An Analysis for Proving Temporal Properties of Biological Systems (Extended Version)

Roberta Gori and Francesca Levi

Department of Computer Science, University of Pisa, Italy

Abstract This paper concerns the application of formal methods to biological systems, modelled specifically in BioAmbients [35], a variant of the Mobile Ambients [4] calculus. Following the semantic-based approach of abstract interpretation, we define a new static analysis that computes an abstract transition system. Our analysis has two main advantages with respect to the analyses appearing in literature: (i) it is able to address *temporal* properties which are more general than *invariant* properties; (ii) it supports, by means of a particular *labelling discipline*, the validation of systems where several copies of an ambient may appear.
Keywords: *Mobile Ambients and BioAmbients calculus, static analysis, abstract interpretation.*

1 Introduction

One of the most interesting and recent applications of computer science is that to systems biology. The great challenge is to understand whether models, originally developed for describing systems of interacting components, can be applied for modeling and analyzing biological systems. This could offer biologists very useful simulation and verification tools that could replace expensive experiments in vitro or guide the experiments by making predictions on their possible results.

Among the many formalisms that have been successfully applied to biology there are traditional specification languages for concurrent and reactive systems [25,20,19], and process calculi, designed for modeling distributed and mobile systems. Process calculi turned out to be very appropriate for describing both the molecular and biochemical aspect, as pioneered by the application of stochastic π-calculus [36,34]. New process calculi have also been proposed in order to faithfully model biological structures such as compartments and membranes, which play a key role in the organization of biomolecular systems. Recent proposals are BioAmbients [35], Beta-Binders [33], and Brane calculi [2].

BioAmbients (BA) is a variant of a very popular calculus for mobile processes, the Mobile Ambients calculus (MA)[4]. The key concept of MA is that of *ambient*. An ambient represents a bounded location where computation happens; ambients are organized into a hierarchy, that can be dynamically modified as a consequence of an ambient movement or dissolution. The concepts of ambient and of ambient movement permit to naturally represent important aspects of molecular systems, such as localization, compartmentalization and hierarchy. For better modeling basic biological concepts, minor modifications are introduced in BA with respect to standard MA. Ambients are nameless; the primitive for opening is replaced by a primitive of merge, which realizes the fusion of two ambients; capabilities have corresponding co-capabilities; new primitives for communication and choice are introduced.

A great advantage of using BA is the variety of formal verification techniques, proposed for MA in the last few years, can be naturally adapted to BA. In particular, due to the intrinsic complexity of biological systems, *static analysis* techniques appear very promising, since they can be applied to infer information on the possible behavior of biological systems that cannot be handled by simulation tools [36,34] or by automatic verification techniques such as model checking [23,24].

Static analyses define safe and computable approximations of the (run-time) behavior of a system, and they have been typically applied in the MA setting (see [28,18,14,21,15,27,11]) for verifying security properties, specifically for proving *invariant* properties. To this aim, they collect information about the reachable states typically by reporting approximate descriptions of the possible nesting of ambients and processes. This information can be exploited to show that certain events *will not happen* in *each* state of the system; for example, that an ambient *will never* end up inside another one; and similarly, that an interaction between two ambients *will never* happen. More complex properties, such as mutual exclusion or properties related to the number of objects appearing in the system, can also be proved, by exploiting more detailed analyses (see for example [14,15,21,18,27]). As expected, some these techniques [28,14,11,21,15] were successfully adapted to the BA calculus (see [30,29,31,32,15]); for example, [32] shows the interest of invariant properties for BA, specifically for distinguishing a system describing a normal LDL degradation process from one presenting mutations or defects.

Nonetheless, we believe that *temporal* properties, much more general than invariant properties, should be addressed in order to reason on real biological systems. Examples of interesting temporal properties could be: for each path of computation "after A interacts with B than it does not interact with C anymore"; for each path of computation " A may happen only after B"; there exists a path of computation where molecule A appears. Such properties could help biologists to better understand both the *spatial* and *temporal* evolution of complex biological systems, such as pathways and networks of proteins, as already pointed out in [5,23,24,1]. It should be clear that the validation of such properties requires *more powerful analyses* able to observe the possible evolution of a system, i.e., analyses which compute a (not too-coarse) approximation of its transition system.

As an example, we consider typical specifications of enzymatic reactions, following the approach proposed in [35] based on ambient movement. The system describes a simplified version of a (irreversible) enzymatic reaction, where a *molecule* interacts with an *enzyme*, then releasing product P.

$$SYS ::= [M]^{mol} \mid [E]^{e} \qquad M ::= \mathtt{in}\, m.\, \mathtt{out}\, n.\, P \qquad E ::= \mathtt{rec}Y.\, \overline{\mathtt{in}}\, m.\, \overline{\mathtt{out}}\, n.\, Y \tag{1}$$

The enzyme and its substrate are modeled by ambients, labelled [1] e and mol, respectively. Processes M and E describe the binding of the molecule to the enzyme and the release of the product. Specifically, the enzyme-substrate binding is modeled as entry of the substrate ambient inside the enzyme ambient; symmetrically, the release of product P is modeled as ambient exit.

In the simple reaction, described in (1), the binding of ambient mol with the enzyme ambient is *necessary* for the release of product P. Even this very simple property, however, cannot be captured by standard reachability analyses for BA and MA [28,18,11,14,21,30,29,31,32,15]. In fact, the reported information concerns the possible contents of ambients, at any evolution step, and therefore shows *both* that ambient mol may reside inside an ambient e and that it may exit by producing product P. Information about the possible moves of the system is obviously needed in order to infer that the former event is a so called *check-point* for the latter.

[1] Notice that in BA labels are attached to ambients as comments, in that ambients are nameless.

The interest of these kind of properties can be better illustrated by considering a more complex situation, where two distinct enzyme e_1 and e_2 appear in the system,

$$SYS ::= [M]^{mol} \mid [E_1]^{e_1} \mid [E_2]^{e_2} \quad E_i ::= \mathtt{rec}Y.\,\overline{\mathtt{in}}\,m_i.\,\overline{\mathtt{out}}\,n_i.\,Y \tag{2}$$

$$M ::= \mathtt{in}\,m_1.\,\mathtt{out}\,n_1.\,\mathtt{in}\,m_2.\,\mathtt{out}\,n_2.\,P \tag{3}$$

$$M ::= \mathtt{in}\,m_1.\,\mathtt{out}\,n_1.\,P_1 + \mathtt{in}\,m_2.\,\mathtt{out}\,n_2.\,P_2 \tag{4}$$

Processes (3) and (4) model two different behaviors of the molecule, namely two different reactions. In case (3) the binding of ambient *mol* with *both* enzymes e_1 and e_2 is *necessary* for the release of product P (this also has to happen in a given order, first e_1 and then e_2). By contrast, in case (4) ambient *mol* can *non-deterministically* bind *either* with e_1 (by releasing product P_1) *or* with e_2 (by releasing product P_2).

The relevant difference between these two systems cannot be captured by standard reachability analyses for BA and MA [28,18,11,14,21,30,29,31,32,15], which predict (in both cases) that ambient *mol* may bind with *both* ambients e_1 and e_2. Analogously to case (1) information about the possible moves of the system is needed in order to say whether the molecule has to bind with both enzyme or whether there is a non-deterministic choice.

Moreover, we observe that, our analysis has to be able to deal with systems where several occurrences of ambients and processes may appear for accurately modelling real biological systems. This feature is crucial, even if we are interested in observing the *qualitative behavior* of processes (as opposite to the *quantitative behavior*), as explained by the following example. We generalize the specification of the simple enzymatic reaction, described in system (1), by introducing several molecule and enzyme ambients,

$$SYS ::= [M]^{mol} \mid \ldots \mid [M]^{mol} \mid [E]^{e} \ldots \mid [E]^{e} \tag{5}$$

$$E ::= \mathtt{rec}Y.\,\overline{\mathtt{in}}\,m.\,\overline{\mathtt{out}}\,n.\,Y \tag{6}$$

$$E ::= \mathtt{rec}Y.\,\overline{\mathtt{in}}\,m.\,\overline{\mathtt{out}}\,n.\,Y \mid \mathtt{rec}Y.\,\overline{\mathtt{in}}\,m.\,\overline{\mathtt{out}}\,n.\,Y \tag{7}$$

Process (6) describes a generalized system that exhibits the expected behavior; any molecule may bind with an enzyme, but *at most* one molecule can reside inside any enzyme ambient, at the time. By contrast, process (7) shows an anomalous behavior of the enzyme which may bind with two distinct molecule, at the time.

It is clear that that defect of the enzyme (due to process (7)) cannot be detected if we analyse the simplified system (1) where just one molecule is present. However, in order to analyze the generalized system (5) we need detailed information: (i) for capturing the difference between processes (6) and (7); and (ii) for distinguishing the occurrences of ambient *mol*. Specifically, we expect to be able prove that the properties described for the simplified version (e.g. process (1)) still hold. This means that, in system (5), process (6) guarantees that, for *any* ambient *mol*, the binding with an enzyme ambient is *necessary* for the release of product P.

Based on the previous motivations we propose a new analysis for BA following the *abstract interpretation* [7,8] approach, more specifically in the style of previous proposals for MA [14,21]. More in details, we extend the approach of [21], basically by enhancing the structure of abstract states, and we derive an abstract transition system (by abstracting the transition steps).

For capturing occurrence counting information, we adopt the approach of the reachability analysis of [16], by recording information about the *number of occurrences* of ambients and capabilities that may appear in any location. Note that this idea is not completely new (see the proposals of [27,13,15]), while in [21,18] a less precise information is tracked since the number of objects, which may occur in the *whole* system, is taken into account. Moreover, in order to accurately handle systems where several copies of ambients may appear, we adopt a special *labelling discipline* for ambients, both in the concrete and in the abstract semantics. Labels are profitably exploited for distinguishing different occurrences of ambients.

The derived abstract transition system is a safe over-approximation in the sense of [6,10], and thus preserves the properties of a fragment of CTL, ∀-CTL without eventually. In this paper, however, we are interested in the validation of systems where multiple occurrences of an ambient may appear (such as system (5) and the analogous generalization of system (2)). Since in this case the standard interpretation of ∀-CTL seems not adequate, we introduce a simple class of temporal properties and we define validation methods (both in the concrete and in the abstract case) exploiting the labels of ambients. The properties can specify typical temporal properties of pathways, such as 'after A interacts with B than it does not interact with C anymore"; for each path of computation " A may happen only after B". This permits to specify and validate the properties, described for processes (5) and for the generalization of process (2), which express the requirements precisely for *any* occurrence of ambient *mol*.

Our analysis is much more informative and powerful with respect to the reachability analyses for BA and MA [28,18,11,14,21,30,29,31,32,15]. This is obviously paid in terms of complexity (in the worst case, the analysis is double exponential); by contrast, most of the reachability analyses of BA and MA [28,11,14,21,30,29,31,32,15] are associated with polynomial time algorithms. A typical approach in abstract interpretation to find a balance between precision and computational cost is to design *widening operators* [9]. We show that this approach can be profitably applied also to our analysis by introducing a simple widening operator which leads to a weaker but more efficient analysis. The widening is obtained by merging information related to different occurrences of ambients with the same label, in any abstract state. In this way, the complexity of the analysis boils down to be exponential; the resulting abstract transition system, however, is still able to validate interesting temporal properties (for example we show the validation of a simple temporal property for the generalisation of system (2)).

The paper is organized as follows. Section 2 introduces the syntax and the semantics of the BioAmbients calculus. In Section 3 we present our analysis and in Section 4 the derived widening operators. Finally, Section 5 presents the temporal logic as well as interesting examples of validation.

2 Syntax and Semantics

For reasons of space, we consider here a simplified version of BioAmbients [35] without communication primitives; the analysis can be extended in a simple way to the full calculus.

In Control Flow Analysis (see for instance [28,11,21]) typically processes are labeled and α-conversion is treated in a particular way, based on a given partition of names. In particular, we consider a set $\mathcal{N}$ (ranged over by $n, m, h, k, \ldots$) of *channel names* such that $\mathcal{N} = \uplus_i \mathcal{N}_i$, $i \in \{1, \ldots, \omega\}$, where $\uplus$ denotes disjoint union and each $\mathcal{N}_i$ is an infinite set. We also consider, in a standard way, an infinite set of recursion variables $\mathcal{V}$ (ranged over by $X, Y, Z, \ldots$). For ambients, we consider an infinite set of *ambients names* $\mathcal{N}_a$ (ranged over by $a, b, c, \ldots$), such that $\mathcal{N}_a \cap \mathcal{N} = \emptyset$ and $\top \in \mathcal{N}_a$, where $\top$ is a distinct symbol used to denote the outermost ambient.

Moreover, we consider an infinite set $\widehat{\mathcal{L}}$ of *run-time labels* (ranged over by $\Psi, \Gamma, \Delta, \ldots$), and then of *ambients labels* $\mathcal{L}_a = \{(a, \Psi) \mid a \in \mathcal{N}_a \text{ and } \Psi \in \widehat{\mathcal{L}}\}$ (ranged over by $A, B \ldots$). Intuitively, an ambient label $A = (a, \Psi)$ shows the name of the ambient a (denoted by $(A)_1$

M,N::=		(*capabilities*)
	$\mathtt{in}\,n$	enter
	$\overline{\mathtt{in}}\,n$	co-enter
	$\mathtt{out}\,n$	exit
	$\overline{\mathtt{out}}\,n$	co-exit
	$\mathtt{merge}\,n$	merge
	$\overline{\mathtt{merge}}\,n$	co-merge

P,Q::=		(*processes*)
	0	inactivity
	$(\nu n)\,P$	restriction
	$P \mid Q$	parallel composition
	X	recursion variable
	$\mathtt{rec}X.\,P$	recursive process
	$[P]^A$	ambient
	$M.\,P$	capability prefix
	$\Sigma_{i\in I} M_i.\,P_i$	capability choice

$[+\mathtt{in}\,m.\,P \mid Q]^A \mid [+\overline{\mathtt{in}}\,m.\,R \mid S]^B \to_\emptyset [[P \mid Q]^A \mid R \mid S]^B$	(In)
$[[+\mathtt{out}\,m.\,P \mid Q]^A \mid +\overline{\mathtt{out}}\,mR \mid S]^B \to_\emptyset [P \mid Q]^A \mid [R \mid S]^B$	(Out)
$[+\mathtt{merge}\,m.\,P \mid Q]^A \mid [+\overline{\mathtt{merge}}\,m.\,R \mid S]^B \to_\emptyset [P \mid Q \mid R \mid S]^A$	(Merge)
$(L = \mathcal{L}_a(P\eta) \quad \mathcal{L}_a(P) \cap L = \emptyset) \Rightarrow \mathtt{rec}X.\,P \to_L P[\mathtt{rec}X.\,P\eta/X]$	(Rec)
$P \to_L Q \Rightarrow (\nu n)\,P \to_L (\nu n)\,Q$	(Res)
$(\mathcal{L}_a(R) \cap \mathcal{L}_a(Q\eta) = \emptyset \quad dom(\eta) = L \quad P \to_L Q) \Rightarrow P \mid R \to_{\eta(L)} Q\eta \mid R$	(Par)
$(P \to_L Q \quad A \notin \mathcal{L}_a(Q\eta) \quad dom(\eta) = L) \Rightarrow [P]^A \to_{\eta(L)} [Q\eta]^A$	(Amb)
$(P' \to_L Q' \quad P \equiv P' \quad Q' \equiv Q) \Rightarrow P \to_L Q$	(Cong)

Table1. BioAmbients Processes and Reduction Rules

using the standard notation for projection) and the run-time label of the ambient Ψ (denoted by $(A)_2$).

The syntax of (labeled) *processes* is defined in Table 1. The constructs for inactivity, parallel composition, restriction are standard (see for instance π-calculus [26]). The inactive process is denoted by 0; parallel composition is denoted by $P \mid Q$; the restriction operator, denoted by $(\nu n)P$, creates a new name n with scope P. Operator $\mathtt{rec}X.\,P$ defines a recursive process (it is convenient to adopt recursion in place of standard replication $!P$). Specific to the ambient calculi, are the ambient construct, $[P]^A$, the capability prefix $M.\,P$, where M is an action or co-action[2], and the derived capability choice primitive $\Sigma_{i\in I} M_i.\,P_i$. Specifically, process $[P]^A$ defines an ambient (labeled) A where process P runs.

For processes we adopt standard syntactical conventions. We often omit the trailing 0, and we assume that parallel composition has the least syntactic precedence. The operator $(\nu n)P$ acts as static binder for channel name n, and induces the standard notions of free and bound names of a process, denoted by $fn(P)$ and $bn(P)$ resp.. Similarly, $\mathtt{rec}X.\,P$ is a binder for X with scope P. In the following, we consider only processes that are closed on recursion variables, e.g. they have no free recursion variables. As usual, we also identify processes which are α-convertible, meaning that they can be made syntactically equals by a change of

[2] For coactions the notation of Safe Ambients [22] is used in place of the standard one.

bound names. In the style of [11,21] we, however, discipline α-conversion by assuming that a bound name m can be replaced only with a name n provided that $n, m \in \mathcal{N}_i$.

Labels are introduced for easing both the analysis (see Section 3) and the specification of the properties (see Section 5), and do not modify the standard behavior of processes (according to the idea that in BA ambients are nameless, differently from standard MA [4]). Specifically, they are designed for handling systems where multiple occurrences of ambients may appear, and for proving properties for *any* occurrence of an ambient. In this sense, given an ambient labeled (a, Ψ): (i) the name a is shared by different occurrences of ambients; (ii) by contrast, the run-time label Ψ is used for distinguishing the occurrences of ambients named a.

For these purposes, we adopt a labeling discipline for processes; in a well-labeled process ambients related to the same name are distinguished by means of distinct run-time labels.

Definition 1 (Well-labelled). *We say that a process P is* well-labeled *iff whenever two ambients $[Q]^A$ and $[R]^B$ appear, such that $(A)_1 = (B)_1$, then $(A)_2 \neq (B)_2$.*

As an example, the following is a (well-labeled) version of the system (5) described in the Introduction,

$$SYS ::= [M]^{(mol,\Psi_1)} \mid \ldots \mid [M]^{(mol,\Psi_h)} \mid [E]^{(e,\Delta_1)} \mid \ldots \mid [E]^{(e,\Delta_k)}$$

In the following, we use $\mathcal{L}_a(P)$ and $\mathcal{N}_a(P)$ for the set of the ambients labels and names appearing in process P, resp.. We also adopt a standard notion of relabeling, by using injective functions $\eta : \mathcal{L}_a \to \mathcal{L}_a$, such that for each $A \in dom(\eta)$, $(A)_1 = (\eta(A))_1$ (this guarantees that relabeling that does not modify the ambients names). The standard notation $P\eta$ is used for relabeling process P according to η.

Reduction Semantics. The semantics of BA is given in the form of a reduction relation; the rules are reported in Table 1. Minor modifications are needed with respect to the standard definition for preserving the condition of well-labeling; specifically, for handling the new occurrences of ambients (related to a given name) which may be produced, as the computation proceeds.

Given that new copies of ambients can only be introduced by the unfolding of recursion, it is enough to generate fresh labels (in particular fresh run-time labels) for those ambients. To this aim, we adopt reduction arrows $\to_L$, where $L \subseteq \mathcal{L}_a$ is the set of fresh ambients labels, introduced by the move.

The reduction axioms (In), (Out) and (Merge) define the basic interactions; they model the movement of an ambient, in or out, of another ambient and the merge of two ambients. They differ from those of MA mainly because ambients are nameless and because actions have corresponding coactions, as in Safe Ambients [22]. Moreover, the primitive *merge* replaces the standard primitive of opening. For compacting the presentation, we adopt a special notation for capability prefix and capability choice, by writing $+M.\,P$ both for process $M.\,P$ and process $\Sigma_{i \in I} M_i.\,Q_i$, where $M = M_i$ and $P = Q_i$ for some $i \in I$.

Another difference with MA is that the unfolding of recursion is modeled as a reduction rule, e.g. (Rec). In rule (Rec) a relabeled version of the recursive process, e.g. $\mathtt{rec}X.\,P\eta$, is used, and the information about the introduced fresh labels $\mathcal{L}_a(P\eta)$ is properly recorded. The inference rules (Res), (Par), (Amb) and (Cong) are standard; they handle reductions in contexts and permit to apply structural congruence. Structural congruence, e.g. relation $\equiv$, is defined in a standard way; we therefore omit the definition that can be found in [35]. Notice that, in case of (Par) and (Amb), the fresh labels are updated (if needed). In this way, in a reduction step $P \rightarrow_L P'$, all the ambients appearing in P maintain their labels, and the labels of the new introduced ambients are fresh.

In the following, we consider only well-labeled processes, and we use $\mathcal{P}$ to denote the set of (well-labeled) processes. Moreover, we say that a process P is *active* if either $P = \Sigma_{i\in I} M_i.\, Q_i$, $P = M.\, Q$ or $P = \mathtt{rec}X.\, P$; analogously, we use $\mathcal{AP}$ to denote the set of (well-labeled) active processes.

Moreover, we say that a context C is *enabling* whenever the hole does not appear under a capability prefix or a recursion; also we say that an ambient, labeled A, is *enabled* in P whenever $P \equiv C[[Q]^A]$ for some enabling context C. We then use $\mathtt{amb}(P), \mathtt{amb}(P, a) \subseteq \mathcal{L}_a$ for denoting the labels of the ambients and of the ambients named a, that are enabled in process P.

The collecting semantics. The *collecting semantics* computes in a standard way the *transition system* derived from the initial (well-labeled) process. The following definitions formalize the domain of interest; both for processes and transitions. We are tacitly assuming to reason up to relabeling and α-conversion. We use $\mathcal{T} = \{P \rightarrow P' \mid P, P' \in \mathcal{P}\}$ for the set of transitions; and, $Ts = \{(Ss, Ss_0, Ts) \mid Ss, Ss_0 \in \wp(\mathcal{P}), \text{ and } Ts \in \wp(\mathcal{T})\}$ for the set of transition systems [3].

Definition 2 (Concrete Domain). *The* concrete domain *is* $\mathcal{A} = \langle Ts, \subseteq\rangle$*, where* $\subseteq$ *is defined component-wise.*

Definition 3 (Collecting Semantics). *Let* $P \in \mathcal{P}$ *be a process such that* $\top \notin \mathcal{N}_a(P)$*. We define* $\mathfrak{S}_{Coll}[\![P]\!] =$ *lfp* F_P*, where* $F_P : \mathcal{A} \rightarrow \mathcal{A}$*, such that for* $Ss, Ss_0 \in \wp(\mathcal{P})$ *and* $Ps \in \wp(\mathcal{T})$*,*

$$F_P(Ss, Ss_0, Ps) = (Ss_0 \cup \bigcup_{\{P_2 \mid P_1 \rightarrow_L P_2,\ P_1 \in Ss\}} \{P_2\},\ \{P\}\ ,\ \bigcup_{\{P_1 \rightarrow_L P_2 \mid P_1 \in Ss\}} \{P_1 \rightarrow P_2\}).$$

3 The Abstraction

The analysis computes an abstract transition system, which is derived, in standard abstract interpretation style, by giving abstract states (that abstract processes) and abstract transitions (that abstract reduction steps among processes). The abstract domain includes a notion of ordering, expressing precision of approximations, and is related to the concrete one through a Galois connection [7,8]. This permits to naturally formalise the correctness of the analysis.

The abstraction is parametric with respect to the choice of *abstract names* and *labels*. We consider an abstract partition of channel names $\mathcal{N}$, $\mathcal{N} = \uplus_i \mathcal{N}_i^\circ$, $i \in \{1, \ldots, h\}$, such that, for each $n, m \in \mathcal{N}_i$ we have $n, m \in \mathcal{N}_j^\circ$. We then consider *abstract channel names* $\mathcal{N}^\circ = \mathcal{N}_{/\cong}$ where $\cong$ is the obvious equivalence induced by the partition. Analogously, we consider *abstract ambient names* $\mathcal{N}_a{}^\circ = \mathcal{N}_{a/\cong}$ by adopting an equivalence relation $\cong$ over $\mathcal{N}_a$. We also consider an infinite set of *runtime labels* $\widehat{\mathcal{L}}^\circ = \widehat{\mathcal{L}} \cup \{\infty\}$ (ranged over by $\overline{\Psi}, \overline{\Delta}, \ldots$); then, we derive in a standard way the *ambients labels* $\mathcal{L}_a{}^\circ = \{(a^\circ, \overline{\Psi}) \mid a^\circ \in \mathcal{N}_a{}^\circ$ and $\overline{\Psi} \in \widehat{\mathcal{L}}^\circ\}$.

In the following, we use $-^\circ$ to denote the abstraction of a label or name $-$, according to the notation for meta-variables of Section 2. Analogously, we consider *abstract processes*

[3] Note that we generalize the usual notion of transition systems by allowing sets of initial states. Moreover, we adopt transitions such as $P \rightarrow P'$, given that the information about the fresh labels is relevant only for the derivation of a reduction step.

which are built according to the syntax of Table 1 by replacing standard names and labels with their abstract versions. As usual, we denote by P° the abstraction of process P, and we use $\mathcal{P}^\circ$ and $\mathcal{AP}^\circ$ for the set of abstract and active abstract processes, resp..

Note that $\widehat{\mathcal{L}}^\circ$ is infinite (indeed there is no a priori abstraction of run-time labels). In the concrete semantics distinct run-time labels are used to distinguish occurrences of ambients with the same name; specifically, each ambient maintains its label, as the computation proceeds, and fresh labels (in particular run-time labels) are introduced only for the new copies of ambients introduced by the unfolding of recursion. Since this approach is obviously not effective (e.g. infinite run-time labels may be generated), in the abstract case, we adopt a different technique. First of all, we introduce methods for approximating the run-time labels, e.g. for merging the information related to distinct run-time labels together; then, we admit that the run-time labels of ambients *can vary*, as the compution proceeds (by properly recording the information in the abstract transitions). In particular, in the analysis (see paragraph 3.2) we apply a particular *labelling discipline* which guarantees that, for any abstract ambient name $a^\circ \in {\mathcal{N}_a}^\circ$, *at most* max_{a° distinct run-time labels $\widehat{\mathcal{L}}^\circ$ can be generated. The bound imposed by parameter max_{a° is guaranteed by means of the special label ∞.

3.1 Abstract domain and Galois connection

Abstract states. Abstract states are the main concept of the analysis; they are designed, along the lines of [21,16], precisely to represent approximate information about processes. In the style of [16] an *abstract state* reports: (i) the abstract labels of the ambients that may appear; and (ii) for each of them, a set of *configurations* describing the possible contents of the related ambients. More in details, a configuration contains both the *abstract labels* of the ambients and the *active abstract processes*, which may appear at top-level, and their number of occurrences. For representing occurrence counting information, we adopt $\mathcal{M} = \{0, 1, [0-\omega], [1-\omega]\}$. Each $\mathtt{m} \in \mathcal{M}$ denotes a *multiplicity*, with the following meaning: 0 and 1 indicate zero and exactly one respectively, the interval $[1-\omega]$ at least one, while the interval $[0-\omega]$ indicates 0 or more.

Example 1. We consider a (well-labelled) version of the system (5) described in the Introduction,

$$\begin{array}{l} SYS ::= [M]^{(mol,\Psi_1)} \mid \ldots \mid [M]^{(mol,\Psi_h)} \mid [E]^{(e,\Delta_1)} \mid \ldots \mid [E]^{(e,\Delta_k)} \\ E ::= \mathtt{rec}Y.\, \overline{\mathtt{in}}\, m.\, \overline{\mathtt{out}}\, n.\, Y \quad M ::= \mathtt{in}\, m.\, \mathtt{out}\, n.\, P \end{array}$$

We also assume that the abstract names and ambient names are defined by the following equivalence classes $\mathcal{N}^\circ = \{n, m\}$, and $\mathcal{N}_a^\circ = \mathcal{N}_a$. According to the ideas of [16], the *best approximation* of system SYS is the following abstract state (to simplify the presentation we use $\top$ stands for $(\top, \Lambda)$, $D_i^\circ = (mol, \Psi_i)$ and $F_i^\circ = (e, \Delta_i)$),

$$\begin{array}{l} S_{1,1}^\circ = \{(\top, C_{0,1}^\circ)\} \bigcup_{i\in\{1,\ldots,h\}} \{(D_i^\circ, C_{1,1}^\circ)\} \bigcup_{i\in\{1,\ldots,k\}} \{(F_i^\circ, C_{2,1}^\circ)\} \\ C_{0,1}^\circ = \{(D_1^\circ, 1), \ldots, (D_h^\circ, 1), (F_1^\circ, 1), \ldots, (F_k^\circ, 1)\} \quad C_{1,1}^\circ = \{(M^\circ, 1)\} \quad C_{2,1}^\circ = \{(E^\circ, 1)\} \\ E^\circ ::= \mathtt{rec}Y.\, \overline{\mathtt{in}}\, m^\circ.\, \overline{\mathtt{out}}\, m^\circ.\, Y \quad M^\circ ::= \mathtt{in}\, m^\circ.\, \mathtt{out}\, m^\circ.\, P^\circ \end{array}$$

State $S_{1,1}^\circ$ is also graphically represented in Fig. 1(a). Configuration $C_{0,1}^\circ$ reports information about the processes running at top-level (represented by a special name $\top$); it shows that *exactly one* ambient labelled D_i°, for each $i \in \{1, h\}$, appears; analogously, for the ambients labelled F_i°, for each $i \in \{1, k\}$. Configuration $C_{1,1}^\circ$ describes the possible contents of ambients named mol (and labelled D_i° for some $i \in \{1, h\}$); pair $(M^\circ, 1)$ says that *exactly* one process abstracted by M° is present. Similarly, $C_{2,1}^\circ$ describes the possible contents of ambients named e (and labelled F_i° for some $i \in \{1, k\}$).

$$\begin{tikzcd}[column sep=small]
 & & & \top \arrow[dlll] \arrow[dl] \arrow[dr] \arrow[drrr] & & & \\
(D_1^\circ, 1) \arrow[dr] & \cdot\cdot & (D_h^\circ, 1) \arrow[dl] & & (F_1^\circ, 1) \arrow[dr] & \cdot\cdot & (F_k^\circ, 1) \arrow[dl] \\
 & (M^\circ, 1) & & & & (E^\circ, 1) &
\end{tikzcd}$$

(a)

$$\begin{tikzcd}
 & \top \arrow[dl] \arrow[dr] & \\
(A_1^\circ, [1-\omega]) \arrow[d] & & (B_1^\circ, [1-\omega]) \arrow[d] \\
(M^\circ, 1) & & (E^\circ, 1)
\end{tikzcd}$$

(b)

Figure1. The abstractions of system SYS graphically

In state $S_{1,1}^\circ$ the approximation does not modify the labels of ambients. As we have already discussed, this approach is not effective and a method for approximating run-time labels have to be introduced. Intuitively, distinct run-time labels, related to the same name, can be represented by a single abstract label, provided that coherent information about the corresponding configurations and multiplicities is reported. As an example, the following is a *safe approximation* of state $S_{1,1}^\circ$, using abstract labels $A_i^\circ = (mol, \Lambda_i)$ and $B_i^\circ = (e, \Phi_i)$,

$$S_{1,2}^\circ = \{(\top, C_{0,2}^\circ), (A_1^\circ, C_{1,1}^\circ), (B_1^\circ, C_{2,1}^\circ))\} \quad C_{0,2}^\circ = \{(A_1^\circ, [1-\omega]), (B_1^\circ, [1-\omega])\}$$

In state $S_{1,2}^\circ$ (depicted also in Fig. 1(b)) all the labels $D_1^\circ, \ldots, D_h^\circ$, for name mol, are represented by label A_1°, and analogously all the labels $F_1^\circ, \ldots, F_k^\circ$, for name e, are represented by label B_1°. The configuration describing $\top$ is updated accordingly; $C_{0,2}^\circ$ reports indeed that *more than* one occurrence of ambients labelled A_1° and B_1° (and thus of ambients named mol and e) appear. Notice that the interpretation of configuration $C_{1,1}^\circ$ is that, *any* ambient named mol contains *exactly* one process abstracted by M°; similarly, for $C_{2,1}^\circ$. In this sense, the counting of occurrences is local, being $[1-\omega]$ the global number of occurrences of processes M°.

It is worth noticing that in system SYS all the instances of ambients named mol and e exhibit the same behaviour, and therefore they can be easily described by the same configuration. Of course, this is not always the case. Therefore it may be convenient to use different labels and configurations for describing occurrences of ambients with the same name but with a different behaviour. As an example, we consider the following system,

$$\begin{aligned} SYS_1 ::= {} & [M]^{(mol,\Psi_1)} \mid \ldots \mid [M]^{(mol,\Psi_{h-1})} \mid [E]^{(e,\Delta_1)} \mid \ldots \mid [E]^{(e,\Delta_{k-1})} \mid \\ & [\overline{\mathtt{out}}\, n.\, E \mid [\overline{\mathtt{out}}\, n.\, P]^{(mol,\Psi_h)}]^{(e,\Delta_k)} \end{aligned}$$

System SYS_1 is a derivative of SYS and describes the situation where: an ambient named mol (with run-time label Ψ_h) has moved inside an ambient named e (with run-time label Δ_k); the remaining instances of ambients named mol and e are still ready to interact. The following abstract states (depicted also in Fig. 2) define safe approximations of system SYS_1,

$$\begin{aligned}
&S_{2,1}^\circ = \{(\top, C_{0,3}^\circ)\} \textstyle\bigcup_{i\in\{1,\ldots,h-1\}} \{(D_i^\circ, C_{1,1}^\circ)\} \bigcup_{i\in\{1,\ldots,k-1\}} \{(F_i^\circ, C_{2,1}^\circ)\} \cup \{(D_h^\circ, C_{1,2}^\circ), (F_k^\circ, C_{2,2}^\circ)\} \\
&C_{0,3}^\circ = \{(D_1^\circ, 1), \ldots, (D_{h-1}^\circ, 1), (F_1^\circ, 1), \ldots, (F_k^\circ, 1)\} \\
&C_{1,2}^\circ = \{(\mathtt{out}\, m^\circ.\, P^\circ, 1)\} \qquad C_{2,2}^\circ = \{(\overline{\mathtt{out}}\, m^\circ.\, E^\circ, 1), (D_h^\circ, 1)\}
\end{aligned}$$

$$\begin{aligned}
&S_{2,2}^\circ = \{(\top, C_{0,4}^\circ), (A_1^\circ, C_{1,1}^\circ), (B_1^\circ, C_{2,1}^\circ), (A_2^\circ, C_{1,2}^\circ), (B_2^\circ, C_{2,3}^\circ)\} \\
&C_{0,4}^\circ = \{(A_1^\circ, [1-\omega]), (B_1^\circ, [1-\omega]), (B_2^\circ, 1)\} \qquad C_{2,3}^\circ = \{(\overline{\mathtt{out}}\, m^\circ.\, E^\circ, 1), (A_2^\circ, 1)\}
\end{aligned}$$

$$\begin{aligned}
&S_{2,3}^\circ = \{(\top, C_{0,5}^\circ), (A_3^\circ, C_{1,1}^\circ), (A_3^\circ, C_{1,2}^\circ), (B_3^\circ, C_{2,1}^\circ), (B_3^\circ, C_{2,4}^\circ)\} \\
&C_{0,5}^\circ = \{(A_3^\circ, [1-\omega]), (B_3^\circ, [1-\omega])\} \qquad C_{2,4}^\circ = \{(\overline{\mathtt{out}}\, m^\circ.\, E^\circ, 1), (A_3^\circ, 1)\}
\end{aligned}$$

$$\begin{aligned}
&S_{2,4}^\circ = \{(\top, C_{0,5}^\circ), (A_3^\circ, C_1^\circ), (B_3^\circ, C_2^\circ)\} \\
&C_1^\circ = \{(\mathtt{out}\, m^\circ.\, P^\circ, [0-\omega]), (M^\circ, [0-\omega])\} \\
&C_2^\circ = \{(\overline{\mathtt{out}}\, m^\circ.\, E^\circ, [0-\omega]), (A_3^\circ, [0-\omega]), (E^\circ, [0-\omega])\}
\end{aligned}$$

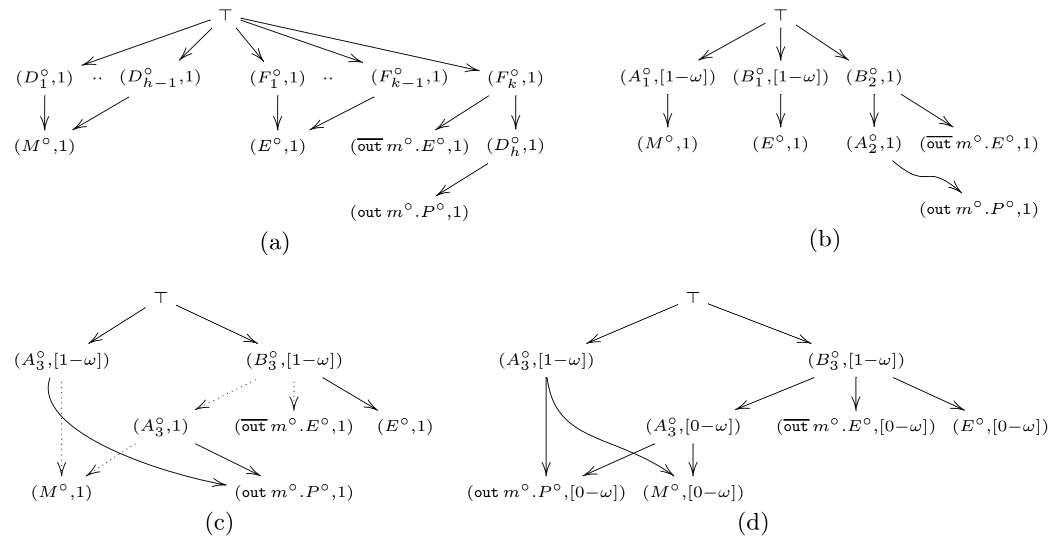


Figure2. The abstractions of SYS_1 graphically

State $S^\circ_{2,1}$ (depicted in Figure 2(a)) is the best approximation of SYS_1, and is obtained similarly as for state $S^\circ_{1,1}$ for SYS (given that there is no approximation of labels).

By constrast, in state $S^\circ_{2,2}$ (depicted in Figure 2(b)) the labels are approximated by using a simple partitioning criteria: the occurrences of ambients with the same name, described by the same configuration, are identified. In this way, the labels $D^\circ_1, \ldots, D^\circ_{h-1}$, for name *mol*, are represented by label A°_1, while label D°_h is represented by A°_2; analogously, the labels $F^\circ_1, \ldots, F^\circ_{k-1}$, for name e, are represented by label B°_1, and label F°_k is represented by B°_2. The configurations are updated accordingly by modifying the multiplicities. As a consequence, label A°_2 identifies the occurrence of *mol*, residing inside the enzyme, while label A°_1 describes the others running at top-level.

A further approximation is introduced in state $S^\circ_{2,3}$ (depicted in Figure 2(c)), where all occurrences of ambients (named) *mol* and e are identified by means of abstract labels A°_3 and B°_3, respectively. Note that label A°_3 reports two possible configurations $C^\circ_{1,1}$ and $C^\circ_{1,2}$ for ambients named *mol*. The interpretation is that the contents of each ambient *mol* may be described *either* by $C^\circ_{1,1}$ *or* by $C^\circ_{1,2}$ (as indicated by the dotted line in Figure 2(c)). This is clearly a loss of information with respect to state $S^\circ_{2,2}$, in that all occurrences of ambients *mol*, in particular those residing at top-level and the one residing inside an ambient e, are identified. Similar consideration holds also for the configurations of ambients named e.

Finally, state $S^\circ_{2,4}$ (depicted in Figure 2(d)) is an approximation of $S^\circ_{2,3}$, obtained by merging the information about distinct configurations of a given label into a single one, e.g. configuration C°_1 for ambients *mol* and C°_2 for ambients e. This information is rather approximate; for example, configuration C°_1 describes all the ambients *mol* appearing in the system, and says that inside any ambient *mol*, zero or more processes $\mathtt{out}\, m^\circ.\, P^\circ$ and M° may appear in parallel. The difference with respect to state $S^\circ_{2,3}$ is obviously relevant; for example, it is not possible to argue that, each ambient *mol*, may contain *either* process $\mathtt{out}\, m^\circ.\, P^\circ$ *or* process M° but not both at the same time. □

Formally, we use $\widehat{\mathcal{PL}} = \mathcal{L}_a{}^\circ \cup \mathcal{AP}^\circ$ to denote the set of abstract ambients labels and abstract active processes; also, we use e to denote a generic element of $\widehat{\mathcal{PL}}$. Moreover, we use $(e, \mathtt{m})$ to denote a generic element of $\mathcal{E} = (\mathcal{L}_a{}^\circ \times \mathcal{M}) \cup (\mathcal{AP}^\circ \times \mathcal{M})$.

Definition 4 (Configurations and Abstract States). *A* configuration C *is a subset of* $\mathcal{E}$ *such that: (i) if* $(e, \mathtt{m}), (e, \mathtt{m}') \in C^\circ$*, then* $\mathtt{m} = \mathtt{m}'$*; and (ii) for each* $(e, \mathtt{m}) \in C^\circ$*,* $\mathtt{m} \neq 0$*.*

An abstract state S° *is a set of pairs* (A°, C°)*, where* C° *is a configuration and* $A^\circ \in \mathcal{L}_a{}^\circ$ *is an ambient label.*

Notice that in configurations, no pair $(e, 0)$ can appear, recording explicitly that there are no occurrences of element e. However, in the following with an abuse of notation we may write $(e, 0) \in C^\circ$ in place of $(e, \mathtt{m}) \notin C^\circ$ for any $\mathtt{m} \in \mathcal{M}$. This notation simplifies the definition of some related operators. In the following, we use $\mathcal{S}^\circ$ for the set of abstract states and $\mathcal{C}^\circ$ for the set of configurations. Given $S \in \mathcal{S}^\circ$, we also use $\mathtt{amb}(S^\circ) = \{A^\circ \mid (A^\circ, C^\circ) \in S^\circ\}$ and $\mathtt{amb}(S^\circ, a^\circ) = \{A^\circ \mid (A^\circ, C^\circ) \in S^\circ, (A^\circ)_1 = a^\circ\}$ for denoting the ambients labels described by a configuration.

We then introduce the information orders on abstract states, formalising precision of approximations. To this aim, we assume that the domain $\mathcal{M}$ of multiplicity comes equipped with the obvious (information) order $\leq_m$ and with the set of operations $+^\circ$ and $-^\circ$, reported in Table 2. Moreover, given two configurations we say that $C_1^\circ \leq^c C_2^\circ$ iff, for each $(e, \mathtt{m}) \in C_1^\circ$ there exists $(e, \mathtt{m}') \in C_2^\circ$ such that $\mathtt{m} \leq_m \mathtt{m}'$.

The ordering over states is rather complex in that we have to take into account the possible approximation of run-time labels (along the lines of the ideas discussed in Example 1). To this aim, we exploit *approximation functions* $\sigma : \mathcal{L}_a{}^\circ \to \mathcal{L}_a{}^\circ$, such that for any $A^\circ \in \mathit{dom}(\sigma)$, $(A^\circ)_1 = (\sigma(A^\circ))_1$; and we define the application of an approximation function to a configuration. Moreover, we introduce an operator $\cup^+$ between configurations that realises their union by adding the multiplicity in the obvious way. Given $C^\circ, C_1^\circ, C_2^\circ \in \wp(\mathcal{E})$,

$$C_1^\circ \cup^+ C_2^\circ = \{(e, \mathtt{m}) \mid (e, \mathtt{m}_i) \in C_i^\circ,\ \text{for each } i \in \{1, 2\},\ \mathtt{m} = \mathtt{m}_1 +^\circ \mathtt{m}_2\}$$

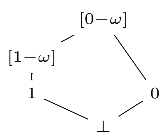
$$C^\circ \sigma = \bigcup{}^+{}_{\{(e,\mathtt{m}) \in C^\circ\}} \{(e\sigma, \mathtt{m})\}$$

Definition 5 (Order on States and Sets of States). *Let* $S_1^\circ, S_2^\circ \in \mathcal{S}^\circ$*,* $Ss_1^\circ, Ss_2^\circ \subseteq \mathcal{S}^\circ$*, and let* σ *be an approximation function, such that* $\mathtt{amb}(S_1^\circ) \subseteq \mathit{dom}(\sigma)$*.*

1. *We say that* $S_1^\circ \sqsubset_\sigma S_2^\circ$ *iff, for each* $(A^\circ, C_1^\circ) \in S_1^\circ$*, there exists* $(\sigma(A^\circ), C_2^\circ) \in S_2^\circ$ *such that* $C_1^\circ \sigma \leq^c C_2^\circ$*.*
2. *We say that* $S_1^\circ \subseteq^\circ S_2^\circ$ *iff there exists* σ *such that* $S_1^\circ \sqsubset_\sigma S_2^\circ$*.*
3. *We say that* $Ss_1^\circ \subseteq^\circ Ss_2^\circ$ *iff, for each* $S_1^\circ \in Ss_1^\circ$*, there exists* $S_2^\circ \in Ss_2^\circ$ *such that* $S_1^\circ \subseteq^\circ S_2^\circ$*;*

Note that the relations of Def. 5 are actually pre-orders. We tacitly assume the corresponding orders obtained by considering the classes modulo the equivalence induced by pre-orders. With an abuse of notation, we use $\mathcal{S}^\circ$ and $\wp(\mathcal{S}^\circ)$ for the corresponding quotient sets. It is important to observe that $\subseteq^\circ$ (in both cases) admits l.u.b. which is indeed the union.

Abstract Transitions. We define abstract transitions and a corresponding ordering. According to the intuition explained above, the run-time labels of ambients can vary, as the



$+^\circ$	0	1	$[1-\omega]$	$[0-\omega]$
0	0	1	$[1-\omega]$	$[0-\omega]$
1	1	$[1-\omega]$	$[1-\omega]$	$[1-\omega]$
$[1-\omega]$	$[1-\omega]$	$[1-\omega]$	$[1-\omega]$	$[1-\omega]$
$[0-\omega]$	$[0-\omega]$	$[1-\omega]$	$[1-\omega]$	$[0-\omega]$

$-^\circ$	1
0	0
1	0
$[1-\omega]$	$[0-\omega]$
$[0-\omega]$	$[0-\omega]$

Table2. Occurrence Counting.

compution proceeds (in the analysis of paragraph 3.2 a specific labelling discipline is applied for these purposes). For tracking the possible evolution of the run-time labels, we need to expand the information reported by standard transitions.

Specifically, we exploit relations $\mathcal{R}^\circ \subseteq (\mathcal{L}_a{}^\circ \cup \{\perp\}) \times (\mathcal{L}_a{}^\circ \cup \{\perp\})$, such that for each $A^\circ \in \mathcal{L}_a^\circ$, if $(A^\circ, B^\circ) \in \mathcal{R}^\circ$, $(A^\circ)_1 = (B^\circ)_1$. Intuitively, $(A^\circ, B^\circ) \in \mathcal{R}^\circ$ says that label A° is replacedby B°; $(A^\circ, \perp) \in \mathcal{R}^\circ$ says that the ambient labelled A° disappears; $(\perp, A^\circ) \in \mathcal{R}^\circ$ says that A° is the label of a new enabled ambient.

Therefore, we consider abstract transitions $\mathcal{T}^\circ = \{S_1^\circ \mapsto^\circ_{\mathcal{R}^\circ} S_2^\circ \mid S_1^\circ, S_2^\circ \in \mathcal{S}^\circ$ and $dom(\mathcal{R}^\circ) = \mathtt{amb}(S_1^\circ)$ and $cod(\mathcal{R}^\circ) = \mathtt{amb}(S_2^\circ)\}$.

In the ordering we guarantee by means of approximation functions that: (i) the source and target state of a transition are approximated; and also that (ii) the approximation over states is consistent with the information reported by the corresponding relations.

Definition 6 (Order on Transitions). *Let $S_{1,1}^\circ \mapsto^\circ_{\mathcal{R}_1{}^\circ} S_{1,2}^\circ, S_{2,1}^\circ \mapsto^\circ_{\mathcal{R}_2{}^\circ} S_{2,2}^\circ \in \mathcal{T}^\circ$ be two transitions. Moreover, let σ_1, σ_2 be approximation functions, such that $\mathtt{amb}(S_{1,1}^\circ) \subseteq dom(\sigma_1)$ and $\mathtt{amb}(S_{1,2}^\circ) \subseteq dom(\sigma_2)$. We say that $S_{1,1}^\circ \mapsto^\circ_{\mathcal{R}_1{}^\circ} S_{1,2}^\circ \sqsubset_{(\sigma_1,\sigma_2)} S_{2,1}^\circ \mapsto^\circ_{\mathcal{R}_2{}^\circ} S_{2,2}^\circ$ iff*

1. *$S_{1,1}^\circ \sqsubset_{\sigma_1} S_{2,1}^\circ$ and $S_{1,2}^\circ \sqsubset_{\sigma_2} S_{2,2}^\circ$;*
2. *for each $A^\circ \in \mathtt{amb}(S_{1,1}^\circ)$: (i) if $\mathcal{R}_1{}^\circ(A^\circ) = \perp$, then $\mathcal{R}_2{}^\circ(\sigma_1(A^\circ)) = \perp$; or (ii) $\sigma_2(\mathcal{R}_1{}^\circ(A^\circ)) \subseteq \mathcal{R}_2{}^\circ(\sigma_1(A^\circ))$;*
3. *$\sigma_2(\mathcal{R}_1{}^\circ(\perp)) \subseteq \mathcal{R}_2{}^\circ(\perp)$.*

Abstract Transition Systems. Based on Def. 5 and 6 it is immediate to derive a suitable ordering over abstract transition systems. Let $Ts^\circ = \{(Ss^\circ, S_0^\circ, Ts^\circ) \mid Ss^\circ \in \wp(\mathcal{S}^\circ)$, $S_0^\circ \in \mathcal{S}^\circ$ and $Ts^\circ \in \wp(\mathcal{T}^\circ)\}\}$

Definition 7 (Order on Transition Systems). *Let $(Ss_1^\circ, S_{1,0}^\circ, Ts_1^\circ), (Ss_2^\circ, S_{2,0}^\circ, Ts_2^\circ) \in Ts^\circ$, and let $S_1^\circ \in Ss_1^\circ, S_2^\circ \in Ss_2^\circ$. We say that S_1°* approximates *S_2°* w.r.t an approximation function *σ_1 iff*

1. *$S_1^\circ \sqsubset_{\sigma_1} S_2^\circ$;*
2. *for each $S_1^\circ \mapsto^\circ_{\mathcal{R}_1{}^\circ} S_1^{\circ\prime} \in Ts_1^\circ$ there exists $S_2^\circ \mapsto^\circ_{\mathcal{R}_2{}^\circ} S_2^{\circ\prime} \in Ts_2^\circ$ and σ_2 such that: (i) $S_1^\circ \mapsto^\circ_{\mathcal{R}_1{}^\circ} S_1^{\circ\prime} \sqsubset_{(\sigma_1,\sigma_2)} S_2^\circ \mapsto^\circ_{\mathcal{R}_2{}^\circ} S_2^{\circ\prime}$; and (ii) $S_1^{\circ\prime}$* approximates *$S_2^{\circ\prime}$* w.r.t. *σ_2.*

Moreover, we say that $(Ss_1^\circ, S_{1,0}^\circ, Ts_1^\circ) \subseteq^\circ (Ss_2^\circ, S_{2,0}^\circ, Ts_2^\circ)$ iff there exists σ, such that $S_{1,0}^\circ$ approximates $S_{2,0}^\circ$ w.r.t σ

Also the relation of Def. 7 is a pre-order. As before, we tacitly assume the corresponding order obtained by considering the classes modulo the equivalence induced by the pre-order. With an abuse of notation, we use Ts° for the corresponding quotient sets.

The abstract domain is defined analogously to the concrete one (see Def. 2) by considering abstract transition systems.

Definition 8 (Abstract Domain). *The* abstract domain *is $\mathcal{A}^\circ = (Ts^\circ, \subseteq^\circ)$, where $\subseteq^\circ$ is the ordering of Def 7.*

Galois Connection. The relation between the concrete and the abstract domain is formalized by establishing a Galois connection, between concrete and abstract transition systems. This formalises the notion of *safe approximation* that guarantees the preservation of the properties of Section 5.

DRes$^\circ$	$\eta^\circ((\nu n^\circ)P^\circ)$	$= \eta^\circ(P^\circ)$
DAmb$^\circ$	$\eta^\circ([P^\circ]^{A^\circ})$	$= (\{(A^\circ, 1)\}, \delta^\circ(A^\circ, P^\circ))$
DZero$^\circ$	$\eta^\circ(0)$	$= (\emptyset,\ \emptyset)$
DPar$^\circ$	$\eta^\circ(P_1 \mid P_2)$	$= (C_1{}^\circ \cup^+ C_2{}^\circ, S_1{}^\circ \cup^\circ S_2{}^\circ)\ \ \eta^\circ(P_i) = (C_i^\circ, S_i^\circ)$ for $i \in \{1, 2\}$
DRec$^\circ$	$\eta^\circ(\mathtt{rec}X.\, P^\circ)$	$= (\{(\mathtt{rec}X.\, P^\circ, 1)\}, \emptyset)$
DPref$^\circ$	$\eta^\circ(M.\, P^\circ)$	$= (\{(M.\, P^\circ, 1)\}, \emptyset)$
DSum$^\circ$	$\eta^\circ(\Sigma_{i\in I} M_i^\circ.\, P_i^\circ)$	$= (\{(\Sigma_{i\in I} M_i^\circ.\, P_i^\circ, 1)\}, \emptyset)$

Table3. Abstract Translation Function.

To this aim, we first introduce a function that, given a process and the label of the enclosing ambient, reports its *best approximation*; this is the most precise abstract state which has enough information about the process. Formally, we define the *translation function* $\delta^\circ : (\mathcal{L}_a{}^\circ \times \mathcal{P}^\circ) \to \mathcal{S}^\circ$ as follows

$$\delta^\circ(A^\circ, P^\circ) = \{(A^\circ, C^\circ)\} \cup S^\circ \quad \text{where} \quad \eta^\circ(P^\circ) = (C^\circ, S^\circ).$$

An auxiliary function function $\eta^\circ : \mathcal{P}^\circ \to (\mathcal{C}^\circ \times \mathcal{S}^\circ)$, reported in Table 3, is exploited; it computes: (i) an abstract configuration reporting both the active processes and the labels of the ambients, occurring at top-level, and their multiplicities; (ii) an abstract state (e.g. a set of configurations) representing the internal ambients. We then use $\alpha^\circ(P)$ for denoting the best approximation of process P with respect to the enclosing ambient $\top$, e.g. $\alpha^\circ(P) = \delta^\circ(\top, P^\circ)$.

Moreover, we introduce the *best approximation* of a concrete transition, e.g. $P \to P'$. For this, we introduce a corresponding relation $\mathcal{R}^\circ$, expressing how the labels of the enabled ambients (specifically their run-time labels) vary. Given $P \to P' \in \mathcal{T}$, we define[4] $\alpha^\circ(P \to P') = \alpha^\circ(P) {\mapsto}^\circ_{\mathcal{R}^\circ} \alpha^\circ(P')$ where

$$\mathcal{R} = \mathtt{id}(\mathtt{amb}(P) \cap \mathtt{amb}(P')) \cup (\{\bot\}, \mathtt{amb}(P') \setminus \mathtt{amb}(P)) \cup (\mathtt{amb}(P) \setminus \mathtt{amb}(P'), \{\bot\}),$$

using $(L, L') = \{(A, B) \mid A \in L,\ B \in L'\}$ and $\mathtt{id}(L) = (L, L)$, for $L, L' \subseteq \mathcal{L}_a$.

Notice that relation $\mathcal{R}$ is derived in a simple way, by reflecting the labelling discipline of the reduction semantics. Specifically, no pair (A, B) with $A \neq B$ could actually appear in $\mathcal{R}$; indeed, all the ambients maintain their labels, as the computation proceeds; fresh labels are introduced only for the new ambients, introduced by the unfolding of recursion.

From this it is immediate to derive the following abstraction and concretization functions between the concrete and abstract domain.

Definition 9. *Let $Ss, Ss_0 \in \wp(\mathcal{P})$, $Ss^\circ \in \wp(\mathcal{S}^\circ)$, $S_0^\circ \in \mathcal{S}$, $Ts \in \wp(\mathcal{T})$ and $Ts^\circ \in \wp(\mathcal{T}^\circ)$. We define $\alpha^\circ : \mathcal{A} \to \mathcal{A}^\circ$ and $\gamma^\circ : \mathcal{A}^\circ \to \mathcal{A}$, where*
$\alpha^\circ((Ss, Ss_0, Ts)) = (\bigcup_{P\in Ss}\{\alpha^\circ(P)\}, \cup_{P\in Ss_0} \alpha^\circ(P), \bigcup_{P_1\to P_2\in Ts}\{\alpha^\circ(P_1 \to P_2)\}$;
$\gamma^\circ((Ss^\circ, S_0^\circ, Ts^\circ)) = (\bigcup_{\{P \mid \{\alpha^\circ(P)\}\subseteq^\circ Ss^\circ\}}\{P\}, \bigcup_{\{P \mid \{\alpha^\circ(P)\}\subseteq^\circ S_0^\circ\}}\{P\},$
$\bigcup_{\{P_1\to P_2 \mid \{\alpha^\circ(P_1\to P_2)\}\subseteq^\circ Ts^\circ\}}\{P_1 \to P_2\})$.

Theorem 1. *The pair $(\alpha^\circ, \gamma^\circ)$ is a* Galois connection *between $\langle \mathcal{A}, \subseteq\rangle$ and $\langle \mathcal{A}^\circ, \subseteq^\circ\rangle$.*

[4] As usual the relation $\mathcal{R}^\circ$ is obtained from $\mathcal{R}$ by replacing the ambient labels by their abstract versions.

3.2 Abstract semantics

The analysis is defined by introducing *abstract transitions* which approximate the unfolding of recursion, the movements of ambients, in and out, and the merge of two ambients (e.g. rules (Rec), (In), (Out) and (Merge) of Table 1). Due to the implicit representation of parallel composition, ambient and restriction in abstract states there are no abstract transitions corresponding to the structural rules and to structural congruence of the reduction semantics, similarly as in [21,16].

The most critical part (w.r.t [16]) concerns the treatment of ambients labels. Our approach is based on the following ideas: (i) we use, for each ambient name a°, at most max_{a° distinct run-time labels (and then we approximate by means of the special label ∞); (ii) at the same time, we introduce a suitable labelling of the instances, related to name a°. Specifically, we apply a labelling discipline, where: ambients that exhibit the same behaviour (e.g. which are described by the same configuration) are identified by means of the same abstract label; analogously, ambients that exhibit different behaviours are distinguished by means of distinct abstract label (provided that the global number of run-time labels for a° is less than max_{a°). This approach guarantees an accurate treatment of ambients with the same name, and at the same time guarantees a bound on the possible size of a state.

In order to formalise these ideas, we consider *normalised states*, which guarantees the intended shape; then we implement the labelling discipline by defining abstract transitions $S_1^\circ \mapsto^\circ_{\mathcal{R}^\circ} S_2^\circ$, where S_1° and S_2° are normalised states.

Definition 10 (Normalised States). *A state $S^\circ \in \mathcal{S}^\circ$ is* normalised *iff, for each $a^\circ \in \mathcal{N}_a^\circ$, and $A, B \in \mathtt{amb}(S^\circ, a^\circ)$,*

1. *if $(A^\circ, C_1^\circ), (B^\circ, C_1^\circ) \in S^\circ$, then $A^\circ = B^\circ$;*
2. *if $(A^\circ, C_1^\circ), (B^\circ, C_2^\circ) \in S^\circ$ and $C_1^\circ \neq C_2^\circ$, then either $(B^\circ)_2 \neq (A^\circ)_2$ or $(B^\circ)_2 = (A^\circ)_2 = \infty$;*
3. *either $\mathtt{amb}(S^\circ, a^\circ) = \{(a^\circ, \infty)\}$ or $\mathtt{amb}(S^\circ, a^\circ) = \{(a^\circ, \Phi_1), \ldots, (a^\circ, \Phi_n)\}$, where $n \leq max_{a^\circ}$.*

Conditions (1) and (2) imposes, for each ambient name a°, a one-to-one correspondence between configurations and run-time labels (except from ∞ which can describe several configurations). Condition (3) explains the meaning of parameter max_{a°. In this way, in a normalised state, for each ambient name a°: *either* at most n (with $n \leq max_{a^\circ}$) distinct run-time labels Φ_i appear, each related to a different configuration; *or* only the special label ∞ appears, related to a set of configurations.

We also introduce a related notion of normalisation, by means of approximation functions (the normalisation of a state is indeed a safe approximation).

Definition 11 (Normalisation). *Let $S^\circ \in \mathcal{S}^\circ$ be a state. We say that an approximation function σ, such that $\mathtt{amb}(S^\circ) = dom(\sigma)$, is a* normalisation *for S° whenever $S^\circ\sigma$[5] is a normalised state.*

Moreover, we say that σ is a minimal normalisation *for S°, whenever for each normalisation σ' for S°, $S^\circ\sigma \subseteq^\circ S^\circ\sigma'$. We also use $\mathcal{M}(S^\circ)$ to denote the set of minimal normalisations for S° (they are equals up to re-labelling).*

Example 2. We consider the systems discussed in Example 1 and we assume that $max_{mol} = 6$, $max_e = 2$ and $max_\top = 0$. States $S_{1,1}^\circ$ and $S_{2,1}^\circ$ (depicted also in Fig. 1(a) and Fig. 2(a)) are the best approximations of systems SYS and SYS_1. Their normalisation is defined

[5] With an abuse of notation $S^\circ\sigma = \{((\sigma(A^\circ), C^\circ\sigma) \mid (A^\circ, C^\circ) \in S^\circ\}$.

by the states $S^\circ_{1,2}$ and $S^\circ_{2,2}$ (depicted also in Fig. 1(b) and Fig. 2(b)). They are obtained exactly by identifying labels describing the same confgurations. If for example we modify the parameters by taking $max_e = 1$, then by normalising $S^\circ_{2,1}$ we obtain

$$\begin{array}{l} {S^\circ_{2,2}}' = \{(\top, {C^\circ_{0,4}}'), (A^\circ_1, C^\circ_{1,1}), (B^\circ_\infty, C^\circ_{2,1}), (A^\circ_2, C^\circ_{1,2}), (B^\circ_\infty, C^\circ_{2,3})\} \\ {C^\circ_{0,4}}' = \{(A^\circ_1, [1-\omega]), (B^\circ_\infty, [1-\omega])\} \end{array}$$

In this case, indeed, the number of labels for name e exceeded the parameter max_e, and therefore both labels B°_1 and B°_2 have to be approximated by $B^\circ_\infty = (e, \infty)$.

It can be proved that each state can be normalised. In particular, given a state S° a normalisation σ for S° has to satisfy the following requirements, for each $a^\circ \in \mathcal{N}^\circ_a$, and $A, B \in \mathtt{amb}(S^\circ, a^\circ)$,

1. $cod(\sigma)$ either contains (a°, ∞) or at most max_{a° distinct labels (a°, Ψ);
2. if $(A)_2 = \infty$, then $(\sigma(A))_2 = \infty$
3. if $(A^\circ, C^\circ_1), (B^\circ, C^\circ_2) \in S^\circ$, $(A^\circ)_2 \neq \infty$ and $(B^\circ)_2 \neq \infty$
   (a) if $C^\circ_1\sigma = C^\circ_2\sigma$, then $\sigma(A^\circ) = \sigma(B^\circ)$;
   (b) if $C^\circ_1\sigma \neq C^\circ_2\sigma$, then either $\sigma(A^\circ) \neq \sigma(B^\circ)$ or $\sigma(A^\circ) = \sigma(B^\circ)$ with $(\sigma(A^\circ))_2 = \infty$.

The transition rules are reported in Table 4 and are explained below; they use some auxiliary notions for updating the states. The following operators remove from a configuration one occurrence of an object e and, similarly, for a set of objects. Let $PL^\circ \subseteq \widehat{\mathcal{PL}}$,

$$C^\circ \setminus^\circ e = C^\circ \setminus \{(e, \mathtt{m})\} \cup \{(e, \mathtt{m} -^\circ 1)\} \qquad C^\circ \setminus^\circ PL^\circ = C^\circ \setminus^\circ_{e \in PL^\circ} e.$$

Moreover, we introduce operators over states for removing a pair (A°, C°) and for replacing in each configuration where it appears, an occurrence of label A° with an occurrence of A°_1, an abstract label with the same name. To this aim, we use $\mathcal{O}_{S^\circ}(e)$ reporting the (global) number of occurrences of object e in the abstract state S°[6],

$$S^\circ \setminus^\circ (A^\circ, C^\circ) = \begin{cases} S^\circ \text{ if } \quad \mathcal{O}_{S^\circ}(A^\circ) \in \{0, [0-\omega], [1-\omega]\} \\ \\ S^\circ \setminus \{(A^\circ, C^\circ)\} \text{ otherwise} \end{cases}$$

$$S^\circ[{}^{A^\circ_1}/_{A^\circ}] = \bigcup_{(D^\circ, C^\circ) \in S^\circ} (D^\circ, C^\circ_1), \text{ where } C^\circ_1 = \begin{cases} (C^\circ \setminus^\circ A^\circ) \cup^+ (A^\circ_1, 1) \text{ if } (A^\circ, m) \in C^\circ \\ C^\circ \qquad\qquad\qquad\qquad \text{otherwise} \end{cases}$$

Notice that the removal depends on the multiplicity of ambients labelled A°, meaning that the pair (A°, C°) is effectively removed only when the global number of occurrences of ambients labelled A° is exactly one.

Moreover, for handling labels we use $\mathtt{new}(A^\circ)$ to generate a fresh label with the same name, e.g. we require that $(\mathtt{new}(A^\circ))_1 = (A^\circ)_1$.

Rule **Rec**$^\circ$ realizes the unfolding of a recursive process $T^\circ = \mathtt{rec}X.\, P^\circ$, local to an ambient labelled A° (this is shown by a configuration C° which contains process T°). The abstract state S° is updated modelling the evolution of one ambient labelled A°, which moves from configuration C° to a new configuration, where the recursive process has been unfolded.

To this aim, we generate a fresh label (e.g. $\mathtt{new}(A^\circ)$) for representing the involved ambient and a new configuration C°_1 for describing its possible contents. Specifically, C°_1 is obtained from configuration C° by adding the translation of the unfolded process and by removing the recursive process T° (according to their multiplicities). Formally, we have $C^\circ_1 = (C^\circ \setminus^\circ T^\circ) \cup^+ C^\circ_2$ where $\eta^\circ(P^\circ[T^\circ/X]) = (C^\circ_2, S^\circ_2)$.

[6] For convenience we also write ${S_1}^\circ \setminus^\circ {S_2}^\circ$ to denote the obvious extension of $\setminus^\circ$ to states.

Then, we consider state $S_1^\circ \cup S_2^\circ$, where S_2° represents the configurations for the new ambients introduced by the unfolding, and S_1° is obtained from state S° precisely by replacing (A°, C°) with $(\mathtt{new}(A^\circ), C_1^\circ)$. The replacement depends on the global number of ambients labelled A°, and is defined by $S_1^\circ = ((S^\circ \setminus^\circ \{(A^\circ, C^\circ)\}) \cup \{(\mathtt{new}(A^\circ), C_1^\circ)\})[{}^{\mathtt{new}(A^\circ)}/{}_{A^\circ}]$. Notice that the replacement of one occurrence of A° with $\mathtt{new}(A^\circ)$ has to be properly propagated into the ambients hierarchy (e.g. in the configurations of the fathers of ambients labelled A°). Finally, state $S_1^\circ \cup S_2^\circ$ is normalised (by means of a a normalisation function σ) in order to guarantee that the labels of S_1° and S_2° are properly merged according to the labelling discipline. Relation R° tracks the variation of labels, in particular of run-time labels, and is defined in a standard way. It records: (i) the evolution of one ambient labelled A° into $\mathtt{new}(A^\circ)$; (ii) that all the other ambients appearing in S° remain unchanged; (iii) that the translation of the recursive process may add new ambients labels (those of S_2°). Notice, however, that the effect of the normalisation function has to be properly propagated also to relation R°. For example, we take $(A^\circ, \sigma(\mathtt{new}(A^\circ)))$, because the fresh label could have been collapsed into another one; analogously, we take $(B^\circ, \sigma(B^\circ))$ for all ambients label B° that are not involved in the move.

The rules $\mathbf{In}^\circ$, $\mathbf{Out}^\circ$, $\mathbf{Merge}^\circ$ are similar; as an example we comment $\mathbf{In}^\circ$. The rule models the movement of an ambient labelled ${A_1}^\circ$ inside an ambient labelled ${A_2}^\circ$, and is applicable whenever they are possible siblings. This means that they may be enclosed, at the same time, inside an ambient (labelled ${A_3}^\circ$) and that they offer the right action or coaction. Formally, it must be the case that: (i) there exists a configuration C_3° for ${A_3}^\circ$ which contains *both* ${A_1}^\circ$ and ${A_2}^\circ$; (ii) there exist configurations ${C_1}^\circ$ and ${C_2}^\circ$ for ${A_1}^\circ$ and ${A_2}^\circ$, where capabilities $\mathtt{in}\, M^\circ$ and $\overline{\mathtt{in}}\, M^\circ$ are ready to fire, respectively. If ${A_1}^\circ$ and ${A_2}^\circ$ coincide, then the movement is possible only if their multiplicities are greater than 1.

The approach is similar to that explained for rule $\mathbf{Rec}^\circ$: (1) we generate fresh labels for describing the instance of ambients labelled A_1°, A_2° A_3° involved in the movement (e.g. $\mathtt{new}(A_i^\circ)$ for $i \in \{1, 2, 3\}$); (2) we design new configurations representing the variation of their contents, due to movement. In particular,

1. $C_{1,1}^\circ$ describes the local process of ambient $\mathtt{new}(A_1^\circ)$; it is obtained from configuration C_1°, by adding the translation of the continuation (process P°) and by removing the executed process $+\mathtt{in}\, m^\circ.\, P^\circ$ (according to their multiplicities);
2. $C_{2,1}^\circ$ describes the local process of ambient $\mathtt{new}(A_2^\circ)$; it is obtained from configuration C_2° similarly as in case 1.. The only difference is that one occurrence of ambient $\mathtt{new}(A_1^\circ)$ is added, for modelling the movement;
3. $C_{3,1}^\circ$ describes the new local process of ambient $\mathtt{new}(A_3^\circ)$; it is defined by $C_{3,1}^\circ = (C_3^\circ \setminus^\circ \{A_1^\circ, A_2^\circ\}) \cup^+ (\mathtt{new}(A_2^\circ), 1)$ taking into account that one instance of ambient A_1° has moved into another location, and that one instance of ambient A_2° has evolved into $\mathtt{new}(A_2^\circ)$.

Then, we consider state $S_1^\circ \cup S_{1,2}^\circ \cup S_{2,2}^\circ$ where $S_{1,2}^\circ \cup S_{2,2}^\circ$ represents the configurations for the new ambients introduced by the move, and S_1° is obtained from state S° precisely by replacing (A_i°, C_i°) with $(\mathtt{new}(A_i^\circ), C_{i,1}^\circ)$, for $i \in \{1, 2, 3\}$. Notice that the effect of the replacement has to be properly propagated into the ambients hierarchy (e.g. in the configurations of the fathers of ambients labelled A_3°). Similarly as in the previous case, the resulting state is normalised, by applying a normalization function σ. Relation $\mathcal{R}^\circ$ also is an immediate extension of that applied in case $\mathbf{Rec}^\circ$.

The abstract semantics is defined similarly to the collecting semantics (see Def. 3); it is the least fixed-point of a function that computes the abstract transition system starting from the normalised abstraction of the process.

Definition 12 (The Abstract Semantics). *Let P be a process such that $\top \notin \mathcal{N}_a(P)$. We define $\mathfrak{S}_{Coll^\circ}[\![P]\!] =$ lfp F_P° for the function $F_P^\circ : \mathcal{A}^\circ \to \mathcal{A}^\circ$, such that (for $\sigma \in \mathcal{M}(\alpha^\circ(P))$*

$$F_P^\circ(Ss^\circ, S_0^\circ, Ps^\circ) = (\{S_0^\circ\} \bigcup_{\{S_2^\circ | S_1^\circ \mapsto^\circ_{\mathcal{R}^\circ} S_2^\circ, S_1^\circ \in Ss^\circ\}} \{S_2^\circ\},\ \alpha^\circ(P)\sigma\ ,\ \bigcup_{\{S_1^\circ \in Ss^\circ\}} \{S_1^\circ \mapsto^\circ_{\mathcal{R}^\circ} S_2^\circ\}).$$

The following theorem shows that the abstract semantics is a safe approximation of the collecting semantics.

Theorem 2 (Safeness). *Let let P be a process such that $\top \notin \mathcal{N}_a(P)$. We have $\alpha^\circ(\mathfrak{S}_{Coll}[\![P]\!]) \subseteq^\circ \mathfrak{S}_{Coll^\circ}[\![P]\!]$.*

As a measure of complexity of our analysis we can consider the size of the abstract system. For this, we observe that the number of possible states that can be generated in the worst case, can be double exponential in the size of the abstract process.

Example 3. We consider the (well-labelled) system (5) described in the Introduction and presented in Example 1.

$$SYS ::= [M]^{(mol,\Psi_1)} \mid \ldots \mid [M]^{(mol,\Psi_h)} \mid [E]^{(e,\Delta_1)} \mid \ldots \mid [E]^{(e,\Delta_k)}$$
$$E ::= \mathtt{rec}Y.\, \overline{\mathtt{in}}\, m.\, \overline{\mathtt{out}}\, n.\, Y \quad M ::= \mathtt{in}\, m.\, \mathtt{out}\, n.\, P$$

We also assume that: (i) the abstract names and ambient names are defined by the following equivalence classes $\mathcal{N}^\circ = \{n, m\}$, and $\mathcal{N}_a^\circ = \mathcal{N}_a$; (ii) $max_{mol} = 6$, $max_e = 2$ and $max_\top = 0$. For simplicity, we consider the following notation for abstract labels: $\top$ stands for $(\top, \infty)$, $A_i^\circ = (mol, \Lambda_i)$ and $B_i^\circ = (e, \Phi_i)$ with $i \in \mathcal{N}$, and $B_\infty^\circ = (e, \infty)$. By applying the analysis[7] we obtain the abstract transition system of Fig. 3. We assume that each transition $S_i^\circ \mapsto S_j^\circ$ of Fig. 3 represents abstract transitions $S_i^\circ \mapsto^\circ_{\mathcal{R}_{i,j}} S_j^\circ$, where $\mathcal{R}_{i,j} = \mathcal{R}_{S_i^\circ, S_j^\circ} \cup \mathtt{id}(\mathtt{amb}(S_i^\circ))$ for each $\mathcal{R}_{S_i^\circ, S_j^\circ}$ listed below.

$S_1^\circ = \{(\top, C_{0,1}^\circ), (A_1^\circ, C_{1,1}^\circ), (B_1^\circ, C_{2,1}^\circ)\}$
$S_2^\circ = \{(\top, C_{0,2}^\circ), (A_1^\circ, C_{1,1}^\circ), (B_1^\circ, C_{2,1}^\circ), (B_2^\circ, C_{2,2}^\circ)\}$
$S_3^\circ = \{(\top, C_{0,3}^\circ), (A_1^\circ, C_{1,1}^\circ), (A_2^\circ, C_{1,2}^\circ), (B_\infty^\circ, C_{2,1}^\circ), (B_\infty^\circ, C_{2,2}^\circ), (B_\infty^\circ, C_{2,3}^\circ)\}$
$S_4^\circ = \{(\top, C_{0,4}^\circ), (A_1^\circ, C_{1,1}^\circ), (B_1^\circ, C_{2,1}^\circ), (B_2^\circ, C_{2,2}^\circ)\}$
$S_5^\circ = \{(\top, C_{0,5}^\circ), (A_1^\circ, C_{1,1}^\circ), (A_2^\circ, C_{1,2}^\circ), (A_3^\circ, C_{1,3}^\circ)(B_\infty^\circ, C_{2,1}^\circ), (B_\infty^\circ, C_{2,2}^\circ), (B_\infty^\circ, C_{2,3}^\circ)\}$
$S_6^\circ = \{(\top, C_{0,6}^\circ), (A_1^\circ, C_{1,1}^\circ), (A_2^\circ, C_{1,2}^\circ), (A_3^\circ, C_{1,3}^\circ)(B_\infty^\circ, C_{2,1}^\circ), (B_\infty^\circ, C_{2,2}^\circ), (B_\infty^\circ, C_{2,3}^\circ)\}$

$C_{0,1}^\circ = \{(A_1^\circ, [0-\omega]), (B_1^\circ, [0-\omega])\}$ $\quad C_{0,2}^\circ = \{(A_1^\circ, [0-\omega]), (B_1^\circ, [0-\omega]), (B_2^\circ, 1)\}$
$C_{0,3}^\circ = \{(A_1^\circ, [0-\omega]), (B_\infty^\circ, [0-\omega])\}$ $\quad C_{0,4}^\circ = \{(A_1^\circ, [0-\omega]), (B_1^\circ, [0-\omega]), (B_2^\circ, [0-\omega])\}$
$C_{0,5}^\circ = \{(A_1^\circ, [0-\omega]), (A_3^\circ, 1), (B_\infty^\circ, [0-\omega])\}$ $\quad C_{0,6}^\circ = \{(A_1^\circ, [0-\omega]), (A_3^\circ, [0-\omega]), (B_\infty^\circ, [0-\omega])\}$
$C_{1,1}^\circ = \{(M^\circ, 1)\}$ $\quad M^\circ ::= \mathtt{in}\, m^\circ.\, \mathtt{out}\, m^\circ.\, P^\circ$ $\quad C_{1,2}^\circ = \{(\mathtt{out}\, m^\circ.\, P^\circ, 1)\}$ $\quad C_{1,3}^\circ = \{(P^\circ, 1)\}$
$C_{2,1}^\circ = \{(E^\circ, 1)\}$ $\quad E^\circ ::= \mathtt{rec}Y.\, \overline{\mathtt{in}}\, m^\circ.\, \overline{\mathtt{out}}\, m^\circ.\, Y$ $\quad C_{2,2}^\circ = \{(E_1^\circ, 1)\}$ $\quad E_1^\circ = \overline{\mathtt{in}}\, m^\circ.\, \overline{\mathtt{out}}\, m^\circ.\, E^\circ$
$C_{2,3}^\circ = \{(E_2^\circ, 1), (A_2^\circ, 1)\}$ $\quad E_2^\circ = \overline{\mathtt{out}}\, m^\circ.\, E^\circ$

$\mathcal{R}_{S_1^\circ, S_2^\circ} = \mathcal{R}_{S_2^\circ, S_4^\circ} = \mathcal{R}_{S_4^\circ, S_4^\circ} = \{(B_1^\circ, B_2^\circ)\}$ $\quad \mathcal{R}_{S_2^\circ, S_3^\circ} = \mathcal{R}_{S_4^\circ, S_3^\circ} = \{(B_1^\circ, B_\infty^\circ), (B_2^\circ, B_\infty^\circ), (A_1^\circ, A_2^\circ)\}$
$\mathcal{R}_{S_3^\circ, S_5^\circ} = \mathcal{R}_{S_5^\circ, S_6^\circ} = \mathcal{R}_{S_6^\circ, S_6^\circ} = \{(A_2^\circ, A_3^\circ)\}$ $\quad \mathcal{R}_{S_3^\circ, S_3^\circ} = \mathcal{R}_{S_5^\circ, S_5^\circ} = \mathcal{R}_{S_6^\circ, S_6^\circ} = \{(A_1^\circ, A_2^\circ)\}$
$\mathcal{R}_{S_3^\circ, S_3^\circ} = \mathcal{R}_{S_5^\circ, S_5^\circ} = \mathcal{R}_{S_6^\circ, S_6^\circ} = \emptyset$

State S_1° is the normalisation of the translation of the initial process SYS (see Example 2). Transition $S_1^\circ \mapsto^\circ_{\mathcal{R}_{1,2}} S_2^\circ$ is obtained by rule $\mathbf{Rec}^\circ$, and models the unfolding of process E° local to a copy of ambient e; specifically labelled B_1°. For modelling the move a fresh label B_2° for name e and a corresponding configuration $C_{2,2}^\circ$, which contains the unfolded process (e.g. E_1°), are generated. The effect of the unfolding inside a copy of ambient e requires also to modify the configuration describing $\top$; in $C_{0,2}^\circ$ the presence of *exactly one* occurrence of ambient B_2° is recorded. Finally, we have $\mathcal{R}_{1,2} = \{(B_1^\circ, B_2^\circ), (B_1^\circ, B_1^\circ), (A_1^\circ, A_1^\circ), (\top, \top)\}$ showing the variation in the labels of ambients

[7] for simplicity, we safely approximate $[1-\omega]$ with $[0-\omega]$.

$$
\begin{tikzcd}
 & S_2^\circ \arrow[r] \arrow[d] & S_4^\circ \arrow[loop right] \arrow[dl] & \\
S_1^\circ \arrow[ur] & S_3^\circ \arrow[r] \arrow[loop below] & S_5^\circ \arrow[r] \arrow[loop below] & S_6^\circ \arrow[loop below]
\end{tikzcd}
$$

Figure3. The abstract transition system

named e. In particular, relation $\mathcal{R}_{1,2}$ says that one occurrence changes its label from B_1° to B_2° while the other occurrences mantain the same label B_1°.

Transition $S_2^\circ \mapsto^\circ_{\mathcal{R}_{2,4}} S_4^\circ$ is similar, and models the unfolding of recursion local to another instance of ambient B_1°. Due to normalisation, only the configuration describing $\top$ is modified; in $C_{0,4}^\circ$ the presence of *more than* one occurrence of ambient B_2° is recorded.

Transition $S_2^\circ \mapsto^\circ_{\mathcal{R}_{2,3}} S_3^\circ$ (and analogously $S_4^\circ \mapsto^\circ_{\mathcal{R}_{4,3}} S_3^\circ$) is derived by rule $\mathbf{In}^\circ$. It models the movement of an occurrence of ambient *mol* inside an ocurrence of ambient e; specifically, the interaction happens between ambients labelled A_1° and B_2°, respectively. State S_3° is the normalisation of the following state,

$$
\begin{array}{l}
{S_3^\circ}' = \{(\top, {C_{0,3}^\circ}'), (A_1^\circ, C_{1,1}^\circ), (A_2^\circ, C_{1,2}^\circ), (B_1^\circ, C_{2,1}^\circ), (B_2^\circ, C_{2,2}^\circ), (B_3^\circ, C_{2,3}^\circ)\} \\
{C_{0,3}^\circ}' = \{(A_1^\circ, [0-\omega]), (B_1^\circ, [0-\omega]), (B_2^\circ, [0-\omega]), (B_3^\circ, 1)\}
\end{array}
$$

For modelling the movement a fresh label A_2° for name *mol* and a corresponding configuration $C_{1,2}^\circ$ (which contains the continuation of process M°) are generated. Analogously, a fresh label B_3° is generated for name e and a corresponding configuration $C_{2,3}^\circ$, recording the presence of one occurrence of ambient *mol* labelled A_2°. In state ${S_3^\circ}'$, however, the number of labels for the ambients named e exceeds the limit $max_e = 2$, and therefore the normalization merges labels B_1°, B_2° and B_3° into the unique label B_∞°. The variation of labels both for ambients named *mol* and e is recorded accordingly in relation $\mathcal{R}_{2,3} = \{(B_1^\circ, B_\infty^\circ), (B_2^\circ, B_\infty^\circ), (A_1^\circ, A_2^\circ), (A_1^\circ, A_1^\circ), (\top, \top)\}$.

Transition $S_3^\circ \mapsto^\circ_{\mathcal{R}_{3,5}} S_5^\circ$ (and analogously $S_5^\circ \mapsto^\circ_{\mathcal{R}_{5,6}\}} S_6^\circ$) is derived by rule $\mathbf{Out}^\circ$. It models the movement of an instance of ambient *mol* out from an instance of ambient e; specifically, the interaction happens between ambients labelled A_2° and B_∞°, respectively. Similarly as in the case of $\mathbf{In}^\circ$, a fresh label A_3° is introduced for name *mol* and a corresponding configuration $C_{1,3}^\circ$ (which contains process P°). Due to normalisation all the labels describing ambients named e are still represented by label B_∞°. The variation of labels for ambients named *mol* is recorded accordingly in relation $\mathcal{R}_{3,5} = \{(A_2^\circ, A_3^\circ), (B_\infty^\circ, B_\infty^\circ), (A_2^\circ, A_2^\circ), (A_1^\circ, A_1^\circ), (\top, \top)\}$.

Finally, notice that loop-transitions are present, due to the presence of several molecule and enzyme ambients in the system; they show that other instances of the involved ambients may repeat one of the previous interactions.

Notice the role of labels and of normalisation for accurately describing the possible contents of ambients with the same name. Labels A_1°, A_2° and A_3° for ambients named *mol* permit to exactly distinguish instances at different evolution steps, e.g. described by different configurations. Instead, label B_∞° is used for describing all the ambients named e and reportss a set of configurations,

$$
C_{2,1}^\circ = \{(E^\circ, 1)\} \quad C_{2,2}^\circ = \{(E_1^\circ, 1)\} \quad C_{2,3}^\circ = \{(E_2^\circ, 1), (A_2^\circ, 1)\}
$$

This information is less precise (see for example the difference between state S_3° and ${S_3^\circ}'$) in the sense that all the instances of ambients named e are labelled B_∞°. As a consequence, their contents may be described by any configuration, $C_{2,i}^\circ$ with $i \in \{1,2,3\}$. This information, however, is crucial for capturing that any instance of an ambient (named) e *either* contains process E° *or* process E_1° *or* process E_2° and in parallel an ambient named *mol* (labelled A_2°). This guarantees that capability $\overline{\mathtt{in}}\, m^\circ$ cannot be exercised, inside any ambient named e, after that an ambient named *mol* is entered.

4 Widening

We derive a new weaker and more efficient analysis by introducing a *widening operator* [9]. Widening operators are designed precisely to speed up the convergency of a fixed-point computation; in this context, a simple widening operator can be defined by a function $\nabla : \mathcal{A}^\circ \to \mathcal{A}^\circ$, which gives an approximation of an element of the abstract domain. This means that $\nabla(Ss_1^\circ, S_{0,1}^\circ, Ts_1^\circ) = (Ss_2^\circ, S_{0,2}^\circ Ts_2^\circ)$ where $(Ss_1^\circ, S_{0,1}^\circ, Ts_1^\circ) \subseteq^\circ (Ss_2^\circ, S_{0,2}^\circ, Ts_2^\circ)$. This function is intended to be applied at each iteration of the fixed-point computation. Formally, given function $F_P^\circ : \mathcal{A}^\circ \to \mathcal{A}^\circ$ of Def. 12, we consider the fixed-point operator $F_P^\nabla : \mathcal{A}^\circ \to \mathcal{A}^\circ$, where $F_P^\nabla((Ss_1^\circ, S_{0,1}^\circ, Ts_1^\circ)) = \nabla(F_P^\circ((Ss_1^\circ, S_{0,1}^\circ, Ts_1^\circ)))$.

The widening we present here is based on the simple idea to approximate, in each state, the information about the ambients with the same name. Specifically, by exploiting the definition of normalized states, we merge, for each ambient name, all the configurations related to the run-time label ∞ into a single configuration. The loss of information is therefore similar to that explained in Example 1, Fig. 2(c) and Fig. 2(d).

This is formalised by the following definition where we exploit the following $\cup^+$ operator over states,

$$\begin{aligned}\cup^+ S^\circ = & \bigcup_{a^\circ \in \in \mathcal{N}_{a^\circ}} \\ & \{(\Delta^\circ, \cup^+_{\in\{1,\ldots,n\}} C_i^\circ) \mid \{(\Delta^\circ, C_1^\circ), \ldots, (\Delta^\circ, C_n^\circ)\} = \{(\Delta^\circ, C^\circ) \in S^\circ \mid \ (\Delta^\circ)_2 = \infty, (\Delta^\circ)_1 = a^\circ\}\} \\ & \quad \cup \{(\Delta^\circ, C^\circ) \in S^\circ \mid \ (\Delta^\circ)_2 \neq \infty, (\Delta^\circ)_1 = a^\circ\}\end{aligned}$$

Definition 13 (Widening). *We define $\nabla : \mathcal{A}^\circ \to \mathcal{A}^\circ$, where*

$$\nabla(Ss^\circ, S_0^\circ, Ts^\circ) = (\{\cup^+ S^\circ\}_{S^\circ \in Ss^\circ}, \cup^+ S_0^\circ, \{\cup^+ S_1^\circ \mapsto^\circ_{\mathcal{R}^\circ} \cup^+ S_2^\circ\}_{S_1^\circ \mapsto^\circ_{\mathcal{R}^\circ} S_2^\circ \in Ts^\circ}).$$

The resulting analysis is exponential and is a safe approximation (w.r.t. the order $\subseteq^\circ$) of the analysis defined in Section 3. Given a process P we denote by $\mathfrak{S}_\nabla [\![P]\!]$ the transition system, obtained by applying the widening operator.

Theorem 3. *Let let P be a process such that $\top \notin \mathcal{N}_a(P)$. We have $\mathfrak{S}_{Coll^\circ} [\![P]\!] \subseteq^\circ \mathfrak{S}_\nabla [\![P]\!]$.*

The following example shows an abstract transition system obtained by applying the widening operator.

Example 4. We generalise the non-deterministic version of the system (2) considered in the Introduction, by introducing several molecule and enzyme ambients,

$$\begin{aligned}& SYS_3 ::= [M]^{(mol,\Psi_1)} \mid \ldots \mid [M]^{(mol,\Psi_h)} \mid [E_1]^{(e_1,\Delta_1)} \mid \ldots \mid [E_1]^{(e_1,\Delta_k)} \mid [E_2]^{(e_2,\Phi_1)} \mid \ldots \mid [E_2]^{(e_2,\Phi_s)} \\ & E_i ::= \texttt{rec}Y.\, \overline{\texttt{in}}\, m_i.\, \overline{\texttt{out}}\, n_i.\, Y \\ & M ::= \texttt{in}\, m_1.\, \texttt{out}\, n_1.\, P_1 + \texttt{in}\, m_2.\, \texttt{out}\, n_2.\, P_2\end{aligned}$$

We also assume that: (i) the abstract names and ambient names are defined by the following equivalence classes $\mathcal{N}^\circ = \{\{n_1, m_1\}, \{n_2, m_2\}$, and $\mathcal{N}_a^\circ = \mathcal{N}_a$; (ii) $max_{mol} = 6$, $max_{e_1} = max_{e_2} = 0$ and $max_\top = 0$. For simplicity, we consider the following notation for abstract labels: $\top$ stands for $(\top, \infty)$, $A_i^\circ = (mol, \Lambda_i)$, $B_\infty^\circ = (e_1, \infty)$ and $C_\infty^\circ = (e_2, \infty)$.

Using the widening operator previously introduced [8] we obtain the abstract transition system of Fig. 4 and Tables 5 and 6. We assume that each transition $S_i^\circ \mapsto S_j^\circ$ of Fig. 4 represents abstract transitions $S_i^\circ \mapsto^\circ_{\mathcal{R}_{i,j}} S_j^\circ$, where $\mathcal{R}_{i,j} = \mathcal{R}_{S_i^\circ, S_j^\circ} \cup \texttt{id}(\texttt{amb}(S_i^\circ))$ for each $\mathcal{R}_{S_i^\circ, S_j^\circ}$ of Table 6.

The abstract transition system is obviously an extension of that presented in Example 3 for the simplified reaction. The situation is more complex because here the molecule may bind *either* with the enzyme e_1 (thus releasing product P_1) *or* with the enzyme e_2 (thus releasing product P_2).

[8] for simplicity, we safely approximate $[1 - \omega]$ with $[0 - \omega]$.

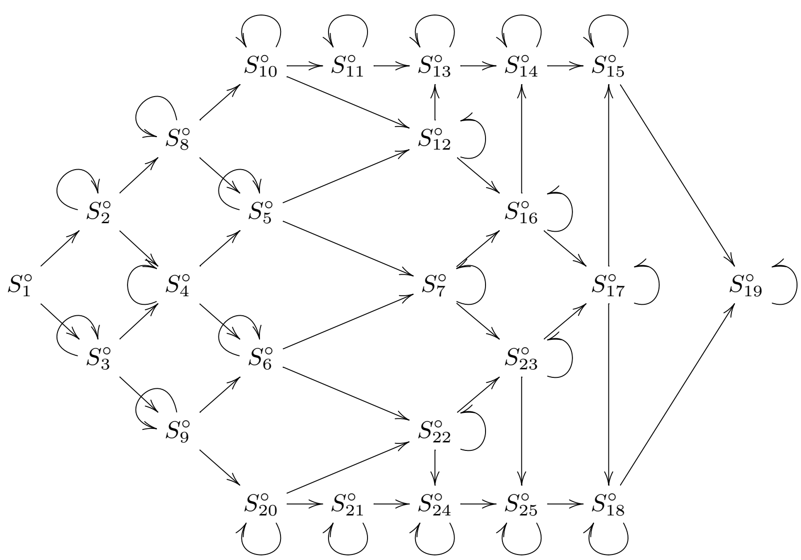


Figure4. The abstract transition system

Moreover, the abstract transition system is slightly different in that $max_{e_1} = max_{e_2} = 0$ requires the application of the widening to the configurations related to names e_1 and e_2.

In order to illustrate the relevant novelties we focus on a particular path of the transition system, which models the interaction of a molecule with an enzyme e_1 (which releases product P_1) and then of another molecule with an enzyme e_2 (which releases product P_2).

State S_1° is the normalisation of the translation of the initial process SYS_3 (note that all the copies of ambients named e_1 and e_2 are described by labels B_∞° and C_∞°, respectively).

Transition $S_1^\circ \overset{\circ}{\longmapsto}_{\mathcal{R}_{1,2}} S_2^\circ$ is obtained by rule $\mathbf{Rec}^\circ$ and models the unfolding of process E_1° local to an ambient e_1 (labelled B_∞°). For modelling the move a new configuration which contains the unfolded process (e.g. $E_{1,1}^\circ$) with multiplicity 1 should be generated for a fresh label for name e_1. However, since the number of labels for name e_1 exceeds the limit $max_{e_1} = 0$, the normalization merges all labels for name e_1 into the unique label B_∞°. Furthermore, the effect of the widening, is to approximate the configurations for B_∞° (e.g. $C_{2,1}^\circ$ and $\{(E_{1,1}^\circ, 1)\}$) into a unique configuration, e.g. $C_{2,2}^\circ$. This introduces a loss of information; indeed $C_{2,2}^\circ = \{(E_1^\circ, [0-\omega]), (E_{1,1}^\circ, [0-\omega])\}$ says that processes E_1° and $E_{1,1}^\circ$ may appear, at the same time, inside any ambient named e_1. Note that $\mathcal{R}_{1,2} = \mathtt{id}(\mathtt{amb}(S_1^\circ))$ shows that there is no variation in the labels of ambients.

Transition $S_2^\circ \overset{\circ}{\longmapsto}_{\mathcal{R}_{2,8}} S_8^\circ$ is derived by rule $\mathbf{In}^\circ$, and models the movement of an ambient *mol* inside an ambient e_1; specifically, the interaction happens between ambients labeled A_1° and B_∞°, respectively. For modelling the movement a fresh label A_2° for name *mol* and a corresponding configuration $C_{1,2}^\circ$ (which contains the continuation of process M°) are generated. By contrast, due to the normalisation and to the widening, all the occurrences of ambients (named) e_1 are still described by label B_∞° and by a single configuration, e.g. $C_{2,3}^\circ$. The variation of labels both for ambients named *mol* and e_1 is recorded accordingly in relation $\mathcal{R}_{2,8} = \{(B_\infty^\circ, B_\infty^\circ), (C_\infty^\circ, C_\infty^\circ), (A_1^\circ, A_2^\circ), (A_1^\circ, A_1^\circ), (\top, \top)\}$.

Transition $S_8^\circ \overset{\circ}{\longmapsto}_{\mathcal{R}_{8,10}} S_{10}^\circ$ (and analogously transition $S_{10}^\circ \overset{\circ}{\longmapsto}_{\mathcal{R}_{10,11}} S_{11}^\circ$) is derived by rule $\mathbf{Out}^\circ$. It models the movement of an ambient *mol* out from an ambient e_1; specifically, the interaction happens between ambients labelled A_2° and B_∞°, respectively. Similarly as in the case of $\mathbf{In}^\circ$, a fresh label A_3° is introduced for name *mol* and a corresponding configuration $C_{1,4}^\circ$ (which contains now the product of the reaction P_1°). Due to normalisation and to the widening all the labels describing ambients named e_1, are still represented by label B_∞° and by a single configuration, e.g. again $C_{2,3}^\circ$. The variation of labels for ambients named *mol* is recorded accordingly in $\mathcal{R}_{8,10} = \{(A_2^\circ, A_3^\circ), (B_\infty^\circ, B_\infty^\circ), (C_\infty^\circ, C_\infty^\circ), (A_2^\circ, A_2^\circ), (A_1^\circ, A_1^\circ), (\top, \top)\}$.

The remaining part of the examined path include the steps passing through states S°_{11}, S°_{13}, S°_{14} S°_{15} and S°_{19}. They model the symmetric interaction, where another molecule interacts with an enzyme e_2, thus releasing product P_2. Due to normalisation and to the widening, all the labels describing ambients named e_2 are always represented by label C°_{∞} and by a single configuration. By contrast, in order to model the possible variations for name *mol* fresh labels A°_4 and A°_5 are generated and corresponding configurations. They are analogous to the labels A°_2 and A°_3 applied in the symmetric interaction with e_1.

Notice that in the examined path the interaction follows a given order. It should be clear that the remaining part of the abstract transition system represents all the possible interleavings between the previous transition steps.

5 Temporal Properties

We present a simple class of temporal properties, which are interesting for expressing properties of biological systems. Specifically, we would like to capture properties such as: (i) is A_1 a *necessary checkpoint* for A_2? meaning that, in any path, a state satisfying A_2 can only appear after a state that satisfies A_1; (ii) is A_2 *always true* after A_1? meaning that, in any path, *after* a state satisfying A_2, A_1 is *always* true.

We specialize the formalization of properties, such as (i) and (ii), to the context of BA, by considering state formulas able to express basic properties of BA processes. Moreover, we exploit the labeling used in the semantics of processes (both in the concrete and in the abstract case) in order to handle systems where multiple copies of ambients may appear. Specifically, we are interested in proving properties which hold for *any* occurrence of an ambient, related to a given name.

Temporal Properties. Let $a, b \in \mathcal{N}_a$ and $P \in \mathcal{AP}$. The *state formulas* of a, denoted by $\mathcal{S}(a)$ (and ranged over by $\phi, \psi \ldots$), are defined by: $[b]^a$, $[P]^a$, $[a]^b$ and $\neg[b]^a$, $\neg[P]^a$, $\neg[a]^b$.

The formulas $\mathcal{S}(a)$ are designed precisely for expressing properties of *each* ambient named a, appearing enabled (ready to interact) in a process; they concern their possible contents and their possible location. Intuitively, $[P]^a$ and $[b]^a$ say that a process P and an ambient named b appear at top-level inside *any* ambient named a, resp.; similarly, $[a]^b$ says that an ambient (named) b is the father of *any ambient* named a. Furthermore, $\neg[b]^a$ (resp. $\neg[a]^b$) says that *any* ambient named a cannot contain ambients named b (resp. cannot be enclosed inside an ambient (named) b).

Notice that state formulas are not closed under negation; in the following, however, we may write for convenience $\neg\phi$, where $\phi \in \{\neg[b]^a, \neg[P]^a, \neg[a]^b\}$ with the obvious meaning.

In order to formalize the meaning of state formulas we observe that in our systems all the ambients related to given name a, are distinguished by means of run-time labels (see Section 2). It is therefore natural to interpret those formulas with respect to a set of run-time labels, expressing the instances of ambients that we want to consider.

Definition 14 (State Formulas). *Let $a \in \mathcal{N}_a$ be an ambient name, $P \in \mathcal{P}$ be a process, $L \subseteq \mathtt{amb}(P, a)$ and $\phi \in \mathcal{S}(a)$ be a state formula. We say that P satisfies ϕ with respect to L, $P \models_L \phi$, iff*

1. *$\phi = [Q]^a$ (resp. $\phi = [b]^a$) and, for all ambients labels $A \in L$, there exists an enabling context C, such that $P \equiv C[[R \mid Q]^A]$ (resp. $P \equiv C[[[Q]^{(b,\Delta)} \mid R]^A]$);*
2. *$\phi = [a]^b$ and, for all ambients labels $A \in L$, there exists an enabling context C, such that $P \equiv C[[[Q]^A \mid R]^{(b,\Delta)}]$;*
3. *$\phi \in \{\neg[b]^a, \neg[P]^a, \neg[a]^b\}$ and, for all ambients labels $A \in L$, it is not the case that $P \models_{\{A\}} \phi$.*

Moreover, we say that $P \models \phi$ *iff* $P \models_{\mathtt{amb}(P,a)} \phi$.

Intuitively, $P \models_L \phi$ says that an ambient named a, appearing enabled in P, satisfies ϕ, whenever its label belongs to L. Consequently, $P \models \phi$ guarantees property ϕ for all the ambients named a.

Temporal formulas are then defined as follows.

Definition 15. *Let* $\phi_1, \phi_2, \phi \in \mathcal{S}(a)$ *be state formulas of* $a \in \mathcal{N}_a$. *The* temporal formulas $\mathcal{T}(a)$ *are defined by:* $\Box\phi$, $\phi_1 \rightsquigarrow \phi_2$ *and* $\phi_1 \lhd \phi_2$.

Intuitively, $\Box\phi$ says that ϕ *is always* true; $\phi_1 \rightsquigarrow \phi_2$ says that ϕ_1 is a *necessary checkpoint* for ϕ_2, and $\phi_1 \lhd \phi_2$ says that ϕ_2 is *always* true *after* ϕ_1. Specifically, the interpretation of a temporal formula $\phi \in \mathcal{T}(a)$ is that the statement expressed by ϕ has to be true for *each* enabled ambient named a. This is formalized as follows, by exploiting the labeling discipline of ambients; we recall that in the concrete semantics (see Table 1) each ambient maintains its label, as the computation proceeds; fresh labels are introduced only for the new ambients introduced by the unfolding of recursion. Given a reduction step $P \to P'$ and $L \subseteq \mathtt{amb}(P,a)$, we use $Im(L) = (\mathtt{amb}(P',a) \cap L) \cup (\mathtt{amb}(P',a) \setminus \mathtt{amb}(P,a))$.

Definition 16 (Temporal Properties). *Let* $Ts = (Ss, Ss_0, Ts)$ *be a transition system, let* $P \in Ss$ *be a process,* $L \subseteq \mathtt{amb}(P,a)$ *and* $\overline{\phi} \in \mathcal{T}(a)$ *be a temporal formula. We say that* P satisfies $\overline{\phi}$ with respect *to* L, $P \models_L \overline{\phi}$, *iff*

1. $\overline{\phi} = \Box\phi$ *and* $P \models_L \phi$, *and for each* $P \to P' \in Ts$, $P' \models_{Im(L)} \overline{\phi}$;
2. $\overline{\phi} = \phi_1 \rightsquigarrow \phi_2$ *and* $P \models_L \neg\phi_2$, *and for each* $P \to P' \in Ts$, $P' \models_{Im(L \setminus L^{yes})} \overline{\phi}$, *where* $L^{yes} = \{A \in L \mid P \models_{\{A\}} \phi_1\}$;
3. $\overline{\phi} = \phi_1 \lhd \phi_2$ *and, for each* $P \to P' \in Ts$, $P' \models_{Im(L^{not})} \overline{\phi}$ *and* $P' \models_{Im(L \setminus L^{not})} \Box\phi_2$, *where* $L^{not} = \{A \in L \mid P \models_{\{A\}} \neg\phi_1\}$.

Moreover, we say that: $P \models \overline{\phi}$ *iff* $P \models_{\mathtt{amb}(P,a)} \overline{\phi}$, *and that* TS *satisfies* $\overline{\phi}$ *iff, for each initial state* $Q \in Ss_0$, $Q \models \overline{\phi}$.

As in the case of state formulas $P \models_L \overline{\phi}$ refers to the considered set of labels L, related to name a. In the case of invariant properties the definition of $P \models_L \Box\phi$ is immediate. We verify that: (i) $P \models_L \phi$ meaning that all the copies of ambients named a, related to labels of L, satisfy ϕ (ii) for all derivates P', $P' \models_{Im(L)} \overline{\phi}$, meaning that the ambients related to L as well as the new ambients (possibly introduced by a recursive step) satisfy the invariant property (this is precisely realized by $Im(L)$).

The semantics of the remaining properties is more complex; as an example we explain case 2. For $P \models_L \phi_1 \rightsquigarrow \phi_2$ we have to guarantee that, for each ambient with label in L, ϕ_2 remains false until the first point where ϕ_1 is true (if any). Therefore, we check $P \models_L \neg\phi_2$; Then, for all derivates P', we require $P' \models_{Im(L \setminus L^{yes})} \overline{\phi}$, meaning that the images of the ambients related to L, for which ϕ_1 does not hold, still satisfy the checkpoint property.

Abstract Verification. We introduce an abstract notion of validation of temporal formulas which is correct in the sense that: if the abstract model of a process satisfies a formula, then the formula holds also in the concrete model. To this aim we design an abstract version of Def. 14 and 16, by considering the relation between the concrete and the abstract model (see Def. 9).

The interpretation of state formulas is given, as in the concrete case, with respect to a set of abstract ambients labels. In the style of [10], the abstract definition requires to define explicitly the interpretation of both positive and negative assertions.

Definition 17 (State Formulas). *Let $a \in \mathcal{N}_a$ be an ambient name, $S^\circ \in \mathcal{S}^\circ$ be an abstract state, $L^\circ \subseteq \mathtt{amb}(S^\circ, a^\circ)$ and $\phi \in \mathcal{S}(a)$ be a state formula. We say that S° satisfies ϕ with respect to L°, $S^\circ \models_{L^\circ} \phi$, iff*

1. *$\phi = [Q]^a$ (resp. $\phi = [b]^a$) and, for all ambients labels $A^\circ \in L^\circ$, and for each configuration $(A^\circ, C^\circ) \in S^\circ$, there exists $(Q, \mathtt{m}) \in C^\circ$, such that $\mathtt{m} \in \{1, [1-\omega]\}$ (resp. $(b, \mathtt{m}) \in C^\circ$, such that $\mathtt{m} \in \{1, [1-\omega]\}$);*
2. *$\phi = [a]^b$ and, for all ambients labels $A^\circ \in L^\circ$, and for each configuration $(D^\circ, C^\circ) \in S^\circ$, such that $(a^\circ, \mathtt{m}) \in C^\circ$, we have $(D^\circ)_1 = b$;*
3. *$\phi = \neg[Q]^a$ (resp. $\phi = \neg[b]^a$) and, for all ambients labels $A^\circ \in L^\circ$, and for each configuration $(A^\circ, C^\circ) \in S^\circ$, we have $(Q^\circ, 0) \in C^\circ$ (resp. $(b^\circ, 0) \in C^\circ$);*
4. *$\phi = \neg[a]^b$ and, for all ambients labels $A^\circ \in L^\circ$, and for each configuration $(D^\circ, C^\circ) \in S^\circ$, such that $(a^\circ, \mathtt{m}) \in C^\circ$ with $\mathtt{m} \in \{1, [1-\omega], [0-\omega]\}$, then $(D^\circ)_1 \neq b^\circ$.*

Moreover, we say that $S^\circ \models \phi$ iff $S^\circ \models_{\mathtt{amb}(S^\circ, a^\circ)} \phi$.

The interpretation of temporal formulas is defined accordingly, by adapting the concrete definition to the abstract labeling discipline, e.g. by considering the possible variation of run-time labels reported by means of relation $\mathcal{R}^\circ$ in a transition $S_1^\circ \mapsto^\circ_{\mathcal{R}^\circ} S_2^\circ$. Given a relation $\mathcal{R}^\circ \subseteq (\mathcal{L}_a{}^\circ \cup \{\perp\}) \times (\mathcal{L}_a{}^\circ \cup \{\perp\})$ and $L^\circ \subseteq \mathcal{L}_a^\circ$, we use $\mathcal{R}^\circ(L^\circ) = \{B^\circ \mid ((A^\circ, B^\circ) \in \mathcal{R}^\circ \wedge A^\circ \in L^\circ) \vee (\perp, B^\circ) \in \mathcal{R}^\circ\}$.

Definition 18 (Temporal Properties). *Let $Ts^\circ = (Ss^\circ, S_0^\circ, Ts^\circ)$ be an abstract transition system, let $S^\circ \in Ss^\circ$ be a state, and let $L^\circ \subseteq \mathtt{amb}(S^\circ, a^\circ)$ and let $\overline{\phi} \in \mathcal{T}(a)$ be a temporal formula. We say that S°* satisfies *$\overline{\phi}$* with respect *to L°, $S^\circ \models_{L^\circ} \overline{\phi}$, iff*

1. *$\overline{\phi} = \Box\phi$ and $S^\circ \models_{L^\circ} \phi$, and for each $S^\circ \mapsto^\circ_{\mathcal{R}^\circ} S^{\circ\prime} \in Ts^\circ$, $S^{\circ\prime} \models_{\mathcal{R}^\circ(L^\circ)} \overline{\phi}$;*
2. *$\overline{\phi} = \phi_1 \rightsquigarrow \phi_2$ and $S^\circ \models_{L^\circ} \neg\phi_2$, and for each $S^\circ \mapsto^\circ_{\mathcal{R}^\circ} S^{\circ\prime} \in Ts^\circ$, $S^{\circ\prime} \models_{\mathcal{R}^\circ(L^\circ \setminus L^{\circ yes})} \overline{\phi}$, where $L^{\circ yes} = \{A^\circ \in L^\circ \mid S^\circ \models_{\{A^\circ\}} \phi_1\}$;*
3. *$\overline{\phi} = \phi_1 \lhd \phi_2$ and, for each $S^\circ \mapsto^\circ_{\mathcal{R}^\circ} S^{\circ\prime} \in Ts^\circ$, $S^{\circ\prime} \models_{R^\circ(L^{\circ not})} \overline{\phi}$ and $S^{\circ\prime} \models_{\mathcal{R}(L^\circ \setminus L^{\circ not})} \Box\phi_2$, where $L^{\circ not} = \{A^\circ \in L^\circ \mid S^\circ \models_{\{A^\circ\}} \neg\phi_1\}$.*

Moreover, we say that: $S^\circ \models \overline{\phi}$ iff $S^\circ \models_{\mathtt{amb}(S^\circ, a^\circ)} \overline{\phi}$, and that TS° satisfies $\overline{\phi}$ iff $S_0^\circ \models \overline{\phi}$.

Theorem 4. *Let $Ts = (Ss, Ss_0, Ts)$ be a transition system an let $Ts^\circ = (Ss^\circ, S_0^\circ, Ts^\circ)$ be an abstract transition system, such that $\alpha^\circ(Ts) \subseteq^\circ Ts^\circ$. For each temporal formula $\overline{\phi} \in \mathcal{T}(a)$, if TS° satisfies $\overline{\phi}$, then TS satisfies $\overline{\phi}$.*

Example 5. We consider the (well-labeled) version of system (5) of the Introduction, presented in Example 3,

$$\begin{array}{l} SYS ::= [M]^{(mol,\Psi_1)} \mid \ldots \mid [M]^{(mol,\Psi_h)} \mid [E]^{(e,\Delta_1)} \mid \ldots \mid [E]^{(e,\Delta_k)} \\ E ::= \mathtt{rec}Y.\, \overline{\mathtt{in}}\, m.\, \overline{\mathtt{out}}\, n.\, Y \quad M ::= \mathtt{in}\, m.\, \mathtt{out}\, n.\, P \end{array}$$

This simple reaction is characterized by a crucial property: for any ambient mol, the binding of ambient with an enzyme ambient is *necessary* for the release of product P. This property can be formalized by formula

$$\overline{\phi} = [mol]^e \rightsquigarrow [P]^{mol}$$

expressing precisely that, for any ambient named mol, the presence of mol inside an ambient e ($[mol]^e$) is a *necessary checkpoint* for the presence of process P at top level ($[P]^{mol}$).

The abstract transition system, presented Example 3 (and depicted in Fig. 3) satisfies the required property. Intuitively, when just one copy of mol and e are in the system in order to verify the checkpoint formula $[mol]^e \rightsquigarrow [P]^{mol}$ we should verify that for every path (starting from the initial state) *either* each state of the path satisfies $\neg[P]^{mol}$ or the states of the path satisfies $\neg[P]^{mol}$ until we find the first state that satisfies $[mol]^e$. When more than one copies of mol and e comes into the picture we need to consider the behavior of all instances of ambient mol. Then the previous formulas have to be verified for *each occurrence* of ambient mol, by taking into account the labeling discipline (e.g. according to Def. 18).

Since all the ambients (named) mol appearing in the system are initially described by label A_1°, we have to check that $S_1^\circ \models_{\{A_1^\circ\}} \overline{\phi}$. For this we immediately observe that $S_1^\circ \models_{\{A_1^\circ\}} \neg[P]^{mol}$ since the process P° cannot appear in any configuration related to label A_1.

Moreover, we observe that in state S_1° there are no occurrences of ambients labeled A_1° (named mol) which satisfies $[mol]^e$; in particular, the ambients labeled A_1° cannot appear in any configuration related a label with name e (e.g. B_1°). As a consequence, for the derivatives of S_1° we still have to consider the image of label A_1°. Hence, we are left to verify that $S_2^\circ \models_{\{A_1^\circ\}} \overline{\phi}$, using the fact that label A_1° does not vary and that no fresh labels are introduced, as reported by relation $\mathcal{R}_{1,2}) = \{(B_1^\circ, B_2^\circ), (B_1^\circ, B_1^\circ), (A_1^\circ, A_1^\circ), (\top, \top)\}$.

A similar argument also applies to state S_2° in that $S_2^\circ \models_{\{A_1^\circ\}} \neg[P]^{mol}$ and there are no occurrences of ambients labeled A_1° which satisfies $[mol]^e$. Consequently, we have only to consider the derivatives of state S_2°, e.g. states S_3° and S_4°, and proving the checkpoint property for the corresponding images of label A_1°. Formally, by taking into account the variation of ambients labels related to the transition step, we have to check that: (i) $S_4^\circ \models_{\{A_1^\circ\}} \overline{\phi}$; and (ii) $S_3^\circ \models_{\{A_1^\circ, A_2^\circ\}} \overline{\phi}$, where A_1° and A_2° are the images of ambients labeled A_1°. Indeed, $\mathcal{R}_{2,4} = \mathcal{R}_{1,2}$ and $\mathcal{R}_{2,3} = \{(B_1^\circ, B_\infty^\circ), (B_2^\circ, B_\infty^\circ), (A_1^\circ, A_2^\circ), (A_1^\circ, A_1^\circ), (\top, \top)\}$.

Case (i) is immediate. In fact, similarly as before $S_4^\circ \models_{\{A_1^\circ\}} \neg[P]^{mol}$. Moreover, there are no occurrences of ambients named mol which satisfies $[mol]^e$. As a consequence, by considering the image of label A_1° for its derivatives, we are left to verify $S_3^\circ \models_{\{A_1^\circ, A_2^\circ\}} \overline{\phi}$ (this is precisely (ii)). Note, in fact, that the loop between S_4° and S_4° is not relevant, because the only variation of labels concerns the ambients named e.

For (ii) it is immediate to check that $S_3^\circ \models_{\{A_1^\circ, A_2^\circ\}} \neg[P]^{mol}$ by taking into account the configurations related both to label A_1° and A_2°. Moreover we observe that in this case, differently from the previous ones, there are some occurrences of ambients named mol which satisfies $[mol]^e$; specifically, this is the case for ambients labeled A_2°. This is true since there exists a unique configuration where A_2° appears, this is the configuration for label B_∞ $C_{2,3}^\circ = \{(E_2^\circ, 1), (A_2^\circ, 1)\}$ which reports the presence of one ambient labeled A_2° inside ambients named e. This guarantees that all the ambients related to A_2°, appearing in the system, reside inside an ambient named e. Hence, in this case for the derivates we have to consider the image of label A_1°; formally, we have $\{A_1^\circ, A_2^\circ\}^{yes} = \{A_2^\circ\}$ meaning that we do not have to consider the images of label A_2° anymore.

We recall that S_3° has two derivates, e.g. S_3° and S_5°, and that the corresponding transitions are decorated by the following relations,

$$\mathcal{R}_{3,3} = \mathtt{id}(S_3^\circ) \text{ or } \mathcal{R}_{3,3} = \{(A_1^\circ, A_2^\circ)\} \cup \mathtt{id}(S_3^\circ)$$

$$\mathcal{R}_{3,5} = \{(A_2^\circ, A_3^\circ), (B_\infty^\circ, B_\infty^\circ), (A_2^\circ, A_2^\circ), (A_1^\circ, A_1^\circ), (\top, \top)\}$$

In the former case, the first transition models the unfolding of recursion for another ambient named e. Therefore, A_1° is the images of ambient labeled A_1° and we have to verify $S_3^\circ \models_{\{A_1^\circ\}} \overline{\phi}$. Note that $S_3^\circ \models_{\{A_1^\circ, A_2^\circ\}} \overline{\phi}$ implies $S_3^\circ \models_{\{A_1^\circ\}} \overline{\phi}$. So we have to verify again $S_3^\circ \models_{\{A_1^\circ, A_2^\circ\}} \overline{\phi}$. The second transition models the entering of another ambient named mol (and labeled A_1°) inside an ambient mol. Therefore, A_1° and A_2° are the images of ambients labeled A_1° and we have to verify again $S_3^\circ \models_{\{A_1^\circ, A_2^\circ\}} \overline{\phi}$.

In the latter case, we are left to prove that $S_5^\circ \models_{\{A_1^\circ\}} \overline{\phi}$, where A_1° is obtained from A_1° by means of relation $\mathcal{R}_{3,5}$. Similarly as before, we have that $S_5^\circ \models_{\{A_1^\circ\}} \neg[P]^{mol}$ and that there are no occurrences of A_1° which satisfies $[mol]^e$. Hence, we have to consider the image of label A_1° for all derivates, e.g. S_5° and S_6°. We recall that the related transitions are decorated by the following relations, $\mathcal{R}_{5,5} = \mathcal{R}_{3,3}$ and $\mathcal{R}_{5,6} = \mathcal{R}_{3,5}$.

In the former case, reasoning as before, we just consider the transition $\mathcal{R}_{5,5}$ which models the entering of another ambient named *mol* (and labeled A_1°) inside an ambient *mol*. Formally, A_1° and A_2° are the images of the ambients labeled A_1°, by means of $\mathcal{R}_{5,5}$, and we have to verify $S_5^\circ \models_{\{A_1^\circ, A_2^\circ\}} \overline{\phi}$. This is an obvious extension of the proof of $S_5^\circ \models_{\{A_1^\circ\}} \overline{\phi}$ discussed above. Again this requires to prove $S_6^\circ \models_{\{A_1^\circ\}} \overline{\phi}$ by exploiting the fact that label A_2° satisfies $[mol]^e$.

In the latter case, we have to check $S_6^\circ \models_{\{A_1^\circ\}} \overline{\phi}$. This follows immediately by observing that $S_6^\circ \models_{\{A_1^\circ\}} \neg[P]^{mol}$ and that there are no occurrences of label A_1° which satisfies $[mol]^e$. Consequently, for the derivatives of S_6° (e.g. S_6°) we have to consider the image of label A_1°. We recall that either $\mathcal{R}_{6,6} = \{(A_2^\circ, A_3^\circ)\}$ or $\mathcal{R}_{6,6} = \{(A_1^\circ, A_2^\circ)\}$. In the former case this require again $S_6^\circ \models_{\{A_1^\circ\}} \overline{\phi}$; in the latter case, this requires $S_6^\circ \models_{\{A_1^\circ, A_2^\circ\}} \overline{\phi}$. We conclude by observing that the reasoning for $S_6^\circ \models_{\{A_1^\circ, A_2^\circ\}} \overline{\phi}$ is analogous to that applied for $S_6^\circ \models_{\{A_1^\circ\}} \overline{\phi}$. Indeed, we have $S_6^\circ \models_{\{A_2^\circ\}} \neg[P]^{mol}$ and, since label A_2° satisfies $[mol]^e$, we have come back again to $S_6^\circ \models_{\{A_1^\circ\}} \overline{\phi}$.

□

Following the guidelines of the previous example, it is immediate to imagine how to express different temporal properties using our logic as well as how to verify them on even more complex biological systems.

Example 6. We consider the generalization of systems (2) introduced in the Introduction and in Example 4,

$$SYS_3 ::= [M]^{(mol,\Psi_1)} \mid \ldots \mid [M]^{(mol,\Psi_h)} \mid [E_1]^{(e_1,\Delta_1)} \mid \ldots \mid [E_1]^{(e_1,\Delta_k)} \mid [E_2]^{(e_2,\Lambda_1)} \mid \ldots \mid [E_2]^{(e_2,\Lambda_s)}$$
$$E_i ::= \mathtt{rec}Y.\, \overline{\mathtt{in}}\, m_i.\, \overline{\mathtt{out}}\, n_i.\, Y$$
$$M ::= \mathtt{in}\, m_1.\, \mathtt{out}\, n_1.\, \mathtt{in}\, m_2.\, \mathtt{out}\, n_2.\, P \qquad (3)$$
$$M ::= \mathtt{in}\, m_1.\, \mathtt{out}\, n_1.\, P_1 + \mathtt{in}\, m_2.\, \mathtt{out}\, n_2.\, P_2 \qquad (4)$$

We recall that processes (3) and (4) describe two completely different behaviors of system SYS_3. In case (3) the binding of *mol* with both enzymes e_1 and e_2 is *necessary* for the release of product P (this binding also has to happen in a given order, first e_1 and then e_2). By contrast, in case (4) ambient *mol* can *non-deterministically* bind *either* with e_1 (by releasing product P_1) *or* with e_2 (by releasing product P_2). These interesting properties of the reactions can be easily expressed as follows,

1. $[mol]^{e_i} \rightsquigarrow [P]^{mol}$ says that, for any ambient *mol*, the binding with an ambient e_i is a *necessary checkpoint* for the release of product P (shown by the presence of P at top level inside *mol*);
2. $[mol]^{e_1} \rightsquigarrow [mol]^{e_2}$ says that, for any ambient *mol*, the binding with an ambient e_1 is a *necessary check-point* for that with an ambient e_2;
3. $[mol]^{e_1} \lhd \neg[mol]^{e_2}$ says that, any ambient *mol* after the binding with an ambient e_1, *will never* react with an ambient e_2 (and the symmetric property is $[mol]^{e_2} \lhd \neg[mol]^{e_1}$ with the obvious meaning).

It is clear that the behavior of system SYS_3 is in both cases an extension of that of the simplified system examined in Examples 3 and 5. Specifically, the validation of case (3) and of the related check-point properties 1. and 2. can be done following the guidelines of Examples 3 and 5. We discuss the most interesting case of process (4) and of property 3.

In particular, we show that the abstract transition system, obtained by applying the widening operator (see Example 4 and Fig. 4) is sufficiently powerful for establishing property $\overline{\phi} = [mol]^{e_1} \lhd \neg[mol]^{e_2}$ (and obviously also its symmetric version). According to Def. 18 we have to exploit the labelling discipline of ambients in order to distinguish the occurrences of ambient *mol*. In this case, however, we have to guarantee that, each occurrence of *mol*, for each path, *either* never satisfies $[mol]^{e_1}$ *or* after a state, which *may* satisfy $[mol]^{e_1}$, will never satisfy $[mol]^{e_2}$ (meaning that it satisfies $\Box\neg[mol]^{e_2}$).

We recall that in the initial state S_1° all the occurrences of ambients (named) mol are described by label A_1°; thus, we have to check $S_1^\circ \models_{\{A_1^\circ\}} \overline{\phi}$. To shorten the presentation we focus on a particular path $S_1^\circ, S_2^\circ, S_8^\circ, S_{10}^\circ, S_{11}^\circ, S_{13}^\circ, S_{14}^\circ, S_{15}^\circ$ and S_{19}°. The remaining cases are similar (in that they model different interleavings between the same actions).

We observe that in state S_1° all the occurrences of mol are related to label A_1° and satisfy $\neg[mol]^{e_1}$. This is because all the ambients named e_1 are labelled B_∞° and are described by the following configuration

$$C_{2,1}^\circ = \{(E_1^\circ, 1)\}$$

This obviously guarantees that any ambient e_1 does not contain occurrences of ambients mol.

Hence, we are left to verify property $\overline{\phi}$ for state S_2° by considering the possible images of label A_1°. This move models the unfolding of process E_1° local to an ambient e_1 (labelled B_∞°). Consequently, there is no variation in the labels related to name mol, and we have to check $S_2^\circ \models_{\{A_1^\circ\}} \overline{\phi}$.

For state S_2° we observe that all the ambients named e_1 are still labelled B_∞° and are described by the following configuration

$$C_{2,2}^\circ = \{(E_1^\circ, [0-\omega]), (E_{1,1}^\circ, [0-\omega])\}$$

This obviously guarantees that any ambient e_1 does not contain occurrences of ambients mol, e.g. all the occurrences of mol (related to label A_1°) satisfy $\neg[mol]^{e_1}$.

Hence, we are to verify property $\overline{\phi}$ for the possible images of label A_1° related to each transition step.

The move from S_2° into S_2° is immediate given that there is no variation of label A_1°. By contrast, the move into S_8° represents the entering of an ambient mol (labelled A_1) inside an ambient e_1. The corresponding evolution relation reports the variation of label A_1 into a fresh label A_2,

$$\mathcal{R}_{2,8} = \{(A_1^\circ, A_1^\circ), (A_1^\circ, A_2^\circ), (B_\infty^\circ, B_\infty^\circ), (C_\infty^\circ, C_\infty^\circ), (\top, \top)\}.$$

Hence, we have to check $S_8^\circ \models_{\{A_1^\circ, A_2^\circ\}} \overline{\phi}$ by considering both labels A_1° and A_2°.

For state S_8° we observe that all the ambients named e_1 are still labelled B_∞° and are described by the following configuration

$$C_{2,3}^\circ = \{(E_1^\circ, [0-\omega]), (E_{1,1}^\circ, [0-\omega]), (E_{1,2}^\circ, [0-\omega]), (A_2^\circ, [0-\omega])\}$$

This means that: the occurrences of mol related to label A_1° satisfy $\neg[mol]^{e_1}$; this is not the case for those related to label A_2° (which may be contained inside an ambient e_1).

Hence, we are left to verify for each transition step: (i) property $\overline{\phi}$ for the images of label A_1°; (ii) property $\Box\neg[mol]^{e_2}$ for the images of label A_2°.

The move from S_8° into S_8° reports again the possible variation of label A_1° into A_2°. Hence, we have to check (i) again $S_8^\circ \models_{\{A_2^\circ, A_1^\circ\}} \overline{\phi}$ and (ii) $S_8^\circ \models_{\{A_2^\circ\}} \Box\neg[mol]^{e_2}$. Condition (ii) is immediate given that all the ambients named e_2 are labelled C_∞° and are described by the following configuration

$$C_{3,1}^\circ = \{(E_2^\circ, 1)\}$$

This obviously guarantees that there are no occurrences of ambients mol inside any ambient e_2.

The move into S_{10}° represents the exit of an ambient mol (labelled A_2°) out from an ambient e_1, as reported by the evolution relation,

$$\mathcal{R}_{8,10} = \{(A_2^\circ, A_3^\circ), (A_1^\circ, A_1^\circ), (A_2^\circ, A_2^\circ), (B_\infty^\circ, B_\infty^\circ), (C_\infty^\circ, C_\infty^\circ), (\top, \top)\}.$$

As a consequence: the images of label A_2° in S_{10}° are labels A_2° and A_3° (the fresh label A_3° is generated precisely for representing the ambient mol (labelled A_2°) which participated to the movement); the image of label A_1° is again A_1°.

This means that we have to check: (i) $S_{10}^\circ \models_{\{A_1^\circ\}} \overline{\phi}$ and (ii) $S_{10}^\circ \models_{\{A_2^\circ, A_3^\circ\}} \Box\neg[mol]^{e_2}$. Condition (ii) is immediate given that all the ambients named e_2 are labelled C_∞° and are described again by configuration $C_{3,1}^\circ$. The same argument used for state S_8° applies.

For (i) we observe that all the ambients named e_1 are still labelled B°_∞ and are described again by configuration $C^\circ_{2,3}$. This means that: the occurrences of *mol* related to label A°_1 satisfy $\neg[mol]^{e_1}$; this is not the case for those related to label A°_2 (which may be contained inside an ambient e_1).

Hence, we are left to verify for each transition step: (i) property $\overline{\phi}$ for the images of label A°_1; (ii) property $\Box\neg[mol]^{e_2}$ for the images of labels A°_2 and A°_3.

The move from S°_{10} into S°_{10} represents the repetition of one of the previous interactions, e.g. the corresponding evolution relations report as possible the variation of label A_1 into A_2 and of label A_2 into A_3. Hence, we have to check (i) $S^\circ_{10} \models_{\{A^\circ_2, A^\circ_1\}} \overline{\phi}$ and again (ii) $S^\circ_{10} \models_{\{A^\circ_2, A^\circ_3\}} \Box\neg[mol]^{e_2}$.

For (i) it is enough to notice that the occurrences of *mol* related to label A°_2 may satisfy $[mol]^{e_1}$. They have been already considered in (ii).

The move into S°_{11} is analogous to the previous one, in that models the exit of another ambient *mol* (labelled A°_2) out from an ambient e_1; the variation of labels is again A_2 into A_3. Hence, we have to check (i) $S^\circ_{11} \models_{\{A^\circ_1\}} \overline{\phi}$ and (ii) $S^\circ_{11} \models_{\{A^\circ_2, A^\circ_3\}} \Box\neg[mol]^{e_2}$. For (ii) and (i) an argument analogous to that applied for state S°_{10} holds.

Hence, we are left to verify for each transition step: (i) property $\overline{\phi}$ for the images of label A°_1; (ii) property $\Box\neg[mol]^{e_2}$ for the images of labels A°_2 and A°_3.

The move from S°_{11} into S°_{11} is analogous to the previous one, and requires in addition to check $S^\circ_{10} \models_{\{A^\circ_2, A^\circ_1\}} \overline{\phi}$. Since the occurrences of *mol* related to label A°_2 may satisfy $[mol]^{e_1}$, they have been already considered in (ii).

Instead, the move into S°_{13} models the unfolding of process E°_2 local to an ambient e_2 (labelled C°_∞). Since there is no variation in the labels of ambients, we have again to prove (i) $S^\circ_{13} \models_{\{A^\circ_1\}} \overline{\phi}$ and (ii) $S^\circ_{13} \models_{\{A^\circ_2, A^\circ_3\}} \Box\neg[mol]^{e_2}$.

For (ii) it is enough to observe that all the ambients named e_2 are labelled C°_∞ and are described by the following configuration

$$C^\circ_{3,2} = \{(E^\circ_2, [0-\omega]), (E^\circ_{2,1}, [0-\omega])\}$$

This obviously guarantee that there are no occurrences of ambients *mol* inside any ambient e_2.

For (i) we observe that all the ambients named e_1 are still labelled B°_∞ and are described again by configuration $C^\circ_{2,3}$. This means that: the occurrences of *mol* related to label A°_1 satisfy $\neg[mol]^{e_1}$; this is not the case for those related to label A°_2 (which may be contained inside an ambient e_1).

Hence, we are left to verify for each transition step: (i) property $\overline{\phi}$ for the images of label A°_1; (ii) property $\Box\neg[mol]^{e_2}$ for the images of labels A°_2 and A°_3.

For the move from S°_{13} to S°_{13} it is enough to repeat an argument similar to that used for those from S°_{10} to S°_{10}. Instead, the move into S°_{14} models the entering of an ambient *mol* (labelled A°_1) inside an ambient e_2 labelled C°_∞. For modelling the movement a fresh label A°_4 for name *mol* and a corresponding configuration $C^\circ_{1,4}$ (which contains the continuation of process M°) are generated. The configuration for label C°_∞ is modified as follows,

$$C^\circ_{3,3} = \{(E^\circ_2, [0-\omega]), (E^\circ_{2,1}, [0-\omega]), (E^\circ_{2,2}, [0-\omega]), (A^\circ_4, [0-\omega])\}.$$

The variation of labels is reported in the corresponding evolution relation

$$\mathcal{R}_{13,14} = \{(A^\circ_1, A^\circ_4), (A^\circ_1, A^\circ_1), (A^\circ_2, A^\circ_2), (A^\circ_3, A^\circ_3), (B^\circ_\infty, B^\circ_\infty), (C^\circ_\infty, C^\circ_\infty), (\top, \top)\}$$

This means that the ambients related to labels A°_2 and A°_3 are not involved in the movement, which concern the occurrences related to label A°_1 only. As a consequence, in state S°_{14} we have to verify (i) $S^\circ_{14} \models_{\{A^\circ_1, A^\circ_4\}} \overline{\phi}$ and (ii) $S^\circ_{14} \models_{\{A^\circ_2, A^\circ_3\}} \Box\neg[mol]^{e_2}$.

Condition (ii) follows immediately by observing configuration $C^\circ_{3,3}$ (note that an ambient named *mol* may appear inside an ambient e_2; this is however related to the fresh label A°_4).

For (i) we observe that all the ambients named e_1 are still labelled B°_∞ and are described again by configuration $C^\circ_{2,3}$. This means that: the occurrences of *mol* related to labels A°_1, A°_4 and A°_5 satisfy $\neg[mol]^{e_1}$; this is not the case for those related to label A°_2 (which may be contained inside an ambient e_1).

Hence, we are left to verify for each transition step: (i) property $\overline{\phi}$ for the images of label A°_1 and A°_4; (ii) property $\Box\neg[mol]^{e_2}$ for the images of labels A°_2 and A°_3.

For the move from S°_{14} to S°_{14} it is enough to repeat an argument similar to that used for those from S°_{11} to S°_{11}. By contrast, the move into S°_{15} models the exit of an ambient *mol* (labelled A°_4) out from an ambient e_2 labelled C°_∞. For modelling the movement a fresh label A°_5 for name *mol* and a corresponding configuration $C^\circ_{1,5}$ (which contains process $P^\circ{}_2$) are generated. This step is similar to the previous one in that no variation of labels A°_2 and A°_3 is possible (in fact, the fresh label A°_5 is the image of A°_4.)

As a consequence, in state S°_{15} we have to verify (i) $S^\circ_{14} \models_{\{A^\circ_1,A^\circ_4,A^\circ_5\}} \overline{\phi}$ and (ii) $S^\circ_{14} \models_{\{A^\circ_2,A^\circ_3\}} \Box\neg[mol]^{e_2}$.

Condition (ii) follows immediately by observing that the configuration for label C°_∞ related to name e_2 is not modified, e.g. $C^\circ_{3,3}$. For (i) we observe that all the ambients named e_1 are still labelled B°_∞ and are described again by configuration $C^\circ_{2,3}$. This means that: the occurrences of *mol* related to labels A°_1 and A°_4 satisfy $\neg[mol]^{e_1}$; this is not the case for those related to label A°_2 (which may be contained inside an ambient e_1).

Hence, we are left to verify for each transition step: (i) property $\overline{\phi}$ for the images of labels A°_1, A°_5 and A°_4; (ii) property $\Box\neg[mol]^{e_2}$ for the images of labels A°_2 and A°_3.

The move into S°_{19} models the exit of another ambient *mol* (labelled A°_4) out from an ambient e_2 labelled C°_∞. It is enough to apply the same argument used for S°_{15}.

We conclude by observing that the possible variations of labels related to the moves from S°_i to S°_i with $i \in \{14, 15, 19\}$ do not require to take into account additional labels, similarly as for the loops of the previous cases.

□

6 Conclusions

This work is motivated by the aim of deriving an abstract transition system for BA/MA, which is able to address *temporal* properties more general than invariant properties (differently from typical reachability analyses [28,18,11,14,21,30,29,31,32,15]). Specifically, in order to accurately handle systems where multiple occurrences of ambients may appear, we have extended the abstract interpretation approach of [21] by introducing: (i) occurrence counting information (in the sense of [27,13,15,16]) and (ii) a particular labelling discipline of ambients. The combination of these technique permits to derive detailed information about the possible contents of ambients, and also to distinguish different occurrences of ambients, at different execution step. In this way, the analysis supports the validation of temporal properties which hold for any occurrence of an ambient (as illustrated by the examples of Section 5).

These features represent a novelty with respect to the analyses proposed in literature. Indeed, the abstract transition systems, which could be derived by extending these approaches, would be rather weak for establishing this kind of properties. This is because: (i) they lack a technique for distinguishing different occurrences of ambients; (ii) most of them [28,30,18] do not maintain occurrence counting information or use a less precise information (by counting the number of objects appering in the whole system). Occurrence counting information is essential for reasoning about the firing of capabilities and for deducing the possible sequences of moves (which are obviously relevant in properties such as checkpoints). The analyses of [27,15] instead compute very precise information about occurrence counting. It is not clear, however, how an abstract transition system could be derived and whether properties such as those discussed in this paper could be captured. A strictly related proposal is presented in [12] for MA, by introducing techniques for deriving a finite abstract model, which can be used for establishing security properties by means of model checking techniques. The derived model, however, is not sufficiently precise for accurately handle systems where multiple copies of ambients may appear; specifically, it cannot validate the temporal properties of the examples of Section 5.

The analysis proposed is rather expensive from a computational point of view. Our approach, however, is quite flexible and offers several possibilities for tuning the precision. The abstraction is parametric, in the sense that one can choose which part of the system he is interested in by defining equivalence classes of ambients labels and names. Moreover, we have introduced a simple widening; further approximations can naturally be introduced by following the widening approach of abstract interpretation. For example, another orthogonal widening operator can be naturally obtained by merging into a unique abstract state the information about different states of the abstract transition system. The derived analysis, which is presented in a related paper [16], is exponential. Although it suffers from the limitations explained for the other reachability analyses for BA and MA [30,29,31,32,15,28,18,11,14,21], it is very interesting for proving invariant properties. Specifically, it is able to very precisely capture *occurrence counting information* as well as simple *causal aspects*. Moreover, the advantage of the widening operators approach is that new different widening operators can be defined and combined together. For example the two widenings we have defined can be combined, in any order, by giving two new approximations. In both cases, the derived analyses are polynomial; we refer the reader to [16] for examples of their applications.

There are several interesting directions for future works. First of all, in this paper we have considered the validation of a simple class of temporal properties expressing typical properties of biological systems, which hold for any occurrence of an ambient. It would be interesting to investigate whether the standard interpretation of ∀-CTL without eventually [6,10] could be adapted in this style, by exploiting the labelling discipline of ambients. This could offer the possibility to validate a wider class of temporal properties for systems where multiple copies of ambients appear. We leave to the future works also the investigation of the preserved properties using logics, desigened specifically for MA [3,24].

In order to realize a tool which implements our analyses, we are currently studying new widening operators and/or implementation techniques which could reduce the complexity. This could be applied to study more complex real biological specifications. Moreover, we are interested in extending our framework in order to take into account stochastic aspects.

References

1. R. Barbuti, S. Cataudella, A. Maggiolo-Schettini, P. Milazzo and A.Troina, *A Probabilistic Calculus for Molecular Systems.* Proc. of Workshop CS & P, Informatik Berichte 170, Humboldt University press, vol 202–216, 2004.
2. L. Cardelli. *Membrane Interactions.* Proc. of BioCONCUR '03, ENTCS, 2003.
3. L. Caires, L. Cardelli. *A Spatial Logic for Concurrency.* Information and Computation, 186, 194-235, 2003.
4. L. Cardelli and A.D. Gordon. *Mobile ambients.* Theoretical Computer Science 240, 177–213, 2000.
5. N. Chabrier, Marc Chiaverini, Vincent Danosand F. Fages. *Modeling and querying biomolecular interaction networks.* Theoretical Computer Science 325(1), 25-44, 2004.
6. M. Clarke, O. Grumberg and E. Long. *Model Checking and Abstraction.* TOPLAS, 16(5), 1512-1542, 1994.
7. P. Cousot and R. Cousot. *Abstract Interpretation: A Unified Lattice Model for Static Analysis of Programs by Construction or Approximation of Fixpoints.* Proc. of POPL'77, 238–252, 1977.
8. P. Cousot and R. Cousot. *Systematic Design of Program Analysis Frameworks.* Proc. of POPL'79 , 269–282, 1979.
9. P. Cousot and R. Cousot. *Comparing the Galois Connection and Widening/Narrowing Approaches to Abstract Interpretation.* Proc. of PLILP'92, LNCS 631, 269–295, 1992.
10. D. Dams, R. Gerth and O. Grumberg. *Abstract Interpretation of Reactive Systems.* TOPLAS, 19(2), 253-291, 1997.
11. P. Degano, F. Levi and C. Bodei. *Safe Ambients: Control Flow Analysis and Security.* Proc. of ASIAN '00, LNCS 1961, 199-214, Springer Verlag, 2000.
12. D. Distefano. *A Parametric Model for the Analysis of Mobile Ambients.* Proc. of APLAS' 05, LNCS 3780, 401–417, Springer Verlag, 2005.
13. J. Feret. *Occurrence Counting Analysis for the pi-calculus.* ENTCS 39, 2001.
14. J. Feret. *Abstract Interpretation-Based Static Analysis of Mobile Ambients.* Proc. of SAS'01, LNCS 2126, 412-430, Springer Verlag, 2001.
15. J. Feret. *Analysis of mobile systems by abstract interpretation.* PhD Thesis, 2005.

16. R.Gori and F. Levi. *A new occurrence Counting analysis for BioAmbients.* Proc. of APLAS '05, LNCS 3780, 381–400, 2005.
17. R.Gori and F. Levi. *An Analysis for proving Temporal Properties of Biological Systems (Extended Version).* Available at `http://www.di.unipi.it/~ levifran/papers.html`, 2006.
18. R. R. Hansen and J. G. Jensen and F. Nielson and H. R.Nielson. *Abstract Interpretation of Mobile Ambients.* Proc. of SAS'99, LNCS 1694, 135-148, Springer-Verlag, 1999.
19. N. Kam, D. Harel, H. Kugler, R. Marelly, A. Pnueli, E.J.A. Hubbard and M.J. Stern. *Formal Modeling of C. elegans Development: A Scenario-Based Approach.* Proc. of CMSB' 03, LNCS 2602, 4-20, 2003.
20. R. Hofestadt and S.Thelen. *Quantitative modeling of biochemical networks.* Silico Biology, volume1, 39-53, 1998.
21. F. Levi and S. Maffeis. *On Abstract Interpretation of Mobile Ambients.* Information and Computation 188, 179–240, 2004.
22. F. Levi and D. Sangiorgi. *Mobile Safe Ambients.* TOPLAS, 25(1), 1–69. ACM Press, 2003.
23. R. Mardare and C. Priami. *Logical Analysis of Biological Systems.* Fundamenta Informaticae, 64, 271–285, 2005.
24. R. Mardare, O. Vagin, P. Quaglia and C. Priami. *Model Checking Biological Systems described using Ambient Calculus.* Proc. of CMSB'04, LNCS 3082, 85–103, 2005.
25. H.Matsuno, A.Doi, M.Nagasaki and S.Miyano. *Hybrid petri net representation of gene regulatory network.* Pacific Symposium on Biocomputing (5), 338-349, 2000.
26. R. Milner, J. Parrow and D. Walker. *A Calculus of Mobile Processes.* Information and Computation, 100, 1-77, 1992.
27. F. Nielson and H.R. Nielson. *Shape analysis for mobile ambients.* Proc. of POPL'00, 142-154, ACM Press, 2000.
28. F. Nielson, H.R. Nielson, R.R. Hansen. *Validating firewalls using flow logics.* Theoretical Computer Science, 283(2), 381-418, 2002.
29. F. Nielson, H.R. Nielson and H. Pilegaard. *Spatial Analysis of BioAmbients.* Proc. of SAS'04, LNCS 3148, pp. 69–83, Springer-Verlag, 2004.
30. F. Nielson, H.R. Nielson, C. Priami and D. Schuch da Rosa. *Control Flow Analysis for BioAmbients.* Proc. of BioCONCUR'03, ENTCS, 2003.
31. F. Nielson, H.R. Nielson, C. Priami and D. Schuch da Rosa. *Static Analysis for Systems Biology.* Proc. of the winter International Symposium on Information and Communication Technologies, 1–6, Trinity College Dublin, 2004.
32. H. Pilegaard, F. Nielson and H.R. Nielson. *Static Analysis of a Model of the LDL Degradation Pathway.* Proc. of CMSB'05, 2005.
33. C.Priami and P. Quaglia. *Beta binders for biological interactions.* Proc. of CMSB'04, LNCS 3082,20–33,2005
34. C. Priami, A. Regev, W. Silverman and E. Shapiro. *Application of a stochastic name-passing calculus to representation and simulation of molecular processes.* Information Processing Letters, 80 (1), 25–31, 2001.
35. A. Regev, E. M. Panina, W. Silverman, L. Cardelli and E. Shapiro. *BioAmbients: an Abstraction for Biological Compartments.* Theoretical Computer Science, 325, 141–167, 2004.
36. A. Regev, W. Silverman and E. Shapiro. *Representation and Simulation of Biochemical Processes using the pi-calculus process algebra.* Proc. of the Pacific Symposium on Biocomputing 2001, 6, 459–470, 2001.

$$\mathbf{Rec}^\circ \quad \frac{(A^\circ, C^\circ) \in S^\circ \qquad (T^\circ, \mathtt{m}) \in C^\circ \qquad T^\circ = \mathtt{rec}X.\,P^\circ}{S^\circ \mapsto^\circ_{\mathcal{R}^\circ\sigma} (S_1^\circ \cup S_2^\circ)\sigma}$$

$\sigma \in \mathcal{M}(S_1^\circ \cup S_2^\circ) \qquad S_1^\circ = ((S^\circ \setminus^\circ \{(A^\circ, C^\circ)\}) \cup \{(\mathtt{new}(A^\circ), C_1^\circ)\})[^{\mathtt{new}(A^\circ)}/_{A^\circ}]$
$C_1^\circ = (C^\circ \setminus^\circ T^\circ) \cup^+ C_2^\circ \quad \eta^\circ(P^\circ[T^\circ/X]) = (C_2^\circ, S_2^\circ)$
$\mathcal{R}^\circ = \{(B^\circ, \sigma(B^\circ)) \mid B^\circ \in \mathtt{amb}(S^\circ) \cap \mathtt{amb}(S_0^\circ)\} \cup \{(A^\circ, \sigma(\mathtt{new}(A^\circ))))\} \cup (\bot, \mathtt{amb}(S_2^\circ\sigma))$

$$\mathbf{In}^\circ \quad \frac{\begin{array}{lll} (A_1^\circ, C_1^\circ) \in S^\circ & (T^\circ, \mathtt{m}_1) \in C_1^\circ & T^\circ = +\mathtt{in}\, m^\circ.\, P^\circ \\ (A_2^\circ, C_2^\circ) \in S^\circ & (T'^\circ, \mathtt{m}_2) \in C_2^\circ & T'^\circ = +\overline{\mathtt{in}}\, m^\circ.\, Q^\circ \\ (A_3^\circ, C_3^\circ) \in S^\circ & (A_1^\circ, \mathtt{m}_3), (A_2^\circ, \mathtt{m}_4) \in C_3^\circ & A_1^\circ = A_2^\circ \rightarrow \mathtt{m}_3 = \mathtt{m}_4 >_m 1 \end{array}}{S^\circ \mapsto^\circ_{\mathcal{R}^\circ\sigma} (S_1^\circ \cup S_{1,2}^\circ \cup S_{2,2}^\circ)\sigma}$$

$\sigma \in \mathcal{M}(S_1^\circ \cup S_{1,2}^\circ \cup S_{2,2}^\circ)$
$S_1^\circ = ((S^\circ \setminus^\circ \bigcup_{i\in\{1,2,3\}} \{(A_i^\circ, C_i^\circ)\})) \bigcup_{i\in\{1,2,3\}} \{(\mathtt{new}(A_i^\circ), C_{i,1}^\circ)\})[^{\mathtt{new}(A_3^\circ)}/_{A_3^\circ}]$
$C_{1,1}^\circ = (C_1^\circ \setminus^\circ T^\circ) \cup^+ C_{1,2}^\circ \quad \eta^\circ(P^\circ) = (C_{1,2}^\circ, S_{1,2}^\circ)$
$C_{2,1}^\circ = (C_2^\circ \setminus^\circ T'^\circ) \cup^+ C_{2,2}^\circ \cup^+ \{(\mathtt{new}(A_1^\circ), 1)\} \quad \eta^\circ(Q^\circ) = (C_{2,2}^\circ, S_{2,2}^\circ)$
$C_{3,1}^\circ = (C_3^\circ \setminus^\circ \{A_1^\circ, A_2^\circ\}) \cup^+ (\mathtt{new}(A_2^\circ), 1)$
$\mathcal{R}^\circ = \{(B^\circ, \sigma(B^\circ)) \mid B^\circ \in \mathtt{amb}(S^\circ) \cap \mathtt{amb}(S_0^\circ)\} \cup \{(A_i^\circ, \sigma(\mathtt{new}(A_i^\circ)))\}_{i\in\{1,2,3\}} \cup (\bot, \mathtt{amb}(S_{1,2}^\circ\sigma \cup S_{2,2}^\circ\sigma))$

$$\mathbf{Out}^\circ \quad \frac{\begin{array}{llll} (A_1^\circ, C_1^\circ) \in S^\circ & (T^\circ, \mathtt{m}_1) \in C_1^\circ & T^\circ = +\mathtt{out}\, m^\circ P^\circ & \\ (A_2^\circ, C_2^\circ) \in S^\circ & (T'^\circ, \mathtt{m}_2) \in C_2^\circ & T'^\circ = +\overline{\mathtt{out}}\, m^\circ.\, Q^\circ & (A_1^\circ, \mathtt{m}_3) \in C_2^\circ \\ (A_3^\circ, C_3^\circ) \in S^\circ & (A_2^\circ, \mathtt{m}_4) \in C_3^\circ & & \end{array}}{S^\circ \mapsto^\circ_{\mathcal{R}^\circ\sigma} (S_1^\circ \cup S_{1,2}^\circ \cup S_{2,2}^\circ)\sigma}$$

$\sigma \in \mathcal{M}(S_1^\circ \cup S_{1,2}^\circ \cup S_{2,2}^\circ)$
$S_1^\circ = ((S^\circ \setminus^\circ \bigcup_{i\in\{1,2,3\}} \{(A_i^\circ, C_i^\circ)\})) \bigcup_{i\in\{1,2,3\}} \{(\mathtt{new}(A_i^\circ), C_{i,1}^\circ)\})[^{\mathtt{new}(A_3^\circ)}/_{A_3^\circ}]$
$C_{1,1}^\circ = (C_1^\circ \setminus^\circ T^\circ) \cup^+ C_{1,2}^\circ \quad \eta^\circ(P^\circ) = (C_{1,2}^\circ, S_{1,2}^\circ)$
$C_{2,1}^\circ = (C_2^\circ \setminus^\circ \{T'^\circ, A_1^\circ) \quad \eta^\circ(Q^\circ) = (C_{2,2}^\circ, S_{2,2}^\circ)$
$C_{3,1}^\circ = (C_3^\circ \setminus^\circ A_2^\circ) \cup^+ \{(\mathtt{new}(A_1^\circ), 1), (\mathtt{new}(A_2^\circ), 1)\}$
$\mathcal{R}^\circ = \{(B^\circ, \sigma(B^\circ)) \mid B^\circ \in \mathtt{amb}(S^\circ) \cap \mathtt{amb}(S_0^\circ)\} \cup \{(A_i^\circ, \sigma(\mathtt{new}(A_i^\circ)))\}_{i\in\{1,2,3\}} \cup (\bot, \mathtt{amb}(S_{1,2}^\circ\sigma \cup S_{2,2}^\circ\sigma))$

$$\mathbf{Merge}^\circ \quad \frac{\begin{array}{lll} (A_1^\circ, C_1^\circ) \in S^\circ & (T^\circ, \mathtt{m}_1) \in C_1^\circ & T^\circ = +\mathtt{merge}\, m^\circ P^\circ \\ (A_2^\circ, C_2^\circ) \in S^\circ & (T'^\circ, \mathtt{m}_2) \in C_2^\circ & T'^\circ = +\overline{\mathtt{merge}}\, m^\circ.\, Q^\circ \\ (A_3^\circ, C_3^\circ) \in S^\circ & (A_1^\circ, \mathtt{m}_3)(A_2^\circ, \mathtt{m}_4) \in C_3^\circ & A_1^\circ = A_2^\circ \rightarrow \mathtt{m}_3 = \mathtt{m}_4 >_m 1 \end{array}}{S^\circ \mapsto^\circ_{\mathcal{R}^\circ\sigma} (S_1^\circ \cup S_{1,2}^\circ \cup S_{2,2}^\circ)\sigma}$$

$\sigma \in \mathcal{M}(S_1^\circ \cup S_{1,2}^\circ \cup S_{2,2}^\circ)$
$S_1^\circ = ((S^\circ \setminus^\circ \bigcup_{i\in\{1,2,3\}} \{(A_i^\circ, C_i^\circ)\})) \bigcup_{i\in\{1,3\}} \{(\mathtt{new}(A_i^\circ), C_{i,1}^\circ)\})[^{\mathtt{new}(A_3^\circ)}/_{A_3^\circ}]$
$C_{1,1}^\circ = (C_1^\circ \setminus^\circ T^\circ) \cup^+ C_{1,2}^\circ \cup^+ C_{2,2}^\circ \quad \eta^\circ(P^\circ) = (C_{1,2}^\circ, S_{1,2}^\circ) \quad \eta^\circ(Q^\circ) = (C_{2,2}^\circ, S_{2,2}^\circ)$
$C_{3,1}^\circ = C_3^\circ \setminus^\circ \{A_1^\circ, A_2^\circ\} \cup^+ \{(\mathtt{new}(A_1^\circ), 1)\}$
$\mathcal{R}^\circ = \{(B^\circ, \sigma(B^\circ)) \mid B^\circ \in \mathtt{amb}(S^\circ) \cap \mathtt{amb}(S_0^\circ)\} \cup \{(A_i^\circ, \sigma(\mathtt{new}(A_i^\circ)))\}_{i\in\{1,3\}} \cup \{(A_2^\circ, \bot)\} \cup (\bot, \mathtt{amb}(S_{1,2}^\circ\sigma \cup S_{2,2}^\circ\sigma))$

Table4. Abstract Transitions.

$S_1^\circ = \{(\top, C_{0,1}^\circ), (A_1^\circ, C_{1,1}^\circ), (B_\infty^\circ, C_{2,1}^\circ), (C_\infty^\circ, C_{3,1}^\circ)\}$
$C_{0,1}^\circ = \{(A_1^\circ, [0-\omega]), (B_\infty^\circ, [0-\omega]), (C_\infty^\circ, [0-\omega])\}$ $\quad C_{1,1}^\circ = \{(M^\circ, 1)\}$ $\quad C_{2,1}^\circ = \{(E_1^\circ, 1)\}$ $\quad C_{3,1}^\circ = \{(E_2^\circ, 1)\}$

$S_2^\circ = \{(\top, C_{0,1}^\circ), (A_1^\circ, C_{1,1}^\circ), (B_\infty^\circ, C_{2,2}^\circ), (C_\infty^\circ, C_{3,1}^\circ)\}$
$C_{2,2}^\circ = \{(E_1^\circ, [0-\omega]), (E_{1,1}^\circ, [0-\omega])\}$ $\quad E^\circ{}_{1,1} ::= \overline{\mathtt{in}}\, m_1^\circ.\, \overline{\mathtt{out}}\, m_1^\circ.\, E_1^\circ$

$S_3^\circ = \{(\top, C_{0,1}^\circ), (A_1^\circ, C_{1,1}^\circ), (B_\infty^\circ, C_{2,1}^\circ), (C_\infty^\circ, C_{3,2}^\circ)\}$
$C_{3,2}^\circ = \{(E_2^\circ, [0-\omega]), (E_{2,1}^\circ, [0-\omega])\}$ $\quad E^\circ{}_{2,1} ::= \overline{\mathtt{in}}\, m_2^\circ.\, \overline{\mathtt{out}}\, m_2^\circ.\, E_2^\circ$

$S_4^\circ = \{(\top, C_{0,1}^\circ), (A_1^\circ, C_{1,1}^\circ), (B_\infty^\circ, C_{2,2}^\circ), (C_\infty^\circ, C_{3,2}^\circ)\}$

$S_5^\circ = \{(\top, C_{0,1}^\circ), (A_1^\circ, C_{1,1}^\circ), (A_2^\circ, C_{1,2}^\circ), (B_\infty^\circ, C_{2,3}^\circ), (C_\infty^\circ, C_{3,2}^\circ)\}$
$C_{1,2}^\circ = \{(M_1^\circ, 1)\}$ $\quad M_1^\circ ::= \mathtt{out}\, m_1^\circ.\, P_1^\circ$ $\quad E_{1,2}^\circ ::= \overline{\mathtt{out}}\, m_1^\circ.\, E_1^\circ$
$C_{2,3}^\circ = \{(E_1^\circ, [0-\omega]), (E_{1,1}^\circ, [0-\omega]), (E_{1,2}^\circ, [0-\omega]), (A_2^\circ, [0-\omega])\}$

$S_6^\circ = \{(\top, C_{0,1}^\circ), (A_1^\circ, C_{1,1}^\circ), (A_4^\circ, C_{1,4}^\circ), (B_\infty^\circ, C_{2,2}^\circ), (C_\infty^\circ, C_{3,3}^\circ)\}$
$C_{1,4}^\circ = \{(M_2^\circ, 1)\}$ $\quad M_2^\circ = \mathtt{out}\, m_2^\circ.\, P_2^\circ$ $\quad E_{2,2}^\circ ::= \overline{\mathtt{out}}\, m_2^\circ.\, E_2^\circ$
$C_{3,3}^\circ = \{(E_2^\circ, [0-\omega]), (E_{2,1}^\circ, [0-\omega]), (E_{2,2}^\circ, [0-\omega]), (A_4^\circ, [0-\omega])\}$

$S_7^\circ = \{(\top, C_{0,1}^\circ), (A_1^\circ, C_{1,1}^\circ), (A_2^\circ, C_{1,2}^\circ), (A_4^\circ, C_{1,4}^\circ), (B_\infty^\circ, C_{2,3}^\circ), (C_\infty^\circ, C_{3,3}^\circ)\}$

$S_8^\circ = \{(\top, C_{0,1}^\circ), (A_1^\circ, C_{1,1}^\circ), (A_2^\circ, C_{1,2}^\circ), (B_\infty^\circ, C_{2,3}^\circ), (C_\infty^\circ, C_{3,1}^\circ)\}$

$S_9^\circ = \{(\top, C_{0,1}^\circ), (A_1^\circ, C_{1,1}^\circ), (A_4^\circ, C_{1,4}^\circ), (B_\infty^\circ, C_{2,1}^\circ), (C_\infty^\circ, C_{3,3}^\circ)\}$

$S_{10}^\circ = \{(\top, C_{0,2}^\circ), (A_1^\circ, C_{1,1}^\circ), (A_2^\circ, C_{1,2}^\circ), (A_3^\circ, C_{1,3}^\circ)(B_\infty^\circ, C_{2,3}^\circ), (C_\infty^\circ, C_{3,1}^\circ)\}$
$C_{0,2}^\circ = \{(A_1^\circ, [0-\omega]), (B_\infty^\circ, [0-\omega]), (C_\infty^\circ, [0-\omega]), (A_3^\circ, 1)\}$ $\quad C_{1,3}^\circ = \{(M_{1,1}^\circ, 1)\}$ $\quad M_{1,1}^\circ ::= P_1^\circ$

$S_{11}^\circ = \{(\top, C_{0,3}^\circ), (A_1^\circ, C_{1,1}^\circ), (A_2^\circ, C_{1,2}^\circ), (A_3^\circ, C_{1,3}^\circ)(B_\infty^\circ, C_{2,3}^\circ), (C_\infty^\circ, C_{3,1}^\circ)\}$
$C_{0,3}^\circ = \{(A_1^\circ, [0-\omega]), (B_\infty^\circ, [0-\omega]), (C_\infty^\circ, [0-\omega]), (A_3^\circ, [0-\omega])\}$

$S_{12}^\circ = \{(\top, C_{0,2}^\circ), (A_1^\circ, C_{1,1}^\circ), (A_2^\circ, C_{1,2}^\circ), (A_3^\circ, C_{1,3}^\circ)(B_\infty^\circ, C_{2,3}^\circ), (C_\infty^\circ, C_{3,2}^\circ)\}$

$S_{13}^\circ = \{(\top, C_{0,3}^\circ), (A_1^\circ, C_{1,1}^\circ), (A_2^\circ, C_{1,2}^\circ), (A_3^\circ, C_{1,3}^\circ)(B_\infty^\circ, C_{2,3}^\circ), (C_\infty^\circ, C_{3,2}^\circ)\}$

$S_{14}^\circ = \{(\top, C_{0,3}^\circ), (A_1^\circ, C_{1,1}^\circ), (A_2^\circ, C_{1,2}^\circ), (A_3^\circ, C_{1,3}^\circ), (A_4^\circ, C_{1,4}^\circ)(B_\infty^\circ, C_{2,3}^\circ), (C_\infty^\circ, C_{3,3}^\circ)\}$

$S_{15}^\circ = \{(\top, C_{0,4}^\circ), (A_1^\circ, C_{1,1}^\circ), (A_2^\circ, C_{1,2}^\circ), (A_3^\circ, C_{1,3}^\circ), (A_4^\circ, C_{1,4}^\circ), (A_5^\circ, C_{1,5}^\circ)(B_\infty^\circ, C_{2,3}^\circ), (C_\infty^\circ, C_{3,3}^\circ)\}$
$C_{0,4}^\circ = \{(A_1^\circ, [0-\omega]), (B_\infty^\circ, [0-\omega]), (C_\infty^\circ, [0-\omega]), (A_3^\circ, [0-\omega]), (A_5^\circ, 1)\}$
$C_{1,5}^\circ = \{(M_{2,1}^\circ, 1)\}$ $\quad M_{2,1}^\circ ::= P_2^\circ$

$S_{16}^\circ = \{(\top, C_{0,2}^\circ), (A_1^\circ, C_{1,1}^\circ), (A_2^\circ, C_{1,2}^\circ), (A_3^\circ, C_{1,3}^\circ), (A_4^\circ, C_{1,4}^\circ)(B_\infty^\circ, C_{2,3}^\circ), (C_\infty^\circ, C_{3,3}^\circ)\}$

$S_{17}^\circ = \{(\top, C_{0,5}^\circ), (A_1^\circ, C_{1,1}^\circ), (A_2^\circ, C_{1,2}^\circ), (A_3^\circ, C_{1,3}^\circ), (A_4^\circ, C_{1,4}^\circ), (A_5^\circ, C_{1,5}^\circ)(B_\infty^\circ, C_{2,3}^\circ), (C_\infty^\circ, C_{3,3}^\circ)\}$
$C_{0,5}^\circ = \{(A_1^\circ, [0-\omega]), (B_\infty^\circ, [0-\omega]), (C_\infty^\circ, [0-\omega]), (A_3^\circ, 1), (A_5^\circ, 1)\}$

$S_{18}^\circ = \{(\top, C_{0,6}^\circ), (A_1^\circ, C_{1,1}^\circ), (A_2^\circ, C_{1,2}^\circ), (A_3^\circ, C_{1,3}^\circ), (A_4^\circ, C_{1,4}^\circ), (A_5^\circ, C_{1,5}^\circ)(B_\infty^\circ, C_{2,3}^\circ), (C_\infty^\circ, C_{3,3}^\circ)\}$
$C_{0,6}^\circ = \{(A_1^\circ, [0-\omega]), (B_\infty^\circ, [0-\omega]), (C_\infty^\circ, [0-\omega]), (A_5^\circ, [0-\omega]), (A_3^\circ, 1)\}$

$S_{19}^\circ = \{(\top, C_{0,7}^\circ), (A_1^\circ, C_{1,1}^\circ), (A_2^\circ, C_{1,2}^\circ), (A_3^\circ, C_{1,3}^\circ), (A_4^\circ, C_{1,4}^\circ), (A_5^\circ, C_{1,5}^\circ)(B_\infty^\circ, C_{2,3}^\circ), (C_\infty^\circ, C_{3,3}^\circ)\}$
$C_{0,7}^\circ = \{(A_1^\circ, [0-\omega]), (B_\infty^\circ, [0-\omega]), (C_\infty^\circ, [0-\omega]), (A_3^\circ, [0-\omega]), (A_5^\circ, [0-\omega])\}$

Table5. The abstract transition system of SYS_3.

$S^\circ_{20} = \{(\top, C^\circ_{0,8}), (A^\circ_1, C^\circ_{1,1}), (A^\circ_4, C^\circ_{1,4}), (A^\circ_5, C^\circ_{1,5})(B^\circ_\infty, C^\circ_{2,1}), (C^\circ_\infty, C^\circ_{3,3})\}$
$C^\circ_{0,8} = \{(A^\circ_1, [0-\omega]), (B^\circ_\infty, [0-\omega]), (C^\circ_\infty, [0-\omega]), (A^\circ_5, 1)\}$

$S^\circ_{21} = \{(\top, C^\circ_{0,9}), (A^\circ_1, C^\circ_{1,1}), (A^\circ_4, C^\circ_{1,4}), (A^\circ_5, C^\circ_{1,5})(B^\circ_\infty, C^\circ_{2,1}), (C^\circ_\infty, C^\circ_{3,3})\}$
$C^\circ_{0,9} = \{(A^\circ_1, [0-\omega]), (B^\circ_\infty, [0-\omega]), (C^\circ_\infty, [0-\omega]), (A^\circ_5, [0-\omega])\}$

$S^\circ_{22} = \{(\top, C^\circ_{0,8}), (A^\circ_1, C^\circ_{1,1}), (A^\circ_4, C^\circ_{1,4}), (A^\circ_5, C^\circ_{1,5})(B^\circ_\infty, C^\circ_{2,2}), (C^\circ_\infty, C^\circ_{3,3})\}$

$S^\circ_{23} = \{(\top, C^\circ_{0,8}), (A^\circ_1, C^\circ_{1,1}), (A^\circ_4, C^\circ_{1,4}), (A^\circ_5, C^\circ_{1,5}), (A^\circ_2, C^\circ_{1,2})(B^\circ_\infty, C^\circ_{2,3}), (C^\circ_\infty, C^\circ_{3,3})\}$

$S^\circ_{24} = \{(\top, C^\circ_{0,9}), (A^\circ_1, C^\circ_{1,1}), (A^\circ_4, C^\circ_{1,4}), (A^\circ_5, C^\circ_{1,5})(B^\circ_\infty, C^\circ_{2,2}), (C^\circ_\infty, C^\circ_{3,3})\}$

$S^\circ_{25} = \{(\top, C^\circ_{0,9}), (A^\circ_1, C^\circ_{1,1}), (A^\circ_4, C^\circ_{1,4}), (A^\circ_5, C^\circ_{1,5}), (A^\circ_2, C^\circ_{1,2})(B^\circ_\infty, C^\circ_{2,3}), (C^\circ_\infty, C^\circ_{3,3})\}$

$\mathcal{R}_{S^\circ_2,S^\circ_8} = \mathcal{R}_{S^\circ_4,S^\circ_5} = \mathcal{R}_{S^\circ_6,S^\circ_7} = \mathcal{R}_{S^\circ_{22},S^\circ_{23}} = \mathcal{R}_{S^\circ_{24},S^\circ_{25}} = \mathcal{R}_{S^\circ_5,S^\circ_5} = \mathcal{R}_{S^\circ_7,S^\circ_7} = \mathcal{R}_{S^\circ_8,S^\circ_8} = \mathcal{R}_{S^\circ_{10},S^\circ_{10}} =$
$\mathcal{R}_{S^\circ_{11},S^\circ_{11}} = \mathcal{R}_{S^\circ_{12},S^\circ_{12}} = \mathcal{R}_{S^\circ_{13},S^\circ_{13}} = \mathcal{R}_{S^\circ_{14},S^\circ_{14}} = \mathcal{R}_{S^\circ_{15},S^\circ_{15}} = \mathcal{R}_{S^\circ_{16},S^\circ_{16}} = \mathcal{R}_{S^\circ_{17},S^\circ_{17}} = \mathcal{R}_{S^\circ_{18},S^\circ_{18}} =$
$\mathcal{R}_{S^\circ_{19},S^\circ_{19}} = \mathcal{R}_{S^\circ_{23},S^\circ_{23}} = \mathcal{R}_{S^\circ_{25},S^\circ_{25}} = \{(A^\circ_1, A^\circ_2)\}$

$\mathcal{R}_{S^\circ_8,S^\circ_{10}} = \mathcal{R}_{S^\circ_{10},S^\circ_{11}} = \mathcal{R}_{S^\circ_5,S^\circ_{12}} = \mathcal{R}_{S^\circ_{12},S^\circ_{13}} = \mathcal{R}_{S^\circ_{18},S^\circ_{19}} = \mathcal{R}_{S^\circ_7,S^\circ_{16}} = \mathcal{R}_{S^\circ_{16},S^\circ_{14}} = \mathcal{R}_{S^\circ_{23},S^\circ_{17}} =$
$\mathcal{R}_{S^\circ_{17},S^\circ_{15}} = \mathcal{R}_{S^\circ_{25},S^\circ_{18}} = \mathcal{R}_{S^\circ_{10},S^\circ_{10}} = \mathcal{R}_{S^\circ_{11},S^\circ_{11}} = \mathcal{R}_{S^\circ_{12},S^\circ_{12}} = \mathcal{R}_{S^\circ_{13},S^\circ_{13}} = \mathcal{R}_{S^\circ_{14},S^\circ_{14}} = \mathcal{R}_{S^\circ_{15},S^\circ_{15}} =$
$\mathcal{R}_{S^\circ_{16},S^\circ_{16}} = \mathcal{R}_{S^\circ_{17},S^\circ_{17}} = \mathcal{R}_{S^\circ_{18},S^\circ_{18}} = \mathcal{R}_{S^\circ_{19},S^\circ_{19}} = \{(A^\circ_2, A^\circ_3)\}$

$\mathcal{R}_{S^\circ_3,S^\circ_9} = \mathcal{R}_{S^\circ_4,S^\circ_6} = \mathcal{R}_{S^\circ_5,S^\circ_7} = \mathcal{R}_{S^\circ_{12},S^\circ_{16}} = \mathcal{R}_{S^\circ_{13},S^\circ_{14}} = \mathcal{R}_{S^\circ_6,S^\circ_6} = \mathcal{R}_{S^\circ_7,S^\circ_7} =$
$\mathcal{R}_{S^\circ_9,S^\circ_9} = \mathcal{R}_{S^\circ_{10},S^\circ_{10}} = \mathcal{R}_{S^\circ_{14},S^\circ_{14}} = \mathcal{R}_{S^\circ_{15},S^\circ_{15}} = \mathcal{R}_{S^\circ_{17},S^\circ_{17}} = \mathcal{R}_{S^\circ_{18},S^\circ_{18}} = \mathcal{R}_{S^\circ_{19},S^\circ_{19}} = \mathcal{R}_{S^\circ_{20},S^\circ_{20}} =$
$\mathcal{R}_{S^\circ_{21},S^\circ_{21}} = \mathcal{R}_{S^\circ_{22},S^\circ_{22}} = \mathcal{R}_{S^\circ_{23},S^\circ_{23}} = \mathcal{R}_{S^\circ_{24},S^\circ_{24}} = \mathcal{R}_{S^\circ_{25},S^\circ_{25}} = \{(A^\circ_1, A^\circ_4)\}$

$\mathcal{R}_{S^\circ_9,S^\circ_{20}} = \mathcal{R}_{S^\circ_6,S^\circ_{22}} = \mathcal{R}_{S^\circ_7,S^\circ_{23}} = \mathcal{R}_{S^\circ_{16},S^\circ_{17}} = \mathcal{R}_{S^\circ_{14},S^\circ_{15}} = \mathcal{R}_{S^\circ_{15},S^\circ_{19}} = \mathcal{R}_{S^\circ_{17},S^\circ_{18}} = \mathcal{R}_{S^\circ_{23},S^\circ_{25}} =$
$\mathcal{R}_{S^\circ_{22},S^\circ_{24}} = \mathcal{R}_{S^\circ_{20},S^\circ_{21}} = \mathcal{R}_{S^\circ_{15},S^\circ_{15}} = \mathcal{R}_{S^\circ_{17},S^\circ_{17}} = \mathcal{R}_{S^\circ_{18},S^\circ_{18}} = \mathcal{R}_{S^\circ_{19},S^\circ_{19}} = \mathcal{R}_{S^\circ_{20},S^\circ_{20}} = \mathcal{R}_{S^\circ_{21},S^\circ_{21}} =$
$\mathcal{R}_{S^\circ_{22},S^\circ_{22}} = \mathcal{R}_{S^\circ_{23},S^\circ_{23}} = \mathcal{R}_{S^\circ_{24},S^\circ_{24}} = \mathcal{R}_{S^\circ_{25},S^\circ_{25}} = \{(A^\circ_4, A^\circ_5)\}$

$\mathcal{R}_{S^\circ_1,S^\circ_2} = \mathcal{R}_{S^\circ_1,S^\circ_3} = \mathcal{R}_{S^\circ_3,S^\circ_4} = \mathcal{R}_{S^\circ_2,S^\circ_4} = \mathcal{R}_{S^\circ_8,S^\circ_5} = \mathcal{R}_{S^\circ_{10},S^\circ_{11}} = \mathcal{R}_{S^\circ_{11},S^\circ_{13}} = \mathcal{R}_{S^\circ_{12},S^\circ_{13}} =$
$\mathcal{R}_{S^\circ_9,S^\circ_6} = \mathcal{R}_{S^\circ_{20},S^\circ_{22}} = \mathcal{R}_{S^\circ_{21},S^\circ_{24}} = \mathcal{R}_{S^\circ_2,S^\circ_2} = \mathcal{R}_{S^\circ_3,S^\circ_3} = \mathcal{R}_{S^\circ_4,S^\circ_4} = \mathcal{R}_{S^\circ_5,S^\circ_5} = \mathcal{R}_{S^\circ_6,S^\circ_6} =$
$\mathcal{R}_{S^\circ_7,S^\circ_7} = \mathcal{R}_{S^\circ_8,S^\circ_8} = \mathcal{R}_{S^\circ_9,S^\circ_9} = \mathcal{R}_{S^\circ_{10},S^\circ_{10}} = \mathcal{R}_{S^\circ_{11},S^\circ_{11}} = \mathcal{R}_{S^\circ_{12},S^\circ_{12}} =$
$\mathcal{R}_{S^\circ_{13},S^\circ_{13}} = \mathcal{R}_{S^\circ_{14},S^\circ_{14}} = \mathcal{R}_{S^\circ_{15},S^\circ_{15}} = \mathcal{R}_{S^\circ_{17},S^\circ_{17}} = \mathcal{R}_{S^\circ_{18},S^\circ_{18}} = \mathcal{R}_{S^\circ_{19},S^\circ_{19}} = \mathcal{R}_{S^\circ_{20},S^\circ_{20}} =$
$\mathcal{R}_{S^\circ_{21},S^\circ_{21}} = \mathcal{R}_{S^\circ_{22},S^\circ_{22}} = \mathcal{R}_{S^\circ_{23},S^\circ_{23}} = \mathcal{R}_{S^\circ_{24},S^\circ_{24}} = \mathcal{R}_{S^\circ_{25},S^\circ_{25}} = \emptyset$

Table6. The abstract transition system of SYS_3.