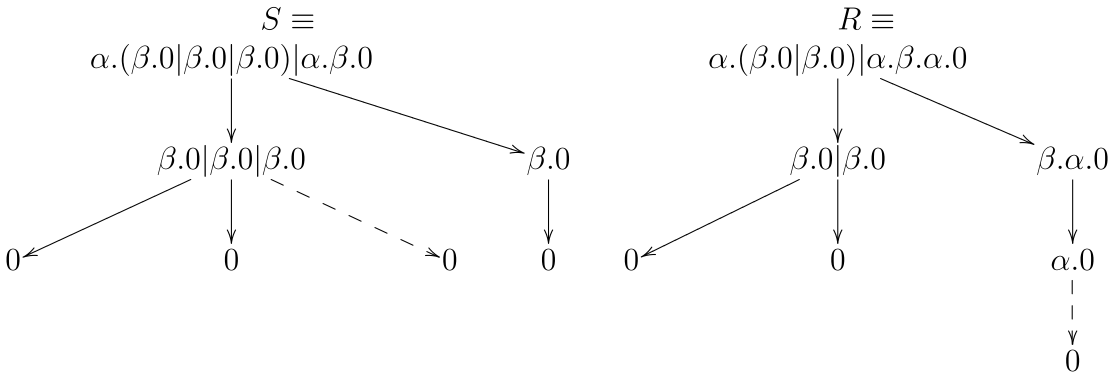
$S \equiv$
$\alpha.(\beta.0|\beta.0|\beta.0)|\alpha.\beta.0$
$\beta.0|\beta.0|\beta.0$
$\beta.0$
0
0
0
0
$R \equiv$
$\alpha.(\beta.0|\beta.0)|\alpha.\beta.\alpha.0$
$\beta.0|\beta.0$
$\beta.\alpha.0$
0
0
$\alpha.0$
0

Figure 1: Syntactic trees

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 5.9.
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 5.9, 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 5.9, 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 5.9, 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 5.9, 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 $P \approx_h^w R$. □

Theorem 5.2 *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 $P \approx_h^w R$. □

Theorem 5.3 (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. □

Theorem 5.4 (Congruence) *$\approx_h^w$ is an equivalence relation on processes having the properties:*

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 5.9, $\alpha.P \approx_{h+1}^w \alpha.Q$.

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 $i = 1..w$, α 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

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

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 $P|Q \approx_{h+1}^w P'|Q'$. □

Theorem 5.5 (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[3]:

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

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 5.4. □

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 the size of the processes, then our relation will describe structurally congruent processes.

Theorem 5.6 *If $P \leq (h, w)$ and $P' \leq (h, w)$ then $P \approx_h^w P'$ iff $P \equiv P'$.*

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

Theorem 5.7 *If $P \approx_h^w Q$ and $P < (h, w)$ then $P \equiv Q$.*

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 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.

Theorem 5.8 *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 5.2.
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, $P \equiv P'$. □

Theorem 5.9 *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. $Q \equiv P$. □

Theorem 5.10 *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 5.5, 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 5.9, that $Q_1 \equiv R$, hence $Q \equiv R|Q_2$. □

Theorem 5.11 *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 $Q|Q'$). □

The next theorem proves that the structural bisimulation is preserved by transitions with the price of decreasing the size.

Theorem 5.12 (Behavioral simulation) *Let $P \approx^w_h Q$.*
1. If $P \xrightarrow{\alpha} P'$ then it exists a transition $Q \xrightarrow{\alpha} Q'$ such that $P' \approx^{w-1}_{h-1} Q'$.
2. If $R < (h,w)$ and $P \xrightarrow{R:\alpha} P'$ then it exists a transition $Q \xrightarrow{R:\alpha} Q'$ 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 5.11 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 $Q' \equiv S'|S''$. □

5.4 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.

Theorem 5.13 (Bound pruning theorem) *For any process $P \in \mathbb{P}$ and any (h, w) exists a process $Q \in \mathbb{P}$ with $P \approx_h^w Q$ and $Q \leq (h, w)$.*

Proof We construct [4] Q inductivelly on h.

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

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

Let P_i' be the result of pruning P_i by (h, w) (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 5.4, that $\alpha_i.P_i \approx_{h+1}^w \alpha_i.P_i'$, hence $P \approx_{h+1}^w P'$. Consider now $P' \equiv (\beta_1.Q_1)^{k_1}|...|(\beta_m.Q_m)^{k_m}$. Let $l_i = min(k_i, w)$ for $i = 1..m$. Further 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, $Q \leq (h + 1, w)$. □

Definition 5.10 *For a process P and 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 5.13.*

Theorem 5.14 *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 5.13. □

Theorem 5.15 $P \leq (h, w)$ *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 5.8 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. $P_{(h,w)} \not\equiv P$. But this is impossible, because the size of a process is unique up to structural congruence, see remark **??**. □

Example 5.3 *Consider the process $P \equiv \alpha.(\ \beta.(\gamma.0|\gamma.0|\gamma.0)\ |\ \beta.\gamma.0\ )\ |\ \alpha.\beta.\gamma.0$.*
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 $P_{(3,2)} = \alpha.(\ \beta.(\gamma.0|\gamma.0)\ |\ \beta.\gamma.0)\ |\ \alpha.\beta.\gamma.0$
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 $P_{(2,2)} = \alpha.(\beta.0|\beta.0)\ |\ \alpha.\beta.0$. Going further we obtain the smaller processes $P_{(0,0)} = 0$, $P_{(1,1)} = \alpha.0$, $P_{(1,2)} = \alpha.0|\alpha.0$, $P_{(2,1)} = \alpha.\beta.0$.

[4] This construction is not necessarily unique.

5.5 Substitutions

For the future constructs is also useful to introduce the substitutions of actions in a process.

Definition 5.11 (The set of actions of a process) *We define inductively, for any process P, its set of actions $Act(P) \subset \mathbb{A}$:*
1. $Act(0) \overset{def}{=} \emptyset$ 2. $Act(\alpha.P) \overset{def}{=} \{\alpha\} \cup Act(P)$ 3. $Act(P|Q) \overset{def}{=} Act(P) \cup Act(Q)$
For $M \subset \mathbb{P}$ we define $Act(M) \overset{def}{=} \bigcup_{P \in M} Act(P)$.

Definition 5.12 *Let $A \subset \mathbb{A}$. We define*

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

Theorem 5.16 *If $A \subset \mathbb{A}$ is finite, then $\mathfrak{P}^A_{(h,w)}$ is finite*[5]*.*

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 $card(\mathfrak{P}^A_{(h+1,w)}) = \underbrace{n^{n^{\cdots^{n}}}}_{h+1}$. □

Definition 5.13 (Action substitution) *We call* action substitution *any mapping $\sigma : \mathbb{A}$**to**$\mathbb{A}$. We extend it, syntactically, to processes, $\sigma : \mathbb{P}$**to**$\mathbb{P}$, by*

1. $\sigma(0) \overset{def}{=} 0$ 2. $\sigma(P|Q) \overset{def}{=} \sigma(P)|\sigma(Q)$ 3. $\sigma(\alpha.P) \overset{def}{=} \sigma(\alpha).\sigma(P)$

For $M \subset \mathbb{P}$ let $\sigma(M) \overset{def}{=} \{\sigma(P) \mid P \in M\}$. We also use M^σ, P^σ for denoting $\sigma(M)$ and $\sigma(P)$. The set of actions of σ, *$act(\sigma)$, is defined as $act(\sigma) \overset{def}{=} \{\alpha, \beta \in \mathbb{A} \mid \alpha \neq \beta,\ \sigma(\alpha) = \beta\}$.*

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

6 Maximal consistency

Anticipating the logic, in this section we define some special sets of processes that will play an essential role in proving the finite model property. Due to their logical properties that will be reveal later, we call these sets *maximal consistent sets of processes*. Intuitively, a maximal consistent set of processes is a set that whenever contains a process contains also any future state of the process (i.e. all the unfolding) and the "point of view" of any observer of this process (we recall that an observer can see a subprocess). Syntactically this means that whenever we have a process in a maximal consistent set, we will also have all the processes that can be obtained by arbitrarily pruning the syntactic tree of our process.

Definition 6.1 *For $M, N \subset \mathbb{P}$ and $\alpha \in \mathbb{A}$ we define:*
$\alpha.M \overset{def}{=} \{\alpha.P \mid P \in M\}$ $\qquad$ $M|N \overset{def}{=} \{P|Q \mid P \in M, Q \in N\}$.

We associate to each process P the set $\pi(P)$ of all processes obtained by arbitrarily pruning the syntactic tree of P.

Definition 6.2 *For $P \in \mathbb{P}$ we define $\pi(P) \subset \mathbb{P}$ inductively by:*
1. $\pi(0) \overset{def}{=} \{0\}$ 2. $\pi(\alpha.P) \overset{def}{=} \{0\} \cup \alpha.\pi(P)$ 3. $\pi(P|Q) \overset{def}{=} \pi(P)|\pi(Q)$
We extend the definition of π to sets of processes $M \subset \mathbb{P}$ by

$$\pi(M) \overset{def}{=} \bigcup_{P \in M} \pi(P).$$

Theorem 6.1 *The next assertions hold:*

1. $P \in \pi(P)$ $\qquad$ 2. $0 \in \pi(P)$ $\qquad$ 3. $P \in \pi(P|Q)$ $\qquad$ 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

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

  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 $P_{(h,w)} \equiv Q_{(h,w)}|R_{(h,w)} \in \pi(Q)|\pi(R) = \pi(P)$.

□

Theorem 6.2 *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 $Act(Q) = Act(Q_1) \cup Act(Q_2) \subseteq \{\alpha\} \cup Act(Q_1) \cup Act(Q_2) = Act(P)$. □

Theorem 6.3 $\pi(\pi(P)) = \pi(P)$.

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 $\pi(\pi(P)) = \pi(Q)|\pi(R) = \pi(Q|R) = \pi(P)$. □

Theorem 6.4 *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 6.3, we obtain $\pi(Q) \subset \pi(P)$. □

Theorem 6.5 *If* σ *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 $\pi(\sigma(P)) = \sigma(\pi(Q))|\sigma(\pi(R)) = \sigma(\pi(Q)|\pi(R)) = \sigma(\pi(P))$. □

Definition 6.3 *A set of processes* $\mathcal{M} \subseteq \mathbb{P}$ *is maximal consistent if it satisfies the conditions*
1. if $P \in \mathcal{M}$ *and* $P \longrightarrow P'$ *then* $P' \in \mathcal{M}$ *2. if* $P \in \mathcal{M}$ *then* $\pi(P) \subset \mathcal{M}$.

Theorem 6.6 *If* $\mathcal{M}$ *is a maximal consistent set of processes and* σ *is a substitution, then* $\mathcal{M}^\sigma$ *is maximal consistent.*

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

Now we introduce a structural bisimulation-like relation on maximal consistent sets of processes.

Definition 6.4 *Let $\mathcal{M}, \mathcal{N} \subset \mathbb{P}$ be maximal consistent sets of processes. We write $\mathcal{M} \approx_h^w \mathcal{N}$ iff*

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

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

We 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 $\mathcal{M} \approx_h^w \mathcal{N}$.

Theorem 6.7 (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 5.3 we obtain $P \approx_{h'}^{w'} Q$. And the same if we start from a process $Q \in N$. These proves that $\mathcal{M} \approx_{h'}^{w'} \mathcal{N}$. □

Definition 6.5 (System of generators) *We say that $M \subset \mathbb{P}$ is a system of generators for $\mathcal{M}$ if $\mathcal{M}$ is the smallest maximal consistent set of processes that contains M. We denote this by $\overline{M} = \mathcal{M}$.*

Definition 6.6 *For any maximal consistent set of processes $\mathcal{M}$ and any (h, w) we define*

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

Theorem 6.8 *For any context $\mathcal{M}$, and any size (h, w) we have $\mathcal{M}_{(h,w)} \approx_w^h \mathcal{M}$.*

Definition 6.7 *Let $A \subset \mathbb{A}$. We denote by $\mathfrak{M}_{(h,w)}^A$ the set of all maximal consistent sets generated by the systems of generators with the size at most (h, w) and with the actions in A:*

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

Theorem 6.9 *If $A \subset \mathbb{A}$ is a finite set of actions, then the following hold:*
1. If $\mathcal{M} \in \mathfrak{M}_{(h,w)}^A$ then $\mathcal{M}$ is a finite maximal consistent set of processes.
2. $\mathfrak{M}_{(h,w)}^A$ 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 5.16. Thus $\overline{M} = \mathcal{M}$ is a finite maximal consistent set.

2.: As $\mathfrak{P}^A_{(h,w)}$ is finite by theorem 5.16, 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. □

The previous theorem shows that for a given finite signature A and for a given dimension (h,w) there exists only a finite set of maximal consistent sets of processes. Further we will prove even more: that having a maximal consistent set $\mathcal{M}$ with actions from A and a dimension (h,w) we can always find, in the finite set $\mathfrak{M}^A_{(h,w)}$, a maximal consistent set $\mathcal{N}$ structural bisimilar with $\mathcal{M}$ at the dimension (h,w). This result will be further used for proving the finite model property for our logic.

Theorem 6.10 *For any maximal consistent set $\mathcal{M}$, and any size (h,w) we have $\mathcal{M}_{(h,w)} \approx^h_w \mathcal{M}$.*

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 $P \approx^h_w Q$. Let $Q \in \mathcal{M}_{(h,w)}$. Since $\overline{M}$ is the smallest maximal consistent set 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 $P \approx^h_w Q$ (since $P \equiv Q$ implies $P \approx^h_w Q$). □

Theorem 6.11 *For any maximal consistent set $\mathcal{M}$ 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 6.1, we obtain, by applying theorem 6.2, $Act(P_{(h,w)}) \subseteq Act(\mathcal{M})$, hence $Act(\{P_{(h,w)} \mid P \in \mathcal{M}\}) \subseteq Act(\mathcal{M})$. Further applying again theorem 6.2, we trivially derive the desired result. □

Theorem 6.12 (Bound pruning theorem) *Let $\mathcal{M}$ be a maximal consistent set of processes. Then for any (h,w) there is a maximal consistent set $\mathcal{N} \in \mathfrak{M}^{Act(\mathcal{M})}_{(h,w)}$ such that $\mathcal{M} \approx^w_h \mathcal{N}$.*

Proof The maximal consistent set $\mathcal{N} = \mathcal{M}_{(h,w)}$ fulfills the requirements of the theorem, by construction. Indeed, it is maximal consistent, and it is generated by the set $N = \{P_{(h,w)} \mid P \in \mathcal{M}\}$. Moreover $N \leq (h,w)$ and, by theorem 6.11, $Act(\mathcal{M}_{(h,w)}) \subseteq Act(\mathcal{M})$. Hence $\mathcal{N} \in \mathfrak{M}^{Act(\mathcal{M})}_{(h,w)}$. □

7 The Logic $\mathcal{L}^{\mathfrak{A}}_{\mathbb{A}}$

In this section we introduce the logic multimodal logic $\mathcal{L}^{\mathfrak{A}}_{\mathbb{A}}$ with modal operators indexed by an "epistemic" signature $\mathfrak{A}$ and a "dynamic" signature $\mathbb{A}$. On $\mathfrak{A}$ we will have defined an algebraical structure homomorphic with CCS.

7.1 Epistemic Agents

Definition 7.1 *Consider a set $\mathcal{A}$ and its extension $\mathcal{A}^+$ generated by the next grammar for $\alpha \in \mathbb{A}$*

$$A := a \in \mathcal{A} \mid \alpha.A \mid A|A$$

Suppose, in addition, that on $\mathcal{A}^+$ it is defined the smallest congruence relation $\equiv$ for which $|$ is commutative and associative. We call the $\equiv$-equivalence classes of $\mathcal{A}^+$ epistemic agents *and we call* atomic agents *the classes corresponding to elements of $\mathcal{A}$. Hereafter we will use $A, A', A_1, ...$ to denote arbitrary epistemic agents.*

Definition 7.2 *We call* society of epistemic agents *any set $\mathfrak{A} \subseteq \mathcal{A}^+$, closed to $\equiv$, satisfying the conditions*
1. if $A_1|A_2 \in \mathfrak{A}$ then $A_1, A_2 \in \mathfrak{A}$ *2. if $\alpha.A \in \mathfrak{A}$ then $A \in \mathfrak{A}$*

7.2 Syntax of $\mathcal{L}_{\mathbb{A}}^{\mathfrak{A}}$

Definition 7.3 *Let $\mathfrak{A}$ be a society of epistemic agents defined for the set $\mathbb{A}$ of actions. We define the language $\mathcal{F}_{\mathbb{A}}^{\mathfrak{A}}$ of $\mathcal{L}_{\mathbb{A}}^{\mathfrak{A}}$, for $A \in \mathfrak{A}$ and $\alpha \in \mathbb{A}$, by:*

$$\phi := \ 0 \mid \top \mid \neg\phi \mid \phi \wedge \phi \mid \phi|\phi \mid \langle\alpha\rangle\phi \mid \langle A : \alpha\rangle\phi \mid K_A\phi.$$

Definition 7.4 (Derived operators) *In addition to the classical boolean operators, we introduce some derived operators*[6]*:*
$1 \overset{def}{=} \neg((\neg 0) \mid (\neg 0))$
$\langle !\alpha\rangle\psi \overset{def}{=} (\langle\alpha\rangle\psi) \wedge 1$
$[a]\phi \overset{def}{=} \neg(\langle a\rangle(\neg\phi))$
$\widetilde{K}_A\phi \overset{def}{=} \neg K_A \neg\phi.$
We convey that the precedence order of the operators in the syntax of $\mathcal{L}_{\mathbb{A}}^{\mathfrak{A}}$ is $\neg,\ K_A,\ \langle\, a\rangle,\ |, \wedge\, , \vee\, , \rightarrow$ where $\neg$ has precedence over all the other operators.

7.3 Process semantics

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

Definition 7.5 (Models and satisfaction) *A model of $\mathcal{L}_{\mathbb{A}}^{\mathfrak{A}}$ is a couple $(\mathcal{M}, I)$ where $\mathcal{M}$ is a maximal consistent set of processes and I : $(\mathfrak{A}, |, \alpha.)$**to**$(\mathcal{M}, |, \alpha.)$ a homomorphism*[7] *of structures such that $I(A) = 0$ iff $A \in \mathcal{A}$.*
We convey to denote $P \overset{I(A):\alpha}{\textbf{to}} Q$ by $P \overset{A:\alpha}{\textbf{to}} Q$.
We define the satisfaction relation, for $P \in \mathcal{M}$, by:
$\mathcal{M}, P \models \top$ *always*

[6] We recall that we use a to range over $\mathbb{A}^*$, while α is used to refer to arbitrary objects of $\mathbb{A}$.

[7] The function I associates to each agent the process it observes. An atomic agent sees always the process 0.

$\mathcal{M}, P \models 0$ *iff* $P \equiv 0$
$\mathcal{M}, P \models \neg\phi$ *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* $P \xrightarrow{\alpha} P'$ *such that* $\mathcal{M}, P' \models \phi$
$\mathcal{M}, P \models \langle A : \alpha\rangle\phi$ *iff there exists a transition* $P \xrightarrow{A:\alpha} P'$ *such that* $\mathcal{M}, P' \models \phi$
$\mathcal{M}, P \models K_A\phi$ *iff* $P \equiv I(A)|R$ *and for all* $I(A)|R' \in \mathcal{M}$ *we have* $\mathcal{M}, I(A)|R' \models \phi$

The semantics of the derived operators will be:
$\mathcal{M}, P \models [a]\phi$ iff for any transition $P \xrightarrow{a} P'$ (if any) we have $\mathcal{M}, P' \models \phi$
$\mathcal{M}, P \models 1$ iff $P \equiv 0$ or $P \equiv \alpha.Q$
$\mathcal{M}, P \models \langle!\alpha\rangle\phi$ iff $P \equiv \alpha.Q$ and $\mathcal{M}, Q \models \phi$
$\mathcal{M}, P \models \widetilde{K}_A\phi$ iff either $P \not\equiv I(A)|R$ for any R, or $\exists I(A)|S \in \mathcal{M}$ such that $\mathcal{M}, I(A)|S \models \phi$

Remark the interesting semantics of the operators K_A and $\widetilde{K}_A$ for $A \in I^{-1}(0)$:
$\mathcal{M}, P \models K_A\phi$ iff $\forall Q \in \mathcal{M}$ we have $\mathcal{M}, Q \models \phi$
$\mathcal{M}, P \models \widetilde{K}_A\phi$ iff $\exists Q \in \mathcal{M}$ such that $\mathcal{M}, Q \models \phi$

Hence $K_A\phi$ and $\widetilde{K}_A\phi$ for an atomic agent A encode, in syntax, the validity and the satisfiability with respect to a given model.

7.4 Bounded finite model property

Definition 7.6 (Size of a formula) *We define* the sizes of a formula*,* ϕ *(*height *and* width*), w.r.t. the homomorphism I, inductively on the structure of formula. Suppose that* $\phi = (h, w)$*,* $\psi = (h', w')$ *and* $I(A) = (h_A, w_A)$*.*

1. $0 = \top \overset{def}{=} (0, 0)$
2. $\neg\phi \overset{def}{=} \phi$
3. $\phi \wedge \psi \overset{def}{=} (max(h, h'), max(w, w'))$
4. $\phi|\psi \overset{def}{=} (max(h, h'), w + w')$
5. $\langle\alpha\rangle\phi \overset{def}{=} (1 + h, 1 + w)$
6. $\langle A : \alpha\rangle\phi = (1 + max(h, h_A), 1 + max(w, w_A))$
7. $K_A\phi \overset{def}{=} (1 + max(h, h_A), 1 + max(w, w_A))$

The next theorem states that ϕ is *"sensitive"* via satisfaction only up to size ϕ. 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 ϕ.

Theorem 7.1 *If* $\phi = (h, w)$*,* $\mathcal{M}, P \models \phi$ *and* $(\mathcal{M}, P) \approx_h^w (\mathcal{N}, Q)$ *then* $\mathcal{N}, Q \models \phi$*.*

Proof We prove it by induction on the syntactical structure of ϕ.

- **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 6.7, 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 5.5, 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 6.7,
  $(\mathcal{M}, P_i) \approx^{w_i}_{max(h_1,h_2)} (\mathcal{N}, Q_i)$. Further, using again theorem 6.7, 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 5.12, 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 6.7, $\mathcal{M} \approx^{w'}_{h'} \mathcal{N}$. 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 5.9, 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 5.9, $P'' \equiv R|S''$.

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 6.7, $(\mathcal{M}, P) \approx^{w'}_{h'} (\mathcal{N}, Q)$ 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.

□

Using this theorem, we conclude that if a process satisfies ϕ w.r.t. a given maximal consistent set of processes, then by pruning the process and the maximal consistent set on the size ϕ, we preserve the satisfiability for ϕ. Indeed the theorems 5.13 and 6.10 prove that if $\phi = (h, w)$ then $(\mathcal{M}, P) \approx^h_w (\mathcal{M}_\phi, P_\phi)$. Hence $\mathcal{M}, P \models \phi$ implies $\mathcal{M}_\phi, P_\phi \models \phi$.

Theorem 7.2 *If $\mathcal{M}, P \models \phi$ then $\mathcal{M}_\phi, P_\phi \models \phi$.*

Proof Let $\phi = (h, w)$. By theorem 6.12, we have $\mathcal{M} \approx^h_w \mathcal{M}_{(h,w)}$. By process pruning theorem 5.13, 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 7.1 establishes $\mathcal{M}_{(h,w)}, P_{(h,w)} \models \phi$ q.e.d. □

Definition 7.7 *We define the set of actions of a formula ϕ, $act(\phi) \subset \mathbb{A}$, inductively by:*

1. $act(0) = act(\top) \overset{def}{=} \emptyset$
2. $act(\langle\alpha\rangle\phi) \overset{def}{=} \{\alpha\} \cup act(\phi)$
3. $act(\neg\phi) = act(\phi)$
4. $act(\phi \wedge \psi) = act(\phi|\psi) \overset{def}{=} act(\phi) \cup act(\psi)$
5. $act(\langle A : \alpha\rangle\phi) = act(K_A\phi) \overset{def}{=} Act(I(A)) \cup act(\phi)$

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

Theorem 7.3 *If $\mathcal{M}, P \models \phi$ and σ 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 ϕ, 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 **??**, 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 $P\overset{\gamma}{\textbf{to}}Q$ 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 $P\overset{\gamma}{\textbf{to}}Q$ 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 $\sigma(P)\overset{\gamma}{\textbf{to}}\sigma(Q)$. 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 γ, or there is such a transition and for any transition $P\overset{\gamma}{\textbf{to}}Q$ we have $\mathcal{M}, Q \not\models \psi$.
If there is no transition of P by γ 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 γ. Thus $\sigma(\mathcal{M}), \sigma(P) \not\models \langle\gamma\rangle\psi$.

   If there are transitions of P by γ, and for any such a transition $P\overset{\gamma}{\textbf{to}}Q$ 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 $\sigma(P)\overset{\gamma}{\textbf{to}}\sigma(Q)$. 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 **??**, $Q \equiv R'|S'''$ 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 **??**, 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 **??**, 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.

Theorem 7.4 (Finite model property) *If $\mathcal{M}, P \models \phi$ then $\exists \mathcal{N} \in \mathfrak{M}_\phi^{act(\phi)+}$ and $Q \in \mathcal{N}$ such that $\mathcal{N}, Q \models \phi$.*

Proof Consider the substitution σ 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 7.3 we obtain $\mathcal{M}^\sigma, P^\sigma \models \phi$. Further we take $\mathcal{N} = \mathcal{M}^\sigma_{(h,w)} \in \mathfrak{M}_{(h,w)}^{act(\phi)^+}$ and $Q = P^\sigma_{(h,w)} \in \mathcal{M}_{(h,w)}^{act(\phi)^+}$, and theorem 7.1 proves the finite model property. □

Because $act(\phi)$ is finite, implying $act(\phi)_+$ finite, Theorem 6.9 proves that $\mathfrak{M}_\phi^{act(\phi)+}$ is finite and any maximal consistent set $\mathcal{M} \in \mathfrak{M}_\phi^{act(\phi)+}$ is finite as well. Thus we obtain the finite model property for our logic. A consequence of theorem 7.4 is the decidability for satisfiability, validity and model checking against the process semantics.

Theorem 7.5 (Decidability) *For $\mathcal{L}_{\mathbb{A}}^{\mathfrak{A}}$ validity, satisfiability and model checking are decidable against the process semantics.*

7.5 Characteristic formulas

In this subsection we use the peculiarities of the dynamic and epistemic operators to define characteristic formulas for processes and finite maximal consistent sets of processes. Such formulas will be useful in providing an appropriate axiomatic system for our logic and, eventually, for proving its completeness.

Definition 7.8 (Characteristic formulas for processes) *We define a class of logical formulas $(f_P)_{P \in \mathbb{P}}$, indexed by ($\equiv$-equivalence classes of) processes, inductively by:*

1. $f_0 \overset{def}{=} 0$ 2. $f_{P|Q} \overset{def}{=} f_P | f_Q$ 3. $f_{\alpha.P} \overset{def}{=} \langle !\alpha \rangle f_P$

We denote by $\mathcal{F}_{\mathbb{P}}$ this class. Obviously $\mathcal{F}_{\mathbb{P}} \subset \mathcal{F}_{\mathbb{A}}^{\mathfrak{A}}$.

We will prove latter that f_P is a characteristic formula for P. Similarly, we can characterize the agents by the process they can see.

Definition 7.9 (Characteristic formulas for agents) *Similarly we introduce a class of logical formulas $(f_A)_{A \in \mathfrak{A}}$, on epistemic agents*

1. $f_A \overset{def}{=} 0$ *for atomic agents $A \in \mathcal{A}$* 2. $f_{A_1|A_2} \overset{def}{=} f_{A_1} | f_{A_2}$ 3. $f_{\alpha.A} \overset{def}{=} \langle !\alpha \rangle f_A$

We denote by $\mathcal{F}_{\mathfrak{A}}$ this class. Obviously $\mathcal{F}_{\mathfrak{A}} \subset \mathcal{F}_{\mathbb{A}}^{\mathfrak{A}}$.

Definition 7.10 (Characteristic formulas for finite sets of processes) *Let $\Phi \subset \mathcal{F}^{\mathfrak{A}}$ be a finite set of formulas and $A \in \mathfrak{A}$ an atomic agent. We define the derived operator*

$$\Delta\Phi \overset{def}{=} K_A\left(\bigvee_{\phi \in \Phi} \phi\right) \wedge \left(\bigwedge_{\phi \in \Phi} \widetilde{K}_A \phi\right)$$

Observe that $\mathcal{M}, P \models \Delta\Phi$ iff for any $Q \in \mathcal{M}$ there exists $\phi \in \Phi$ such that $\mathcal{M}, Q \models \phi$ and for any $\phi \in \Phi$ there exists $Q \in \mathcal{M}$ such that $\mathcal{M}, Q \models \phi$. Observe also that it is irrelevant which atomic agent A we choose to define Δ, as the epistemic operators of any atomic agent can encode validity and satisfiability.

Further we exploit the semantics of this operator for defining characteristic formulas for finite maximal consistent sets of processes.

Definition 7.11 (Characteristic formulas for finite maximal consistent sets) *If $\mathcal{M}$ is a finite maximal consistent set of processes, we define $f_{\mathcal{M}} \stackrel{def}{=} \Delta\{f_P \mid P \in \mathcal{M}\}$.*

8 Axiomatic system

Consider the subset of logical formulas introduced by the next syntax and defined for $\alpha \in \mathbb{A}$

$$f := \langle !\alpha \rangle 0 \mid \langle !\alpha \rangle f \mid f|f$$

We denote the class of these formulas by $\mathcal{F}$. By construction, $\mathcal{F} \subset \mathcal{F}^{\mathfrak{A}}_{\mathbb{A}}$. Hereafter we use f, g, h for denoting arbitrary formulas from $\mathcal{F}$, while ϕ, ψ, ρ will be used for formulas in $\mathcal{F}^{\mathfrak{A}}_{\mathbb{A}}$.

Theorem 8.1 $\mathcal{F} \cup \{0\} = \mathcal{F}_{\mathbb{P}}$.

Hereafter is proposed a Hilbert-style axiomatic system for $\mathcal{L}^{\mathfrak{A}}_{\mathbb{A}}$. We assume the axioms and the rules of propositional logic. In addition we will have a set of spatial axioms and rules, of dynamic axioms and rules and of epistemic axioms and rules. We will also have a class of mixed axioms and rules that combine different operators.

Spatial axioms

$\vdash \top|\bot \to \bot$

$\vdash \phi|0 \leftrightarrow \phi$

$\vdash \phi|\psi \to \psi|\phi$

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

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

$\vdash (f \wedge \phi|\psi) \to \bigvee_{f \leftrightarrow g|h} (g \wedge \phi)|(h \wedge \psi)$

Spatial rules

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

Axiom E8 states the propagation of the inconsistency from a subsystem to the upper system.

Axioms E8, E8 and E8 depict the structure of abelian monoid projected by the parallel operator on the class of processes.

Concerning axiom E8, 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$8 states a monotony property for the parallel operator.

Dynamic axioms

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

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

$\vdash 0 \vee \langle !\alpha\rangle\top \to [\beta]\bot$, for $\alpha \neq \beta$

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

Dynamic rules

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

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

The first dynamic axiom, axiom E8, 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 a, then the bigger system performs it as a whole.

Axiom E8 is just the (K)-axiom for the dynamic operator.

Axiom E8 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, α_i, for $i = 1..n$, axiom E8.2 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 α, axiom E8 states that a system described by a guarded process can perform one and only one action, the guarding one.

Rule E$_R$8 is the classic necessity rule used for the dynamic operator.

Rule E$_R$8 is, in a sense, a counterpart of axiom E8 establishing the action of the operator $[a]$ in relation to the parallel operator.

Epistemic axioms

$\vdash K_A\top \leftrightarrow f_A|\top$

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

$\vdash K_A\phi \to \phi$

$\vdash K_A\phi \to K_AK_A\phi$.

$\vdash K_A\top \to (\neg K_A\phi \to K_A\neg K_A\phi)$

Axioms involving atomic agents

If A' is an atomic agent and A is any agent then

$\vdash K_A\phi \leftrightarrow (K_A\top \wedge K_{A'}(K_A\top \to \phi))$

$\vdash K_{A'}\phi \wedge \psi|\rho \to (K_{A'}\phi \wedge \psi)|(K_{A'}\phi \wedge \rho)$

$\vdash K_{A'}\phi \to [a]K_{A'}\phi$

$\vdash K_{A'}\phi \to (K_A\top \to K_AK_{A'}\phi)$

Epistemic rules

If $\vdash \phi$ then $\vdash K_A\top \to K_A\phi$.

Axiom E8 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 E8 which is just the axiom (T) - necessity axiom, for the epistemic operator.

Also axiom E8 is well known in epistemic logics. It states that our epistemic agents satisfy *the positive introspection property*, i.e. if A knows something then it knows that it knows that thing.

Axiom E8 states a variant of the *negative introspection*, saying that if an agent A is active and if it doesn't know ϕ, then it knows that it doesn't know ϕ. The novelty in our axiom is the precondition $K_A\top$ 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 E8 provides a full description of the knowledge of any agent A based on the knowledge of any atomic agent.

Axioms E8, E8 and E8 present $K_{A'}\phi$ as a syntactic encryption of validity.

Rule E$_R$8 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.

Mixed axioms

$\vdash \langle A : \alpha\rangle\top \to K_A\top$.

$\vdash f_A \to (\langle\alpha\rangle\phi \leftrightarrow \langle A : \alpha\rangle\phi)$

$\vdash \langle A : \alpha\rangle\phi \wedge \langle A|A' : \alpha\rangle\top \to \langle A|A' : \alpha\rangle\phi$

Mixed rules

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

Rule E$_R$8 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.

Theorem 8.2 *If $\beta \neq \alpha_i$ for $i = 1..n$ then* $\vdash \langle !\alpha_1\rangle\top|...|\langle !\alpha_n\rangle\top \to [\beta]\bot$

Theorem 8.3 *If $\mathcal{M} \ni P$ is a finite context and* $\vdash c_{\mathcal{M}} \wedge c_P \to K_0\phi$ *then* $\vdash c_{\mathcal{M}} \to \phi$.

sectionSoundness of the system $\mathcal{L}_{\mathbb{A}}^{\mathfrak{A}}$

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.

Theorem 8.4 (Soundness) *The system $\mathcal{L}_{\mathbb{A}}^{\mathfrak{A}}$ is sound w.r.t. process semantics.*

Proof The soundness of $\mathcal{L}_{\mathbb{A}}^{\mathfrak{A}}$ 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 E8] $\models \top|\bot \rightarrow \bot$

Proof Suppose that it exists a maximal consistent set $\mathcal{M}$ 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 maximal consistent set $\mathcal{M}$ and process $P \in \mathcal{M}$ such that $\mathcal{M}, P \models \top|\bot$, i.e. for any maximal consistent set $\mathcal{M}$ 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 E8] $\models \phi|0 \leftrightarrow \phi$.

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 E8] $\models \phi|\psi \rightarrow \psi|\phi$.

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 E8] $\models (\phi|\psi)|\rho \rightarrow \phi|(\psi|\rho)$.

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 E8] $\models \phi|(\psi \vee \rho) \rightarrow (\phi|\psi) \vee (\phi|\rho)$

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 $\mathcal{M}, P \models (\phi|\psi) \vee (\phi|\rho)$. □

Now we prove that the formulas f_P defined before are characteristic formulas.

Theorem 8.5 *If $P \in \mathcal{M}$, then $\mathcal{M}, P \models f_P$.*

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

The case $P \equiv 0$**:** $\mathcal{M}, 0 \models f_0$, because $0 \in \mathcal{M}$, $f_0 = 0$ and $\mathcal{M}, 0 \models 0$.

The case $P \equiv Q|R$**:** we have $Q, R \in \mathcal{M}$ and $f_P = f_Q|f_R$. By the inductive hypothesis $\mathcal{M}, Q \models f_Q$ and $\mathcal{M}, R \models f_R$, so $\mathcal{M}, Q|R \models f_Q|f_R$. Hence $\mathcal{M}, P \models f_P$.

The case $P \equiv \alpha.Q$**:** we have $P \xrightarrow{\alpha} Q$, hence $Q \in \mathcal{M}$. Moreover, $f_P = \langle\alpha\rangle f_Q \wedge 1$. By the inductive hypothesis $\mathcal{M}, Q \models f_Q$. Because $P \xrightarrow{\alpha} Q$, we obtain $\mathcal{M}, P \models \langle\alpha\rangle f_Q$, and because $P \equiv \alpha.Q$ is a guarded process, we have also $\mathcal{M}, P \models 1$. Hence $\mathcal{M}, P \models f_P$. □

Theorem 8.6 $\mathcal{M}, P \models f_Q$ *iff* $P \equiv Q$.

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

- if $P = R|S$ and $Q = S|R$, we have $\mathcal{M}, R|S \models f_R|f_S$ and using the soundness of axiom E8, we obtain $\mathcal{M}, R|S \models f_S|f_R$, i.e. $\mathcal{M}, P \models f_Q$
- if $P = (R|S)|U$ and $Q = R|(S|U)$ we have $\mathcal{M}, P \models (f_R|f_S)|f_U$. Using the soundness of axiom E8, we obtain $\mathcal{M}, P \models f_Q$. Similarly $\mathcal{M}, Q \models f_P$, using the soundness of axioms E8 and E8.
- if $P = Q|0$ then $\mathcal{M}, P \models f_Q|0$, i.e., by using the soundness of axiom E8, $\mathcal{M}, P \models f_Q$. Similarly reverse, form $\mathcal{M}, Q \models f_Q$ we derive, by using the soundness of axiom E8, $\mathcal{M}, Q \models f_Q|0$, i.e. $\mathcal{M}, Q \models f_P$.
- if $P = P'|R$ and $Q = Q'|R$ with $P' \equiv Q'$ and $\mathcal{M}, P' \models f_{Q'}$, because $\mathcal{M}, R \models f_R$, we obtain that $\mathcal{M}, P \models f_{Q'}|f_R$, i.e. $\mathcal{M}, P \models f_Q$.
- if $P = \alpha.P'$ and $Q = \alpha.Q'$ with $P' \equiv Q'$ and $\mathcal{M}, P' \models f_{Q'}$, as $P \xrightarrow{\alpha} P'$, then $\mathcal{M}, P \models \langle\alpha\rangle f_{Q'}$. But $\mathcal{M}, P \models 1$, because P is a guarded process, hence $\mathcal{M}, P \models \langle\alpha\rangle f_{Q'} \wedge 1$, i.e. $\mathcal{M}, P \models f_Q$.

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

- if $Q \equiv 0$, then $\mathcal{M}, P \models f_0$, means $\mathcal{M}, P \models 0$. Hence $P \equiv 0$.
- if $Q \equiv R|S$ then $\mathcal{M}, P \models f_Q$ is equivalent with $\mathcal{M}, P \models f_R|f_S$. So $P \equiv U|V$, $\mathcal{M}, U \models f_R$ and $\mathcal{M}, V \models f_S$. By the inductive hypothesis we obtain that $U \equiv R$ and $V \equiv S$. Hence $P \equiv Q$.
- if $Q \equiv \alpha.R$, then $\mathcal{M}, P \models f_Q$ is equivalent with $\mathcal{M}, P \models \langle\alpha\rangle f_R \wedge 1$. So $P \xrightarrow{\alpha} P'$ with $\mathcal{M}, P' \models f_R$. 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 E8] $\models (f \wedge \phi|\psi) \rightarrow \bigvee_{f \leftrightarrow g|h}(g \wedge \phi)|(h \wedge \psi)$

Proof Suppose that $\mathcal{M}, S \models f \wedge \phi|\psi$. Then there exists a process P such that $f = f_P$.
Hence $S \equiv P$ (by theorem 8.6) and $S \equiv S_1|S_2$ with $\mathcal{M}, S_1 \models \phi$ and $\mathcal{M}, S_2 \models \psi$.
But $\mathcal{M}, S_1 \models f_{S_1}$ and $\mathcal{M}, S_2 \models f_{S_2}$, by theorem 8.5.
Hence $\mathcal{M}, S_1 \models \phi \wedge f_{S_1}$ and $\mathcal{M}, S_2 \models \psi \wedge f_{S_2}$.
And because $P \equiv S \equiv S_1|S_2$, we obtain $\mathcal{M}, P \models (\phi \wedge f_{S_1})|(\psi \wedge f_{S_2})$, hence $\mathcal{M}, P \models (f \wedge \phi|\psi) \rightarrow \bigvee_{f \leftrightarrow g|h}(g \wedge \phi)|(h \wedge \psi)$, q.e.d. □

[Soundness of rule E$_R$8] 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 E8] $\models \langle a\rangle\phi|\psi \rightarrow \langle a\rangle(\phi|\psi)$.

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

[Soundness of axiom E8] $\models [a](\phi \rightarrow \psi) \rightarrow ([a]\phi \rightarrow [a]\psi)$

Proof Let $\mathcal{M}, P \models [a](\phi \rightarrow \psi)$ and $\mathcal{M}, P \models [a]\phi$. If there is no P' such that $P \xrightarrow{a} P'$, then $\mathcal{M}, P \models [a]\psi$. 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. $\mathcal{M}, P \models [a]\psi$. □

[Soundness of axiom E8] For $\alpha \neq \beta$ we have

$$\models 0 \vee \langle !\alpha\rangle\top \rightarrow [\beta]\bot.$$

Proof If $\mathcal{M}, P \models 0$ then $P \equiv 0$ and there is no transition $0 \xrightarrow{\beta} P'$, hence $\mathcal{M}, P \not\models \langle\beta\rangle\top$, i.e. $\mathcal{M}, P \models [\beta]\bot$.
Suppose that $\mathcal{M}, P \models \langle !\alpha\rangle\top$. Then necessarily $P \equiv \alpha.P_1$. But if $\alpha \neq \beta$, there is no transition

$$\alpha.P_1 \xrightarrow{\beta} P'.$$

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

[Soundness of axiom E8] $\models \langle !\alpha\rangle\phi \rightarrow [\alpha]\phi$

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$8] If $\models \phi$ then $\models [a]\phi$.

Proof Let $\mathcal{M}$ be a maximal consistent set and $P \in \mathcal{M}$ a process. If there is no P' such that $P \xrightarrow{a} P'$, then $\mathcal{M}, P \models [a]\phi$. 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 $\mathcal{M}, P \models [a]\phi$. □

[Soundness of rule E$_R$8]

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

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 $\models \phi \rightarrow [a]\phi'$ and $\models \psi \rightarrow [a]\psi'$, we derive $\mathcal{M}, Q \models [a]\phi'$ and $\mathcal{M}, R \models [a]\psi'$. We analyze some cases:

- if P cannot perform a transition by a, then $\mathcal{M}, P \models [a]\bot$, and using the soundness of axiom E8 and rule E$_R$8 we derive

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

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

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

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

- if $Q\overset{a}{\mathbf{to}}Q'$ and $R\overset{a}{\mathbf{to}}R'$ then $P\overset{a}{\mathbf{to}}P'$ has either the form $Q|R\overset{a}{\mathbf{to}}Q'|R$ or $Q|R\overset{a}{\mathbf{to}}Q|R'$. 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 $P\overset{a}{\mathbf{to}}P'$ we have $\mathcal{M}, P' \models (\phi'|\psi \vee \phi|\psi')$, i.e. $\mathcal{M}, P \models [a](\phi'|\psi \vee \phi|\psi')$.

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

Soundness of the epistemic axioms and rules

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

[Soundness of axiom E8] $\models f_A|\top \leftrightarrow K_A\top$

Proof If $\mathcal{M}, P \models f_A|\top$ then $P \equiv R|S$, with $\mathcal{M}, S \models f_A$. Then $P \equiv I(A)|R$. And because for any $I(A)|R' \in \mathcal{M}$ we have $\mathcal{M}, I(A)|R' \models \top$, we derive $\mathcal{M}, P \models K_A\top$.
Suppose now the reverse, i.e. that $\mathcal{M}, P \models K_A\top$. Then $P \equiv I(A)|R$. But $\mathcal{M}, P \models f_P$, hence $\mathcal{M}, P \models f_A|f_R$.
Because $\models f_A \rightarrow \top$, using the soundness of rule E$_R$8, we derive $\models f_A|f_R \rightarrow f_A|\top$ from where we conclude that $\mathcal{M}, P \models f_A|\top$. □

[Soundness of axiom E8] $\models K_A\phi \wedge K_A(\phi \rightarrow \psi) \rightarrow K_A\psi$

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

[Soundness of axiom E8] $\models K_A\phi \rightarrow \phi$.

Proof If $\mathcal{M}, P \models K_A\phi$ then $P \equiv I(A)|R$ and for any $I(A)|S \in \mathcal{M}$ we have $\mathcal{M}, I(A)|S \models \phi$, i.e. $\mathcal{M}, I(A)|R \models \phi$, so $\mathcal{M}, P \models \phi$. □

[Soundness of axiom E8] $\models K_A\phi \to K_AK_A\phi$.

Proof Suppose that $\mathcal{M}, P \models K_A\phi$, then $P \equiv I(A)|R$ and for any $I(A)|S \in \mathcal{M}$ we have $\mathcal{M}, I(A)|S \models \phi$. Let $I(A)|S' \in \mathcal{M}$ be arbitrarily chosen. As for any $I(A)|S \in \mathcal{M}$ we have $\mathcal{M}, I(A)|S \models \phi$, we derive that $\mathcal{M}, I(A)|S' \models K_A\phi$. But $I(A)|S'$ has been arbitrarily chosen, so for any $I(A)|S \in \mathcal{M}$ we have $\mathcal{M}, I(A)|S \models K_A\phi$, and because $P \equiv I(A)|R$ we obtain $\mathcal{M}, P \models K_AK_A\phi$. □

[Soundness of axiom E8] $\models K_A\top \to (\neg K_A\phi \to K_A\neg K_A\phi)$

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

In the next lemmas of this subsection we will denote by A' an atomic agent.

[Soundness of axiom E8]

$$\models K_A\phi \leftrightarrow (K_A\top \wedge K_{A'}(K_A\top \to \phi)).$$

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

Suppose now that $\mathcal{M}, P \models K_A\top \wedge K_{A'}(K_A\top \to \phi)$. From $\mathcal{M}, P \models K_A\top$ we derive $P \equiv I(A)|R$.
Because $\mathcal{M}, P \models K_{A'}(K_A\top \to \phi)$, we obtain that for any process $S \in \mathcal{M}$ we have $\mathcal{M}, S \models K_A\top \to \phi$. Hence, for any process $S|I(A) \in \mathcal{M}$ we have $\mathcal{M}, S|I(A) \models \phi$ (because $\mathcal{M}, S|I(A) \models K_A\top$). And because $P \equiv I(A)|R$, we derive $\mathcal{M}, P \models K_A\phi$. □

[Soundness of axiom E8]

$$\models K_{A'}\phi \wedge \psi|\rho \to (K_{A'}\phi \wedge \psi)|(K_{A'}\phi \wedge \rho).$$

Proof Suppose that $\mathcal{M}, P \models K_{A'}\phi \wedge \psi|\rho$ then $\mathcal{M}, P \models K_{A'}\phi$ and $\mathcal{M}, P \models \psi|\rho$.
$\mathcal{M}, P \models K_{A'}\phi$ 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 $\mathcal{M}, P' \models K_{A'}\phi$ and $\mathcal{M}, P'' \models K_{A'}\phi$.
Hence $\mathcal{M}, P' \models \psi \wedge K_{A'}\phi$ and $\mathcal{M}, P'' \models \rho \wedge K_{A'}\phi$. As $P \equiv P'|P''$, we obtain further $\mathcal{M}, P \models (K_{A'}\phi \wedge \psi)|(K_{A'}\phi \wedge \rho)$. □

[Soundness of axiom E8] $\models K_{A'}\phi \to [a]K_{A'}\phi$

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

[Soundness of axiom E8] $\models K_{A'}\phi \to (K_A\top \to K_A K_{A'}\phi)$

Proof Suppose that $\mathcal{M}, P \models K_{A'}\phi$ and $\mathcal{M}, P \models K_A\top$.
$\mathcal{M}, P \models K_{A'}\phi$ gives that for any $R \in \mathcal{M}$ we have $\mathcal{M}, R \models \phi$.
$\mathcal{M}, P \models K_A\top$ means that $P \equiv I(A)|S$. Because for any $R \in \mathcal{M}$ we have $\mathcal{M}, R \models \phi$, we obtain that for any $I(A)|S' \in \mathcal{M}$ we have $\mathcal{M}, I(A)|S' \models K_{A'}\phi$, and because $P \equiv I(A)|S$ we obtain $\mathcal{M}, P \models K_A K_{A'}\phi$. □

[Soundness of rule E$_R$8] If $\models \phi$ then $\models K_A\top \to K_A\phi$

Proof If $\models \phi$ then for any maximal consistent set $\mathcal{M}$ and any process $P \in \mathcal{M}$ we have $\mathcal{M}, P \models \phi$. Suppose now that $\mathcal{M}, P \models K_A\top$. Then $P \equiv I(A)|R$. Because $\mathcal{M}, S \models \phi$ for each $S \in \mathcal{M}$, we derive that for any $S|I(A) \in \mathcal{M}$ we have $\mathcal{M}, S|I(A) \models \phi$. Hence $\mathcal{M}, P \models K_A\phi$. □

Soundness of the mixed axioms and rules

[Soundness of axiom E$^+$8]

$$\models \langle A : \alpha\rangle\top \to K_A\top$$

Proof Suppose that $\mathcal{M}, P \models \langle A : \alpha\rangle\top$ then there exists a reduction
$P\overset{A:\alpha}{\textbf{to}}P'$, hence $P \equiv I(A)|R$. Now, because for any $I(A)|S \in \mathcal{M}$ we have $\mathcal{M}, I(A)|S \models \top$ we derive that $\mathcal{M}, P \models K_A\top$. □

[Soundness of axiom E$^+$8]

$$\models f_A \to (\langle\alpha\rangle\phi \leftrightarrow \langle A : \alpha\rangle\phi)$$

Proof If $\mathcal{M}, P \models f_A \wedge \langle\alpha\rangle\phi$ then $P \equiv I(A)$ and $\mathcal{M}, I(A) \models \langle\alpha\rangle\phi$. So, there is a transition $I(A)\overset{\alpha}{\textbf{to}}R$ with $\mathcal{M}, R \models \phi$. But $I(A)\overset{\alpha}{\textbf{to}}R$ is equivalent with $I(A)\overset{A:\alpha}{\textbf{to}}R$. Hence $\mathcal{M}, P \models \langle A : \alpha\rangle\phi$.
Reverse, if $\mathcal{M}, P \models f_A \wedge \langle A : \alpha\rangle\phi$ then $P \equiv I(A)$ and $\mathcal{M}, I(A) \models \langle A : \alpha\rangle\phi$. So, there is a transition $I(A)\overset{A:\alpha}{\textbf{to}}R$ with $\mathcal{M}, R \models \phi$. But $I(A)\overset{A:\alpha}{\textbf{to}}R$ is equivalent with $I(A)\overset{\alpha}{\textbf{to}}R$. Hence $\mathcal{M}, P \models \langle\alpha\rangle\phi$. □

[Soundness of axiom E$^+$8]

$$\models \langle A_1 : \alpha\rangle\phi \wedge \langle A_1|A_2 : \alpha\rangle\top \to \langle A_1|A_2 : \alpha\rangle\phi$$

Proof Suppose that $\mathcal{M}, R \models \langle A_1 : \alpha\rangle\phi \wedge \langle A_1|A_2 : \alpha\rangle\top$.
Then $\mathcal{M}, R \models \langle A_1 : \alpha\rangle\phi$ and $\mathcal{M}, R \models \langle A_1|A_2 : \alpha\rangle\top$.
But $\mathcal{M}, R \models \langle A_1 : \alpha\rangle\phi$ means that it exists the reduction $R \overset{A_1:\alpha}{\textbf{to}} R'$ and $\mathcal{M}, R' \models \phi$, i.e. $R \equiv I(A_1)|S$, $I(A_1)\overset{\alpha}{\textbf{to}}P$ and $R' \equiv P|S$.
$\mathcal{M}, R \models \langle A_1|A_2 : \alpha\rangle\top$ means that $R \equiv I(A_1)|I(A_2)|V$, i.e. $S \equiv I(A_2)|V$.
But $I(A_1) \overset{A_1:\alpha}{\textbf{to}} P$ gives $I(A_1)|I(A_2) \overset{A_1|A_2:\alpha}{\textbf{to}} P|I(A_2)$, hence $R \overset{A_1|A_2:\alpha}{\textbf{to}} R'$ and $\mathcal{M}, R' \models \phi$, that means $\mathcal{M}, R \models \langle A_1|A_2 : \alpha\rangle\phi$. □

[Soundness of rule E$_R$8] If $\models \bigvee_{\mathcal{M}\in\mathfrak{M}_\phi^{act(\phi)+}} f_{\mathcal{M}} \to \phi$ then $\models \phi$.

Proof Suppose that $\models \bigvee_{\mathcal{M}\in\mathfrak{M}_\phi^{act(\phi)+}} f_{\mathcal{M}} \to \phi$ 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 7.4, we obtain that it exists a maximal consistent set $\mathcal{N}' \in \mathfrak{M}_\phi^{act(\phi)+}$ 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 maximal consistent set $\mathcal{N}' \in \mathfrak{M}_\phi^{act(\phi)+}$ and a process $R \in \mathcal{N}'$ with $\mathcal{N}', R \models \neg\phi$. Because $\mathcal{N}', R \models f_{\mathcal{N}'}$, we derive $\mathcal{N}', R \models \bigvee_{\mathcal{M}\in\mathfrak{M}_\phi^{act(\phi)+}} f_{\mathcal{M}}$.
But $\models \bigvee_{\mathcal{M}\in\mathfrak{M}_\phi^{act(\phi)+}} f_{\mathcal{M}} \to \phi$ implies $\mathcal{N}', R \models \bigvee_{\mathcal{M}\in\mathfrak{M}_\phi^{act(\phi)+}} f_{\mathcal{M}} \to \phi$, 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. $\models \phi$. □

9 Some theorems

Theorem 9.1 *If $P \not\equiv Q$ then $\vdash f_P \to \neg f_Q$.*

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 $f_Q = \langle\alpha\rangle f_R \wedge 1|f_S$ that implies, using theorem 9.10, $\vdash f_Q \to \langle\alpha\rangle f_R|f_S$, and applying axiom E8, $\vdash f_Q \to \langle\alpha\rangle(f_R|f_S)$.
But $\vdash f_R|f_S \to \top$ and applying theorem 9.13, we obtain
$\vdash \langle\alpha\rangle(f_R|f_S) \to \langle\alpha\rangle\top$.
Hence, $\vdash f_Q \to \langle\alpha\rangle\top$. Then $\vdash \neg\langle\alpha\rangle\top \to \neg f_Q$.
Axiom E8 gives $\vdash 0 \to \neg\langle\alpha\rangle\top$ hence, in the end, $\vdash 0 \to \neg f_Q$, i.e. $\vdash f_P \to \neg f_Q$.

- **the case** $P \equiv P'|P''$**:** we have $f_P = f_{P'}|f_{P''}$. 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 $\vdash f_{Q'} \to \neg f_{P'}$ or $\vdash f_{Q''} \to \neg f_{P''}$. Because this is happening for any decomposition of Q, we can apply theorem 9.12 and we obtain
$\vdash f_Q \to \neg(f_{P'}|f_{P''})$, i.e. $\vdash f_Q \to \neg f_P$. Hence $\vdash f_P \to \neg f_Q$.

- **the case $P \equiv \alpha.P'$:** $f_P = 1 \wedge \langle\alpha\rangle f_{P'}$, so $\vdash f_P \rightarrow 1 \wedge \langle\alpha\rangle\top$.
  But axiom E8.2 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 $\vdash f_P \rightarrow \neg\langle\beta\rangle\top$.
  - if $Q \equiv 0$ we already proved that $\vdash f_Q \rightarrow \neg f_P$ (because $P \not\equiv 0$), so $\vdash f_P \rightarrow \neg f_Q$
  - if $Q \equiv \beta.Q'|Q''$ for some $\beta \neq \alpha$, then $\vdash f_Q \rightarrow \langle\beta\rangle\top$, hence $\vdash \neg\langle\beta\rangle\top \rightarrow \neg f_Q$. But we proved that $\vdash f_P \rightarrow \neg\langle\beta\rangle\top$. Hence $\vdash f_P \rightarrow \neg f_Q$.
  - if $Q \equiv \alpha.Q_1|...|\alpha.Q_k$ for $k > 1$, then $\vdash f_Q \rightarrow \neg 0|\neg 0$ (as $\vdash 0 \rightarrow \neg f_{\alpha.Q_1}$ and $\vdash 0 \rightarrow \neg f_{\alpha.Q_2|...|\alpha.Q_k}$). Then $\vdash f_Q \rightarrow \neg 1$, i.e.
    $\vdash 1 \rightarrow \neg f_Q$. But $\vdash f_P \rightarrow 1$. Hence $\vdash f_P \rightarrow \neg f_Q$.
  - 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 $\vdash f_{Q'} \rightarrow \neg f_{P'}$. Further, applying theorem 9.14, we obtain $\vdash [\alpha]f_{P'} \rightarrow [\alpha]\neg f'_Q$, i.e.
    $\vdash [\alpha]f_{P'} \rightarrow \neg\langle\alpha\rangle f_{Q'}$ that gives, because $f_Q = 1 \wedge \langle\alpha\rangle f_{Q'}$,
    $\vdash [\alpha]f_{P'} \rightarrow \neg f_Q$.
    Now, using axiom E8, $\vdash 1 \wedge \langle\alpha\rangle f_{P'} \rightarrow [\alpha]f_{P'}$, so $\vdash f_P \rightarrow [\alpha]f_{P'}$, and, combining it with the previous result, we derive $\vdash f_P \rightarrow \neg f_Q$.

□

Theorem 9.2 *If $P \equiv Q$ then $\vdash f_P \leftrightarrow f_Q$.*

Proof We prove it verifying the congruence rules:

- if $P = R|S$ and $Q = S|R$ then $\vdash f_R|f_S \leftrightarrow f_S|f_R$ from theorem 9.7, i.e. $\vdash f_P \leftrightarrow f_Q$
- if $P = (R|S)|U$ and $Q = R|(S|U)$ then theorem 9.8 we have
  $\vdash (f_R|f_S)|f_U \leftrightarrow f_R|(f_S|f_U)$, i.e. $\vdash f_P \leftrightarrow f_Q$
- if $P = Q|0$ then axiom E8 gives $\vdash f_Q|0 \leftrightarrow f_Q$, i.e. $\vdash f_P \leftrightarrow f_Q$.
- if $P = P'|R$ and $Q = Q'|R$ with $P' \equiv Q'$ and $\vdash f_{P'} \leftrightarrow f_{Q'}$ then rule E_R8 gives $\vdash f_{P'}|f_R \leftrightarrow f_{Q'}|f_R$. Hence $\vdash f_P \leftrightarrow f_Q$.
- if $P = \alpha.P'$ and $Q = \alpha.Q'$ with $P' \equiv Q'$ and $\vdash f_{P'} \leftrightarrow f_{Q'}$ then theorem 9.13 gives $\vdash \langle\alpha\rangle f_{P'} \leftrightarrow \langle\alpha\rangle f_{Q'}$, so $\vdash (\langle\alpha\rangle f_{P'} \wedge 1) \leftrightarrow (\langle\alpha\rangle f_{Q'} \wedge 1)$. Hence $\vdash f_P \leftrightarrow f_Q$.

□

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

Theorem 9.3 *If $\mathcal{M}$ is a finite maximal consistent set and $P \in \mathcal{M}$ then $\mathcal{M}, P \models f_{\mathcal{M}}$.*

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

If $\mathcal{M}$ is a finite maximal consistent set and $P \in \mathcal{M}$ then

$$\mathcal{M}, P \models f_{\mathcal{M}} \wedge f_P.$$

Theorem 9.4 *If $\mathcal{M}, P \models f_{\mathcal{N}}$ then $\mathcal{N} = \mathcal{M}$.*

Proof Suppose that $\mathcal{M}, P \models f_{\mathcal{N}}$, then $\mathcal{M}, P \models K_0(\bigvee_{Q \in \mathcal{N}} f_Q)$, i.e. for any $R \in \mathcal{M}$ we have $\mathcal{M}, R \models \bigvee_{Q \in \mathcal{N}} f_Q$. Hence, for any $R \in \mathcal{M}$ there exists a process $Q \in \mathcal{N}$ with $\mathcal{M}, R \models f_Q$, or equivalently, $R \equiv Q$.
Now $\mathcal{M}, P \models \bigwedge_{Q \in \mathcal{N}} \widetilde{K}_0 f_Q$ gives that for any $Q \in \mathcal{N}$ we have
$\mathcal{M}, P \models \widetilde{K}_0 f_Q$, i.e. there exists a process $R \in \mathcal{M}$ such that $\mathcal{M}, R \models f_Q$, 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 $M = N$. □

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.

Theorem 9.5 $\vdash \top|\top \leftrightarrow \top$

Proof Obviously $\vdash \top|\top \rightarrow \top$. As $\vdash 0 \rightarrow \top$, using rule E$_R$8, we obtain $\vdash \top|0 \rightarrow \top|\top$. Further axiom E8 gives us $\vdash \top \rightarrow \top|\top$. □

Theorem 9.6 *If $\vdash \phi$ then $\vdash \theta|\rho \rightarrow \phi|\rho$*

Proof Because $\vdash \phi$ implies $\vdash \theta \rightarrow \phi$, using rule E$_R$8 we obtain the result. □

Theorem 9.7 $\vdash \phi|\psi \leftrightarrow \psi|\phi$

Proof We use axiom E8 in both directions. □

Theorem 9.8 $\vdash (\phi|\psi)|\rho \leftrightarrow \phi|(\psi|\rho)$

Proof We use axiom E8 and theorem 9.7. □

Theorem 9.9 $\vdash \phi|(\psi \vee \rho) \leftrightarrow (\phi|\psi) \vee (\phi|\rho)$

Proof $\vdash \psi \rightarrow \psi \vee \rho$ so, using rule E$_R$8, $\vdash \phi|\psi \rightarrow \phi|(\psi \vee \rho)$. 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 E8. □

Theorem 9.10 $\vdash \phi|(\psi \wedge \rho) \rightarrow (\phi|\psi) \wedge (\phi|\rho)$

Proof Because $\vdash \psi \wedge \rho \rightarrow \psi$, by applying rule E$_R$8, 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.

Theorem 9.11 *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$8 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, ϕ and ψ, if considering any parallel decomposition of our system (process) $P \equiv Q|R$, we obtain that either Q doesn't satisfy ϕ or R doesn't satisfy ψ, then our system P does not satisfy the parallel composition of the two specifications, $\phi|\psi$.

Theorem 9.12 *If for any decomposition* $P \equiv Q|R$ *we have* $\vdash f_Q \rightarrow \neg\phi$ *or* $\vdash f_R \rightarrow \neg\psi$ *then* $\vdash f_P \rightarrow \neg(\phi|\psi)$.

Proof $\vdash f_Q \rightarrow \neg\phi$ is equivalent with $\vdash f_Q \wedge \phi \rightarrow \bot$ and because $\vdash f_R \wedge \psi \rightarrow \top$, we obtain, by theorem 9.11 $\vdash (f_Q \wedge \phi)|(f_R \wedge \psi) \rightarrow \bot|\top$. And using axiom E8, we derive

$$\vdash (f_Q \wedge \phi)|(f_R \wedge \psi) \rightarrow \bot$$

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

$$\vdash (f_Q \wedge \phi)|(f_R \wedge \psi) \rightarrow \bot$$

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

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

But axiom E8 gives

$$\vdash (f_P \wedge \phi|\psi) \to \bigvee_{P\equiv Q|R} (f_Q \wedge \phi)|(f_R \wedge \psi)$$

hence

$$\vdash (f_P \wedge \phi|\psi) \to \bot,\ i.e.\ \vdash f_P \to \neg(\phi|\psi).$$

□

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 $\vdash f_Q \to \neg\phi$ or $\vdash f_R \to \neg\psi$ be fulfilled by all the possible decompositions of P. If only a decomposition $P \equiv Q|R$ exists such that $\vdash f_Q \to \neg\phi$ or $\vdash f_R \to \neg\psi$, 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 $\mathcal{M}, P \models \phi|\psi$.

9.1 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.

Theorem 9.13 (Monotonicity) *If* $\vdash \phi \to \psi$ *then* $\vdash \langle a\rangle\phi \to \langle a\rangle\psi$.

Proof $\vdash \phi \to \psi$ implies $\vdash \neg\psi \to \neg\phi$. Using rule E_R8 we obtain $\vdash [a](\neg\psi \to \neg\phi)$ and axiom E8 gives $\vdash [a]\neg\psi \to [a]\neg\phi$. This is equivalent with $\vdash \neg\langle a\rangle\psi \to \neg\langle a\rangle\phi$, i.e. $\vdash \langle a\rangle\phi \to \langle a\rangle\psi$. □

Theorem 9.14 *If* $\vdash \phi \to \psi$ *then* $\vdash [a]\neg\psi \to [a]\neg\phi$.

Proof If $\vdash \phi \to \psi$ then, by theorem 9.13, $\vdash \langle a\rangle\phi \to \langle a\rangle\psi$, hence $\vdash \neg\langle a\rangle\psi \to \neg\langle a\rangle\phi$, that gives $\vdash [a]\neg\psi \to [a]\neg\phi$. □

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

Theorem 9.15 *If P cannot do any transition by α then* $\vdash f_P \to [\alpha]\bot$.

Proof We prove it by induction on the structure of P.
The case $P \equiv 0$**:** axiom E8 implies $\vdash 0 \rightarrow [\alpha]\bot$ which proves this case, because $f_0 = 0$.
The case $P \equiv \alpha_1.P_1|...|\alpha_n.P_n$**:** as P cannot perform α we have $\alpha \neq \alpha_i$ for $i = 1..n$. We have $f_P = (\langle\alpha_1\rangle f_{P_1} \wedge 1)|...|(\langle\alpha_n\rangle f_{P_n} \wedge 1)$. From $\vdash f_{P_i} \rightarrow \top$ we derive, using theorem 9.13, $\vdash (\langle\alpha_i\rangle f_{P_i} \wedge 1) \rightarrow (\langle\alpha_i\rangle\top \wedge 1)$. Further, we apply theorem 9.11 and obtain $\vdash f_P \rightarrow (\langle\alpha_1\rangle\top \wedge 1)|...|(\langle\alpha_n\rangle\top \wedge 1)$. Axiom E8.2 gives that for $\alpha \neq \alpha_i$, $\vdash (\langle\alpha_1\rangle\top \wedge 1)|...|(\langle\alpha_n\rangle\top \wedge 1) \rightarrow [\alpha]\bot$. Hence $\vdash f_P \rightarrow [\alpha]\bot$. □

Theorem 9.16 $\vdash f_P \rightarrow [\alpha]\bigvee\{f_Q \mid P \xrightarrow{\alpha} Q\}$

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 α, hence, by theorem 9.15, $\vdash f_P \rightarrow [\alpha]\bot$. But
$\vdash \neg\bigvee\{f_Q \mid P \xrightarrow{\alpha} Q\} \rightarrow \top$, and using theorem 9.14, we derive

$$\vdash [\alpha]\bot \rightarrow [\alpha]\bigvee\{f_Q \mid P \xrightarrow{\alpha} Q\}$$

Combining this with $\vdash f_P \rightarrow [\alpha]\bot$, we derive

$$\vdash f_P \rightarrow [\alpha]\bigvee\{f_Q \mid P \xrightarrow{\alpha} Q\}$$

The case $P \equiv \alpha.P'$**:** then $\{f_Q \mid P \xrightarrow{\alpha} Q\} = \{f_{P'}\}$ and $f_P = \langle\alpha\rangle f_{P'} \wedge 1$. Applying axiom E8 we obtain $\vdash f_P \rightarrow [\alpha]f_{P'}$. Hence

$$\vdash f_P \rightarrow [\alpha]\bigvee\{f_Q \mid P \xrightarrow{\alpha} Q\}$$

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

$$\vdash f_{\alpha.P'} \rightarrow [\alpha]\bigvee\{f_{Q'} \mid \alpha.P' \xrightarrow{\alpha} Q'\}$$

and

$$\vdash f_{P''} \rightarrow [\alpha]\bigvee\{f_{Q''} \mid P'' \xrightarrow{\alpha} Q''\}$$

We apply rule E_R8 and obtain

$$\vdash f_P \rightarrow [\alpha](f_{\alpha.P'}|\bigvee\{f_{Q''} \mid P'' \xrightarrow{\alpha} Q''\} \vee \bigvee\{f_{Q'} \mid \alpha.P' \xrightarrow{\alpha} Q'\}|f_{P''})$$

Using theorem 9.9, we obtain this result equivalent with

$$\vdash f_P \rightarrow [\alpha]\bigvee\{f_Q \mid P \xrightarrow{\alpha} Q\}$$

□

Theorem 9.17 *If* $\vdash \bigvee\{f_Q \mid P \xrightarrow{\alpha} Q\} \rightarrow \phi$ *then* $\vdash f_P \rightarrow [\alpha]\phi$

Proof If $\vdash \bigvee\{f_Q \mid P \xrightarrow{\alpha} Q\} \to \phi$ then rule E_R8 gives

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

and further axiom E8 gives $\vdash [\alpha] \bigvee\{f_Q \mid P \xrightarrow{\alpha} Q\} \to [\alpha]\phi$. But theorem 9.16 gives $\vdash f_P \to [\alpha] \bigvee\{f_Q \mid P \xrightarrow{\alpha} Q\}$, hence $\vdash f_P \to [\alpha]\phi$. □

Theorem 9.18 $\vdash \langle A : \alpha\rangle\top \leftrightarrow f_A|\top$.

Epistemic results

We begin by stating that an atomic agent is always active: it always performs its *"inactivity"* expressed by 0. Hereafter, in this section, we use A' to denote an arbitrary atomic agent, even if this it will not be specified.

Theorem 9.19 $\vdash K_{A'}\top$.

Proof Trivial consequence of axiom E8 and axiom E8. □

The next result states that an agent knows something only if it is active.

Theorem 9.20 $\vdash K_A\phi \to K_A\top$.

Proof Trivial consequence of axiom E8. □

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

Theorem 9.21 $\vdash K_A\phi \wedge K_A\psi \leftrightarrow K_A(\phi \wedge \psi)$

Proof $\vdash \phi \to (\psi \to (\phi \wedge \psi))$. Using rule E_R8, we obtain

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

We apply axiom E8 twice, and obtain

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

i.e.

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

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

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

Reverse, we apply rule E_R8 to $\vdash \phi \wedge \psi \to \psi$ and then axiom E8, and obtain $\vdash K_A\top \to (K_A(\phi \wedge \psi) \to K_A\phi)$. But $\vdash K_A(\phi \wedge \psi) \to K_A\top$, hence $\vdash K_A(\phi \wedge \psi) \to K_A\phi$.
Similarly $\vdash K_A(\phi \wedge \psi) \to K_A\psi$. □

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

Theorem 9.22 $\vdash K_A K_A \phi \leftrightarrow K_A \phi$.

Proof Axiom E8 gives $\vdash K_A \phi \to K_A K_A \phi$, and axiom E8 gives $\vdash K_A K_A \phi \to K_A \phi$. □

Theorem 9.23 (Monotonicity of knowledge)

$$\textit{If } \vdash \phi \to \psi \textit{ then } \vdash K_A \phi \to K_A \psi$$

Proof Because $\vdash \phi \to \psi$, we can use rule E_R8 and obtain $\vdash K_A \top \to K_A(\phi \to \psi)$. But theorem 9.20 gives $\vdash K_A \phi \to K_A \top$, hence $\vdash K_A \phi \to K_A(\phi \to \psi)$ where from we derive

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

This entails, using axiom E8, $\vdash K_A \phi \to K_A \psi$. □

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*.

Theorem 9.24 $\vdash K_{A_1|A_2} \top \to K_{A_1} \top$.

Proof Axiom E8 gives $\vdash K_{A_1|A_2} \top \leftrightarrow f_{A_1} | f_{A_2} | \top$ and $\vdash K_{A_1} \top \leftrightarrow f_{A_1} | \top$. But $\vdash f_{A_2} \to \top$ and applying rule E_R8, we obtain $\vdash f_{A_1} | f_{A_2} | \top \to f_{A_1} | \top$. Hence $\vdash K_{A_1|A_2} \top \to K_{A_1} \top$. □

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

Theorem 9.25 $\vdash K_A \neg\phi \to \neg K_A \phi$.

Proof Axiom E8 gives $\vdash K_A \neg\phi \to \neg\phi$ and $\vdash K_A \phi \to \phi$. The last is equivalent with $\vdash \neg\phi \to \neg K_A \phi$, and combined with the first entails $\vdash K_A \neg\phi \to \neg K_A \phi$. □

Theorem 9.26 (Consistency theorem) $\vdash K_A \phi \to \neg K_A \neg\phi$.

Proof By using the negative form of theorem 9.25 □

Theorem 9.27 $\vdash K_{A'} \phi \to (K_A \top \to K_A \phi)$

Proof Axioms E8 gives $\vdash K_{A'} \phi \to \phi$ and applying the monotonicity of knowledge, $\vdash K_A K_{A'} \phi \to K_A \phi$.
Now axiom E8 provides $\vdash K_{A'} \phi \wedge K_A \top \to K_A K_{A'} \phi$. Thus $\vdash K_{A'} \phi \wedge K_A \top \to K_A \phi$, that is equivalent with $\vdash K_{A'} \phi \to (K_A \top \to K_A \phi)$. □

Theorem 9.28 $\vdash \widetilde{K}_{A'} \phi \leftrightarrow K_{A'} \widetilde{K}_{A'} \phi$

Proof By definition, we have $\vdash \widetilde{K}_{A'}\phi \leftrightarrow \neg K_{A'}\neg\phi$, and because $\vdash K_{A'}\top$, we derive $\vdash \widetilde{K}_{A'}\phi \rightarrow (\neg K_{A'}\neg\phi \wedge K_{A'}\top)$.

But axiom E8 entails $\vdash (\neg K_{A'}\neg\phi \wedge K_{A'}\top) \rightarrow K_{A'}\neg K_{A'}\neg\phi$, i.e.

$$\vdash (\neg K_{A'}\neg\phi \wedge K_{A'}\top) \rightarrow K_{A'}\widetilde{K}_{A'}\phi$$

Hence $\vdash \widetilde{K}_{A'}\phi \rightarrow K_{A'}\widetilde{K}_{A'}\phi$.

We have also $\vdash K_{A'}\widetilde{K}_{A'}\phi \rightarrow \widetilde{K}_{A'}\phi$, by applying axiom E8. □

Theorem 9.29 $\vdash \widetilde{K}_{A'}\phi \wedge \psi|\rho \rightarrow (\widetilde{K}_{A'}\phi \wedge \psi)|(\widetilde{K}_{A'}\phi \wedge \rho)$

Proof Axiom E8 instantiated with $\phi = \widetilde{K}_{A'}\phi$ gives

$$\vdash K_{A'}\widetilde{K}_{A'}\phi \wedge \psi|\rho \rightarrow (K_{A'}\widetilde{K}_{A'}\phi \wedge \psi)|(K_{A'}\widetilde{K}_{A'}\phi \wedge \rho)$$

Further, using theorem 9.28, we obtain the wanted result. □

Theorem 9.30 $\vdash \widetilde{K}_{A'}\phi \rightarrow [\alpha]\widetilde{K}_{A'}\phi$

Proof Axiom E8 instantiated with $\phi = \widetilde{K}_{A'}\phi$ gives

$$\vdash K_{A'}\widetilde{K}_{A'}\phi \rightarrow [\alpha]K_{A'}\widetilde{K}_{A'}\phi$$

Further, using theorem 9.28, we obtain the wanted result. □

Theorem 9.31 $\vdash \widetilde{K}_{A'}\phi \rightarrow (K_A\top \rightarrow K_A\widetilde{K}_{A'}\phi)$

Proof Axiom E8 instantiated with $\phi = \widetilde{K}_{A'}\phi$ gives

$$\vdash K_{A'}\widetilde{K}_{A'}\phi \rightarrow (K_A\top \rightarrow K_AK_{A'}\widetilde{K}_{A'}\phi)$$

Further, using theorem 9.28, we obtain the wanted result. □

Theorems referring to maximal consistent sets

In this section we focus on results that involve the characteristic formulas of finite maximal consistent sets. We try to show, in this way, how sensitive our system is with respect to maximal consistent sets. Further, these results will be used in proving the completeness.

Theorem 9.32 *If $\mathcal{M}$ is a finite maximal consistent set and $R \notin \mathcal{M}$ then* $\vdash f_{\mathcal{M}} \to \neg f_R$.

Proof Because $f_{\mathcal{M}} = K_{A'}(\bigvee_{P\in\mathcal{M}} f_P) \wedge (\bigwedge_{P\in\mathcal{M}} \widetilde{K}_{A'} f_P)$ we derive that

$$\vdash f_{\mathcal{M}} \to K_{A'}(\bigvee_{P\in\mathcal{M}} f_P)$$

But from axiom E8 $\vdash K_{A'}(\bigvee_{P\in\mathcal{M}} f_P) \to \bigvee_{P\in\mathcal{M}} f_P$, so $\vdash f_{\mathcal{M}} \to \bigvee_{P\in\mathcal{M}} f_P$. Further theorem 9.1 gives $\vdash f_P \to \neg f_R$ (as $R \notin \mathcal{M}$ and $P \in \mathcal{M}$ implies $R \not\equiv P$) which implies $\vdash \bigvee_{P\in\mathcal{M}} f_P \to \neg f_R$. But we proved that $\vdash f_{\mathcal{M}} \to \bigvee_{P\in\mathcal{M}} f_P$. Hence $\vdash f_{\mathcal{M}} \to \neg f_R$. □

Theorem 9.33 *If $\mathcal{M}$ is a finite maximal consistent set then*

$$\vdash (f_{\mathcal{M}} \wedge \phi|\psi) \to (f_{\mathcal{M}} \wedge \phi)|(f_{\mathcal{M}} \wedge \psi)$$

Proof Observe that, by applying axiom E8, we obtain

$$\vdash (K_{A'}\theta_1 \wedge \widetilde{K}_{A'}\theta_2 \wedge \widetilde{K}_{A'}\theta_3) \wedge \phi|\psi \to (\widetilde{K}_{A'}\theta_2 \wedge \widetilde{K}_{A'}\theta_3) \wedge (K_{A'}\theta_1 \wedge \phi)|(K_{A'}\theta_1 \wedge \psi) \quad (2)$$

If, further, we apply theorem 9.29 once, we obtain

$$\vdash (\widetilde{K}_{A'}\theta_3 \wedge \widetilde{K}_{A'}\theta_2) \wedge (K_{A'}\theta_1 \wedge \phi)|(K_{A'}\theta_1 \wedge \psi) \to$$
$$\widetilde{K}_{A'}\theta_3 \wedge (\widetilde{K}_{A'}\theta_2 \wedge K_{A'}\theta_1 \wedge \phi)|(\widetilde{K}_{A'}\theta_2 \wedge K_{A'}\theta_1 \wedge \psi)$$

Hence

$$\vdash (K_{A'}\theta_1 \wedge \widetilde{K}_{A'}\theta_2 \wedge \widetilde{K}_{A'}\theta_3) \wedge \phi|\psi \to \widetilde{K}_{A'}\theta_3 \wedge (\widetilde{K}_{A'}\theta_2 \wedge K_{A'}\theta_1 \wedge \phi)|(\widetilde{K}_{A'}\theta_2 \wedge K_{A'}\theta_1 \wedge \psi)$$

If we apply again theorem 9.29 we obtain

$$\vdash \widetilde{K}_{A'}\theta_3 \wedge (\widetilde{K}_{A'}\theta_2 \wedge K_{A'}\theta_1 \wedge \phi)|(\widetilde{K}_{A'}\theta_2 \wedge K_{A'}\theta_1 \wedge \psi) \to$$
$$(\widetilde{K}_{A'}\theta_3 \wedge \widetilde{K}_{A'}\theta_2 \wedge K_{A'}\theta_1 \wedge \phi)|(\widetilde{K}_{A'}\theta_3 \wedge \widetilde{K}_{A'}\theta_2 \wedge K_{A'}\theta_1 \wedge \psi)$$

hence

$$\vdash (K_{A'}\theta_1 \wedge \widetilde{K}_{A'}\theta_2 \wedge \widetilde{K}_{A'}\theta_3) \wedge \phi|\psi \to$$
$$(\widetilde{K}_{A'}\theta_3 \wedge \widetilde{K}_{A'}\theta_2 \wedge K_{A'}\theta_1 \wedge \phi)|(\widetilde{K}_{A'}\theta_3 \wedge \widetilde{K}_{A'}\theta_2 \wedge K_{A'}\theta_1 \wedge \psi)$$

Because $f_{\mathcal{M}} = K_{A'}(\bigvee_{Q\in\mathcal{M}} f_Q) \wedge (\bigwedge_{Q\in\mathcal{M}} \widetilde{K}_{A'} f_Q)$, we can use the same idea, applying theorem 9.29 once for each process in $\mathcal{M}$ (being finite) and we obtain

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

□

Theorem 9.34 *If $\mathcal{M}$ is a finite maximal consistent set then* $\vdash (f_{\mathcal{M}} \wedge \phi|\psi) \rightarrow (f_{\mathcal{M}} \wedge \phi)|\psi$

Proof From the previous theorem, 9.33, we have

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

Theorem 9.10 gives

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

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

Theorem 9.35 *If $\mathcal{M}$ is a finite maximal consistent set then* $\vdash f_{\mathcal{M}} \rightarrow [\alpha] f_{\mathcal{M}}$

Proof Observe that, by applying axiom E8, we obtain

$$\vdash K_{A'}\theta_1 \wedge \widetilde{K}_{A'}\theta_2 \wedge \widetilde{K}_{A'}\theta_3 \rightarrow (\widetilde{K}_{A'}\theta_2 \wedge \widetilde{K}_{A'}\theta_3) \wedge [\alpha]K_{A'}\theta_1$$

If, further, we apply theorem 9.30 once, we obtain

$$\vdash (\widetilde{K}_{A'}\theta_3 \wedge \widetilde{K}_{A'}\theta_2) \wedge [\alpha]K_{A'}\theta_1 \rightarrow \widetilde{K}_{A'}\theta_3 \wedge [\alpha]\widetilde{K}_{A'}\theta_2 \wedge [\alpha]K_{A'}\theta_1,\ i.e.$$

$$\vdash (\widetilde{K}_{A'}\theta_3 \wedge \widetilde{K}_{A'}\theta_2) \wedge [\alpha]K_{A'}\theta_1 \rightarrow \widetilde{K}_{A'}\theta_3 \wedge [\alpha](\widetilde{K}_{A'}\theta_2 \wedge K_{A'}\theta_1)$$

Hence

$$\vdash (K_{A'}\theta_1 \wedge \widetilde{K}_{A'}\theta_2 \wedge \widetilde{K}_{A'}\theta_3) \rightarrow \widetilde{K}_{A'}\theta_3 \wedge [\alpha](\widetilde{K}_{A'}\theta_2 \wedge K_{A'}\theta_1)$$

If we apply again theorem 9.30 we obtain

$$\vdash \widetilde{K}_{A'}\theta_3 \wedge [a](\widetilde{K}_{A'}\theta_2 \wedge K_{A'}\theta_1) \rightarrow [\alpha](\widetilde{K}_{A'}\theta_3 \wedge \widetilde{K}_{A'}\theta_2 \wedge K_{A'}\theta_1)$$

hence

$$\vdash (K_{A'}\theta_1 \wedge \widetilde{K}_{A'}\theta_2 \wedge \widetilde{K}_{A'}\theta_3) \rightarrow [\alpha](\widetilde{K}_{A'}\theta_3 \wedge \widetilde{K}_{A'}\theta_2 \wedge K_{A'}\theta_1)$$

As $f_{\mathcal{M}} = K_{A'}(\bigvee_{Q\in\mathcal{M}} f_Q) \wedge (\bigwedge_{Q\in\mathcal{M}} \widetilde{K}_{A'} f_Q)$, we can use the same idea, applying theorem 9.30 once for each process in $\mathcal{M}$ (being finite) and we obtain

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

□

Theorem 9.36 *If $\mathcal{M}$ is a finite maximal consistent set then* $\vdash f_{\mathcal{M}} \to (K_A\top \to K_A f_{\mathcal{M}})$

Proof Observe that, by applying axiom E8, we obtain

$$\vdash K_{A'}\theta_1 \wedge \widetilde{K}_{A'}\theta_2 \wedge \widetilde{K}_{A'}\theta_3 \to (\widetilde{K}_{A'}\theta_2 \wedge \widetilde{K}_{A'}\theta_3) \wedge (K_A\top \to K_AK_{A'}\theta_1)$$

If, further, we apply theorem 9.31 once, we obtain

$$\begin{gathered}\vdash (\widetilde{K}_{A'}\theta_3 \wedge \widetilde{K}_{A'}\theta_2) \wedge (K_A\top \to K_AK_{A'}\theta_1) \to \\ \widetilde{K}_{A'}\theta_3 \wedge (K_A\top \to K_A\widetilde{K}_{A'}\theta_2) \wedge (K_A\top \to K_AK_{A'}\theta_1),\ i.e.\end{gathered}$$

$$\vdash (\widetilde{K}_{A'}\theta_3 \wedge \widetilde{K}_{A'}\theta_2) \wedge (K_A\top \to K_AK_{A'}\theta_1) \to \widetilde{K}_{A'}\theta_3 \wedge (K_A\top \to (K_A\widetilde{K}_{A'}\theta_2 \wedge K_AK_{A'}\theta_1))$$

i.e., using 9.21,

$$\vdash (\widetilde{K}_{A'}\theta_3 \wedge \widetilde{K}_{A'}\theta_2) \wedge (K_A\top \to K_AK_{A'}\theta_1) \to \widetilde{K}_{A'}\theta_3 \wedge (K_A\top \to K_A(\widetilde{K}_{A'}\theta_2 \wedge K_{A'}\theta_1))$$

Hence

$$\vdash (K_{A'}\theta_1 \wedge \widetilde{K}_{A'}\theta_2 \wedge \widetilde{K}_{A'}\theta_3) \to \widetilde{K}_{A'}\theta_3 \wedge (K_A\top \to K_A(\widetilde{K}_{A'}\theta_2 \wedge K_{A'}\theta_1))$$

If we apply again the theorems 9.31 and 9.21 we obtain

$$\vdash [\widetilde{K}_{A'}\theta_3 \wedge (K_A\top \to K_A(\widetilde{K}_{A'}\theta_2 \wedge K_{A'}\theta_1))] \to [K_A\top \to K_A(\widetilde{K}_{A'}\theta_3 \wedge \widetilde{K}_{A'}\theta_2 \wedge K_{A'}\theta_1)]$$

hence

$$\vdash (K_{A'}\theta_1 \wedge \widetilde{K}_{A'}\theta_2 \wedge \widetilde{K}_{A'}\theta_3) \to [K_A\top \to K_A(\widetilde{K}_{A'}\theta_3 \wedge \widetilde{K}_{A'}\theta_2 \wedge K_{A'}\theta_1)]$$

Because $f_{\mathcal{M}} = K_{A'}(\bigvee_{Q\in\mathcal{M}} f_Q) \wedge (\bigwedge_{Q\in\mathcal{M}} \widetilde{K}_{A'} f_Q)$, we can use the same idea, applying theorem 9.31 once for each process in $\mathcal{M}$ (being finite) and we obtain

$$\vdash f_{\mathcal{M}} \to (K_A\top \to K_A f_{\mathcal{M}})$$

□

Theorem 9.37 *If $\mathcal{M}$ is a finite maximal consistent set and* $\vdash f_{\mathcal{M}} \to (\phi \to \psi)$ *then* $\vdash f_{\mathcal{M}} \to (\phi|\rho \to \psi|\rho)$.

Proof $\vdash f_{\mathcal{M}} \to (\phi \to \psi)$ implies $\vdash (f_{\mathcal{M}} \wedge \phi) \to \psi$ where we apply rule E_R8 and obtain $\vdash (f_{\mathcal{M}} \wedge \phi)|\rho \to \psi|\rho$. But theorem 9.34 gives $\vdash (f_{\mathcal{M}} \wedge \phi|\rho) \to (f_{\mathcal{M}} \wedge \phi)|\rho$. Combining these two results we obtain
$\vdash (f_{\mathcal{M}} \wedge \phi|\rho) \to \psi|\rho$, i.e. $\vdash f_{\mathcal{M}} \to (\phi|\rho \to \psi|\rho)$. □

Theorem 9.38 *If for a finite maximal consistent set $\mathcal{M} \ni P$ and any decomposition $P \equiv Q|R$ we have*

$$\vdash f_{\mathcal{M}} \rightarrow (f_Q \rightarrow \neg\phi) \textit{ or } \vdash f_{\mathcal{M}} \rightarrow (f_R \rightarrow \neg\psi) \textit{ then } \vdash f_{\mathcal{M}} \rightarrow (f_P \rightarrow \neg(\phi|\psi)).$$

Proof If $\vdash f_{\mathcal{M}} \rightarrow (f_Q \rightarrow \neg\phi)$ then we have, equivalently, $\vdash f_{\mathcal{M}} \wedge f_Q \rightarrow \neg\phi$, i.e. $\vdash f_Q \rightarrow (f_{\mathcal{M}} \rightarrow \neg\phi)$, hence $\vdash f_Q \rightarrow \neg(f_{\mathcal{M}} \wedge \phi)$.
Similarly $\vdash f_{\mathcal{M}} \rightarrow (f_R \rightarrow \neg\psi)$ gives $\vdash f_R \rightarrow \neg(f_{\mathcal{M}} \wedge \psi)$.

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

$$\vdash f_Q \rightarrow \neg(f_{\mathcal{M}} \wedge \phi) \textit{ or } \vdash f_R \rightarrow \neg(f_{\mathcal{M}} \wedge \psi).$$

Then we can apply theorem 9.12 and we obtain

$$\vdash f_P \rightarrow \neg((f_{\mathcal{M}} \wedge \phi)|(f_{\mathcal{M}} \wedge \psi)) \tag{3}$$

But theorem 9.33 entails $\vdash f_{\mathcal{M}} \wedge \phi|\psi \rightarrow (f_{\mathcal{M}} \wedge \phi)|(f_{\mathcal{M}} \wedge \psi)$, hence $\vdash \neg((f_{\mathcal{M}} \wedge \phi)|(f_{\mathcal{M}} \wedge \psi)) \rightarrow \neg(f_{\mathcal{M}} \wedge \phi|\psi)$, and applying this result to (3), we obtain

$$\vdash f_P \rightarrow \neg(f_{\mathcal{M}} \wedge \phi|\psi) \textit{ that is equivalent with } \vdash f_{\mathcal{M}} \rightarrow (f_P \rightarrow \neg(\phi|\psi))$$

□

Further we prove a maximal consistent set-sensitive version of rule E$_R$8.

Theorem 9.39 *If* $\vdash f_{\mathcal{M}} \rightarrow \phi$ *then* $\vdash f_{\mathcal{M}} \rightarrow [\alpha]\phi$.

Proof If we apply rule E$_R$8 to $\vdash f_{\mathcal{M}} \rightarrow \phi$ we obtain $\vdash [\alpha](f_{\mathcal{M}} \rightarrow \phi)$. But axiom E8 gives $\vdash [\alpha](f_{\mathcal{M}} \rightarrow \phi) \rightarrow ([\alpha]f_{\mathcal{M}} \rightarrow [\alpha]\phi)$, hence $\vdash [\alpha]f_{\mathcal{M}} \rightarrow [\alpha]\phi$. Theorem 9.35 proves that $\vdash f_{\mathcal{M}} \rightarrow [\alpha]f_{\mathcal{M}}$ which gives further $\vdash f_{\mathcal{M}} \rightarrow [\alpha]\phi$. □

The next result is a maximal consistent set-sensitive variant of rule E$_R$8.

Theorem 9.40 *If* $\vdash f_{\mathcal{M}} \rightarrow \phi$ *then* $\vdash f_{\mathcal{M}} \rightarrow (K_A\top \rightarrow K_A\phi)$.

Proof If we apply rule E$_R$8 to $\vdash f_{\mathcal{M}} \rightarrow \phi$, we obtain

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

But axiom E8 gives further $\vdash K_Q(f_{\mathcal{M}} \rightarrow \phi) \rightarrow (K_Q f_{\mathcal{M}} \rightarrow K_Q\phi)$. Hence $\vdash K_Q\top \wedge K_Q f_{\mathcal{M}} \rightarrow K_Q\phi$ that is equivalent with

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

Now, theorem 9.36 ensures that $\vdash f_{\mathcal{M}} \rightarrow (K_A\top \rightarrow K_Q f_{\mathcal{M}})$.
Hence $\vdash f_{\mathcal{M}} \rightarrow (K_A\top \rightarrow K_A\phi)$. □

Theorem 9.41 *If* $\vdash f_{\mathcal{M}} \to (K_Q\psi \to \phi)$ *then* $\vdash f_{\mathcal{M}} \to (K_Q\psi \to K_Q\phi)$.

Proof We apply theorem 9.40 to $\vdash f_{\mathcal{M}} \to (K_Q\psi \to \phi)$ and we obtain $\vdash f_{\mathcal{M}} \to (K_Q\top \to K_Q(K_Q\psi \to \phi))$, i.e. $\vdash (f_{\mathcal{M}} \wedge K_Q\top) \to K_Q(K_Q\psi \to \phi)$.
But axiom E8 gives $\vdash K_Q(K_Q\psi \to \phi) \to (K_QK_Q\psi \to K_Q\phi)$. Now if we use theorem 9.22 we obtain further

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

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

$$\vdash f_{\mathcal{M}} \to (K_Q\top \to (K_Q\psi \to K_Q\phi))$$

which is equivalent with $\vdash f_{\mathcal{M}} \to (K_Q\top \wedge K_Q\psi \to K_Q\phi)$.
Theorem 9.20 proved that $\vdash K_Q\psi \to K_Q\top$, result which, combined with the previous one, gives further $\vdash f_{\mathcal{M}} \to (K_Q\psi \to K_Q\phi)$. □

Theorem 9.42 *If* $Q|R \in \mathcal{M}$ *then* $\vdash f_{\mathcal{M}} \to (f_Q|f_R \to \neg\phi)$ *implies* $\vdash f_{\mathcal{M}} \to \neg K_Q\phi$.

Proof Because $\vdash f_R \to \top$, rule E$_R$8 gives $\vdash f_Q|f_R \to f_Q|\top$ that gives further $\vdash f_{\mathcal{M}} \to (f_Q|f_R \to f_Q|\top)$. Combining this result with the hypothesis of the theorem, $\vdash f_{\mathcal{M}} \to (f_Q|f_R \to \neg\phi)$, we obtain

$$\vdash (f_{\mathcal{M}} \wedge f_Q|f_R) \to (f_Q|\top \wedge \neg\phi), \text{ i.e. } \vdash f_{\mathcal{M}} \to (f_Q|f_R \to (f_Q|\top \wedge \neg\phi))$$

But $\vdash (f_Q|\top \wedge \neg\phi) \leftrightarrow \neg(f_Q|\top \to \phi)$, hence

$$\vdash f_{\mathcal{M}} \to (f_Q|f_R \to \neg(f_Q|\top \to \phi)) \tag{4}$$

Axiom E8 ensure that $\vdash K_0(f_Q|\top \to \phi) \to (f_Q|\top \to \phi)$ or, equivalently, $\vdash \neg(f_Q|\top \to \phi) \to \neg K_0(f_Q|\top \to \phi)$, that, used in (4) gives

$$\vdash f_{\mathcal{M}} \to (f_Q|f_R \to \neg K_0(f_Q|\top \to \phi)) \tag{5}$$

But theorem 9.19 gives $\vdash K_0\top$, that can be used in (5) providing

$$\vdash f_{\mathcal{M}} \to (f_Q|f_R \to (K_0\top \wedge \neg K_0(f_Q|\top \to \phi))) \tag{6}$$

The negative introspection, axiom E8, infers

$$\vdash (K_0\top \wedge \neg K_0(f_Q|\top \to \phi)) \to K_0\neg K_0(f_Q|\top \to \phi) \tag{7}$$

Combining (6) and (7) we obtain

$$\vdash f_{\mathcal{M}} \to (f_Q|f_R \to K_0\neg K_0(f_Q|\top \to \phi)) \tag{8}$$

But (8) is equivalent with $\vdash (f_{\mathcal{M}} \wedge f_Q|f_R) \to K_0\neg K_0(f_Q|\top \to \phi)$, and because $Q|R \in \mathcal{M}$, we can apply rule E$_R$8.3 and obtain

$$\vdash f_{\mathcal{M}} \rightarrow \neg K_0(K_Q\top \rightarrow \phi) \tag{9}$$

But from axiom E8 we derive $\vdash K_Q\phi \rightarrow K_0(K_Q\top \rightarrow \phi)$, hence

$$\vdash \neg K_0(K_Q\top \rightarrow \phi) \rightarrow \neg K_Q\phi \tag{10}$$

Combining (9) with (10) we obtain $\vdash f_{\mathcal{M}} \rightarrow \neg K_Q\phi$, q.e.d. □

The next result is a maximal consistent set-sensitive version of theorem 9.11.

Theorem 9.43 *If* $\vdash f_{\mathcal{M}} \rightarrow (\phi \rightarrow \psi)$ *and* $\vdash f_{\mathcal{M}} \rightarrow (\rho \rightarrow \theta)$ *then* $\vdash f_{\mathcal{M}} \rightarrow (\phi|\rho \rightarrow \psi|\theta)$.

Proof To $\vdash f_{\mathcal{M}} \rightarrow (\phi \rightarrow \psi)$ we can apply theorem 9.37 and we obtain $\vdash f_{\mathcal{M}} \rightarrow (\phi|\rho \rightarrow \psi|\rho)$, i.e. $\vdash (f_{\mathcal{M}} \wedge \phi|\rho) \rightarrow \psi|\rho$ which implies

$$\vdash (f_{\mathcal{M}} \wedge \phi|\rho) \rightarrow (f_{\mathcal{M}} \wedge \psi|\rho) \tag{11}$$

The same theorem 9.37 can be applied to $\vdash f_{\mathcal{M}} \rightarrow (\rho \rightarrow \theta)$ giving $\vdash f_{\mathcal{M}} \rightarrow (\psi|\rho \rightarrow \psi|\theta)$, i.e.

$$\vdash (f_{\mathcal{M}} \wedge \psi|\rho) \rightarrow \psi|\theta \tag{12}$$

Further, combining (11) and (12) we derive $\vdash (f_{\mathcal{M}} \wedge \phi|\psi) \rightarrow \psi|\theta$, hence $\vdash f_{\mathcal{M}} \rightarrow (\phi|\psi \rightarrow \psi|\theta)$. □

Theorem 9.44 *If* $\vdash f_{\mathcal{M}} \rightarrow (\phi \rightarrow \psi)$ *then* $\vdash f_{\mathcal{M}} \rightarrow (\langle\alpha\rangle\phi \rightarrow \langle\alpha\rangle\psi)$.

Proof $\vdash f_{\mathcal{M}} \rightarrow (\phi \rightarrow \psi)$ implies $\vdash f_{\mathcal{M}} \rightarrow (\neg\psi \rightarrow \neg\phi)$ where, applying theorem 9.39, we obtain $\vdash f_{\mathcal{M}} \rightarrow [\alpha](\neg\psi \rightarrow \neg\phi)$. But axiom E8 gives $\vdash [\alpha](\neg\psi \rightarrow \neg\phi) \rightarrow ([\alpha]\neg\psi \rightarrow [\alpha]\neg\phi)$. Hence $\vdash f_{\mathcal{M}} \rightarrow ([\alpha]\neg\psi \rightarrow [\alpha]\neg\phi)$, i.e. $\vdash f_{\mathcal{M}} \rightarrow (\neg\langle\alpha\rangle\psi \rightarrow \neg\langle\alpha\rangle\phi)$. Concluding, $\vdash f_{\mathcal{M}} \rightarrow (\langle\alpha\rangle\phi \rightarrow \langle\alpha\rangle\psi)$. □

The next result is a variant of theorem 9.17, but sensitive to the maximal consistent set.

Theorem 9.45

$$\textit{If } \vdash f_{\mathcal{M}} \rightarrow (\bigvee\{f_Q \mid P \xrightarrow{\alpha} Q\} \rightarrow \phi) \textit{ then } \vdash f_{\mathcal{M}} \rightarrow (f_P \rightarrow [\alpha]\phi)$$

Proof If $\vdash f_{\mathcal{M}} \rightarrow (\bigvee\{f_Q \mid P \xrightarrow{\alpha} Q\} \rightarrow \phi)$ then theorem 9.39 gives $\vdash f_{\mathcal{M}} \rightarrow [\alpha](\bigvee\{f_Q \mid P \xrightarrow{\alpha} Q\} \rightarrow \phi)$ and further axiom E8 gives

$$\vdash f_{\mathcal{M}} \rightarrow ([\alpha]\bigvee\{f_Q \mid P \xrightarrow{\alpha} Q\} \rightarrow [\alpha]\phi)$$

But theorem 9.16 gives

$$\vdash f_P \rightarrow [\alpha]\bigvee\{f_Q \mid P \xrightarrow{\alpha} Q\}$$

hence $\vdash f_{\mathcal{M}} \wedge f_P \rightarrow [\alpha]\phi$, i.e. $\vdash f_{\mathcal{M}} \rightarrow (f_P \rightarrow [\alpha]\phi)$. □

10 Completeness of $\mathcal{L}_{\mathbb{A}}^{\mathfrak{A}}$ against process semantics

Further we state the completeness of $\mathcal{L}_{\mathbb{A}}^{\mathfrak{A}}$ with respect to process semantics. The intuition is that, because f_P and $f_{\mathcal{M}}$ are characteristic formulas, we should have an equivalence between $\mathcal{M}, P \models \phi$ and $\vdash f_{\mathcal{M}} \wedge f_P \to \phi$ (of course for finite maximal consistent sets) as both can be read as *the process $P \in \mathcal{M}$ has the property ϕ.*

The 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 (prove) properties of processes.

If $\mathcal{M}$ is a finite maximal consistent set then $\mathcal{M}, P \models \phi$ iff $\vdash f_{\mathcal{M}} \wedge f_P \to \phi$.

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

- **The case $\phi = 0$:** $\mathcal{M}, P \models 0$ implies $P \equiv 0$. But $f_{A'} = 0$ and $\vdash 0 \to 0$, hence $\vdash 0 \wedge f_{\mathcal{M}} \to 0$. This gives $\vdash f_{\mathcal{M}} \wedge f_P \to \phi$.

- **The case $\phi = \top$:** we have always $\mathcal{M}, P \models \top$ and $\vdash f_P \wedge f_{\mathcal{M}} \to \top$, hence $\vdash f_P \wedge f_{\mathcal{M}} \to \phi$.

- **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 $\vdash f_{\mathcal{M}} \wedge f_P \to \phi_1$ and $\vdash f_{\mathcal{M}} \wedge f_P \to \phi_2$. Hence $\vdash f_{\mathcal{M}} \wedge f_P \to (\phi_1 \wedge \phi_2)$, i.e. $\vdash f_{\mathcal{M}} \wedge f_P \to \phi$.

- **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,
  $\vdash f_{\mathcal{M}} \wedge f_Q \to \phi_1$ and $\vdash f_{\mathcal{M}} \wedge f_R \to \phi_2$, i.e.
  $\vdash f_{\mathcal{M}} \to (f_Q \to \phi_1)$ and $\vdash f_{\mathcal{M}} \to (f_R \to \phi_2)$.
  Hence, using theorem 9.43 we obtain $\vdash f_{\mathcal{M}} \to (f_Q | f_R \to \phi_1 | \phi_2)$, i.e. $\vdash f_{\mathcal{M}} \wedge f_P \to \phi$.

- **The case $\phi = K_A \top$:** $\mathcal{M}, P \models K_A \top$ iff $P \equiv I(A)|R$, iff $f_P = f_A | f_R$.
  Using rule E$_R$8 we obtain $\vdash f_A | f_R \to f_A | \top$, further using axiom E8 $\vdash f_A | f_R \to K_A \top$, i.e. $\vdash f_P \to K_A \top$. Hence $\vdash f_{\mathcal{M}} \wedge f_P \to \phi$.

- **The case $\phi = K_A \psi$:** $\mathcal{M}, P \models K_A \psi$, and because $\vdash K_A \psi \to K_A \top$ (by theorem 9.20), using the soundness, we obtain that $\mathcal{M}, P \models K_A \top$. Now, we apply the previous case that gives
  $$\vdash f_{\mathcal{M}} \wedge f_P \to K_A \top \tag{13}$$
  $\mathcal{M}, P \models K_A \psi$ is equivalent with $P \equiv I(A)|R$ and for any $I(A)|S \in \mathcal{M}$ we have $\mathcal{M}, I(A)|S \models \psi$. Then the inductive hypothesis gives
  $$\text{for any } I(A)|S \in \mathcal{M} \text{ we have } \vdash (f_{\mathcal{M}} \wedge f_A | f_S) \to \psi \tag{14}$$
  Consider now a process $I(A)|S \notin \mathcal{M}$. Because $\mathcal{M}$ is finite, we apply theorem 9.32 and obtain $\vdash f_{\mathcal{M}} \to \neg(f_A | f_S)$ or equivalent,
  $\vdash f_{\mathcal{M}} \wedge (f_A | f_S) \to \bot$. But $\vdash \bot \to \psi$, hence
  $$\text{for any } I(A)|S \notin \mathcal{M} \text{ we have } \vdash (f_{\mathcal{M}} \wedge f_A | f_S) \to \psi \tag{15}$$

Now (14) and (15) together give

$$\text{for any } S \in \mathcal{M} \text{ we have } \vdash (f_{\mathcal{M}} \wedge f_A | f_S) \rightarrow \psi \tag{16}$$

i.e., using theorem 9.9,

$$\vdash (f_{\mathcal{M}} \wedge f_A | \bigvee_{S \in \mathcal{M}} f_S) \rightarrow \psi \tag{17}$$

But

$$\vdash K_{A'}(\bigvee_{S \in \mathcal{M}} f_S) \rightarrow \bigvee_{S \in \mathcal{M}} f_S, \ hence \ \vdash f_{\mathcal{M}} \rightarrow \bigvee_{S \in \mathcal{M}} f_S$$

Now, we can apply rule E$_R$8 and obtain

$$\vdash f_A | f_{\mathcal{M}} \rightarrow f_A | \bigvee_{S \in \mathcal{M}} f_S, \ hence \ \vdash (f_A | f_{\mathcal{M}} \wedge f_{\mathcal{M}}) \rightarrow (f_A | \bigvee_{S \in \mathcal{M}} f_S \wedge f_{\mathcal{M}})$$

In this point, using (17) we obtain

$$\vdash (f_A | f_{\mathcal{M}} \wedge f_{\mathcal{M}}) \rightarrow \psi \tag{18}$$

We have $\vdash f_{\mathcal{M}} \rightarrow (\top \rightarrow f_{\mathcal{M}})$ and $\vdash f_{\mathcal{M}} \rightarrow (f_A \rightarrow f_A)$ where from, applying theorem 9.37, we can derive $\vdash f_{\mathcal{M}} \rightarrow (f_A | \top \rightarrow f_A | f_{\mathcal{M}})$, i.e. $\vdash f_M \wedge f_A | \top \rightarrow f_A | f_{\mathcal{M}}$ and further

$$\vdash (f_M \wedge f_A | \top) \rightarrow (f_{\mathcal{M}} \wedge f_A | f_{\mathcal{M}})$$

Using this result together with (18), we obtain further

$$\vdash (f_M \wedge f_A | \top) \rightarrow \psi, \ i.e. \ \vdash f_M \rightarrow (f_A | \top \rightarrow \psi)$$

where we can apply axiom E8 that gives

$$\vdash f_{\mathcal{M}} \rightarrow (K_A \top \rightarrow \psi)$$

applying theorem 9.41, we obtain

$$\vdash f_{\mathcal{M}} \rightarrow (K_A \top \rightarrow K_A \psi), \ i.e. \ \vdash (f_{\mathcal{M}} \wedge K_A \top) \rightarrow K_A \psi \tag{19}$$

But (13) gives

$$\vdash f_{\mathcal{M}} \wedge f_P \rightarrow K_A \top \text{ where from } \vdash (f_{\mathcal{M}} \wedge f_P) \rightarrow (f_{\mathcal{M}} \wedge K_A \top)$$

and using this in (19),

$$\vdash (f_{\mathcal{M}} \wedge f_P) \rightarrow K_A \psi \ i.e. \ \vdash (f_{\mathcal{M}} \wedge f_P) \rightarrow \phi.$$

- **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

  $$\vdash f_{\mathcal{M}} \wedge f_{P'} \rightarrow \psi$$

  $P \xrightarrow{\alpha} P'$ means that $P \equiv \alpha.R|S$ and $P' \equiv R|S$, so $f_P = (\langle\alpha\rangle f_R \wedge 1)|f_S$ and $f_{P'} = f_R|f_S$. So $\vdash f_{\mathcal{M}} \wedge f_R|f_S \rightarrow \psi$, i.e. $\vdash f_{\mathcal{M}} \rightarrow (f_R|f_S \rightarrow \psi)$ and using theorem 9.44

  $$\vdash f_{\mathcal{M}} \rightarrow (\langle\alpha\rangle(f_R|f_S) \rightarrow \langle\alpha\rangle\psi) \qquad (20)$$

  theorem 9.10 gives $\vdash f_P \rightarrow \langle\alpha\rangle f_R|f_S \wedge 1|f_S$, hence

  $$\vdash f_P \rightarrow \langle\alpha\rangle f_R|f_S \qquad (21)$$

  Axiom E8 gives

  $$\vdash \langle\alpha\rangle f_R|f_S \rightarrow \langle\alpha\rangle(f_R|f_S) \qquad (22)$$

  Hence, from (20), (21) and (22) we derive

  $$\vdash f_{\mathcal{M}} \rightarrow (f_P \rightarrow \langle\alpha\rangle\psi),\ i.e.\ \vdash (f_{\mathcal{M}} \wedge f_P) \rightarrow \langle\alpha\rangle\psi$$

- **The case $\phi = \langle A : \alpha\rangle\psi$:** $\mathcal{M}, P \models \langle A : \alpha\rangle\psi$ ensures us that α is active.

  - **the subcase $\psi = \top$:** $\mathcal{M}, P \models \langle A : \alpha\rangle\top$ gives $P \equiv I(A)|R$, hence $f_P = f_A|f_R$. But $\vdash f_R \rightarrow \top$ and, using rule E_R^+8, $\vdash f_A|f_R \rightarrow f_A|\top$. Now using theorem 9.18 we obtain

    $$\vdash f_P \rightarrow \langle A : \alpha\rangle\top,\ hence\ \vdash f_{\mathcal{M}} \wedge f_P \rightarrow \langle A : \alpha\rangle\top$$

  - **the subcase $\psi \neq \top$:** $\mathcal{M}, P \models \langle A : \alpha\rangle\psi$ implies $P \equiv I(A)|R$, exists $Q \in \mathcal{M}$ such that $I(A) \xrightarrow{\alpha} Q$ and $\mathcal{M}, Q|R \models \psi$. Using the inductive hypothesis we obtain

    $$\vdash f_{\mathcal{M}} \wedge f_{Q|R} \rightarrow \psi$$

    But $I(A) \xrightarrow{\alpha} Q$ means that $I(A) \equiv \alpha.Q'|S$ and $Q \equiv Q'|S$. Then $\vdash f_{\mathcal{M}} \wedge f_{Q|R} \rightarrow \psi$ means $\vdash f_{\mathcal{M}} \wedge f_{Q'}|f_S|f_R \rightarrow \psi$, i.e.

    $$\vdash f_{\mathcal{M}} \rightarrow (f_{Q'}|f_S|f_R \rightarrow \psi)$$

    Further we obtain

    $$\vdash f_{\mathcal{M}} \rightarrow (\langle\alpha.Q' : \alpha\rangle(f_{Q'}|f_S|f_R) \rightarrow \langle\alpha.Q' : \alpha\rangle\psi)$$

    while axiom E^+8 gives

    $$\vdash \langle\alpha.Q' : \alpha\rangle f_{Q'}|f_S|f_R \rightarrow \langle\alpha.Q' : \alpha\rangle(f_{Q'}|f_S|f_R),$$

    hence

    $$\vdash f_{\mathcal{M}} \rightarrow (\langle\alpha.Q' : \alpha\rangle f_{Q'}|f_S|f_R \rightarrow \langle\alpha.Q' : \alpha\rangle\psi)$$

and because $\vdash f_P \to \langle \alpha.Q' : \alpha\rangle f_{Q'}|f_S|f_R$, due to axiom E$^+$8, we derive further

$$\vdash f_{\mathcal{M}} \to (f_P \to \langle \alpha.Q' : \alpha\rangle\psi) \tag{23}$$

But $\mathcal{M}, P \models \langle A : \alpha\rangle\psi$ gives $\mathcal{M}, P \models \langle A : \alpha\rangle\top$ (because from $\vdash \psi \to \top$ we derive $\vdash \langle A : \alpha\rangle\psi \to \langle A : \alpha\rangle\top$). But, from the previous case, $\mathcal{M}, P \models \langle A : \alpha\rangle\top$ is equivalent with $\vdash f_{\mathcal{M}} \wedge f_P \to \langle A : \alpha\rangle\top$. Hence

$$\vdash f_{\mathcal{M}} \to (f_P \to \langle \alpha.Q'|S : \alpha\rangle\top) \tag{24}$$

Axiom E$^+$8 gives

$$\vdash \langle \alpha.Q' : \alpha\rangle\psi \wedge \langle \alpha.Q'|S : \alpha\rangle\top \to \langle \alpha.Q'|S : \alpha\rangle\psi$$

and as (23) and (24) give

$$\vdash f_{\mathcal{M}} \to (f_P \to \langle \alpha.Q' : \alpha\rangle\psi \wedge \langle \alpha.Q'|S : \alpha\rangle\top)$$

we obtain further

$$\vdash f_{\mathcal{M}} \wedge f_P \to \langle A : \alpha\rangle\psi$$

- **The case $\phi = \neg\psi$:** we argue by induction on the syntactical structure of ψ.
  - **the subcase $\psi = 0$:** $\mathcal{M}, P \models \neg 0$ means that $P \not\equiv 0$. Then we can apply theorem 9.1 and obtain $\vdash f_P \to \neg 0$.
    So $\vdash f_{\mathcal{M}} \wedge f_P \to \neg 0$.
  - **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, $\vdash f_{\mathcal{M}} \wedge f_P \to \neg\psi_1$ or $\vdash f_{\mathcal{M}} \wedge f_P \to \neg\psi_2$, where from we obtain $\vdash f_{\mathcal{M}} \wedge f_P \to \psi$
  - **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 $\vdash f_{\mathcal{M}} \wedge f_P \to \psi_1$ which is equivalent with $\vdash f_{\mathcal{M}} \wedge f_P \to \phi$.
  - **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

    $$\vdash f_{\mathcal{M}} \to (f_Q \to \neg\psi_1) \textit{ or } \vdash f_{\mathcal{M}} \to (f_R \to \neg\psi_2)$$

    then we can apply theorem 9.38 that gives

    $$\vdash f_{\mathcal{M}} \wedge f_P \to \neg\psi.$$

  - **the subcase $\psi = K_{A'}\psi_1$, A' is atomic agent:** $\mathcal{M}, P \models \neg K_{A'}\psi_1$ means $\exists R \in \mathcal{M}$ such that $\mathcal{M}, R \models \neg\psi_1$. Using the inductive hypothesis,
    $\vdash f_{\mathcal{M}} \wedge f_R \to \neg\psi_1$, i.e. $\vdash f_{\mathcal{M}} \to (f_R|f_0 \to \neg\psi_1)$. Now theorem 9.42 gives $\vdash f_{\mathcal{M}} \to \neg K_{A'}\psi_1$, hence $\vdash f_{\mathcal{M}} \wedge f_P \to \neg K_{A'}\psi_1$.

- **the subcase $\psi = K_A\psi_1$, A is not atomic agent:** we distinguish two cases
  - **the sub-subcase $\psi_1 = \top$:** $\mathcal{M}, P \models \neg K_A\top$ implies that $I(A)$ is not a subprocess of P. Then for any $R \in \mathcal{M}$ we have $P \not\equiv I(A)|R$. Then theorem 9.1 gives us $\vdash f_A|f_R \to \neg f_P$. From here we can infer

    $$\vdash f_A| \bigvee_{S\in\mathcal{M}} f_S \to \neg f_P \tag{25}$$

    But

    $$\vdash K_{A'}(\bigvee_{S\in\mathcal{M}} f_S) \to \bigvee_{S\in\mathcal{M}} f_S,\ hence\ \vdash f_{\mathcal{M}} \to \bigvee_{S\in\mathcal{M}} f_S$$

    Now, we can apply rule E$_R$8 and obtain

    $$\vdash f_A|f_{\mathcal{M}} \to f_A| \bigvee_{S\in\mathcal{M}} f_S$$

    In this point, using (25) we obtain

    $$\vdash f_A|f_{\mathcal{M}} \to \neg f_P \tag{26}$$

    We have $\vdash f_{\mathcal{M}} \to (\top \to f_{\mathcal{M}})$ and $\vdash f_{\mathcal{M}} \to (f_A \to f_A)$ where from, applying theorem 9.37, we can derive $\vdash f_{\mathcal{M}} \to (f_A|\top \to f_A|f_{\mathcal{M}})$, i.e. $\vdash f_M \wedge f_A|\top \to f_A|f_{\mathcal{M}}$ Using this result together with (26), we obtain further

    $$\vdash (f_M \wedge f_A|\top) \to \neg f_P,\ i.e.\ \vdash f_M \wedge f_P \to \neg(f_A|\top)$$

    and axiom E8 gives

    $$\vdash f_{\mathcal{M}} \wedge f_P \to \neg K_A\top.$$

  - **the sub-subcase $\psi_1 \neq \top$:** we distinguish two more cases $\mathcal{M}, P \models \neg K_A\top$ and $\mathcal{M}, P \models K_A\top$.
    - **if** $\mathcal{M}, P \models \neg K_A\psi_1$ and $\mathcal{M}, P \models \neg K_A\top$, we have $\vdash f_{\mathcal{M}} \wedge f_P \to \neg K_A\top$ (proved before). Moreover, because $\vdash K_A\psi_1 \to K_A\top$ (theorem 9.20) we have $\vdash \neg K_A\top \to \neg K_A\psi_1$ which gives $\vdash f_{\mathcal{M}} \wedge f_P \to \neg K_A\psi_1$.
    - **if** $\mathcal{M}, P \models \neg K_A\psi_1$ and $\mathcal{M}, P \models K_A\top$, $\exists I(A)|S \in \mathcal{M}$ with $\mathcal{M}, I(A)|Q \models \neg\psi_1$. Using the inductive hypothesis we obtain $\vdash f_{\mathcal{M}} \to (f_S|f_A \to \neg\psi_1)$ and from theorem 9.42 that $\vdash f_{\mathcal{M}} \to \neg K_A\psi_1$. Hence $\vdash f_{\mathcal{M}} \wedge f_P \to \neg K_A\psi_1$.

- **the subcase $\psi = \langle a\rangle\psi_1$:** $\mathcal{M}, P \models \neg\langle a\rangle\psi_1$ is equivalent with $\mathcal{M}, P \models [a]\neg\psi_1$.

  If there is a process $Q \in \mathcal{M}$ such that $P \xrightarrow{a} Q$, then for any $Q \in \mathcal{M}$ such that $P \xrightarrow{a} Q$ we have $\mathcal{M}, Q \models \neg\psi_1$. Using the inductive hypothesis we obtain that for any $Q \in \mathcal{M}$ such that $P \xrightarrow{a} Q$ we have $\vdash f_{\mathcal{M}} \wedge f_Q \to \neg\psi_1$, i.e.

  $$\vdash f_{\mathcal{M}} \wedge \bigvee\{f_Q \mid P \xrightarrow{a} Q\} \to \neg\psi_1$$

or equivalently

$$\vdash f_{\mathcal{M}} \to (\bigvee\{f_Q \mid P \xrightarrow{a} Q\} \to \neg\psi_1)$$

Using theorem 9.45, we obtain $\vdash f_{\mathcal{M}} \wedge f_P \to [a]\neg\psi_1$.

If there is no process $Q \in \mathcal{M}$ such that $P\overset{a}{\mathbf{to}}Q$ then theorem 9.15 gives $\vdash f_P \to [a]\bot$. But $\vdash \psi_1 \to \top$, hence $\vdash [a]\bot \to [a]\neg\psi_1$. So, also in this case we have $\vdash f_{\mathcal{M}} \wedge f_P \to [a]\neg\psi_1$.

($\Longleftarrow$) Let $\vdash f_{\mathcal{M}} \wedge f_P \to \phi$. Suppose that $\mathcal{M}, P \not\models \phi$. Then $\mathcal{M}, P \models \neg\phi$. Using the reversed implication we obtain $\vdash f_{\mathcal{M}} \wedge f_P \to \neg\phi$, thus
$\vdash f_{\mathcal{M}} \wedge f_P \to \bot$. But from corollary 9 we have $\mathcal{M}, P \models f_{\mathcal{M}} \wedge f_P$ 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.

Definition 10.1 (Provability and consistency) *We say that a formula $\phi \in \mathcal{F}_{\mathbb{A}}^{\mathfrak{A}}$ is* provable in $\mathcal{L}_{\mathbb{A}}^{\mathfrak{A}}$ *(or $\mathcal{L}_{\mathbb{A}}^{\mathfrak{A}}$-*provable *for short), if ϕ can be derived, as a theorem, using the axioms and the rules of $\mathcal{L}_{\mathbb{A}}^{\mathfrak{A}}$. We denote this by $\vdash \phi$.*
We say that a formula $\phi \in \mathcal{F}_{\mathbb{A}}^{\mathfrak{A}}$ is consistent in $\mathcal{L}_{\mathbb{A}}^{\mathfrak{A}}$ *(or $\mathcal{L}_{\mathbb{A}}^{\mathfrak{A}}$-*consistent *for short) if $\neg\phi$ is not $\mathcal{L}_{\mathbb{A}}^{\mathfrak{A}}$-provable.*

Definition 10.2 (Satisfiability and validity) *We call a formula $\phi \in \mathcal{F}_{\mathbb{A}}^{\mathfrak{A}}$* satisfiable *if there exists a maximal consistent set $\mathcal{M}$ and a process $P \in \mathcal{M}$ such that $\mathcal{M}, P \models \phi$.*
We call a formula $\phi \in \mathcal{F}_{\mathbb{A}}^{\mathfrak{A}}$ validity *if for any maximal consistent set $\mathcal{M}$ and any process $P \in \mathcal{M}$ we have $\mathcal{M}, P \models \phi$. In such a situation we write $\models \phi$.*
Given a maximal consistent set $\mathcal{M}$, we denote by $\mathcal{M} \models \phi$ the situation when for any $P \in \mathcal{M}$ we have $\mathcal{M}, P \models \phi$.

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

If ϕ is $\mathcal{L}_{\mathbb{A}}^{\mathfrak{A}}$-consistent then exists a maximal consistent set $\mathcal{M}$ and a process $P \in \mathcal{M}$ such that $\mathcal{M}, P \models \phi$.

Proof Suppose that for any maximal consistent set $\mathcal{M}$ 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 maximal consistent set $\mathcal{M}$ and any process $P \in \mathcal{M}$ we have $\mathcal{M}, P \models \neg\phi$. Using lemma 10, we obtain $\vdash f_{\mathcal{M}} \wedge f_P \to \neg\phi$. Hence $\vdash f_{\mathcal{M}} \wedge \bigvee_{P \in \mathcal{M}} f_P \to \neg\phi$. But $\vdash f_{\mathcal{M}} \to \bigvee_{P \in \mathcal{M}} f_P$ which, combined with the previous result, implies $\vdash f_{\mathcal{M}} \to \neg\phi$.
Thus for each finite maximal consistent set $\mathcal{M}$ we have $\vdash f_{\mathcal{M}} \to \neg\phi$. But then for each maximal consistent set $\mathcal{M} \in \mathfrak{M}_{\neg\phi}^{act(\neg\phi)+}$ we have $\vdash f_{\mathcal{M}} \to \neg\phi$. As $\mathfrak{M}_{\neg\phi}^{act(\neg\phi)+}$ is finite, we can infer further $\vdash \bigvee_{\mathcal{M} \in \mathfrak{M}_{\neg\phi}^{act(\neg\phi)+}} f_{\mathcal{M}} \to \neg\phi$. Now, applying rule E_R8, we obtain $\vdash \neg\phi$. This contradicts with the hypothesis of consistency of ϕ. Hence, it exists a maximal consistent set $\mathcal{M}$ and a process $P \in \mathcal{M}$ such that $\mathcal{M}, P \models \phi$. □

Theorem 10.1 (Completeness) *The $\mathcal{L}_{\mathbb{A}}^{\mathfrak{A}}$ system is complete with respect to process semantics.*

Proof Suppose that ϕ is a valid formula with respect to our semantics, but ϕ is not provable in the system $\mathcal{L}_{\mathbb{A}}^{\mathfrak{A}}$. Then neither is $\neg\neg\phi$, so, by definition, $\neg\phi$ is $\mathcal{L}_{\mathbb{A}}^{\mathfrak{A}}$-consistent. It follows, from lemma 10, that $\neg\phi$ is satisfiable with respect to process semantics, contradicting the validity of ϕ. □

11 Concluding remarks

In this paper we developed a special type of dynamic-epistemic logic, $\mathcal{L}_{\mathbb{A}}^{\mathfrak{A}}$, designed for semantics built on process calculi. This logic is meant to be used for expressing properties of multiagent distributed systems. In this respect the society of agents $\mathfrak{A}$ came with an algebraical structure that depicts the distribution of the modules of a system which are observed by the epistemic agents. In expressing this we used operators from spatial logics together with operators characteristic for dynamic-epistemic logics.

Our logic is expressive enough for describing the two levels of evolution of the multiagent systems, i.e. it can express the evolution of the system as well as the evolution of the epistemic status of the agents. Validity and satisfiability in a model can be expressed in our syntax, and this feature, combined with the possibility to characterize processes and finite maximal consistent sets argue on utility of our logic.

In the context of decidability, our sound and complete axiomatic system provides a powerful tool for making predictions on the evolution of the concurrent distributed systems.

With respect to dynamic-epistemic logics, our logic came with the expressivity given by the algebraical semantics. Also the ontology of the agents is more complex than in the classical approaches. We can speak about the knowledge of agents A', A'' but also about the knowledge of the agent $A'|A''$ which subsumes the knowledge of A', of A'', and the knowledge derived from the fact that what A' and A'' see are modules running in parallel as parts of the same system. Similarly the knowledge of $\alpha.A$ is the knowledge of an agent that, in a future moment, might became the agent A. All these aspects are new for epistemic logics and important in applications.

With respect to the logics of processes, our logic can be seen as an extension of Hennessy-Milner logic with the parallel operator and with epistemic operators. The lasts can be also used to express global properties over unknown contexts. In this respect the epistemic operators can be considered as alternative to the guarantee operator of the classical spatial logics that eventually produces a logic adequately expressive and decidable. In spatial logic the guarantee operator is introduced, as the adjoint of parallel operator, by the following semantics

$\mathcal{M}, P \models \phi \triangleright \psi$ iff for any $P' \in \mathcal{M}$ such that $\mathcal{M}, P' \models \phi$ and $P|P' \in \mathcal{M}$ we have $\mathcal{M}, P|P' \models \psi$.

Our logic is more expressive than guarantee-free dynamic spatial logic, as the first can express global properties, but 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:

$$K_A\phi \overset{def}{=} f_A|\top \wedge (\neg(f_A|\top \rightarrow \phi) \triangleright \bot).$$

Our approach has also a theoretical relevance on the direction of introduction a class of equational-coequational logics for process algebraical semantics. As underlined before, such logics would be able to encode properties involving the program constructors as well as properties concerning the transition systems or observational equivalences. All these are directly related with important applications of distributed systems.

References

[1] A. Baltag, A Logic for Suspicious Players: Epistemic Actions and Belief Updates in Games. Bulletin Of Economic Research vol. 54(1), 2002

[2] A. Baltag and L.S. Moss. Logics for Epistemic Programs, Synthese vol. 139(2) (Special Section: Knowledge, Rationality and Action). Ed. J. Symons, J. Hintikka, Springer Science-Business Media B.V. ISSN: 0039-7857, 2004

[3] A. Baltag and L.S. Moss and S. Solecki. The Logic of Public Announcements. Common Knowledge and Private Suspicions, CWI Technical Report SEN-R9922, 1999

[4] J. F. A. K. van Benthem. Logic for information update, In Proc. of TARK01, 2001

[5] S. D. Brookes and C. A. R. Hoare and A. W. Roscoe, A Theory of Communicating Sequential Processes, Journal of ACM vol.31(3), 1984

[6] C. Calcagno, L. Cardelli and A. D. Gordon, Deciding validity in a spatial logic for trees, In Proc. of ACM Workshop on Types in Language Design and Implementation, 2003

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

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

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

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

[11] L. Cardelli and A. D. Gordon, Mobile Ambients, In Proc. of FOSSACS '98, 1998

[12] M. Dam, Relevance Logic and Concurrent Composition, In Proc. of Third Annual Symposium on Logic in Computer Science, IEEE Computer Society, 1988

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

[14] H. van Ditmarsch, Knowledge games, Bulletin of Economic Research vol.53(4), 2001

[15] R. Fagin et al. Reasoning about Knowledge, MIT Press, 1995

[16] M. Gabbay and A. Pitts, A New Approach to Abstract Syntax Involving Binders, Formal Aspects of Computing, to appear

[17] J. Gerbrandy and W. Groeneveld, Reasoning about information change, Journal of Logic, Language and Information vol.6, 1997

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

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

[20] J. Hintikka: Knowledge and Belief, Ithaca, N.Y.: Cornell University Press, 1962

[21] A. Kurz and D. Pattinson, Coalgebras and Modal Logic for Parameterised Endofunctors, CWI Technical Report, SEN-R0040, 2002

[22] A. Kurz and J. Rosicky, Modal Predicates and Coequations, In Proc. of CMCS'02, ENTCS vol.65.1, 2002

[23] R. Mardare. Logical analysis of Complex Systems. Dynamic Epistemic Spatial Logics, Ph.D. thesis, DIT, University of Trento, 2006

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

[25] R. Mardare and C. Priami. Dynamic Epistemic Spatial Logics, Technical Report, 03/2006, Microsoft Research Center for Computational and Systems Biology, Trento, Italy, 2006, available from http://www.cosbi.eu

[26] R. Mardare. Dynamic-Epistemic reasoning on distributed systems, Technical Report, 2007, Microsoft Research Center for Computational and Systems Biology, Trento, Italy, 2006, available from http://www.cosbi.eu

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

[28] R. Milner, Communicating and Mobile Systems: the Pi-Calculus, Cambridge University Press, 1999

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

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

[31] D. Sangiorgi and D. Walker, The Pi-calculus. A Theory of Mobile Processes, Cambridge University Press, 2001

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