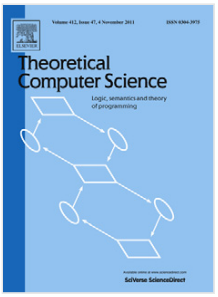
Accepted Manuscript



An analysis for proving probabilistic termination of biological systems

Roberta Gori, Francesca Levi

PII: S0304-3975(12)01002-X
DOI: 10.1016/j.tcs.2012.10.058
Reference: TCS 9116

To appear in: *Theoretical Computer Science*

Received date: 6 December 2010
Revised date: 13 July 2012
Accepted date: 26 October 2012

Please cite this article as: R. Gori, F. Levi, An analysis for proving probabilistic termination of biological systems, *Theoretical Computer Science* (2012), doi:10.1016/j.tcs.2012.10.058

An Analysis for Proving Probabilistic Termination of Biological Systems

Roberta Gori and Francesca Levi
Dipartimento di Informatica
Largo Pontecorvo 2
gori@di.unipi.it levifran@di.unipi.it

Abstract

In this paper we apply the *abstract interpretation* approach for approximating the behavior of biological systems, modeled specifically using the Chemical Ground Form calculus, a simple stochastic calculus rich enough to model the dynamics of biochemical reactions.

The analysis is based on the idea of representing a set of experiments, which differ only for the initial concentrations, by abstracting the multiplicity of reagents present in a solution, using intervals. For abstracting the probabilistic semantics, modeled as a Discrete-Time Markov Chain, we use a variant of *Interval Markov Chains*, where probabilistic and non-deterministic steps are combined together. The abstract probabilistic semantics is systematically derived from an abstract Labeled Transition System. The abstract probabilistic model safely approximates the set of concrete experiments and reports conservative *lower* and *upper* bounds for probabilistic termination.

Keywords: Chemical Ground Form Calculus, Abstract Interpretation, Probabilistic Termination

1. Introduction

Process calculi, originally designed for modeling distributed and mobile systems, are nowadays one of the most popular formalisms for the specification of biological systems. In this new application domain, a great effort has been devoted for adapting traditional models to characterize the molecular and biochemical aspects of biological systems. On one hand, the proposals, such as BioAmbients [49], Beta-Binders [47], and Brane calculi [10], aim at expressing the concepts of hierarchy, compartment and membrane, which play a key role in the organization of biomolecular systems. On the other hand, there is a new interest in the design of calculi able to capture the *quantitative* aspect (both time and probability) of real life applications, in the style of stochastic π-calculus [46, 48, 50].

A variety of automated methods for analysis and verification can be applied to biological systems modeled using a stochastic process calculus in order to

deduce information about their complex dynamics. The quantitative analysis is a fundamental task to better understand the behavior of biological systems, to test possible hypothesis of biologists and to observe fundamental properties which can guide future *in vitro* experiments.

A well-established approach relies on *stochastic simulation* techniques, based on the well-known results of Gillespie [26] (SSA). For stochastic π-calculus, the tools BioSpi [50] and SPiM [43, 44] explore a given evolution of the biological system model over a given time interval, thus realizing a virtual experiment. By performing a substantial number of simulation runs statistically relevant results about the possible behavior of biological systems can be achieved.

The principal alternative is based on *quantitative model checking*, a formal verification technique which supports the validation of (quantitative) temporal properties over all the runs of a biological system model. Tools such as PRISM [31] applies to models formalized as a *Discrete-Time Markov Chain* (DTMC), as a *Markov Decision Process* (MDP) as well as a *Continuous-Time Markov Chain* (CTMC). In this framework, the properties to be validated can be expressed in the probabilistic logic PCTL [29] or in the continuous-time logic CSL [36]. As an example, it is possible to answer to the following queries about the behaviour of biological systems: (i) what is the probability to reach a state where the concentration of molecule A is greater than n? (ii) What is the probability to reach a state, where the concentration of molecule A is greater than n, within a given time interval? (iii) In the long run, what is the probability that the concentration of molecule A reaches a level n, and then remains within certain bounds? Such properties have been demonstrated to capture important aspects of typical biological systems, discussed in literature, including complex pathways and systems which exhibits an oscillatory behaviour [14, 8, 9, 30, 3, 2, 6].

Unfortunately, the practical application of automatic model checking tools to biological systems revealed serious limitations. One specific feature of biological processes is that they are composed of a huge number of processes with identical behavior, such as thousands of molecules of the same type. Therefore, the state space of the model is often too large or even infinite. Another drawback is that typically the experimental data concerning the model are not precisely known. As a consequence, the biological system model has to be analyzed under different scenarios, namely by varying both the concentration levels of reagents and the rates of reactions of the experiment.

Approximation techniques preserving the validation of temporal properties have been established to be one of the most effective ways for overcoming these limitations. In particular, *static analysis* techniques provide automatic and decidable methods for establishing properties of programs (even infinite), by computing in a systematic way safe approximations of their (run-time) behavior. This approach has been widely applied for analyzing qualitative properties of traditional process calculi for mobile systems [7, 25, 39, 41] and also of biologically inspired process calculi [27, 42, 45, 6].

In this paper, we investigate the application of abstraction techniques to probabilistic model checking in the context of stochastic process calculi. The technique of approximation that we propose aims to reduce the complexity of the

analysis of a given biological system under several different scenarios. The idea is to calculate an *abstract probabilistic model* which represents the behaviour of a *set of experiments* for the biological system w.r.t. different initial concentrations of reagents. Probabilistic model checking of the abstract probabilistic model gives an approximated result for the probability of a property (that is *lower* and *upper* bounds) rather than exact value. The interval of probability reported by the analysis includes the exact values for the probability of the property for all the experiments which are approximated and therefore gives information on the possible effect on the probability due to the variation on the initial concentrations.

As a specification language we choose the *Chemical Ground Form* (CGF)[12] calculus because it is simple and expressive enough for modeling the dynamics of biochemical reactions. The calculus is a variant for biological systems of stochastic π-calculus without communication. Moreover, we consider the property of *probabilistic termination* (discussed for CGF in [53]), a particular probabilistic reachability property expressing the probability of a system to terminate. Formally, the probability of termination is captured by the probability of the set of runs reaching a terminated state, in the DTMC modeling the probabilistic semantics of a CGF system. Probabilistic termination (and more general probabilistic reachability properties) cannot be observed through stochastic simulation techniques given that their validation requires an exhaustive exploration of the model to be analyzed.

We propose an approximation technique for probabilistic termination of CGF which is based on the *abstract interpretation* [17, 18] approach. Therefore, the set of experiments for a biological system is modeled by an abstract CGF system where the information about the multiplicities of reagents, present in a solution, is approximated by means of intervals of integers [16]. Moreover, the abstract probabilistic model for the set of experiments is obtained through a systematic and effective approximation of the semantics. The abstract probabilistic model for an abstract CGF system satisfies two important properties: it *safely approximates* all DTMCs that model the probabilistic semantics of a concrete CGF system which is represented by the abstract one; and it gives lower and upper bounds for probabilistic termination which are *conservative* w.r.t. the set of experiments which are approximated.

The complete methodology is illustrated in Fig. 1. In the concrete case, the probabilistic semantics (DTMC) of a CGF system is derived from a *Labeled Transition System* (LTS) semantics (this is represented by function $\mathbf{H}$ depicted in Fig. 1). In the LTS, transition labels record a label (identifying the reaction) and the corresponding rate. In a standard way, for each state the probability of a move is calculated from the the rate of the move and from the rate of all the moves exiting from the state.

In the abstract case, the approximated semantics is obtained in a similar way through the definition of an abstract LTS semantics for abstract CGF systems and the derivation of a corresponding abstract probabilistic semantics (this is represented by function $\mathbf{H}^\circ$ in Fig. 1).

It is well-known that models combining probabilistic and non-deterministic

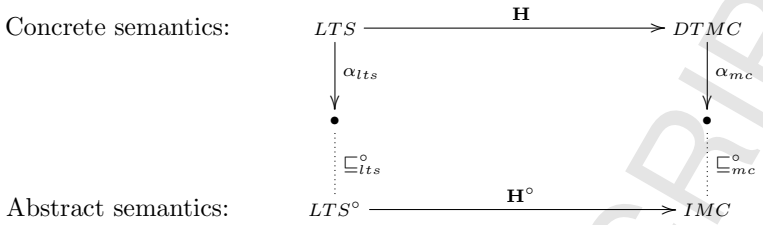


Figure 1: The complete picture

steps, are particularly adequate for abstracting probabilistic models such as DTMC. In these models, each state has associated a set of probability distributions, reflecting the non-determinism introduced by the abstraction over the state space. In MDP [22, 23, 1] each state has associated a set of probability distributions, describing the probability to move in any other state. Analogously, in *Interval Markov Chains* [51, 24, 32], each move has associated an interval of probability, representing a possible range for the probability of that move. In both cases, the validation of probabilistic temporal properties reports *lower* and *upper* bounds, rather than exact values. As expected, the lower and upper bounds are obtained by considering the worst-case and best-case scenario w.r.t. all non-deterministic choices, respectively.

Nonetheless, in our application to probabilistic termination the partition of the state space of the abstract probabilistic model is critical. As an example, we consider the two very simple DTMCs, illustrated in Fig. 2 (a) and (b), which have initial states S_0 and S'_0, respectively. In both cases, the system terminates with probability 1, that is it *universally terminates*. In order to reason on the abstraction of a set of DTMCs, it is convenient to built the *best abstraction* with respect to a given partition of the state space. The best abstraction is the abstract probabilistic model, which safely approximates both DTMCs and which is sound with respect to the property to be proved. Notice that in order to preserve probabilistic termination (and similarly probabilistic reachability properties) it must be the case that each abstract state has associated a set of probability distributions which over-approximates the concrete ones. We illustrate the abstraction which can be obtained using an MDP given that a model such as Interval Markov Chain presents similar problems in terms of precision.

The MDP[1] shown in Fig. 2 (c) is the best abstraction of the DTMCs, shown in Fig. 2 (a) and (b), by considering the partition of the concrete state space into the abstract states $\{S_0, S'_0\}$ and $\{S_1\}$. Actually, each abstract state has a

[1]For MDPs we use the notation of PRISM. In the figure there are two distributions for state $\{S_0, S'_0\}$: the first one is identified by the arrows exiting from $\{S_0, S'_0\}$ and labeled with **0** followed by colon and the probability of the transition, the second one by arrows labeled with **1**, while there is just one distribution for state $\{S_1\}$ identified by the arrow labeled **0**.

set of probability distributions which are precisely the union of the probability distributions, associated to each corresponding concrete state.

The validation of probabilistic termination over the abstract probabilistic model gives the following results: the *lower* and *upper* bound for the probability of reaching a terminated state, from the initial state $\{S_0, S_0'\}$, are 0 and 1 respectively. Notice that the lower bound is calculated by minimizing the probability of the computations reaching a $\forall$-*terminated* state, e.g. an abstract state which represents only terminated states. Conversely, the upper bound is calculated by maximizing the probability of the computations reaching a $\exists$-*terminated* state, e.g. an abstract state which represents at least a terminated state. In particular, the abstract state $\{S_1\}$ is $\forall$-terminated (and thus also $\exists$-terminated), while the abstract state $\{S_0, S_0'\}$ is $\exists$-terminated (but it is not $\forall$-terminated). As a consequence, the lower and upper bounds are obtained by choosing the probability distributions ρ_1 and ρ_0 for the initial state $\{S_0, S_0'\}$ respectively,

$$\begin{array}{ll} \rho_0(\{S_0, S_0'\}) = 0, & \rho_0(\{S_1\}) = 1 \\ \rho_1(\{S_0, S_0'\}) = 1, & \rho_1(\{S_1\}) = 0. \end{array}$$

Intuitively, the probability distribution ρ_0 models the move into the abstract state $\{S_1\}$ (which is $\forall$-terminated), while the probability distribution ρ_1 models the behaviour of the system which remains forever in the initial abstract state $\{S_0, S_0'\}$ (which is $\exists$-terminated). The distinction between $\exists$-terminated and $\forall$-terminated abstract states in the calculation of the lower and upper bound for probabilistic termination is necessary to safely approximate probabilistic termination and it is typical of abstract model checking techniques [51, 24, 32, 22, 23].

Even if the MDP of Fig. 2 (c) is the best abstraction of the DTMCs of Fig. 2 (a) and (b), the abstraction over the state space leads to a dramatic loss of information. The problem illustrated by the previous example is related to *hybrid* states, namely abstract states representing both concrete *terminated* and *non terminated* states. As it should be clear, the initial state $\{S_0, S_0'\}$ in the MDP of Fig. 2 (c) is precisely an hybrid state.

In order to validate in a more accurate way the property of probabilistic termination we define a methodology, where the hybrid states are eliminated from the abstract state space, by construction.

In the abstract LTS semantics the abstract states are abstract multisets where the multiplicity of reagents is approximated by intervals of integers. Moreover, the abstract transition labels record a label (identifying the reaction) as well as information about the possible rate of the reaction (represented by an interval of rates). The definition of the abstract transition relation uses a partitioning of hybrid states which guarantees that each abstract state approximates either terminated or non terminated concrete states. Due to the splitting of hybrid states, it may be the case that an abstract state has different exiting abstract transitions which share the same label. Such abstract transitions approximate the same reaction (identified by the label) for different concentrations of the reagents, which participate in the reaction. Thus, they approximate the

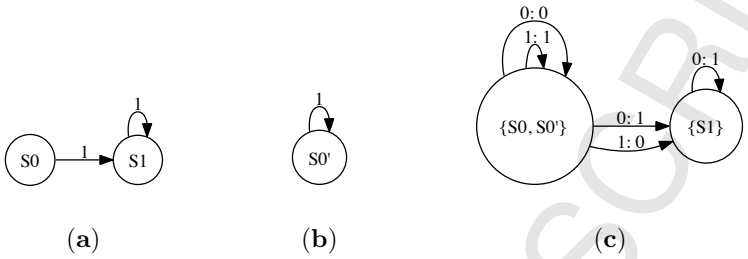


Figure 2: Two universally terminating DTMC's and an MDP that approximates them.

same reaction but for different concrete states which are represented by the abstract source state. This situation, which we call a *conflict* between abstract transitions, is explicitly captured by means of the labels corresponding to reactions.

The information about conflict recorded by the labels, corresponding to reactions, can be profitably exploited in order to limit the non-determinism introduced by the abstraction, in the derivation of the corresponding abstract probabilistic semantics. Intuitively, this information can be used to more precisely calculate the set of probability distributions, which can be assigned to each abstract state.

For these purposes, we adopt as abstract probabilistic model a generalization of standard Interval Markov Chains, called *Labeled Interval Markov Chains* (IMC), where moves are decorated by labels in addition to intervals of probability. Using labels, similarly as in the abstract LTS semantics, it is possible to maintain the information about the possible conflict between different moves from a given abstract state. The model IMC provides a more precise representation of the set of probability distributions which are associated to each abstract state with respect to the standard model using just intervals of probability.

In order to define the abstract probabilistic semantics of an abstract CGF we give a translation from abstract LTS into IMC (represented by function $\mathbf{H}^{\circ}$ in Fig. 1). The most difficult part of the derivation from abstract LTS into IMC consists of the computation of the interval of probability, corresponding to a move. We propose an effective technique where the intervals of probability are calculated from the information recorded on abstract transition labels: the abstract rates (intervals of rates) and the labels identifying the reactions. Intuitively, for each abstract state the interval of probability corresponding to a move is derived from the abstract rate of the move and from the abstract rates of the alternative moves from the considered abstract state. The information about conflict, recorded by the labels, is exploited to determine which moves from the abstract state may coexist in the concrete behaviour for one of the

concrete states which are represented by the abstract one. Moreover, we adopt a symbolic approach in the representation of intervals of rates which supports a more precise calculation of the corresponding intervals of probability given that it maintains relational information about the possible values of reagent variables.

Finally, we prove the soundness of the proposed approach with respect to probabilistic termination using standard abstract interpretation concepts. We prove both for the LTS and probabilistic semantics that their abstract versions *safely approximate* the corresponding concrete semantics. This shows that the abstract semantics of an abstract CGF system approximates the concrete semantics for each concrete CGF system, which is represented by the abstract one. The proof is based on the definition of approximation orders, both on the domain of abstract LTS and on the domain of IMC (represented by $\sqsubseteq^{\circ}_{lts}$ and $\sqsubseteq^{\circ}_{mc}$ in Fig. 1, respectively). In the style of [20, 22, 23, 51, 32], the approximation order allows us to compare two abstract semantics in terms of precision and thus to say when an abstract semantics is a safe approximation of another one. Moreover, the proof uses abstraction functions to relate the concrete semantics, both LTS and probabilistic, to their abstract versions (functions α_{lts} and α_{mc} in Fig. 1, respectively). The abstraction function both on the domain of LTS and on the domain of DTMC reports an abstract version which is equivalent to the concrete one.

Furthermore, we prove that the IMC of an abstract CGF system gives *conservative* lower and upper bounds for probabilistic termination. This guarantees that the interval of probability for probabilistic termination, calculated over the IMC of an abstract CGF system, includes the exact value of probabilistic termination, calculated over the DTMC, for each CGF system which is represented by the abstract one.

To validate the usefulness of our approach in the context of biological systems modeling, we apply abstract probabilistic model checking to verify probabilistic termination of a 2-way oscillator, in standard, partially doped and fully doped versions, in the style of [11, 3].

The paper is organized as follows. Section 2 introduces the CGF calculus, the LTS semantics, the model DTMC and the related probabilistic termination property, and the probabilistic semantics of CGF in terms of DTMC. Section 3 presents the formalization in CGF of the 2-way oscillator and illustrates probabilistic termination for the system. Section 4 presents the abstract LTS semantics. Section 5 introduces the model IMC and the related probabilistic termination property. Section 6 presents the abstract probabilistic semantics of CGF, that is the translation from abstract LTS into IMC. Finally, Section 7 shows the application of abstract probabilistic model checking to the 2-way oscillator, using PRISM.

Remark This paper is a revised and extended version of [28]. A related paper [15] presents a similar approach, which computes a weaker approximation, able to address probabilistic reachability properties. The analysis proposed here is also sound for general probabilistic reachability properties, following the arguments presented in [15].

E	$::= 0 \mid X = S,\ E$		Environment
S	$::= 0 \mid \pi^{\lambda}.P + S$		Molecules
P	$::= 0 \mid X \mid P$		Solutions
π	$::= {a_r}^{\lambda} \mid \overline{a}_r{}^{\mu} \mid {\tau_r}^{\theta}$	$a \in \mathcal{N}$ and $r \in \mathbb{R}^+$	Basic Actions

Table 1: Syntax of CGF

2. The Concrete Framework

The CGF calculus [12] is a fragment of stochastic π-calculus [46, 43] without communication. The calculus is designed for modeling basic chemical reactions, in particular *unary reactions* (a molecule may spontaneously degrade into components), *hetero binary reactions* (two molecules of different species may collide and produce other molecules) and *homeo binary reactions* (two molecules of the same species may collide and produce other molecules).

We present a Labeled Transition System semantics of CGF, which is a variant of that originally proposed in [12] (commented in Section 2.4). Then, we present the probabilistic model of DTMC and the related property of probabilistic termination. Finally, we introduce the probabilistic semantics of CGF in terms of DTMC.

2.1. Labeled Transition System Semantics

The syntax of (annotated) CGF is defined in Table 1. We consider a set $\mathcal{N}$ (ranged over by $a, b, c, \ldots$) of *names*, a set $\mathcal{L}$ (ranged over by $\lambda, \mu \ldots$) of *tags*, and a set $\mathcal{X}$ (ranged over by X,Y,....) of *variables* (representing reagents).

A CGF is defined as a pair (E, P) where E is a *species environment* and P is a *solution*. The environment E is a (finite) list of reagent definitions $X_i = S_i$ for distinct variables X_i and molecules S_i describing the interaction capabilities. A molecule S may do nothing, may change after a delay or may interact with other reagents. The interactions are defined by: ${\tau_r}^{\theta}$ representing a delay at rate r (where $r \in \mathbb{R}^+$ and $\theta \in \mathcal{L}$ is a tag); ${a_r}^{\lambda}$ and $\overline{a}_r{}^{\mu}$ modeling the input and output on channel a at rate r (where $r \in \mathbb{R}^+$ and $\lambda, \mu \in \mathcal{L}$ are tags), respectively. Each channel always has the same rate. A solution P is a parallel composition of variables, that is a finite list of reagents. The rates associated to basic actions are the parameters of the exponential distribution which regulates the stochastic behavior.

Notice that we annotate basic actions with tags $\lambda \in \mathcal{L}$. Tags are exploited in order to identify exactly the actions which participate in a move. For these purposes, we consider *well-formed* environments; an environment E is well-formed if the tags occurring in the definitions of E are all distinct. In the following, we assume that in a CGF (E, P) the environment E is well-formed and each variable X, occurring in E or in P, has a corresponding definition in E.

Given an environment E and a reagent variable $X \in \mathcal{X}$ we use $E(X)$ for denoting the molecule which defines X in E. Moreover, use $\pi^{\lambda}.P \in S$ to indicate

that process $\pi^{\lambda}.P$ appears in the molecule S (that is $S = \ldots + \pi^{\lambda}.P + \ldots$). In the following, $\mathcal{L}(S)$ and $\mathcal{L}(E)$ denote the set of tags appearing in the molecule S and in the environment E, respectively.

We introduce an LTS semantics for CGF where: solutions are represented as *multisets* and *transition labels* record a label, representing the tag of the basic action which participates in the move (or the tags of the basic actions which participate in the move), the number of occurrences of the related reagent variable (variables) and the rate of the basic action.

Definition 2.1 (Multiset). *A* multiset *is a function $M : \mathcal{X} \to \mathbb{N}$. We use $\mathcal{M}$ for the set of multisets.*

In the following, we call $M(X)$ the multiplicity of reagent X in the multiset M. We may also represent multisets as sets of pair (m, X), where m is the multiplicity of reagent X, using a standard notation, where pairs with multiplicity 0 are omitted.

For multisets we use standard operations of sum and difference, $\oplus$ and $\ominus$, such that $\forall M, N \in \mathcal{M}$, $\forall X \in \mathcal{X}$,

$$M \oplus N(X) = M(X) + N(X)$$
$$M \ominus N(X) = M(X) \mathbin{\widehat{-}} N(X) \quad \text{where } n \mathbin{\widehat{-}} m = \begin{cases} n - m & \text{if } n - m \geq 0, \\ 0 & \text{otherwise.} \end{cases}$$

Moreover, we define the translation of a solution P into a multiset of reagents $[\![P]\!]$ in the obvious way: $[\![0]\!] = \{\}$ and $[\![X|P]\!] = \{(1, X)\} \oplus [\![P]\!]$.

For describing the behavior of a solution (represented by a multiset of reagents) we adopt a labeled transition relation of the form

$$M \xrightarrow{\Theta, \Delta, r} M'$$

where $r \in \mathbb{R}^+$, $\Theta \in \widehat{\mathcal{L}} = \mathcal{L} \cup (\mathcal{L} \times \mathcal{L})$, $\Delta \in \widehat{Q} = \mathbb{N} \cup (\mathbb{N} \times \mathbb{N})$ such that $arity(\Theta) = arity(\Delta)$. The component $\Theta \in \widehat{\mathcal{L}}$ is a *label*, which describes the reaction and records either the tag of the action which changes after a delay (a unary reaction) or the pair of tags of the actions which synchronize (a binary reaction). The components $\Delta \in \widehat{Q}$ and $r \in \mathbb{R}^+$ give information needed for computing the rate of the reaction, that is the multiplicity of the reagent (reagents) which participates (participate) and the rate associated to the basic action.

The transition relation for multisets is defined by the rules Table 2, reasoning with respect to an environment E. There are two transition rules describing delay and synchronization, respectively. Rule (**Delay**) models the move of a process ${\tau_r}^{\lambda}.Q$ appearing in the definition of reagent X. The transition label records the tag λ together with the multiplicity of reagent X (e.g $M(X)$) as well as the rate of delay r. Rule (**Sync**) models the synchronization between two complementary processes ${a_r}^{\lambda}.Q_1$ and ${\bar{a}_r}^{\mu}.Q_2$ appearing in the definition of reagents X and Y (that may even coincide[2]). The transition label records the

[2]This is the case of homeo reactions.

$$(\textbf{Delay}) \quad \frac{\tau_r{}^{\lambda}.Q \in E(X)}{E \vdash M \xrightarrow{\lambda, M(X), r} (M \ominus (1, X)) \oplus [\![Q]\!]}$$

$$(\textbf{Sync}) \quad \frac{a_r{}^{\lambda}.Q_1 \in E(X) \qquad \bar{a}_r{}^{\mu}.Q_2 \in E(Y)}{E \vdash M \xrightarrow{(\lambda,\mu),(M(X),M(Y)),r} ((M \ominus (1, X)) \ominus (1, Y)) \oplus [\![Q_1]\!] \oplus [\![Q_2]\!]}$$

Table 2: Transition relation

tags λ and μ together with the multiplicities of reagents X and Y (e.g $M(X)$ and $M(Y)$) as well as the rate of the channel r.

Notice that we admit explicit transitions even for reactions involving reagent variables having multiplicity 0 in the multiset M (thus having rate 0). This choice simplifies the definition of the abstraction (as discussed in Section 2.4)

We recall that the environment is well-formed, e.g. basic actions have distinct tags. As a consequence, the transitions having a solution M as source have distinct labels too. More in detail, for each label $\Theta \in \widehat{\mathcal{L}}$ we may have *at most one* transition, decorated by label Θ, leaving from M. We therefore adopt the following definition of LTS.

Definition 2.2 (LTS). *A* labeled transition system *is a tuple* $(S, \rightarrow, M_0, E)$ *where:*

i) $S \subseteq \mathcal{M}$ *is the set of states,* $M_0 \in S$ *is the initial state and* E *is the environment;*

ii) $\rightarrow \subseteq S \times \widehat{\mathcal{L}} \times \widehat{Q} \times \mathbb{R}^+ \times S$ *is a set of transitions, such that, for each* $M \xrightarrow{\Theta,\Delta_1,r_1} M_1, M \xrightarrow{\Theta,\Delta_2,r_2} M_2$*, we have* $\Delta_1 = \Delta_2$*,* $r_1 = r_2$ *and* $M_1 = M_2$*.*

In the following, we use $\mathcal{LTS}$ to denote the set of LTS. The semantics of a multiset M_0 is defined as $\mathsf{LTS}((E, M_0)) = (S, \rightarrow, M_0, E)$, which denotes the LTS, obtained by transitive closure, starting from the initial state M_0, using the rules of Table 2 w.r.t. the environment E. The LTS describing the semantics of a CGF (E, P) is defined by $\mathsf{LTS}((E, [\![P]\!]))$.

Moreover, given a transition $t = M \xrightarrow{\Theta,\Delta,r} M'$ we use $\mathsf{label}(t)$ to denote the label Θ, and $\mathsf{source}(t), \mathsf{target}(t)$ to denote its source and target states M and M', respectively. Similarly, for a set of transitions TS, we use $\mathsf{label}(TS) = \bigcup_{t \in TS} \mathsf{label}(t)$. We also use

$$\begin{aligned} \mathsf{Ts}(M, M') = &\ \{t \mid \mathsf{source}(t) = M \text{ and } \mathsf{target}(t) = M'\} \\ \mathsf{Ts}(M) = &\ \{t \mid \mathsf{source}(t) = M\} \end{aligned}$$

for describing the transitions from a multiset M to a multiset M' and all transitions leaving from multiset M, respectively.

2.2. Discrete-Time Markov Chains

We introduce the probabilistic model of DTMC and we define the property of probabilistic termination. Given a finite or countable set of states $S \subseteq \mathcal{M}$ we denote with

$$\begin{aligned}&\mathsf{SDistr}(S) = \{\rho \mid \rho\colon S \to [0,1]\},\\ &\mathsf{Distr}(S) = \{\rho \mid \rho \in \mathsf{SDistr}(S) \text{ and } \textstyle\sum_{M\in S} \rho(M) = 1\}\end{aligned}$$

the set of (discrete) probability *pseudo-distributions* and of *distributions* on S, respectively.

Definition 2.3 (DTMC). *A DTMC is a tuple* $(S, \mathbf{P}, \mathbf{L}, M_0)$ *where:*

i) $S \subseteq \mathcal{M}$ *is a* finite or countable *set of states and* $M_0 \in S$ *is the initial state;*

ii) $\mathbf{P}\colon S \to \mathsf{Distr}(S)$ *is the* probability transition function*;*

iii) $\mathbf{L} : S \to (S \to \wp(\widehat{\mathcal{L}}))$ *is a* labeling function *such that* $\mathbf{L}(M)(M') \cap \mathbf{L}(M)(M'') = \emptyset$ *if* $M' \neq M''$.

In DTMC state transitions are equipped with probabilities, specifically $\mathbf{P}(M)(M')$ reports the probability of moving from state M to state M'. In addition, $\mathbf{L}(M)(M') \in \wp(\widehat{\mathcal{L}})$ reports the set of labels corresponding to the move from state M to state M'. Notice that the labels have no semantic significance here, while they are exploited to simplify the abstraction (see Section 2.4).

In the following, we restrict our attention to *finitely branching* DTMC, meaning that for each state $M \in S$ the set $\{M' \mid \mathbf{P}(M)(M') > 0\}$ is finite. We use $\mathcal{MC}$ for the set of (finitely branching) DTMC.

We are interested in *probabilistic termination*, that is on the probability to reach a state that is *terminated*. Probabilistic termination is given by the probability of the set of terminated paths, which can be calculated by considering a probability space over paths of the DTMC [35].

Given a DTMC $(S, \mathbf{P}, \mathbf{L}, M_0)$, a path π is a non-empty sequence of states of S. We denote the i-th state in a path π by $\pi[i]$, and the length of π by $|\pi|$. The set of paths over S is denoted by $\mathsf{Paths}(S)$. The set of finite paths over S is denoted by $\mathsf{FPaths}(S)$. $C(M)$ denotes the set of paths starting from the state $M \in S$ and $C(\pi)$, with $\pi \in \mathsf{FPaths}(S)$, denotes the set of paths that have the finite path π as prefix.

Definition 2.4 (Probability of paths). *Let* $(S, \mathbf{P}, \mathbf{L}, M_0)$ *be a DTMC. Let* $\mathcal{C} = \bigcup_{\pi\in\mathsf{FPaths}(S)} C(\pi)$ *be the cylinders,* $\mathcal{B}$ *be the smallest* σ*-algebra containing* $\mathcal{C}$*, and* $M \in \mathcal{M}$ *a state. The tuple* $(\mathsf{Paths}(S), \mathcal{B}, \mathbf{P}_M)$ *is a probability space, where* $\mathbf{P}_M$ *is the unique measure satisfying, for all path* $M_0 \dots M_n$*,*

$$\mathbf{P}_M(C(M_0 \dots M_n)) = \begin{cases} 1 & \text{if } M_0 = M \wedge n = 0\\ \mathbf{P}(M_0, M_1) \cdot \ldots \cdot \mathbf{P}(M_{n-1}, M_n) & \text{if } M_0 = M \wedge n > 0\\ 0 & \text{otherwise}\end{cases}$$

Given a DTMC $(S, \mathbf{P}, \mathbf{L}, M_0)$, we say that a state $M \in S$ is *terminated* iff $\mathbf{P}(M)(M') = 0$, for each $M' \in S$ with $M' \neq M$. A path is *terminated* if it leads to a terminated state.

Definition 2.5 (Probabilistic termination). *Let $mc = (S, \mathbf{P}, \mathbf{L}, M_0)$ be a DTMC. The probability of reaching a* terminated state*, from $M \in S$, is*

$$\mathsf{Reach}_{mc}(M) = \mathbf{P}_M(\{\pi \in C(M) \mid \quad \pi[\,|\pi|\,] \textit{ is terminated } \}).$$

Since the set of paths of Definition 2.5 is a set of finite paths and the DTMCs that we consider are finitely branching, the set of paths of Definition 2.5 is countable. Indeed, it can be seen as $\bigcup_i \{\pi \mid \pi[\,|\pi|\,] \text{ is terminated and } |\pi| = i\}$.

It is worth mentioning that $\mathsf{Reach}_{mc}(M)$ can be specified as a linear equation system, similarly as for standard probabilistic reachability properties of the logic PCTL. The system can be solved either by applying direct methods or by computing the least fixpoint by means of standard iterative methods. For more detail on probabilistic model checking we refer the interested reader to [38, 31, 36].

In order to simplify the proofs, it is convenient to exploit the following formulation of $\mathsf{Reach}_{mc}(M)$ as a fixpoint equation. Let $mc = (S, \mathbf{P}, \mathbf{L}, M_0)$ be a DTMC. Let us define the following order on pseudo-distributions $\rho_1, \rho_2 \in \mathsf{SDistr}(S)$, we say that $\rho_1 \subseteq \rho_2$ iff for each $M \in S$, $\rho_1(M) \leq \rho_2(M)$. $\cup$ stands for the least upper bound with respect to the underlying order $\subseteq$.

For each $i \in \mathbb{N}$, we define a pseudo-distribution on S, $\rho^i_{mc} \in \mathsf{SDistr}(S)$, where for each $M \in S$,

$$\rho^i_{mc}(M) = \begin{cases} 1 & \text{if } M \text{ is terminated,} \\ 0 & \text{if } i = 0 \wedge M \text{ is non-terminated,} \\ \Sigma_{M' \in S} \mathbf{P}(M)(M') \cdot \rho^{i-1}_{mc}(M') & \text{otherwise.} \end{cases}$$

Intuitively, $\rho^i_{mc}(M)$ reports the probability to reach a terminated state, starting from M, after at most i steps. Note that $\forall i$, $\rho^i_{mc} \subseteq \rho^{i+1}_{mc}$, this can be proved by induction on i. Since the set of *pseudo-distributions* on S constitutes a complete lattice, there exists the least fixpoint,

$$\mathsf{Reach}_{mc}(M) = \bigcup_{i \in \{0,\ldots,\infty\}} \rho^i_{mc}(M)$$

2.3. Probabilistic Semantics

We define the probabilistic semantics of CGF, by giving a translation from LTS into DTMC. In order to calculate the probability of moving from a state M to a state M' we proceed as follows: (i) we extract the rate corresponding to the move by exploiting the rate of each transition included in $\mathsf{Ts}(M, M')$; (ii) then, we calculate the related probability taking into account the rate of all the transitions exiting from M (contained in $\mathsf{Ts}(M)$).

Let $(S, \rightarrow, M_0, E)$ be an LTS. We introduce functions rate, going from transitions $\rightarrow$ to $\mathbb{R}^{>=0}$, $\mathbf{R} : S \times S \rightarrow \mathbb{R}^{>=0}$ and $\mathbf{E} : S \rightarrow \mathbb{R}^{>=0}$ such that, for each $t = M \xrightarrow{\Theta,\Delta,r} M' \in \rightarrow$ and $M, M' \in S$,

$$\mathsf{rate}(t) = \begin{cases} n \cdot r & \Theta = \lambda,\ \Delta = n, \\ n \cdot (m \widehat{-} 1) \cdot r & \Theta = (\lambda, \mu),\ \Delta = (n, m),\ \lambda, \mu \in \mathcal{L}(E(X)), \\ n \cdot m \cdot r & \Theta = (\lambda, \mu),\ \Delta = (n, m), \\ & \lambda \in \mathcal{L}(E(X)), \mu \in \mathcal{L}(E(Y)), X \neq Y, \end{cases}$$

$$\mathbf{R}(M, M') = \textstyle\sum_{t \in \mathsf{Ts}(M,M')} \mathsf{rate}(t), \qquad \mathbf{E}(M) = \textstyle\sum_{M'' \in S} \mathbf{R}(M, M'').$$

As expected rate of a transition $\mathsf{rate}(\mathrm{t})$ is derived from the information recorded on its transition label. For computing $\mathsf{rate}(t)$ it is necessary to take into account the number of distinct transitions t that may occur in the multiset M. Thus, the result depends on the rate r of the basic action, on the multiplicities of the reagents which participate (recorded by Δ) and on the type of reaction (unary or binary) (recorded by Θ). If label Θ is a singleton then the rate is obtained by multiplying r with the number of occurrences of the reagent variable X, that is n. If label Θ is a pair, corresponding to an interaction between two distinct reagents X and Y, then the rate is obtained by multiplying r with the number of occurrences of both reagent variables, that is n and m. If X and Y coincide the calculation is similar taking into account that each occurrence of reagent X cannot interact with itself. Notice that the resulting rate may even be zero. This is the case, for example, whenever two reagents X and Y interact and one of the two has multiplicity zero; or whenever a reagent X with multiplicity 1 interacts with X itself.

Moreover, $\mathbf{R}(M, M')$ reports the rate corresponding to the move from M to M', while $\mathbf{E}(M)$ is the *exit rate*. The probability of moving from M to M' is computed from $\mathbf{R}(M, M')$ and from the exit rate $\mathbf{E}(M)$, in a standard way.

Definition 2.6 (Derivation of the DTMC). *We define the* probabilistic translation *function* $\mathbf{H} : \mathcal{LTS} \rightarrow \mathcal{MC}$ *such that* $\mathbf{H}((S, \rightarrow, M_0, E)) = (S, \mathbf{P}, \mathbf{L}, M_0)$, *where*

1. $\mathbf{P} : S \rightarrow \mathsf{Distr}(S)$ *is the* probability transition function*, such that for each* $M, M' \in S$*:*
   - **a)** *if* $\mathbf{E}(M) > 0$*, then* $\mathbf{P}(M)(M') = \mathbf{R}(M, M')/\mathbf{E}(M)$*;*
   - **b)** *if* $\mathbf{E}(M) = 0$*, then* $\mathbf{P}(M)(M) = 1$ *and* $\mathbf{P}(M)(M') = 0$ *for* $M' \neq M$*.*
2. $\mathbf{L} : S \rightarrow (S \rightarrow \wp(\widehat{\mathcal{L}}))$ *is the* labeling function*, such that, for each* $M, M' \in S$*,* $\mathbf{L}(M, M') = \mathsf{label}(\{t \in \mathsf{Ts}(M, M') \mid \mathsf{rate}(t) > 0\})$.

Notice that in the translation the labels are transferred from the transitions of the LTS to the DTMC. Due to the particular labeling of the LTS semantics, also the DTMC, modeling the probabilistic semantics of a CGF process, satisfies the property that all the moves leaving from a state, are decorated by disjoint sets of labels.

2.4. Abstract Interpretation

It is worth mentioning that in the Abstract Interpretation [17, 18] approach to static analysis the choice of the concrete semantics is crucial. On one hand, the concrete semantics typically influences the precision of the abstraction. On the other hand, the abstract semantics has to be proved correct with respect to the concrete version. Thus, it is convenient to adopt similar definitions both in the concrete and in the abstract case. In our framework, this argument applies both to the LTS semantics and to the probabilistic semantics.

As far as it concerns the LTS semantics, we have adopted an LTS semantics where: the environment is annotated, the solutions are represented by multisets and transition labels record a label (representing the tags of the actions which participates in the move), the number of occurrences of the related reagent variables and the rate of the basic action.

Such a semantics permits to prove in a simpler way the soundness of the abstract LTS semantics. Specifically, the definition of function α_{lts} used to relate concrete and abstract LTS and the proof of soundness (Theorem 4.14). Moreover, using an explicit representation of transitions having rate 0 simplifies the definition of the approximation order $\sqsubseteq^{\circ}_{lts}$ over abstract LTS.

Furthermore, since environments are well-formed the LTS semantics has a particular labeling, as it is formalized by condition (ii) of Definition 2.2. This is essential for capturing in the abstract case the conflict between abstract transitions. We also record on transition labels information about the multiplicity of reagents and about the rate of the action in place of the rate of the transition (that is $\mathsf{rate}(t)$). In the abstract case, this approach permits to maintain relational information about the possible multiplicity of reagent variables. Both features are profitably exploited in order to derive a more precise probabilistic semantics, in particular they are used to limit the loss of information in the calculation of the abstract probabilities (as it is commented in Sections 5 and 6).

Analogously in the case for the probabilistic semantics we adopt a labeled version of DTMC in order to simplify the correspondence with the probabilistic abstract model. Specifically, such a modification simplifies the definition of function α_{MC} used to relate concrete and abstract probabilistic models and the proof of soundness (Theorems 6.4 and 6.5).

The LTS semantics originally proposed in [12] was simpler. The approach uses a normal form for solutions and environments, based on indexing both the basic actions and the occurrences of reagent variables (even of the same variable). Transition labels record the index of the action (the indexes of the actions) participating in the move and the associated rate, similarly as in our definition. The main difference with our definition is that in that case each transition describes exactly the delay of a given instance of a reagent variable X or the synchronization between two instances of reagent variables X and Y. However, the corresponding probabilistic semantics in terms of DTMC is equivalent given that the rates of different transitions, modeling the same reaction, are summed in order to derive the related probabilities.

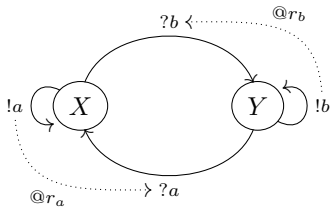


Figure 3: Groupie stochastic interacting automaton

3. A 2-way Oscillator

To illustrate probabilistic termination we consider a biochemical system that exhibits an oscillatory behavior. The system, presented in [13], is composed by a set of entities interacting with each other. The behavior of a single entity can be represented by the stochastic interacting automaton in Fig. 3; it has two possible states, X and Y. A single automaton performs no interaction, while it may interact with other automata. Two automata in state X are stable since they both offer $!a$ and $?b$ and no interaction is possible. Analogously for two automata in state Y. If one automata is in state X and another is in state Y then *either* they can interact on channel a at rate r_a, and both move to state X, *or* they can interact on channel b at rate r_b, and both move to state Y. Such automata are called *groupies* because they aim to be similar: two automata in different states switch to equal states. The system exhibits an oscillatory behavior in the number of X and Y. However, when the groupies form a single homogeneous population of all X or of all Y the system is terminated: no automaton can further change state.

The following example shows a possible formalization of the system in CGF.

Example 3.1. *The following environment models the 2-way oscillator,*

$$E \triangleq \quad X = a_r^{\lambda}.X + \bar{b}_r^{\delta}.Y, \quad Y = \bar{a}_r^{\mu}.X + b_r^{\eta}.Y.$$

Reagents X and Y may interact together in two possible ways: either *along channel a* or *along channel b (we assume that both reactions have the same rate r). The former case models the reaction $R_1 : X + Y \to X + X$, while the latter case models the reaction $R_2 : X + Y \to Y + Y$.*

By considering the CGF (E, M_3) with initial solution $M_3 = \{(3, X), (3, Y)\}$ we obtain the LTS $\mathsf{LTS}((E, M_3))$ illustrated in Fig. 4 where

$$M_2 = \{(2, X), (4, Y)\} \quad M_1 = \{(1, X), (5, Y)\} \quad M_0 = \{(6, Y)\}$$
$$M_4 = \{(4, X), (2, Y)\} \quad M_5 = \{(5, X), (1, Y)\} \quad M_6 = \{(6, X)\}$$

and , for simplicity, we have omitted the transitions having at least one multiplicity equal to 0. Note that this simplification will be adopted in all the examples of the paper.

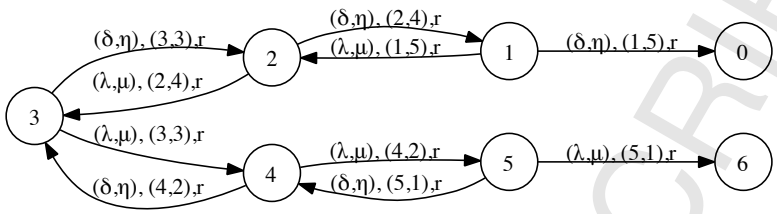


Figure 4: The LTS semantics

The LTS reports for each state, except for states M_0 and M_6, two transitions: the move with label (λ, μ) models reaction R_1, while the move with label (δ, η) models reaction R_2. The transitions record also the multiplicities of reagents X and Y, in each state, and the rate of basic actions r.

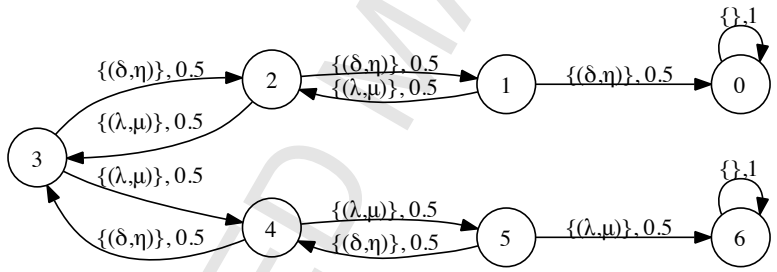


Figure 5: The DTMC

Fig. 5 illustrates the DTMC $\mathbf{H}(\mathsf{LTS}((E, M_3)))$ *derived from the LTS of Fig. 4, where we have omitted the transitions having rate equal to 0. Note that this simplification will be adopted in all the examples of the paper.*

As expected, states M_0 and M_6 are terminated, while the other states have two possible moves corresponding to reactions R_1 and R_2 which happen with the same probability. The probability to reach a terminated state from the initial solution M_3 is exactly 1, showing a null probability to oscillate forever (thus the system universally terminates).

□

In the previous example we have considered a simple experiment for a small number of reagents X and Y and we have proved that the system *universally*

terminates. It should be clear that an analogous probabilistic behavior can be generalized to any initial concentration of reagents X and Y. Actually, the concentrations of reagents X and Y modify the rate of reactions R_1 and R_2 but not their probabilities. Thus, no matter how many reagents X and Y are present in the initial solution, the system universally terminates. A similar argument also applies to the experiments realized by varying the rate of the two reactions.

Notice that the initial concentration of reagents X and Y as well as the rates of the reactions have a great impact on the amplitude of oscillations and the time required by the oscillation to stop. The observation of these properties requires to consider the Continuos-Time Markov Chain (in place of the DTMC) and a continuos-time logic (such as CSL [29, 36]), as it is discussed in [3] for similar oscillators.

Probabilistic model checking can also be applied to validate other *probabilistic reachability properties* of the 2-way oscillator which yield a better understanding of the dynamics of the system. For example, it is interesting to be able to calculate the probability that the groupies form an homogeneous population of all X or of all Y. For the initial concentrations of reagents X and Y considered in Example 3.1, this is the probability to reach states M_6 and M_0, respectively; thus, in this example where the initial concentrations of X and Y are equal, the two configurations can be reached with the same probability $\frac{1}{2}$. Note, however, that the probability of reaching one of the two configurations strictly depends on the initial concentrations of reagents X and Y, therefore, in the general case the probability that the groupies form an homogeneous population of all X or of all Y can be different.

There has been considerable success recently in analyzing biological systems using tools based on formal methods. The approach based on quantitative model checking is exhaustive, that is all possible evolutions of the system are analyzed. This formal verification technique has been applied to address a wide class of quantitative behavioral queries about the dynamics of biological models. The principal alternative relies on the application of simulation-based techniques. The discrete stochastic approach, based on SSA [26], allows to observe possible evolutions of a biochemical system, whose rates are controlled by exponential distributions. Traditionally, time-dependent analysis of biological systems uses a deterministic approach based on ordinary differential equations (ODE).

The probability of termination (as well as the probability to reach a given configuration) cannot be inferred by applying discrete stochastic simulation techniques, even by performing a large number of simulation runs. As it is illustrated [11, 3, 2], these techniques are adequate for capturing other fundamental aspects about the dynamics of biochemical systems, which exhibit an oscillatory behavior. Specifically, it is possible to deduce information about the amplitude and regularity of the oscillations over time. The deterministic approach, based on ODE, can give different results by considering the same initial conditions. Cardelli [11] shows that the ODE extracted from automaton of Fig. 3 describes a deterministic never stopping oscillator.

The relationship between deterministic and stochastic simulation techniques for biological systems is still subject to research. In particular, [3, 11] investi-

gate the application of these approaches to more complex variant of the 2-way oscillator, described by the automaton of Fig. 3.

4. Abstract Labeled Transition System Semantics

We introduce the abstract LTS semantics which is based on the abstraction of multisets, proposed in [15], where the multiplicities of reagents are approximated by intervals of integers [16]. Moreover, we prove the soundness of the abstract LTS w.r.t. the concrete LTS. In the style of [20], an approximation order over abstract LTS is used for expressing precision and soundness of approximations.

4.1. Abstract States

We present the abstract states and we formalize the relation with multisets as a standard Galois connection [18]. In order to approximate the information related to the multiplicities of reagents present in a solution we adopt the domain of intervals of integers [16]. In more detail, we adopt

$$\mathcal{I} = \{[m, n] \mid m \in \mathbb{N}, n \in \mathbb{N} \cup \{\infty\}, \text{ if } m \neq \infty \text{ then } m \leq n\}.$$

Note that intervals can never be empty. Over intervals we consider the order $\sqsubseteq_I$, defined as $[m, n] \sqsubseteq_I J$ iff $m, n \in J$. The least upper bound on $\mathcal{I}$, denoted here by $\sqcup_I$, is the union of intervals. Moreover, the order $\sqsubseteq_I$ extends naturally to pairs of intervals; i.e. for intervals $I_i, J_i \in \mathcal{I}$ with $i \in \{1, 2\}$, $(I_1, I_2) \sqsubseteq_I (J_1, J_2)$ iff $I_1 \sqsubseteq_I J_1$ and $I_2 \sqsubseteq_I J_2$.

Over intervals $\mathcal{I}$ we use the following operations of sum and difference, for $I, J \in \mathcal{I}$ with $max(J) \neq \infty$,

$$I + J = \begin{cases} [min(I) + min(J), max(I) + max(J)] & \text{if } max(I) \neq \infty, \\ [min(I) + min(J), \infty] & \text{otherwise.} \end{cases}$$

$$I - J = \begin{cases} [min(I) \widehat{-} max(J), max(I) \widehat{-} min(J)] & \text{if } max(I) \neq \infty, \\ [min(I) \widehat{-} max(J), \infty] & \text{otherwise.} \end{cases}$$

Note the use of the $max(J)$ in computing the minimum of the interval $I - J$ and, analogously, and the use of the $min(J)$ in computing the maximum.

The abstract states are abstract multisets where multiplicities are replaced by intervals of multiplicities.

Definition 4.1 (Abstract states). *An* abstract state *is a function $M^\circ : \mathcal{X} \to \mathcal{I}$. We also use $\mathcal{M}^\circ$ for the set of abstract states.*

Over abstract states, we introduce abstract operations of sum and difference, such that $\forall M^\circ, N^\circ \in \mathcal{M}^\circ$, $\forall X \in \mathcal{X}$,

$$(M^\circ \oplus^\circ N^\circ)(X) = M^\circ(X) + N^\circ(X), \quad (M^\circ \ominus^\circ N^\circ)(X) = M^\circ(X) - N^\circ(X).$$

In the following we use $M^\circ[I/X]$ for denoting the abstract state obtained from M° replacing the abstract multiplicity of reagent $X \in \mathcal{X}$ with the interval $I \in \mathcal{I}$.

Since an interval represents a set of multiplicities, it is immediate to define the following approximation order over abstract states.

Definition 4.2 (Order on states). *Let $M_1^\circ, M_2^\circ \in \mathcal{M}^\circ$, we say that $M_1^\circ \sqsubseteq^\circ M_2^\circ$ iff, for each reagent $X \in \mathcal{X}$, $M_1^\circ(X) \sqsubseteq_I M_2^\circ(X)$.*

Obviously, given a multiset M there exists an abstract multiset which is its best (most precise) approximation.

Definition 4.3 (Best approximation). *The best approximations of a multiplicity $n \in \mathbb{N}$, of a pair of multiplicities $(n, m) \in \mathbb{N} \times \mathbb{N}$ and of a multiset $M \in \mathcal{M}$, are denoted by the symbol $\bullet$ and are defined as follows:*

1. $n^\bullet = [n, n]$,
2. $(n, m)^\bullet = (n^\bullet, m^\bullet)$,
3. $\forall X \in \mathcal{X}, M^\bullet(X) = M(X)^\bullet$.

The relation between sets of multisets and abstract states is formalized as a Galois connection [18]. The *abstraction function* $\alpha : \mathcal{P}(\mathcal{M}) \to \mathcal{M}^\circ$ reports the *best approximation* for each set of multisets S; that is, the abstract state obtained as the least upper bound (denoted by $\sqcup^\circ$) of the best approximations of each $M \in S$. Its counterpart is the *concretization function* $\gamma : \mathcal{M}^\circ \to \mathcal{P}(\mathcal{M})$ which reports the set of multisets represented by an abstract state. For example, the abstract multiset $\{([1, 2], X)\}$ represents the set of multisets $\{(1, X), (2, X)\}$.

Definition 4.4. *We define $\alpha : \mathcal{P}(\mathcal{M}) \to \mathcal{M}^\circ$ and $\gamma : \mathcal{M}^\circ \to \mathcal{P}(\mathcal{M})$ such that, for each $S \in \mathcal{P}(\mathcal{M})$ and $M^\circ \in \mathcal{M}^\circ$:*

1. $\alpha(S) = \bigsqcup^\circ_{M \in S} M^\bullet$;
2. $\gamma(M^\circ) = \{M' \mid M'^\bullet \sqsubseteq^\circ M^\circ\}$.

The abstraction and concretization functions are a Galois connection.

Theorem 4.5. *The pair (α, γ) is a* Galois connection *between $(\mathcal{P}(\mathcal{M}), \subseteq)$ and $(\mathcal{M}^\circ, \sqsubseteq^\circ)$.*

The proof of Theorem 4.5 is straight-forward and can be found in AppendixA.

4.2. Abstract transitions

We adopt an abstract transition relation of the form

$$M_1^\circ \xrightarrow[\circ]{\Theta, \Delta^\circ, r} M_2^\circ$$

where $\Theta \in \widehat{\mathcal{L}} = \mathcal{L} \cup (\mathcal{L} \times \mathcal{L})$, $\Delta^\circ \in \widehat{Q}^\circ = \mathcal{I} \cup (\mathcal{I} \times \mathcal{I})$, with $arity(\Theta) = arity(\Delta^\circ)$, and $r \in \mathbb{R}^+$. Similarly as in the concrete case, $\Theta \in \widehat{\mathcal{L}}$ is a *label* which describes

the reaction and records either the tag of the action which changes after a delay (a unary reaction) or the pair of tags of the actions which synchronize (a binary reaction). The component $\Delta^\circ \in \widehat{Q}^\circ$ is either an *interval* or a *pair of intervals*, representing the possible multiplicity of the reagent (reagents) which participates (participate) in the reaction. As in the concrete case, $r \in \mathbb{R}^+$ is the rate of the basic action.

In a naive approach (as the one proposed in [15]) an abstract transition is intended to approximate *all the concrete moves*, corresponding to the reactions associated to label Θ, for each multiset M_1 approximated by the abstract state M_1°. This means that each concrete transition $M_1 \xrightarrow{\Theta,\Delta,r} M_2$ is such that: the multiplicity (multiplicities) Δ is included in the interval (intervals) Δ° and M_2 is approximated by the abstract state M_2°.

To illustrate the approach of [15], we can consider the environment E commented in Example 3.1 which models reactions $R_1 : X + Y \to X + X$ and $R_2 : X + Y \to Y + Y$,

$$E \triangleq \quad X = a_r^\lambda.X + \bar{b}_r^\delta.Y, \quad Y = \bar{a}_r^\mu.X + b_r^\eta.Y.$$

Moreover, we consider a simple experiment represented by the abstract state

$$M_5^\circ = \{([1,3], X), ([1,3], Y)\}.$$

The abstract state M_5° describes a set of 9 experiments; thus, the abstract semantics has to model the system described by E w.r.t. all different initial concentrations. For example, for approximating reaction R_1, that is the synchronization between X and Y along channel a, we would obtain the following abstract transition labeled (λ, μ),

$$M_5^\circ \xrightarrow[\circ]{(\lambda,\mu),([1,3],[1,3]),r} M_5^{\circ\prime} \tag{1}$$

with $M_5^{\circ\prime} = \{([2,4], X), ([0,2], Y)\}$. In this way, however, the abstract transition (1) introduces an *hybrid* state the abstract state $M_5^{\circ\prime}$ representing both terminated states, where the concentration of reagent Y is zero and therefore no reaction can longer be applied, and non-terminated states, where reagent Y is still available.

It should be clear that the moves corresponding to reaction R_1 could be better approximated by adopting two different abstract transitions, such as

$$M_5^\circ \xrightarrow[\circ]{(\lambda,\mu),([1,3],[1,1]),r} M_6^\circ \tag{2}$$

$$M_5^\circ \xrightarrow[\circ]{(\lambda,\mu),([1,3],[2,3]),r} M_7^\circ \tag{3}$$

where $M_6^\circ = \{([2,4], X), ([0,0], Y)\}$ and $M_7^\circ = \{([2,4], X), ([1,2], Y)\}$. Using the abstract transitions (2) and (3), the moves corresponding to reaction R_1 represented by (1) are split and the hybrid state is eliminated. Notice that the transitions (2) and (3) share label (λ, μ) which identifies the reaction R_1.

In order to better handle probabilistic termination, we introduce here a refinement of the LTS semantics, presented in [15], where hybrid states are eliminated, following the ideas illustrated by the previous example. Notice that abstract transitions and (2) and (3) can be obtained from transition (1), by splitting the target state $M_5^{\circ\prime}$ and the interval of multiplicity for reagent variable Y, recorded in the abstract transition label of (1).

Table 3 presents the abstract transition rules, reasoning with respect to an environment E. Such rules can be thought as obtained by a two-steps process. First, a simple version of the abstract transition is obtained similarly as the corresponding concrete ones, by replacing multiplicities with intervals of multiplicities and the operations of sum and difference with their abstract versions $\oplus^\circ$ and $\ominus^\circ$. Then, the resulting abstract transition is refined in order to avoid hybrid states.

(**Delay-a**) $$\frac{\tau_r{}^{\lambda}.Q \in E(X)}{E \vdash M^\circ \xrightarrow[\circ]{\lambda, I_x, r} M_1^\circ}$$

where

$$M_1^\circ \in \ \bigtriangledown_E^{\mathcal{M}}((M^\circ \ominus^\circ \{(1^\bullet, X)\}) \oplus^\circ [\![Q]\!]^\bullet) \quad \text{and}$$
$$I_x = \ \bigtriangledown^{\mathcal{T}}(M^\circ(X), 1^\bullet, [\![Q]\!]^\bullet(X), M_1^\circ(X)).$$

(**Sync-a**) $$\frac{a_r{}^{\lambda}.Q_1 \in E(X) \qquad \bar{a_r}{}^{\mu}.Q_2 \in E(Y)}{E \vdash M^\circ \xrightarrow[\circ]{(\lambda,\mu),(I_x,I_y),r} M_1^\circ}$$

where, for $Z \in \{X, Y\}$,

$$M_1^\circ \in \ \bigtriangledown_E^{\mathcal{M}}(((M^\circ \ominus^\circ \{(1^\bullet, X)\}) \ominus^\circ \{(1^\bullet, Y)\}) \oplus^\circ [\![Q_1]\!]^\bullet \oplus^\circ [\![Q_2]\!]^\bullet) \text{ and}$$
$$I_Z = \ \bigtriangledown^{\mathcal{T}}(M^\circ(Z), ((1^\bullet, X) \oplus^\circ (1^\bullet, Y))(Z), ([\![Q_1]\!]^\bullet \oplus^\circ [\![Q_2]\!]^\bullet)(Z), M_1^\circ(Z)).$$

Table 3: Abstract transition relation

The abstract transition rules of Table 3 exploit the following operators to detect and split hybrid states. The idea is to use simple constraints to express the applicability of the reactions modeled by an environment E and then test the abstract states w.r.t. such constraints. To this aim we first define the domain of simple inequality constraints over reagent variables $\mathcal{X}$.

Definition 4.6 (Inequality constraints). *We define the set $\mathcal{V}$ of inequality constraints. Let $X \in \mathcal{X}$ and $a \in \{1, 2\}$,*

- *the basic constraints $X \geq a$ belong to $\mathcal{V}$,*
- *let $v_1, v_2 \in \mathcal{V}$ be basic constraint of the form $X \geq 1$, the boolean conjunction of v_1 and v_2, denoted by $v_1 \wedge v_2$, is in $\mathcal{V}$.*

Given an environment E it is easy to extract a set of inequality constraints expressing the enabling of each reaction. Formally, we define a function $\mathbb{A}_p$ which reports the *environment constraints* for an environment E,

$$\begin{array}{rll} \mathbb{A}_p(E) = & \{X \geq 1 \mid \tau_r{}^{\lambda}.Q \in E(X)\} & \cup \\ & \{X \geq 2 \mid a_r{}^{\lambda}.Q_1 \in E(X), \bar{a_r}{}^{\mu}.Q_2 \in E(X)\} & \cup \\ & \{X \geq 1 \wedge Y \geq 1 \mid a_r{}^{\lambda}.Q_1 \in E(X), \bar{a_r}{}^{\mu}.Q_2 \in E(Y), X \neq Y\}. & \end{array}$$

An abstract state M° is hybrid if it represents (at least) a non-terminated state and (at least) a terminated state. Thus, M° is hybrid if it represents: a concrete state where at least one reaction is enabled and a concrete state where all reactions are blocked. In order to capture these requirements by means of the environment constraints $\mathbb{A}_p$ it is necessary to define whether an abstract state satisfies a constraint $v \in \mathcal{V}$ or whether it satisfies its negation, denoted by $\neg v$.

Definition 4.7. *Let $M^\circ \in \mathcal{M}^\circ$ and $v, v' \in \mathcal{V}$ be basic constraints, we say that*

- $M^\circ \models v$ *iff* $v = X \geq a$ *and* $max(M^\circ(X)) \geq a$,
- $M^\circ \models v \wedge v'$ *iff* $M^\circ \models v$ *and* $M^\circ \models v'$,
- $M^\circ \models \neg v$ *iff* $v = X \geq a$ *and* $min(M^\circ(X)) < a$,
- $M^\circ \models \neg(v \wedge v')$ *iff* $M^\circ \models \neg v$ *or* $M^\circ \models \neg v'$.

We say that $M^\circ \not\models v$ iff $M^\circ \models v$ does not hold, and $M^\circ \not\models \neg v$ iff $M^\circ \models \neg v$ does not hold.

Intuitively, the abstract state M° satisfies a constraint on variable X if *there exists a value for X in the interval $M^\circ(X)$ which satisfies such a constraint.* Note that it can be the case that both $M^\circ \models v$ *and* $M^\circ \models \neg v$. Indeed, if $M^\circ(X) = [0, 1]$ and $v = X \geq 1$, then $M^\circ \models v$ and $M^\circ \models \neg v$.

Given an abstract state M° and an environment E, it is useful to denote the subset of environment constraints $\mathbb{A}_p(E)$ which M° satisfies. For $M^\circ \in \mathcal{M}^\circ$, with $\mathbb{S}_E(M^\circ)$ we indicate a set of constraint $V \subseteq \mathbb{A}_p(E)$ such that $\forall v \in V$, $M^\circ \models v$.

Definition 4.8 (Hybrid state). *An abstract state $M^\circ \in \mathcal{M}^\circ$ is* hybrid *w.r.t. an environment E iff: (i) $|\mathbb{S}_E(M^\circ)| > 0$ and (ii) $\forall v \in \mathbb{S}_E(M^\circ)$, $M^\circ \models \neg v$.*

Condition (i) assures that M° represents (at least one) non-terminated state, while Condition (ii) assures that M° also represents (at least one) terminated state. An abstract state M° is hybrid w.r.t. an environment E whenever there exist values for reagent variables which enable at least a reaction of E and also there exist (other) values which do not enable any reaction of E.

Once an hybrid state w.r.t. an environment E is detected, the idea is to split it into a set of non-hybrid states, using the environment constraints $\mathbb{A}_p(E)$. To

this aim, we introduce an operator $\bigtriangledown_E^{\mathcal{M}} : \mathcal{M}^\circ \to \mathcal{P}(\mathcal{M}^\circ)$. The goal of this operator is that, for each abstract state M'° resulting from the partitioning of an hybrid state M° (that is $M'^\circ \in \bigtriangledown_E^{\mathcal{M}}(M^\circ)$) it must be the case that M'° represents either non-terminated concrete states or terminated concrete states. The partitioning of M° is realized using the inequality constraints $\mathbb{S}_E(M^\circ)$ and guarantees that each abstract state M'°, for each $v \in \mathbb{S}_E(M^\circ)$, either satisfies v or it satisfies its negation $\neg v$.

The main operator $\bigtriangledown_E^{\mathcal{M}} : \mathcal{M}^\circ \to \mathcal{P}(\mathcal{M}^\circ)$ uses an auxiliary operator $\bigtriangledown_E^{\mathcal{I}} : \mathcal{M}^\circ \times \mathcal{X} \to \mathcal{P}(\mathcal{I})$ over intervals. The operator over intervals is applied in order to partition the interval of multiplicity $M^\circ(X)$ for each reagent variable $X \in \mathcal{X}$, separately.

For each reagent variable $X \in \mathcal{X}$, the interval of multiplicity $M^\circ(X)$ is partitioned using the basic constraints $X \geq a$ contained in $\mathbb{S}_E(M^\circ)$. To simplify the notation, in the following we write $X \geq a \triangleleft V$ for $V \subseteq \mathcal{V}$ if $X \geq a$ appears in V either as basic constraint or in a conjunction of basic constraints. The result of the partitioning of the interval $M^\circ(X)$ depends on the role of reagent variable X in the reactions modeled by environment E. If $X \geq 1 \in \mathbb{S}_E(M^\circ)$ and $X \geq 2 \notin \mathbb{S}_E(M^\circ)$, then each reaction involving reagent X is unary or binary so that it is enough to partition the interval $[0, n]$. By contrast, if $X \geq 2 \in \mathbb{S}_E(M^\circ)$ then reagent X participates in a homeo reaction so that also the interval $[1, n]$ has to be partitioned.

Given an environment E, we define the operators $\bigtriangledown_E^{\mathcal{M}} : \mathcal{M}^\circ \to \mathcal{P}(\mathcal{M}^\circ)$ and $\bigtriangledown_E^{\mathcal{I}} : \mathcal{M}^\circ \times \mathcal{X} \to \mathcal{P}(\mathcal{I})$ as follows, for $M^\circ \in \mathcal{M}^\circ$ and $X \in \mathcal{X}$,

$$\bigtriangledown_E^{\mathcal{M}}(M^\circ) = \begin{cases} \{M_1^\circ | \forall X \in \mathcal{X}, M_1^\circ(X) \in \bigtriangledown_E^{\mathcal{I}}(M^\circ, X)\} & \text{if } M^\circ \text{ is hybrid w.r.t. } E, \\ \{M^\circ\} & \text{otherwise.} \end{cases}$$

$\bigtriangledown_E^{\mathcal{I}}(M^\circ, X) =$

- $\begin{cases} \{[1,1],[2,n]\} & \text{if } X \geq 2 \triangleleft \mathbb{S}_E(M^\circ) \text{ and } M^\circ(X) = [1,n], \\ \{[0,0],[1,1],[2,n]\} & \text{if } X \geq 2 \triangleleft \mathbb{S}_E(M^\circ) \text{ and } M^\circ(X) = [0,n], \end{cases}$
- $\{[0,0],[1,n]\}$ if $X \geq 1 \triangleleft \mathbb{S}_E(M^\circ), X \geq 2 \notin \mathbb{S}_E(M^\circ)$ and $M^\circ(X) = [0,n]$,
- $\{M^\circ(X)\}$ otherwise.

Notice that when the target state of an abstract transition is partitioned, the information about the multiplicity of reagent variables, recorded on abstract transition labels, has to be split accordingly. To this aim the rules of Table 3 use the operator $\bigtriangledown^{\mathcal{T}} : \mathcal{I} \times \mathcal{I} \times \mathcal{I} \times \mathcal{I} \to \mathcal{I}$, such that for $I_1, I_2, I_3, I_4 \in \mathcal{I}$,

$$\bigtriangledown^{\mathcal{T}}(I_1, I_2, I_3, I_4) = \sqcup_I \{I \mid I \sqsubseteq_I I_1 \text{ such that } I - I_2 + I_3 = I_4\}.$$

To illustrate the rules of Table 3 we consider again the environment E commented in Example 3.1, the abstract state $M_5^\circ = \{([1,3], X), ([1,3], Y)\}$.

The abstract transitions (2) and (3) can be obtained by applying rule (**Sync-a**). In this case the inequality constraints, expressing the enabling of reactions $R_1 : X + Y \to X + X$ and $R_2 : X + Y \to Y + Y$, are

$$\mathbb{A}_p(E) = X \geq 1 \wedge Y \geq 1.$$

Transition (1) is the result of the first step of the application of rule (**Sync-a**) to state M_5°. The target state $M_5^{\circ\prime} = \{([2,4], X), ([0,2], Y)\}$ is hybrid w.r.t. E given that $M_5^{\circ\prime} \models X \geq 1 \wedge Y \geq 1$ but also $M_5^{\circ\prime} \models \neg(X \geq 1 \wedge Y \geq 1)$ (since $M_5^{\circ\prime} \models \neg(Y \geq 1)$).

The abstract state $M_5^{\circ\prime}$ is partitioned using the constraint $X \geq 1 \wedge Y \geq 1$. We obtain

$$\bigtriangledown_E^{\mathcal{M}}({M_5}'^{\circ}) = \{M_6^\circ, M_7^\circ\}$$

where $M_6^\circ = \{([2,4], X), ([0,0], Y)\}$ and $M_7^\circ = \{([2,4], X), ([1,2], Y)\}$. In this case $\bigtriangledown_E^{\mathcal{I}}({M_5}'^{\circ}, Y) = \{[0,0], [1,2]\}$ since $Y \geq 1 \lhd \mathbb{S}_E({M_5}'^{\circ})$ and ${M_5}'^{\circ}(Y) = [0,2]$, while $\bigtriangledown_E^{\mathcal{I}}({M_5}'^{\circ}, X) = \{[2,4]\}$, since $X \geq 1 \lhd \mathbb{S}_E({M_5}'^{\circ})$ but ${M_5}'^{\circ}(X) = [2,4]$. Notice that the abstract states M_6° and M_7° are the target states of transitions (2) and (3), respectively.

Finally, the intervals of multiplicity $[1,3]$ for reagent variables X and Y, recorded on the abstract transition label (1) have to partitioned accordingly. For target state M_6° we have that $I_y = [1,1]$, since $[1,1]$ is the biggest (therefore also the upper bound) between the intervals I contained in ${M_5}'^{\circ}(Y) = [1,3]$ such that $I - 1^\bullet = M_6^\circ(Y) = [0,0]$. Analogously, $I_x = [1,3]$, since $[1,3]$ is the biggest among the intervals I contained in ${M_5}'^{\circ}(X) = [1,3]$ such that $I - 1^\bullet + 2^\bullet = M_6^\circ(X) = [2,4]$. This yields to the intervals of multiplicity in the abstract transition label of (2). The intervals of multiplicity reported on transition (3) can be obtained in a similar way by considering the target state M_7°.

Next result proves that the refinement operator $\bigtriangledown_E^{\mathcal{M}}$ eliminates hybrid states.

Theorem 4.9. *Let E be an environment and let $M^\circ \in \mathcal{M}^\circ$. Each $M'^\circ \in \bigtriangledown_E^{\mathcal{M}}(M^\circ)$ is a non-hybrid state w.r.t. E.*

The proof of Theorem 4.9 can be found in AppendixA.

We introduce the definition of an abstract LTS.

Definition 4.10 (Abstract LTS). *An* abstract labeled transition system *is a tuple $(S^\circ, \to_\circ, M_0^\circ, E)$ where:*

i) *$S^\circ \subseteq \mathcal{M}^\circ$ is a set of abstract states and $M_0^\circ \in S^\circ$ is the initial state;*

ii) *$\to_\circ \subseteq S^\circ \times \widehat{\mathcal{L}} \times \widehat{Q}^\circ \times \mathbb{R}^+ \times S^\circ$ is the set of abstract transitions such that $M^\circ \xrightarrow[\circ]{\Theta, \Delta_1^\circ, r_1} M_1^\circ$, $M^\circ \xrightarrow[\circ]{\Theta, \Delta_2^\circ, r_2} M_2^\circ$, if $M_1^\circ = M_2^\circ$ then also $r_1 = r_2$, $\Delta_1^\circ = \Delta_2^\circ$.*

In the following we use $\mathcal{LTS}^\circ$ to denote the set of abstract LTS. We also assume that all notations defined for LTS are adapted in the obvious way. Hence, we write $\mathsf{LTS}^\circ((E, M_0^\circ)) = (S^\circ, \to_\circ, M_0^\circ, E)$ for the abstract LTS, obtained from the initial abstract state M_0° by transitive closure of the rules in Table 3, w.r.t. the environment E.

Remark 4.11. *In the abstract case, differently from the concrete one (presented in Definition 2.2) it may be the case that different transitions exiting from an abstract state M° share the same label $\Theta \in \widehat{\mathcal{L}}$, associated to a given reaction. We call such a situation a* conflict*. Actually, each multiset M represented by the abstract state M° has a move corresponding to reaction Θ which is approximated by exactly* one *of those abstract moves. As an example, for the abstract state $M_5^\circ = \{([1,3], X), ([1,3], Y)\}$ and the environment E commented in Example 3.1, the abstract transitions (2) and (3) share the label (λ, μ) which identifies the reaction R_1. It should be clear that the label (λ, μ) captures the relevant information: each multiset represented by M_5° realizes a move corresponding to label (λ, μ) which is abstracted* either *by (2)* or *by (3). This information recorded by the labels is exploited in order to limit the non-determinism introduced by the abstraction, following the methodology presented in Sections 5 and 6.*

4.3. Soundness

We introduce the concepts necessary for reasoning about the soundness and precision of the abstract LTS w.r.t. the concrete ones.

In the style of [20], we introduce an approximation order $\sqsubseteq^\circ_{lts}$ over abstract LTS in order to compare the behavior of two abstract LTS in terms of precision. Intuitively, ${lts_1}^\circ \sqsubseteq^\circ_{lts} {lts_2}^\circ$ says that the abstract LTS ${lts_2}^\circ$ is *coarser* than the abstract LTS ${lts_1}^\circ$ (or equivalently that it is a *safe approximation*).

Definition 4.12 (Order on abstract LTS). *Let $lts_i^\circ = (S_i^\circ, \rightarrow_\circ^i, M_{0,i}^\circ, E)$ with $i \in \{1, 2\}$ be abstract LTS. For $M_1^\circ \in S_1^\circ, M_2^\circ \in S_2^\circ$, we say that ${M^\circ}'_1 \preccurlyeq_{lts} {M^\circ}'_2$ iff there exists a relation $R \subseteq S_1^\circ \times S_2^\circ$ such that ${M^\circ}'_1 R {M^\circ}'_2$ and if ${M^\circ}_1 R M_2^\circ$ then:*

1. *$M_1^\circ \sqsubseteq^\circ M_2^\circ$;*
2. *$\mathsf{label}(\mathsf{Ts}({M_1}^\circ)) = \mathsf{label}(\mathsf{Ts}({M_2}^\circ))$;*
3. *there exists a function $H_t : \mathsf{Ts}({M_1}^\circ) \rightarrow \mathsf{Ts}({M_2}^\circ)$ such that, for each $t_1^\circ \in \mathsf{Ts}({M_1}^\circ)$, $t_1^\circ = M_1^\circ \xrightarrow[\circ]{\Theta, \Delta_1^\circ, r} N_1^\circ$, $H_t(t_1^\circ) = t_2^\circ$ where $t_2^\circ = M_2^\circ \xrightarrow[\circ]{\Theta, \Delta_2^\circ, r} N_2^\circ$, $\Delta_1^\circ \sqsubseteq_I \Delta_2^\circ$, $N_1^\circ \neq M_1^\circ$ iff $N_2^\circ \neq M_2^\circ$, $N_1^\circ R N_2^\circ$.*

We say that $lts_1^\circ \sqsubseteq^\circ_{lts} lts_2^\circ$ iff $M_{0,1}^\circ \preccurlyeq_{lts} M_{0,2}^\circ$.

The approximation order for abstract LTS is based on a simulation between abstract states. More in detail, we say that M_2° *simulates* M_1° ($M_1^\circ \preccurlyeq_{lts} M_2^\circ$) whenever: 1) M_2° approximates M_1°; 2) the set of labels of transitions leaving from M_1° is the same than the one of transitions leaving from M_2°; 3) there exists a function $H_t : \mathsf{Ts}({M_1}^\circ) \rightarrow \mathsf{Ts}({M_2}^\circ)$ between the transitions of M_1° and M_2° mapping target states different from the source state M_1° in target states different from M_2°. In more detail, each move $M_1^\circ \xrightarrow[\circ]{\Theta, \Delta_1^\circ, r} N_1^\circ$ has to be matched by a move $M_2^\circ \xrightarrow[\circ]{\Theta, \Delta_2^\circ, r} N_2^\circ$, related to the same label Θ, and such that $\Delta_1^\circ \sqsubseteq_I \Delta_2^\circ$, showing that the interval of multiplicities are properly approximated and N_2° *simulates* N_1°. We also require that $N_1^\circ \neq M_1^\circ \Leftrightarrow N_2^\circ \neq M_2^\circ$ in order to guarantee

that approximations preserve the self-loops without introducing new ones. This is a necessary condition for assuring the correctness in the case of termination properties. It is worth noting that approximation without the previous condition can be profitably used for proving simple reachability properties (see [15]).

We also introduce a function, called *best abstraction*, which can be used to relate concrete LTSs to abstract LTSs. In detail, the best abstraction of a concrete LTS lts gives an abstract LTS which is equivalent to the concrete lts.

Definition 4.13 (Best abstraction of LTS). *We define* $\alpha_{lts} : \mathcal{LTS} \to \mathcal{LTS}^{\circ}$ *such that*

$$\alpha_{lts}((S, \to, M_0, E)) = (\{M^{\bullet}\}_{M \in S}, \to^{\bullet}, M_0{}^{\bullet}, E)$$

where $\to^{\bullet} = \{M^{\bullet} \xrightarrow[\circ]{\Theta,\Delta^{\bullet},r} M_1^{\bullet} \mid M \xrightarrow{\Theta,\Delta,r} M_1 \in \to\}$.

Note that $\alpha_{lts}(lts)$ does not introduce any approximation, indeed, it has exact intervals of multiplicities, both in states and transitions.

Using function α_{lts}, we can formally define when an abstract LTS lts° *safely approximates* a concrete lts, i.e., $\alpha_{lts}(lts) \sqsubseteq^{\circ}_{lts} lts^{\circ}$.

The following theorem shows that the abstract LTS derived from an abstract state M° safely approximates the concrete LTS $\mathsf{LTS}((E, M))$, for any M represented by M°. Specifically, the abstract LTS $\mathsf{LTS}^{\circ}((E, M^{\circ}))$ safely approximates (w.r.t. the order $\sqsubseteq^{\circ}_{lts}$) the best abstraction of LTS $\mathsf{LTS}((E, M))$ for each M represented by M°.

Theorem 4.14 (Soundness of the LTS). *Let E be an environment and $M^{\circ} \in \mathcal{M}^{\circ}$. For each $M \in \gamma(M^{\circ})$, we have*

$$\alpha_{lts}(\mathsf{LTS}((E, M))) \sqsubseteq^{\circ}_{lts} \mathsf{LTS}^{\circ}((E, M^{\circ})).$$

The proof of Theorem 4.14 can be found in AppendixA.

4.4. Complexity and widening operators

Let us now discuss the complexity of the proposed approach. First, we focus on the complexity of finding and splitting hybrid states. To help the intuition, in this presentation, to detect an hybrid state, splitting it, splitting the incoming abstract transitions and then deriving the new abstract transitions leaving from such a state, have been described as four separated steps. However, an efficient implementation computes $\mathbb{S}_E(M^{\circ})$ and uses it to detect if the state is hybrid and, at the same time, to determine which are the abstract transitions enabled for that state. If the state is hybrid, the information on the split intervals is used to determine directly the abstract transitions enabled for the split state. Moreover, once an abstract rule is applied, allowing an abstract state M° to move into an abstract state M_1°, the information on the multiplicity of reagents that vary are used, together with $\mathbb{S}_E(M^{\circ})$, to determine the new set of constraints $\mathbb{S}_E(M_1{}^{\circ})$.

More important is to give a bound on the number of states and transitions of the abstract LTS which models the semantics of a CGF process, that is $\mathsf{LTS}^{\circ}((E, M^{\circ}))$ for some environment E and initial abstract state M°.

$\mathsf{LTS}^\circ((E, M^\circ))$ represents a *set of concrete* LTSs for all the multisets which are approximated by M°.

In it worth noting that the abstract LTS proposed in [15] has exactly as many states and abstract transitions as the biggest LTS it represents. Moreover, in such a semantics each abstract state M° has exactly n exiting transitions, where n is the number of reactions in the environment E. Each abstract transition is decorated by a distinct label Θ identifying the reaction of the environment which is realized.

In the refined LTS proposed here each abstract transition (related to a label Θ) can be approximated by several abstract transitions (related to label Θ) due to the partitioning of hybrid states.

Given an abstract state which is hybrid w.r.t. the environment E it is possible to give a bound on the number of abstract states obtained from the splitting of M°. Let n_1 be the number of variables appearing in homeo reactions enabled in M° and whose interval of multiplicity is actually split, while n_2 is the number of variables appearing just in unary or binary reactions enabled in M° and whose interval of multiplicity is actually split. In the worst case the abstract state M° is partitioned into $(3)^{n_1} \times (2)^{n_2}$ different abstract states. Notice that $(3)^{n_1} \times (2)^{n_2}$ is also the maximum number of different transitions with the same label leaving from an abstract state. Therefore, for all abstract state M°, the cardinality of $\mathsf{Ts}(M^\circ)$ is $n \times (3)^{n_1} \times (2)^{n_2}$, in the worst case.

More in detail, to give a bound on the number of variables that were actually split, we have to compute the number of variables X such that $M^\circ \models (X \geq a)$ and $M^\circ \models \neg(X \geq a)$ with $(X \geq a) \triangleleft \mathbb{S}_E(M^\circ)$. In the worst case, whenever no information on the set of variables X having the previous property can be deduced from reactions of E, a bound for $n_1 + n_2$ can be computed considering the number of different variables appearing in $\mathbb{S}_E(M^\circ)$ and then, by further approximations, of different reagents appearing in the inequality constraints of $\mathbb{A}_p(E)$.

Finally, note that the set of states obtained by the splitting has some interesting properties; (i) there is at least one terminated state; (ii) among the non-terminated states obtained from the splitting, only one will have the same set of enabled reactions than the original state, all the other non-terminated states will have much less reactions enabled. In more detail, assuming no homeo reactions enabled in M° and denoting with n the number of reactions enabled for the original state, the splitting will originate $\binom{n}{k}$ states with k reaction enabled, for $k \in \{1, ...n\}$.

It should be clear that the complexity of the abstract model depends on the number of hybrid states that are generated applying the rules of the abstract semantics. Therefore it strictly depends on the characteristics of the system and on the set of experiments we want to model. However, it can be useful to give an upper bound on the number of states (and therefore of transitions) that our abstract model will have in the worst case. Such bound can be used to decide when it is the case to apply such method. For this reason, let us compare the numbers of states of our abstract model (in the worst case) w.r.t. the number of states of the biggest LTS it represent, let's say $\overline{lts}$. By our LTS semantics,

each concrete state M of $\overline{lts}$ has exactly n exiting transitions and, in the worst case, n different states (remember that n was the number of reactions in the environment E). Of course, some of these transitions will have at least one multiplicities equal to 0 and therefore could be omitted. Moreover, some of the n states that we derive could be not new distinct states. However, in the worst case, the biggest number of states of $\overline{lts}$ can be computed as $\Sigma_{i=1}^{h} n^i$, where $h \in [0, \infty]$ is the maximal distance[3] from a state of the transition system to the initial state. Let us consider now our abstract LTS model which represents a set of concrete LTSs that include $\overline{lts}$. If the set of concrete LTSs that we want to approximate coincides with $\overline{lts}$, then our abstract model substantially coincides with $\overline{lts}$. Otherwise, to give an upper bound in the worst case, we can count the number of states obtained splitting *each state right after the application of each reaction*. The worst case is obtained splitting each state according to the reaction of E that produces more intervals. In this case such splitting, partitions the hybrid state in a set of at most 4 states. In more detail, let $m = 4$ if the environment E contains a binary reaction that consumes both reactant X and Y without adding neither a new occurrence of X neither of Y, $m = 3$ if the environment E contains at least an homeo reaction[4], $m = 2$ in any other case. Then $\Sigma_{i=1}^{h}(n \times m)^i$ constitute an upper bound on the number of states and transitions of the abstract model. Note that $\Sigma_{i=1}^{h}(n \times m)^i$ is a number that is a lot greatest than the number of states and transitions in our abstract model but it is the only one we can calculate considering a generic environment E, moreover, it is obtained considering the splitting of each state according to the worst case scenario without taking into account the terminated states. Actually, in any case, the dimension (number of states and transitions) of the abstract model we construct will be smaller than sum of all the states and transitions of each LTS it represents.

In any case, in order to reduce the number of non-terminated abstract states, several widening operators can be designed.

One idea is to define a widening operator that will allow us to more naturally model reverse reactions, that are reactions that allows the system to return back to a previously encountered state. The problem arises in the abstract setting when we split an hybrid state and then apply a reverse reaction. Indeed, in general, applying a reverse reaction to a split state will not lead to a previously derived state. That is because the split state contains more precise information w.r.t. the previously derived states.

To overcome this problem, here we propose the following widening operator. Given a state M°, we first compute the new abstract state M'°, result of the application of the transition rules of Table 3. Then, if $M'^\circ \neq M^\circ$ and there

[3]The distance is defined as the minimal length of the path connecting two states.

[4]For a sake of simplicity, in this paper we have presented a splitting that partition an interval in 3 for variables appearing in homeo reaction. A more efficient partitioning would split the interval in 2 if a variables appears as premise of homeo reactions only and in 3 if it appears as premise in homeo *and* binary or unary reaction. In that case, m become 2 also for some environments containing homeo reactions.

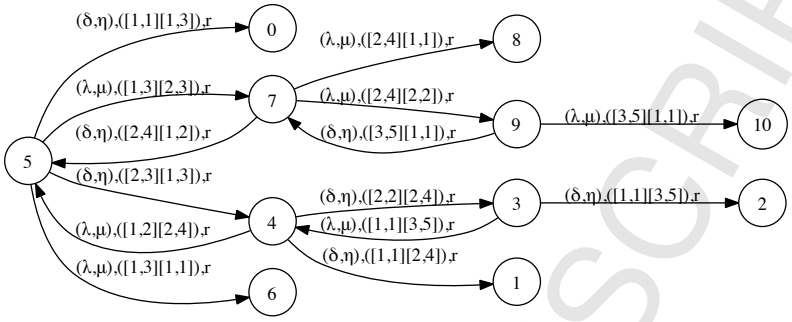


Figure 6: The LTS semantics.

exists one previously derived state along a path leading to M°, let us call it M_1° , such that $M_1^\circ \neq M^\circ$ and $M_1^\circ \sqsupset_I M'^\circ$[5], we approximate M'° by M_1°. Of course, this will reduce the number of new generated abstract states.

In the following we always assume the application of the previous widening operator to each derivation step.

Example 4.15. *We consider the environment E commented in Example 3.1 which models reactions $R_1 : X + Y \to X + X$ and $R_2 : X + Y \to Y + Y$,*

$$E \triangleq \quad X = a_r^\lambda.X + \bar{b}_r^\delta.Y, \quad Y = \bar{a}_r^\mu.X + b_r^\eta.Y.$$

Fig. 6 shows the complete abstract LTS for the initial abstract state $M_5^\circ = \{([1,3],X),([1,3],Y)\}$, where

$$\begin{array}{llll} {M_0}^\circ = & \{([0,0],X),([2,4],Y)\} & {M_6}^\circ = & \{([2,4],X),([0,0],Y)\} \\ {M_4}^\circ = & \{([1,2],X),([2,4],Y)\} & {M_1}^\circ = & \{([0,0],X),([3,5],Y)\} \\ {M_3}^\circ = & \{([1,1],X),([3,5],Y)\} & {M_2}^\circ = & \{([0,0],X),([4,6],Y)\} \\ {M_7}^\circ = & \{([2,4],X),([1,2],Y)\} & {M_8}^\circ = & \{([3,5],X),([0,0],Y)\} \\ {M_9}^\circ = & \{([3,5],X),([1,1],Y)\} & {M_{10}}^\circ = & \{([4,6],X),([0,0],Y)\} \end{array}$$

Note that, for each abstract state, the moves corresponding to reaction R_1 are labeled by (λ,μ), while the moves corresponding to reaction R_2 are labeled by (δ,η). Finally, note the effect of the application of the widening operator. For example, starting from state ${M_4}^\circ$, the move corresponding to reaction R_1 (labeled (δ,η)) lead the system to state ${M_3}^\circ$. On the other hand, starting from ${M_3}^\circ$, the move corresponding to reaction R_2 (labeled (λ,μ)) allows the system to

[5]If more than one such state exists, the order $\sqsubseteq^\circ$, a total order on variables of $\mathcal{X}$ and the order $\sqsubseteq_I$ on $\mathcal{I}$ can be used to deterministically choose one.

go back in state $M_4{}^\circ$. Observe that this behavior "mimic" the one of the concrete LTS (see Fig. 5) and follows our intuition that R_1 and R_2 are, in some ways, one the reverse reaction of the other. However, without the widening, from state $M_3{}^\circ$ the system would not go back *to state $M_4{}^\circ$, but it would evolve (with a transition labeled (λ, μ)) in a new state $\{([2,2], X), ([2,4], Y)\}\sqsubset^\circ M_4{}^\circ$.*

5. Labeled Interval Markov Chains

We present a *generalization* of Interval Markov Chains [51, 24], called *Labeled Interval Markov Chains* (IMC[6]), and the related notion of probabilistic termination. Moreover, we introduce the concepts necessary to prove the soundness of the abstract probabilistic semantics of CGF w.r.t. probabilistic termination (presented in Section 6). The notions presented for IMC are adapted from those proposed in [51, 24] for standard Interval Markov Chains and similarly in [22, 23] for Markov Decision Process (MDP).

5.1. The probabilistic model

The model of Interval Markov Chains [51, 24] combines probabilistic and non-deterministic steps. Thus, each state has associated a set of probability distributions describing the probability to move in any other state. In the standard model transitions report intervals of probability, which represent *lower* and *upper* bounds on the concrete probabilities. Unfortunately, this model is not adequate to abstract a set of DTMC. Indeed, it may give not accurate results for probabilistic termination, even when considering a partitioning of the abstract state space which does not contain hybrid states. As an example we consider again the system commented in Examples 3.1 and 4.15.

Example 5.1. *We examine the probabilistic behavior of the system considering the initial abstract state*

$$M_5^\circ = \{([1,3], X), ([1,3], Y)\}$$

w.r.t. the environment E, modeling reactions $R_1 : X + Y \to X + X$ and $R_2 : X + Y \to Y + Y$,

$$E ::= \quad X = a_r^\lambda.X + \bar{b}_r^\delta.Y, \quad Y = \bar{a}_r^\mu.X + b_r^\eta.Y.$$

We recall that the abstract states M_6°, M_7°, M_0° and M_4° are reachable from M_5°, where

$$M_6{}^\circ = \{([2,4], X), ([0,0], Y)\} \quad M_7{}^\circ = \{([2,4], X), ([1,2], Y)\}$$
$$M_0{}^\circ = \{([0,0], X), ([2,4], Y)\} \quad M_4{}^\circ = \{([1,2], X), ([2,4], Y)\}.$$

[6]Note that the acronym IMC is also used in the literature to indicate Hermanns' Interactive Markov Chains.

The fragment of LTS reporting the transitions exiting from the abstract state M_5° is shown in Fig. 7(a).

In order to reason which intervals of probability could be (safely) assigned to the moves of M_5°, it is convenient to examine the set of concrete probability distributions, for each concrete multiset M_5, abstracted by M_5°, that is for each concrete multiset $M_5 \in \gamma(M_5^\circ)$. For the initial solution, containing exactly 3 occurrences of reagents X and Y, the probabilistic semantics is illustrated by the DTMC, shown in Fig. 5 and commented in Example 3.1. Other concentrations of reagents X and Y show analogous behaviors.

We observe that, for each $M_5 \in \gamma(M_5^\circ)$, there are two possible synchronizations between reagents X and Y: one corresponding to reaction R_1 and the other one corresponding to reaction R_2. For each multiset, the two alternative moves always happen with probability $1/2$.

Moreover, each multiset M_5 by realizing reaction R_1 evolves into a solution, which is abstracted either *by M_7° (where reagent Y is still available) or by M_6° (where reagent Y is consumed). Analogously, for reaction R_2 and the abstract states M_4° and M_0°.*

As a consequence, the abstract probability distributions which can be assigned to the abstract state M_5° and which over-approximate *(include) the concrete probability distributions for each multiset $M_5 \in \gamma(M_5^\circ)$ are:*

$$\begin{array}{llll} \rho_1(M_7^\circ) = 1/2, & \rho_1(M_6^\circ) = 0, & \rho_1(M_0^\circ) = 1/2, & \rho_1(M_4^\circ) = 0, \\ \rho_2(M_7^\circ) = 1/2, & \rho_2(M_6^\circ) = 0, & \rho_2(M_0^\circ) = 0, & \rho_2(M_4^\circ) = 1/2, \\ \rho_3(M_7^\circ) = 0, & \rho_3(M_6^\circ) = 1/2, & \rho_3(M_0^\circ) = 1/2, & \rho_3(M_4^\circ) = 0, \\ \rho_4(M_7^\circ) = 0, & \rho_4(M_6^\circ) = 1/2, & \rho_4(M_0^\circ) = 0, & \rho_4(M_4^\circ) = 1/2. \end{array}$$

It should be clear that intervals of probabilities representing the abstract probability distributions ρ_i with $i \in \{1, \ldots, 4\}$ could be obtained by considering the minimum *and* maximum *probability, for each move. The intervals we would obtain in this way are illustrated in Fig. 7(b).*

Notice that the intervals of probability in Fig. 7(b) represent in addition to the probability distributions ρ_i, with $i \in \{1, \ldots, 4\}$, also the following abstract probability distributions,

$$\begin{array}{llll} \rho_5(M_7^\circ) = 1/2, & \rho_5(M_6^\circ) = 1/2, & \rho_5(M_0^\circ) = 0, & \rho_5(M_4^\circ) = 0, \\ \rho_6(M_7^\circ) = 0, & \rho_6(M_6^\circ) = 0, & \rho_6(M_0^\circ) = 1/2, & \rho_6(M_4^\circ) = 1/2. \end{array}$$

The probability distributions ρ_5 and ρ_6 do not describe any concrete behavior for a concrete state $M_5 \in \gamma(M_5^\circ)$. Probability distribution ρ_5 models a probabilistic choice between two moves corresponding to reaction R_1, corresponding to different concentrations of reagent variables X and Y. Similarly, probability distribution ρ_6 models a probabilistic choice between two moves corresponding to reaction R_2, corresponding to different concentrations of reagent variables X and Y.

Note that there is a conflict *between the transitions (t_1°) and (t_2°) (see Fig.7(a)) and between the transitions (t_3°) and (t_4°), respectively. This information about*

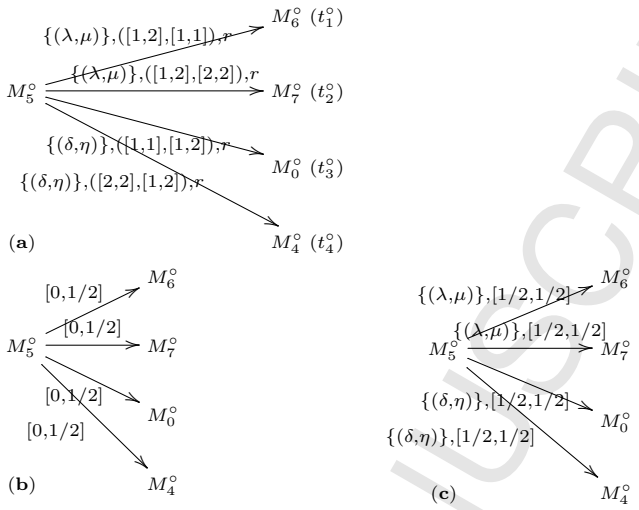


Figure 7: The intervals of probabilities and the labeled transitions for M_5°.

conflict is represented in the abstract LTS semantics by means of labels: the transitions abstracting reaction R_1 are decorated by label (λ, μ) and the moves abstracting reaction R_2 are decorated by label (δ, η). □

The previous example shows that standard Interval Markov Chains typically introduce a serious loss of information w.r.t. the concrete behavior, even if we consider the most precise intervals of probability which over-approximates the set of concrete probability distributions of a move (namely their *best abstraction*). Notice that the methodology explained in the Example 5.1 for computing the intervals of probability of a move is not effective given that it requires to calculate for each multiplicity of reagent variables, abstracted by intervals, *all the concrete probability distributions*, e.g. the values of concrete rates of all transitions.

Since labels in the abstract LTS precisely represent conflicting moves, the idea is to enrich with labels the standard model of Interval Markov Chains. Using labels and a corresponding notion of conflict, it is possible to more accurately represent the set of probability distributions represented by intervals of probability.

Definition 5.2 (IMC). *A* Labeled Interval Markov Chain *is a tuple* $(S^\circ, \mathbf{P}^-, \mathbf{P}^+, \mathbf{L}, M_0^\circ)$ *where*

1. $S^\circ \subseteq \mathcal{M}^\circ$ *is a countable set of abstract states and* ${M_0}^\circ \in S^\circ$ *is the* initial state*;*
2. $\mathbf{P}^-, \mathbf{P}^+ \colon S^\circ \to \mathsf{SDistr}(S^\circ)$ *are the* lower *and* upper bounds *on probabilities, such that for each* ${M_1}^\circ, {M_2}^\circ \in S^\circ$, $\mathbf{P}^-({M_1}^\circ)({M_2}^\circ) \leq \mathbf{P}^+({M_1}^\circ)({M_2}^\circ)$*;*

3. $\mathbf{L} : S^\circ \to (S^\circ \to \wp(\widehat{\mathcal{L}}))$ *is a* labeling function.

As in the standard model, $\mathbf{P}^-({M_1}^\circ)({M_2}^\circ)$ and $\mathbf{P}^+({M_1}^\circ)({M_2}^\circ)$ define the *lower* and *upper* bound probability, for the move from ${M_1}^\circ$ to ${M_2}^\circ$, respectively. In addition, $\mathbf{L}({M_1}^\circ)({M_2}^\circ)$ reports the set of labels corresponding to the move. In the following we use $\mathcal{IMC}^\circ$ to denote the set of IMC.

Intervals of probability represent sets of *admissible* distributions. Obviously, the notion of admissible distribution has to be slightly adapted from the one given for the standard model [51, 24]. Actually, it is necessary to take into account the conflict between (sets of) labels.

Definition 5.3 (Conflict of labels). *Let $\alpha, \beta \in \wp(\widehat{\mathcal{L}})$ be sets of labels. We say that α is in* conflict *with β iff there exists $\vartheta \in \widehat{\mathcal{L}}$ such that $\alpha = \{\vartheta\} = \beta$.*

Note that to be in conflict two sets of labels has to be singleton. To help the intuition, consider the two sets of labels $\{\alpha, \beta\}$ and $\{\beta\}$. The set $\{\alpha, \beta\}$ should not be considered in conflict with the set $\{\beta\}$ since the move associated to $\{\alpha, \beta\}$ may approximate a move labeled α while the move associated to $\{\beta\}$ may approximate a move labeled β of the same concrete state M represented by M°.

The notion of conflict between labels induces a corresponding notion of conflict between states. Let $(S^\circ, \mathbf{P}^-, \mathbf{P}^+, \mathbf{L}, M_0^\circ)$ be an IMC and $M^\circ \in S^\circ$. We say that $NS^\circ \subseteq S^\circ$ is a set of *consistent states* w.r.t. M° iff: (i) for each $M_1^\circ, M_2^\circ \in NS^\circ$, there is no conflict between the sets of labels $\mathbf{L}(M^\circ)(M_1^\circ)$ and $\mathbf{L}(M^\circ)(M_2^\circ)$; (ii) NS° is a maximal set of states satisfying (i).

Definition 5.4 (Admissible distribution). *Let $mc^\circ = (S^\circ, \mathbf{P}^-, \mathbf{P}^+, \mathbf{L}, M_0^\circ)$ be an* IMC *and let $M^\circ \in S^\circ$. We say that a probability distribution $\rho \in \mathsf{Distr}(S^\circ)$ is* admissible *for M° iff there exists a set of* consistent states *$NS^\circ \subseteq S^\circ$ such that, for each $M_1^\circ \in S^\circ$: if $M_1^\circ \in NS^\circ$, then $\mathbf{P}^-(M^\circ)(M_1^\circ) \leq \rho(M_1^\circ) \leq \mathbf{P}^+(M^\circ)(M_1^\circ)$; $\rho(M_1^\circ) = 0$, otherwise. We use $\mathsf{ADistr}_{mc^\circ}(M^\circ)$ for the set of admissible distributions for M°.*

Intuitively, an admissible distribution for an abstract state M° corresponds to a set of consistent states NS° and reports a value included in the interval of probability, for each state contained in NS° and zero otherwise.

Example 5.5. *We consider the abstract states M_5°, M_6°, M_7°, M_0° and M_4°, commented in Example 5.1.*

The IMC *illustrated in Fig. 7(c) reports four consistent sets of states w.r.t. M_5°: (1) $\{M_6^\circ, M_0^\circ\}$, (2) $\{M_6^\circ, M_4^\circ\}$; (3) $\{M_7^\circ, M_0^\circ\}$ and (4) $\{M_7^\circ, M_4^\circ\}$. Thus, the admissible distributions for M_5°, corresponding to (1)-(4), are exactly the distributions $\rho_1 - \rho_4$, discussed in Example 5.1.*

Notice that the combinations (1)-(4) represent the probabilistic choices between reactions R_1 and R_2, corresponding to different concentrations of reagent variables X and Y. As a consequence, the IMC *of Fig.7(c) not only over-approximates the probabilistic semantics for each concrete multiset represented*

by M_5°, but also it is their most precise approximation. The advantages of the new IMC *model with respect to the standard one in terms of precision become clear by comparing the* IMC *of Fig. 7(c) with the model without labels Fig. 7(b).*□

In an IMC, for each state, there is a choice between the distributions yielding the probability to reach successor states. This non-determinism is resolved by means of a *scheduler*, that can be defined similarly as in [51, 24].

The notions of paths $\mathsf{Paths}()$, finite paths $\mathsf{FPaths}()$ and cylinder for IMC are analogous to the ones presented for DTMC (see Section 2.2). We therefore adopt similar notations.

Definition 5.6 (Scheduler). *Let $mc^\circ = (S^\circ, \mathbf{P}^-, \mathbf{P}^+, \mathbf{L}, M_0^\circ)$ be an* IMC*, a* scheduler *is a function $A\colon \mathsf{FPaths}(S^\circ) \to \mathsf{Distr}(S^\circ)$ such that $A(\pi^\circ) \in \mathsf{ADistr}_{mc^\circ}(\pi^\circ[|\pi^\circ|])$ for any abstract path $\pi^\circ \in \mathsf{FPaths}(S^\circ)$. We use $\mathsf{Adv}(mc^\circ)$ to denote the set of schedulers.*

Given a scheduler which resolves the non-determinism, a probability space over paths can be defined analogously as for DTMC (see Definition 2.4). In the following, we use $\mathbf{P}^A_{M^\circ}$ for denoting the probability space, starting from the abstract state M° w.r.t. the scheduler $A \in \mathsf{Adv}(mc^\circ)$.

An IMC gives both *lower* and *upper* bounds for probabilistic termination which can be computed by considering the *worst* and *best* scenarios w.r.t. all the schedulers. For capturing probabilistic termination we have to introduce the concept of terminated abstract state.

Given an IMC $mc^\circ = (S^\circ, \mathbf{P}^-, \mathbf{P}^+, \mathbf{L}, M_0^\circ)$, it holds that a state $M^\circ \in S^\circ$ is $\forall$-*terminated* iff for each $\rho \in \mathsf{ADistr}_{mc^\circ}(M^\circ)$ $\rho(M^\circ) = 1$, while M° is $\exists$-*terminated* iff there exists a $\rho \in \mathsf{ADistr}_{mc^\circ}(M^\circ)$ such that $\rho(M^\circ) = 1$.

The *lower bound* for probabilistic termination is obtained by minimizing the probability of the paths reaching a $\forall$-*terminated* state, while the *upper bound* for probabilistic termination is obtained by maximizing the probability of the paths reaching a $\exists$-*terminated* state.

Definition 5.7 (Probabilistic termination). *Consider the following* IMC*, $mc^\circ = (S^\circ, \mathbf{P}^-, \mathbf{P}^+, \mathbf{L}, M_0^\circ)$. The* lower *and* upper bound *for probabilistic termination, starting from $M^\circ \in S^\circ$, are*

$$\mathsf{Reach}^-_{mc^\circ}(M^\circ) = \inf_{A \in \mathsf{Adv}(mc^\circ)} \mathbf{P}^A_{M^\circ}(\{\pi^\circ \in C(M^\circ) \mid \pi^\circ[i] \text{ is } \forall\text{-terminated for some } i \geq 0\})$$

$$\mathsf{Reach}^+_{mc^\circ}(M^\circ) = \sup_{A \in \mathsf{Adv}(mc^\circ)} \mathbf{P}^A_{M^\circ}(\{\pi^\circ \in C(M^\circ) \mid \pi^\circ[i] \text{ is } \exists\text{-terminated for some } i \geq 0\})$$

Similarly as for DTMC, both $\mathsf{Reach}^-_{mc^\circ}(M^\circ)$ and $\mathsf{Reach}^+_{mc^\circ}(M^\circ)$ can be calculated by a fixpoint computation. We refer the interested reader to [5, 22, 23, 24] for more detail.

In order to simplify the proofs, it is convenient to exploit the following formulation of $\mathsf{Reach}^-_{mc^\circ}(M^\circ)$ and $\mathsf{Reach}^+_{mc^\circ}(M^\circ)$ as fixpoint equations.

Let $mc^\circ = (S^\circ, \mathbf{P}^-, \mathbf{P}^+, \mathbf{L}, , M_0^\circ)$ be an IMC. For each $i \in \mathbb{N}$, we define pseudo-distributions on S°, $\rho^{-,i}_{mc^\circ}, \rho^{+,i}_{mc^\circ} \in \mathsf{SDistr}(S)$, where for each $M^\circ \in S^\circ$,

$$\rho^{-,i}_{mc^\circ}(M^\circ) = \begin{cases} 1 & \text{if } M^\circ \text{ is } \forall\text{-terminated,} \\ 0 & \text{if } i = 0 \text{ and} \\ & M^\circ \text{ is non } \forall\text{-terminated,} \\ \inf\limits_{\rho \in \mathsf{ADistr}_{mc^\circ}(M^\circ)} \sum\limits_{M_1^\circ \in S^\circ} \rho(M_1^\circ) \cdot \rho^{-,i-1}_{mc^\circ}(M_1^\circ) & \text{otherwise.} \end{cases}$$

$$\rho^{+,i}_{mc^\circ}(M^\circ) = \begin{cases} 1 & \text{if } M^\circ \text{ is } \exists\text{-terminated,} \\ 0 & \text{if } i = 0 \text{ and} \\ & M^\circ \text{ is non } \exists\text{-terminated,} \\ \sup\limits_{\rho \in \mathsf{ADistr}_{mc^\circ}(M^\circ)} \sum\limits_{M_1^\circ \in S^\circ} \rho(M_1^\circ) \cdot \rho^{+,i-1}_{mc^\circ}(M_1^\circ) & \text{otherwise.} \end{cases}$$

By induction on i, it can be proved that $\forall i$, $\rho^{-,i}_{mc^\circ} \subseteq \rho^{-,i+1}_{mc^\circ}$ and $\rho^{+,i}_{mc^\circ} \subseteq \rho^{+,i+1}_{mc^\circ}$. Since the set of *pseudo-distributions* on S constitutes a complete lattice, the following least fixpoints exist,

$$\mathsf{Reach}^-_{mc^\circ}(M^\circ) = \bigcup_{i \in \{0,\ldots,\infty\}} \rho^{-,i}_{mc^\circ}(M^\circ),$$
$$\mathsf{Reach}^+_{mc^\circ}(M^\circ) = \bigcup_{i \in \{0,\ldots,\infty\}} \rho^{+,i}_{mc^\circ}(M^\circ).$$

Finally, notice that the problem of model checking our IMC can be reduced, as in the case of standard Interval Markov Chains, to the verification of a corresponding MDP obtained by exploiting the labels and considering the so-called extreme distributions. Roughly speaking, such MDP has the same abstract states than the corresponding IMC. Moreover, the set $\{\rho_1, ..., \rho_n\}$ of distributions associated to an abstract state M° can be computed in the following way; for each combination of moves (from M°) with non conflicting labels, for each move of the selected combination except one, the probability value of distribution ρ_i for the move has to coincides with one of two bounds of the interval of probabilities for such move. Note that the probability value for the remaining move is univocally determined by the property that $\rho_i \in \mathsf{Distr}$. In Section 7.3 we will show that the complexity of this reduction from the IMC to the MDP model is comparable to the analogous one for standard Interval Markov Chains. Analogously to the case of Interval Markov Chains, more efficient iterative algorithms, which construct a basic feasible solution *on-the-fly*, can also be defined to model check IMC (see [51, 24] and [33] where transition probabilities of a uniform CTMC are abstracted by intervals and then interpreted as a CTMDP).

5.2. Soundness and Precision of Approximations

We now introduce the notions necessary for reasoning on the soundness and precision of IMC w.r.t. the property of probabilistic termination.

In the style of [51, 24, 22, 23], and analogously to what we have done for abstract LTSs in Section 4.3, we introduce an approximation order $\sqsubseteq^\circ_{mc}$ in

order to compare the behavior of two IMC in terms of precision. Intuitively, ${mc_1}^\circ \sqsubseteq^\circ_{mc} {mc_2}^\circ$ says that the IMC ${mc_2}^\circ$ is *coarser* than the IMC ${mc_1}^\circ$ (or equivalently that it is a *safe approximation*).

Definition 5.8 (Order on IMC). *Let* $mc_i^\circ = (S_i{}^\circ, \mathbf{P}_i^-, \mathbf{P}_i^+, \mathbf{L}, M_{0,i}^\circ)$ *be two* IMC *and let* $M_i^\circ \in S_i^\circ$*, for* $i \in \{1,2\}$*. We say that* ${M^\circ}'_1 \preccurlyeq_{mc} {M^\circ}'_2$ *iff there exists a relation* $R \subseteq S_1^\circ \times S_2^\circ$ *such that* ${M^\circ}'_1 R {M^\circ}'_2$ *and if* $M_1^\circ R M_2^\circ$ *then:*

1. $M_1^\circ \sqsubseteq^\circ M_2^\circ$*;*
2. *for each distribution* $\rho_1 \in \mathsf{ADistr}(M_1^\circ)$ *there exists a pseudo-distribution* $\delta \in \mathsf{Distr}(S_1^\circ \times S_2^\circ)$ *and a distribution* $\rho_2 \in \mathsf{ADistr}(M_2^\circ)$ *such that, for any* ${N_1}^\circ \in {S_1}^\circ$ *and* ${N_2}^\circ \in {S_2}^\circ$*:*
   (a) $\rho_1(N_1^\circ) = \sum_{N_2^\circ \in S_2^\circ} \delta(N_1^\circ, N_2^\circ)$ *and* $\rho_2(N_2^\circ) = \sum_{N_1^\circ \in S_1^\circ} \delta(N_1^\circ, N_2^\circ)$*;*
   (b) *if* $\delta(N_1^\circ, N_2^\circ) > 0$ *then*
      i. $M_1^\circ \neq N_1^\circ$ *iff* $M_2^\circ \neq N_2^\circ$*;*
      ii. $N_1^\circ \preccurlyeq_{mc} N_2^\circ$*.*

We say that ${mc_1}^\circ \sqsubseteq^\circ_{mc} {mc_2}^\circ$ *iff* $M_{0,1}^\circ \preccurlyeq_{mc} M_{0,2}^\circ$*.*

The approximation order $\sqsubseteq^\circ_{mc}$ is based on a sort of probabilistic simulation between abstract states. In particular, an abstract state M_2° simulates an abstract state M_1° ($M_1^\circ \preccurlyeq_{mc} M_2^\circ$) provided that: 1. M_2° approximates M_1°; 2. the set of admissible distributions for M_2° *over-approximates* that of M_1°. Condition 2. requires that each probability distribution ρ_1, associated to M_1°, is matched by a corresponding probability distribution ρ_2, associated to M_2°. Given that different abstract states of S_1° can be abstracted by the same abstract state of S_2°, then their values of probability reported by ρ_1 have to be summed up in the probability distribution ρ_2. This calculation is realized by means of a pseudo-distribution $\delta \in \mathsf{Distr}(S_1^\circ \times S_2^\circ)$, as it is captured by requirement (a). As in the case of Definition 4.12, requirement (b) assures us that approximations preserves the self-loops without introducing new ones.

The following theorem shows that the notion of approximation order $\sqsubseteq^\circ_{mc}$ is *sound* for the property of probabilistic termination. If ${mc_2}^\circ$ safely approximates ${mc_1}^\circ$, that is ${mc_1}^\circ \sqsubseteq^\circ_{mc} {mc_2}^\circ$, then the lower and upper bounds for probabilistic termination over ${mc_1}^\circ$ are finer than those over ${mc_2}^\circ$. Obviously, this result refers to the values of probability calculated for two abstract states M_1° and M_2° of ${mc_1}^\circ$ and ${mc_2}^\circ$ such that $M_1^\circ \preccurlyeq_{mc} M_2^\circ$ (thus, including the initial states).

Theorem 5.9 (Soundness of the order). *Let* $mc_i^\circ = (S_i{}^\circ, \mathbf{P}_i^-, \mathbf{P}_i^+, \mathbf{L}_i, M_{0,i}^\circ)$ *be two* IMC *and let* $M_i{}^\circ \in S_i{}^\circ$*, for* $i \in \{1,2\}$*. If* $M_1{}^\circ \preccurlyeq_{mc} M_2{}^\circ$*, then*

$$\mathsf{Reach}^-_{mc_2^\circ}(M_2{}^\circ) \leq \mathsf{Reach}^-_{mc_1^\circ}(M_1{}^\circ) \leq \mathsf{Reach}^+_{mc_1^\circ}(M_1{}^\circ) \leq \mathsf{Reach}^+_{mc_2^\circ}(M_2{}^\circ).$$

The proof of Theorem 5.9 can be found in AppendixB.

Similarly as in the case of abstract LTS, we introduce a *best abstraction* function which can be used to relate DTMC and IMC.

Definition 5.10 (Best abstraction). *We define* $\alpha_{MC} : \mathcal{MC} \rightarrow \mathcal{IMC}^{\circ}$ *such that*

$$\alpha_{MC}((S, \mathbf{P}, \mathbf{L}, M_0)) = (\{M^{\bullet}\}_{M \in S}, \mathbf{P}^{-}_{\alpha}, \mathbf{P}^{+}_{\alpha}, \mathbf{L}, M_0{}^{\bullet}),$$

where $\mathbf{P}^{-}_{\alpha}(M_1{}^{\bullet}, M_2{}^{\bullet}) = \mathbf{P}^{+}_{\alpha}(M_1{}^{\bullet}, M_2{}^{\bullet}) = \mathbf{P}(M_1)(M_2)$.

Also in this case, the IMC $\alpha_{MC}(mc)$ which is the best approximation of a DTMC mc, gives a representation equivalent to mc. In particular, $\alpha_{MC}(mc)$ has exact intervals of multiplicity in the abstract states and exact intervals of probability on transitions. As a consequence of the previous definition and of the Condition iii) of Definition 2.3, we can state the following proposition.

Proposition 5.11. *Let* $mc = (S, \mathbf{P}, \mathbf{L}, M_0)$ *be a DTMC. For all* $M \in S$,

$$\mathsf{Reach}_{mc}(M) = \mathsf{Reach}^{+}_{\alpha_{MC}(mc)}(M^{\bullet}) = \mathsf{Reach}^{-}_{\alpha_{MC}(mc)}(M^{\bullet})$$

Using function α_{MC}, we can formally define when an IMC mc° safely approximates a DTMC mc, i.e., $\alpha_{MC}(mc) \sqsubseteq^{\circ}_{mc} mc^{\circ}$.

6. Abstract Probabilistic Semantics

We define the abstract probabilistic semantics of CGF, by giving a systematic method for deriving an IMC from an abstract LTS. Moreover, we prove the soundness of the abstract probabilistic semantics with respect to the set of DTMC which are approximated. The main result shows that abstract probabilistic model checking reports lower and upper bounds for probabilistic termination which are conservative with respect to the concrete ones.

6.1. Derivation of the IMC

The abstract LTS semantics reports on transitions a label representing the reaction (obtained from the tags of the basic actions which participate in the move), intervals of multiplicity representing a possible range of multiplicities for the related reagent variables, and the rate of the basic action. Therefore, the IMC derived from an abstract LTS will have for each move a set of labels, corresponding to the set of reactions, and a related interval of probability. Obviously, the difficult part of the translation consists in computing the *intervals of probability* for each move from the information recorded on the associated abstract transition labels.

The methodology that is applied for calculating the intervals of probability corresponding to a move from an abstract state M° to an abstract state M'° is similar to the one used in the concrete case. First, the *abstract rate* of the move from M° to M'° is derived from the abstract rates of the abstract transitions from M° to M'° (reported by $\mathsf{Ts}(M^{\circ}, M'^{\circ})$). Then, the related interval of probability is calculated by taking into account the abstract rate of the abstract transitions exiting from M° (reported by $\mathsf{Ts}(M^{\circ})$).

We recall that in the concrete case, the *exit rate* for a multiset M represents precisely the rate of *all the transitions* exiting from M (reported by $\mathsf{Ts}(M)$). In

the abstract case, however, the conflict expressed by labels shows that not all the abstract transitions exiting from an abstract state M° approximate moves of the same multiset M that is represented by M° (e.g. $M \in \gamma(M^\circ)$). It should be clear that the information on conflicting labels has to be profitably exploited in order to limit the non-determinism introduced by the abstraction and thus to derive more precise intervals of probability.

A possible strategy for exploiting the labeling of the abstract LTS consists of considering, for any abstract state M°, *different abstract exit rates*, each corresponding to a maximal set of transitions of $\mathsf{Ts}(M^\circ)$ having non conflicting labels. In this case, the interval of probability for the move from M° to an abstract state M'° requires to take into account all the abstract exit rates for M° which contain a transition of $\mathsf{Ts}(M^\circ, M'^\circ)$. Intuitively, the interval of probability can be calculated by combining the abstract rate of the move $\mathsf{Ts}(M^\circ, M'^\circ)$ with each abstract exit rate for M° that includes a transition of $\mathsf{Ts}(M^\circ, M'^\circ)$.

Note that, in the abstract case, the *abstract rate* of a transition will be an *interval of rates* that can be derived from the information recorded on abstract transition labels, similarly as in the concrete case. Intuitively, the abstract rate of a transition can be obtained, by multiplying the rate r of the basic action with the minimum and the maximum multiplicities of the reagent variables, which participate in the move.

In order to illustrate the proposed technique for calculating the intervals of probability we consider again the system commented in Examples 3.1, 4.15 and 5.1 and we examine the situation for the abstract state M_5°,

$$M_5^\circ = \{([1,3], X), ([1,3], Y)\}.$$

The fragment of abstract LTS reporting the transitions exiting from M_5° (denoted by t_1°, t_2°, t_3° and t_4°) is illustrated in Fig. 7(a), where

$$\begin{array}{ll} {M_6}^\circ = \{([2,4], X), ([0,0], Y)\} & {M_7}^\circ = \{([2,4], X), ([1,2], Y)\} \\ {M_0}^\circ = \{([0,0], X), ([2,4], Y)\} & {M_4}^\circ = \{([1,2], X), ([2,4], Y)\} \end{array}$$

We also recall that the environment E models the reactions $R_1 : X + Y \to X + X$ and $R_2 : X + Y \to Y + Y$. The transitions modeling reaction R_1 are decorated by label (λ, μ), while those modeling reaction R_2 are decorated by label (δ, η).

For M_5° there are four combinations of transitions with non conflicting labels: (a) t_1° and t_3°, (b) t_1° and t_4°, (c) t_2° and t_3°, (d) t_2° and t_4°. Each combination (a), (b), (c) or (d) lead to a different *abstract exit rate* for M_5°, denoted by $\mathbf{E}_a^\circ(M_5^\circ), \mathbf{E}_b^\circ(M_5^\circ)$, $\mathbf{E}_c^\circ(M_5^\circ)$ and $\mathbf{E}_d^\circ(M_5^\circ)$, respectively.

The abstract exit rates $\mathbf{E}_a^\circ(M_5^\circ), \mathbf{E}_b^\circ(M_5^\circ)$, $\mathbf{E}_c^\circ(M_5^\circ)$ and $\mathbf{E}_d^\circ(M_5^\circ)$ can be used in order to calculate the interval of probability associated to the abstract transitions t_1°, t_2°, t_3° and t_4°. As an example, we explain how the interval of probability for the move from M_5° to M_6° (corresponding to transition t_1°) can be derived. In this case, we have to take into account two abstract exit rates, corresponding to combinations (a) and (b), that include transition t_1°.

The calculation requires to compute the abstract rates of transitions t_1°,t_3° and t_4°. For each transition the abstract rate can easily be derived by multiplying the rate r of both reactions with the minimum and the maximum multiplicities of reagents X and Y, in the corresponding intervals of multiplicity. Thus, we obtain the following intervals of rates

$$\begin{aligned}\mathsf{rate}^\circ({t_1}^\circ) &= [1 \cdot r, 2 \cdot r]\\ \mathsf{rate}^\circ({t_3}^\circ) &= [1 \cdot r, 2 \cdot r]\\ \mathsf{rate}^\circ({t_4}^\circ) &= [2 \cdot r, 4 \cdot r]\end{aligned}$$

Then, for the abstract exit rates $\mathbf{E}_a^\circ(M_5^\circ)$ and $\mathbf{E}_b^\circ(M_5^\circ)$ related to combinations (a) and (b), we have the following intervals of rates,

$$\mathbf{E}_a^\circ(M_5^\circ) = \mathsf{rate}^\circ({t_1}^\circ) + \mathsf{rate}^\circ({t_3}^\circ) = [2 \cdot r, 4 \cdot r]$$

$$\mathbf{E}_b^\circ(M_5^\circ) = \mathsf{rate}^\circ({t_1}^\circ) + \mathsf{rate}^\circ({t_4}^\circ) = [3 \cdot r, 6 \cdot r].$$

Now, the interval of probability for the move corresponding to t_1° can easily be derived from the previous information. For each combination $i \in \{a, b\}$, by minimizing and maximizing the expression $\frac{\mathsf{rate}^\circ({t_1}^\circ)}{\mathbf{E}_i^\circ(M_5^\circ)}$ we obtain a lower and an upper bound for the probability of the move t_1° w.r.t. to combination (i). Hence, the interval of probability for the move t_1° can be derived from the lower and upper bounds of each combination. We obtain

$$min(\frac{\mathsf{rate}^\circ({t_1}^\circ)}{\mathbf{E}_a^\circ(M_5^\circ)}) = 1/4 \qquad max(\frac{\mathsf{rate}^\circ({t_1}^\circ)}{\mathbf{E}_a^\circ(M_5^\circ)}) = 1 \tag{4}$$

$$min(\frac{\mathsf{rate}^\circ({t_1}^\circ)}{\mathbf{E}_b^\circ(M_5^\circ)}) = 1/6 \qquad max(\frac{\mathsf{rate}^\circ({t_1}^\circ)}{\mathbf{E}_b^\circ(M_5^\circ)}) = 2/3. \tag{5}$$

Thus, the interval of probability for the move t_1° is [1/6,1].

The technique illustrated by the previous example has two main drawbacks: (i) the intervals of probability obtained are not accurate; (ii) it is computationally very expensive.

As far as it concerns (i), the technique uses a direct calculation of the abstract rates of transitions which introduces a clear loss of information. For example, let us consider the interval of probability $[1/4, 1]$ for the move t_1°, corresponding to combination (a), as it illustrated in (4). The minimum and maximum values for the expression (4) do not correspond to any coherent values for the reagent variables X and Y appearing in reactions R_1 and R_2. In other words, in this calculation, the relational information about the concentrations of reagents X and Y is lost.

Hence, we propose a *symbolic approach* for computing the abstract rates that better exploits the information on the possible multiplicity of reagents, recorded

on abstract transition labels. The idea is that the abstract rate assigned to a transition will be represented by a *symbolic expression on reagent variables*, expressing again an interval of rates.

By applying a symbolic approach, we will obtain for the move t_1° and combination (a) the following expression

$$\frac{\mathsf{rate}^\circ(t_1{}^\circ)}{\mathbf{E}_a^\circ(M_5^\circ)} = \frac{X \cdot Y \cdot r}{X \cdot Y \cdot r + X \cdot Y \cdot r} \text{ where } X \in [1,2], Y \in [1,2] \tag{6}$$

Expression (6) is derived from the abstract rates of transitions t_1° and t_3°, similarly as it is explained in the calculation of (4). Moreover, for each transition the abstract rate can easily be computed from the information reported on the abstract transition labels: the number of reagent variables X and Y, which interact in reactions R_1 and R_2, the related intervals of multiplicity representing their possible number of occurrences and the rate of the basic action r.

Then, by minimizing and maximizing expression (6) we will obtain lower and upper bound for the probability of the move t_1° related to combination (a),

$$min(\frac{\mathsf{rate}^\circ(t_1{}^\circ)}{\mathbf{E}_a^\circ(M_5^\circ)}) = max(\frac{\mathsf{rate}^\circ(t_1{}^\circ)}{\mathbf{E}_a^\circ(M_5^\circ)}) = 1/2 \tag{7}$$

The minimum of the symbolic expression corresponds to the values $X = 1$ and $Y = 1$, while the maximum corresponds to the values $X = 2$ and $Y = 2$. Notice that the interval of probability $[1/4, 1]$ for the move t_1°, related to combination (a), calculated in (4) using a direct calculation of abstract rates, is much less precise than the corresponding exact interval $[1/2, 1/2]$, obtained in (7).

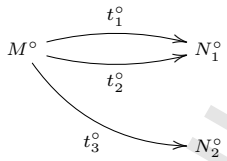
As far as it concerns (ii), the previously proposed methodology for computing the interval of probability for the moves from an abstract state M° requires to calculate different *abstract exit rates*, each corresponding to a maximal set of transitions included in $\mathsf{Ts}(M^\circ)$ with non conflicting labels. In particular, the derivation of the interval of probability for the move from M° to M'° requires to take into account all the abstract exit rates for M° which contain a transition of $\mathsf{Ts}(M^\circ, M'^\circ)$. Specifically, the abstract rate of the move $\mathsf{Ts}(M^\circ, M'^\circ)$ has to be combined with each abstract exit rate for M° that includes a transition of $\mathsf{Ts}(M^\circ, M'^\circ)$. In order to reduce the complexity of the calculation of the intervals of probability we propose a more efficient approximated calculation, based on the idea of computing, for an abstract state M°, a *unique exit rate* for each abstract state M'°. The abstract exit rate of M° with respect to M'°, denoted by $\mathbf{E}^\circ_{M'^\circ}(M^\circ)$, reports the abstract rate of all the transitions, contained in $\mathsf{Ts}(M^\circ)$, which *may appear in parallel with the transitions of* $\mathsf{Ts}(M^\circ, M'^\circ)$. In this case, the interval of probability for the move from M° to M'° can be derived from the abstract rate of the move $\mathsf{Ts}(M^\circ, M'^\circ)$ and from the abstract exit rate of M° with respect to M'°.

We now introduce the concepts that are necessary to formally define the abstract probabilistic function that translates an abstract LTS into an IMC.

In order to simplify the presentation we introduce the formal definition of the translation from abstract LTS to IMC, for a particular class of LTS. More in detail, we consider abstract LTS where more than one transition may be decorated by the same label but the following condition on labels holds

$$\forall M^\circ, N_1^\circ, \nexists t^\circ \in \mathsf{Ts}(M^\circ, N_2^\circ), max(\mathsf{rate}^\circ(t^\circ)) > 0, N_2^\circ \neq N_1^\circ, \quad \text{such that}$$
$$\mathsf{label}(\{t^\circ \in \mathsf{Ts}(M^\circ, N_1^\circ) \mid \ max(\mathsf{rate}^\circ(t^\circ)) > 0\}) \supset \mathsf{label}(t^\circ) \supset \emptyset \quad (8)$$

Roughly speaking the previous condition avoids the situation illustrated in Fig.8



with $\mathsf{label}(t_2^\circ) = \mathsf{label}(t_3^\circ)$ and $\mathsf{label}(t_1^\circ) \neq \mathsf{label}(t_2^\circ)$.

Figure 8: A LTS not satisfying Condition(8)

This case complicates the calculation of the exit rate, corresponding to the move from M° to N_1°, because the rates of transitions t_1° and t_2° cannot simply be summed up. Actually, the conflict between the labels of t_2° and t_3° has to be taken into account.

Note that we need the set inclusion to be strict in the Condition(8), indeed, if $\mathsf{label}(\{t^\circ \in \mathsf{Ts}(M^\circ, N_1^\circ) \mid \ max(\mathsf{rate}^\circ(t^\circ)) > 0\})$ was equal to $\mathsf{label}(t^\circ) \supset \emptyset$, then we were in the standard case where two different transitions share the same label, and in this case, the conflict can be well captured by the labeling function $\mathsf{label}(.)$.

In AppendixB, we will discuss how to cope with the more general situation illustrated in Fig.8.

In order to express the abstract rates (representing intervals of rates) in a symbolic way we adopt the following domain of *constrained symbolic expressions* (expression for short) $\mathcal{E}$. An *expression* $e \in \mathcal{E}$ is a pair $(z, c) : \mathcal{Z} \times \mathcal{C}$ such that

1. $z \in \mathcal{Z}$ is a term over reagent variables $\mathcal{X}$ and the arithmetic operators $\{+, \cdot, /, \widehat{-}\}$,
2. $c \in \mathcal{C}$ is a set of *membership constraints* of the form $X \in I$, where $X \in \mathcal{X}$ and $I \in \mathcal{I}$.

We require that each expression $(z, c) \in \mathcal{E}$ is *well-formed* meaning that, for each variable X occurring in z, there exists exactly one constraint $X \in I$ occurring in c.

Moreover, we define the operators $+^\circ$ and $/^\circ$ on expressions of $\mathcal{E}$ as follows,

$$(z_1, c_1) +^\circ (z_2, c_2) \quad = \quad (z_1 \ + \ z_2, \bigcup_{X \in \mathcal{X}} \{X \in \bigcup^\circ_{(X \in I) \in c_i, i \in \{1,2\}} I\}),$$

$$(z_1, c_1) /^\circ (z_2, c_2) \quad = \quad (z_1 \ / \ z_2, c_1 \cup \{(X \in I) \in c_2 \ \mid \nexists (X \in I') \in c_1\}).$$

Then, similarly as in the concrete case we introduce functions that calculate the *abstract rate* of an abstract transition, the *abstract rate* of a move and the *abstract exit rate* for an abstract state.

Let $(S^\circ, \rightarrow^\circ, {M_0}^\circ, E)$ be an abstract LTS, ${M'}^\circ \in S^\circ$ be an abstract state and $Ts^\circ \subseteq \rightarrow^\circ$ be a set of abstract transitions. We define functions $\mathsf{rate}^\circ : TS^\circ \rightarrow \mathcal{E}$, $\mathbf{R}^\circ : S^\circ \times S^\circ \rightarrow \mathcal{E}$ and $\mathbf{E}^\circ_{M'^\circ} : S^\circ \rightarrow \mathcal{E}$, such that for each $M^\circ \in S^\circ$ and $t^\circ = M^\circ \xrightarrow[\circ]{\Theta,\Delta^\circ,r} {M'}^\circ \in \rightarrow^\circ$,

$$\mathsf{rate}^\circ(t^\circ) = \begin{cases} (X \cdot r, \{X \in I\}) & \Theta = \lambda, \Delta^\circ = I, \lambda \in \mathcal{L}(E(X)), \\ (X \cdot (X \widehat{-} 1) \cdot r, \{X \in I\}) & \Theta = (\lambda, \mu), \Delta^\circ = (I, I), \lambda, \mu \in \mathcal{L}(E(X)), \\ (X \cdot Y \cdot r, \{X \in I, Y \in I'\}) & \Theta = (\lambda, \mu), \Delta^\circ = (I, I'), \lambda \in \mathcal{L}(E(X)), \\ & \mu \in \mathcal{L}(E(Y)), X \neq Y. \end{cases}$$

$$\begin{array}{lcl} \mathbf{R}^\circ(M^\circ, {M'}^\circ) & = & \sum^\circ_{t^\circ \in \mathsf{Ts}(M^\circ, {M'}^\circ)} \mathsf{rate}^\circ(t^\circ) \\ \mathbf{E}^\circ_{M'^\circ}(M^\circ) & = & \sum^\circ_{(z,c) \in \mathsf{rate}(\mathsf{Ts}_{\setminus {M'}^\circ}(M^\circ) \cup \mathsf{Ts}(M^\circ, {M'}^\circ))} (z, c) \\ \mathsf{rate}(Ts^\circ) & = & \{r_\Theta \mid \Theta \in \widehat{\mathcal{L}}, r_\Theta = \bigcup^\circ_{\{t^\circ \in Ts^\circ, \mathsf{label}(t^\circ) = \Theta\}} \mathsf{rate}(t^\circ)\} \\ \mathsf{Ts}_{\setminus {M'}^\circ}(M^\circ) & = & \{t^\circ \in \mathsf{Ts}(M^\circ) \mid \mathsf{target}(t^\circ) \neq {M'}^\circ, \mathsf{label}(t^\circ) \text{ not in conflict} \\ & & \quad \text{with } \mathsf{label}(\mathsf{Ts}(M^\circ, {M'}^\circ))\} \end{array}$$

Similarly as in the concrete case, the expression $\mathsf{rate}^\circ(t^\circ)$ reports the *abstract rate* (representing an interval of rates) of transition t° that depends on the rate r of the basic action, on the intervals of multiplicities of the reagents which participate (recorded by Δ°) and on the type of reaction (recorded by Θ).

Function $\mathbf{R}^\circ(M^\circ, {M'}^\circ)$ reports the *abstract rate* (representing an interval of rates) of the move from M° to ${M'}^\circ$. This is calculated by summing up the expressions representing the interval of rates for all transitions from M° to ${M'}^\circ$ (reported by $\mathsf{Ts}(M^\circ, {M'}^\circ)$).

Moreover, $\mathbf{E}^\circ_{M'^\circ}(M^\circ)$ gives the *abstract exit rate* of an abstract state M° with respect to an abstract state ${M'}^\circ$. This is the abstract rate of all the transitions exiting from M° which may appear in parallel with the transitions in $\mathsf{Ts}(M^\circ, {M'}^\circ)$. In particular, $\mathsf{Ts}_{\setminus {M'}^\circ}(M^\circ) \subseteq \mathsf{Ts}(M^\circ)$ reports the transitions which may appear in parallel with a transition of $\mathsf{Ts}(M^\circ, {M'}^\circ)$. In the calculation of $\mathbf{E}^\circ_{M'^\circ}(M^\circ)$ the abstract rates of transitions with the same label are merged (namely approximated) by taking the union of the membership constraints.

In conclusion, the interval of probability for the move from an abstract state M° to an abstract state ${M'}^\circ$ can be calculated from the expressions $\mathbf{R}^\circ(M^\circ, {M'}^\circ)$ and $\mathbf{E}^\circ_{M'^\circ}(M^\circ)$. Intuitively, the lower and upper bounds for the probability of that move are obtained by minimizing and maximizing the solution of the expression $\mathbf{R}^\circ(M^\circ, {M'}^\circ)/^\circ\mathbf{E}^\circ_{M'^\circ}(M^\circ)$, respectively.

Definition 6.1. *We define the* abstract probabilistic translation *function* $\mathbf{H}^\circ : \mathcal{LTS}^\circ \rightarrow \mathcal{IMC}^\circ$ *such that* $\mathbf{H}^\circ((S^\circ, \rightarrow^\circ, {M_0}^\circ, E)) = (S^\circ, \mathbf{P}^-, \mathbf{P}^+, \mathbf{L}, M_0^\circ)$ *where*

- $\mathbf{P}^-$, $\mathbf{P}^+$: $S^\circ \to \mathsf{SDistr}(S^\circ)$ *are the* lower *and* upper *probability functions, such that for each* $M^\circ \in S^\circ$*:*

  a) *for each* $M'^\circ \in S^\circ$*, such that* $max(\mathbf{E}^\circ_{M'^\circ}(M^\circ)) > 0$*, if* $min(\mathbf{R}^\circ(M^\circ, M'^\circ)) = 0$*, then also* $\mathbf{P}^-(M^\circ)(M'^\circ) = 0$*, otherwise,* $\mathbf{P}^-(M^\circ)(M'^\circ) = min(\mathbf{R}^\circ(M^\circ, M'^\circ)/^\circ\mathbf{E}^\circ_{M'^\circ}(M^\circ))$*. Analogously, the* $\mathbf{P}^+$ *function is obtained by substituting in the previous definition, the min function with the max function;*

  b) *if, for each* $M'^\circ \in S^\circ$*,* $max(\mathbf{E}^\circ_{M'^\circ}(M^\circ)) = 0$*, then* $\mathbf{P}^+ = \mathbf{P}^-$*,* $\mathbf{P}^+(M^\circ)(M^\circ) = 1$*, and* $\forall M'^\circ \neq M^\circ$*,* $\mathbf{P}^+(M^\circ), (M'^\circ) = 0$*;*

  c) *if,* $\exists M'^\circ \in S^\circ$*, such that* $max(\mathbf{E}^\circ_{M'^\circ}(M^\circ)) > 0$ *and* $min(\mathbf{E}^\circ_{M'^\circ}(M^\circ)) = 0$ *then* $\mathbf{P}^+(M^\circ)(M^\circ) = 1$*, and* $\mathbf{P}^-(M^\circ), (M^\circ) = 0$*.*

- $\mathbf{L} : S^\circ \to (S^\circ \to \wp(\widehat{\mathcal{L}}))$ *is a labeling function such that* $\forall M^\circ_1, M^\circ_2 \in S^\circ$*,* $\mathbf{L}(M^\circ_1, M^\circ_2) = \mathsf{label}(\{t^\circ \in \mathsf{Ts}(M^\circ_1, M^\circ_2) \mid max(\mathsf{rate}^\circ(t^\circ)) > 0\})$.

The lower and upper bound probabilities for the move from M° to M'° are computed by minimizing and maximizing the solution of the expression $\mathbf{R}^\circ(M^\circ, M'^\circ)/^\circ\mathbf{E}^\circ_{M'^\circ}(M^\circ)$, respectively. This reasoning has to be properly combined with the special cases when $max(\mathbf{E}^\circ_{M'^\circ}(M^\circ)) = 0$ or $min(\mathbf{E}^\circ_{M'^\circ}(M^\circ)) = 0$. When $max(\mathbf{E}^\circ_{M'^\circ}(M^\circ)) = 0$ all the states represented by M° are terminated, while when $min(\mathbf{E}^\circ_{M'^\circ}(M^\circ)) = 0$ at least one state represented by M° is terminated.

In order to find the maximum and minimum of an expression $e = (z, c) \in \mathcal{E}$, when it's not trivial, it's sufficient to evaluate the symbolic term z for the *stationary points* (that can be found by differentiate z and by setting the result equal to 0) and for the boundaries of the intervals in c constraining variables of z.

Remark 6.2. *It is worth stressing the role of the information recorded on abstract transition labels in the calculation of the abstract probabilistic semantics. We adopt abstract transitions such as* $M^\circ_1 \xrightarrow[\circ]{\Theta, \Delta^\circ, r} M^\circ_2$ *where* $r \in \mathbb{R}^+$*,* $\Theta \in \widehat{\mathcal{L}}$ *and* $\Delta^\circ \in \widehat{Q}^\circ = \mathcal{I} \cup (\mathcal{I} \times \mathcal{I})$*. Similarly as in the concrete case,* Θ *is a label reporting the tag (the tags) of the basic action (actions), which participate (participates) in the move,* Δ° *reports consistent intervals of multiplicity, while* r *is the rate of the basic action.*

The label Θ *identifies the reaction and it allows us to observe the cases of conflicting labels. This information not only is translated into the corresponding probabilistic semantics but also it is exploited in order to calculate the intervals of probability corresponding to the move.*

Moreover, the components r *and* Δ° *record the rate of the basic action and the intervals of multiplicity of the reagent variables, which participate in the move. This information supports the symbolic approach in the calculation of abstract rates which gives finer intervals of probability w.r.t. the approach based on the direct calculation of rates.*

6.2. Soundness with respect to Probabilistic Termination

We prove the soundness of the abstract probabilistic semantics of CGF with respect to probabilistic termination.

The following theorems show properties of the probabilistic translation function $\mathbf{H}^\circ : \mathcal{LTS}^\circ \to \mathcal{IMC}^\circ$ which are used for proving the main theorem (Theorem 6.5). Theorem 6.3 shows that function $\mathbf{H}^\circ$ preserves the approximation order. If an abstract LTS lts_2° safely approximates an abstract LTS lts_1°, then the IMC derived from lts_2° safely approximates the one derived from lts_1°.

Theorem 6.3. *Let* $lts_i^\circ = ({S_i}^\circ, {\rightarrow_i}^\circ, {M_{0,i}}^\circ, E)$ *be two abstract LTS. If* $lts_1^\circ \sqsubseteq_{lts}^\circ lts_2^\circ$ *then* $\mathbf{H}^\circ(lts_1^\circ) \sqsubseteq_{mc}^\circ \mathbf{H}^\circ(lts_2^\circ)$.

Theorem 6.4. *Let* E *be an environment and* $M_0 \in \mathcal{M}$ *be a multiset. We have*

$$\alpha_{MC}(\mathbf{H}(\mathsf{LTS}((E, M_0)))) \sqsubseteq_{mc}^\circ \mathbf{H}^\circ(\alpha_{lts}(\mathsf{LTS}((E, M_0)))).$$

Next main result derives directly from Theorem 6.4 and the soundness of the abstract LTS semantics (given in Theorem 4.14). The theorem shows the soundness of the IMC describing the abstract probabilistic semantics of an abstract state M_0°, $\mathbf{H}^\circ(\mathsf{LTS}^\circ((E, M_0^\circ)))$, with respect to the set of DTMCs that are represented. For each multiset M_0 represented by the abstract state M_0° (that is $M_0 \in \gamma(M_0^\circ)$) the corresponding DTMC is given by $\mathbf{H}(\mathsf{LTS}((E, M_0)))$. Thus, we prove that the IMC $\mathbf{H}^\circ(\mathsf{LTS}^\circ((E, M_0^\circ)))$ *safely approximates* (w.r.t. the approximation order $\sqsubseteq_{mc}^\circ$)) the IMC, which is the *best abstraction* of the DTMC $\mathbf{H}(\mathsf{LTS}((E, M_0)))$.

Theorem 6.5 (Soundness of IMC). *Let* E *be an environment and* $M_0^\circ \in \mathcal{M}^\circ$ *be an abstract state. For each multiset* $M_0 \in \gamma(M_0^\circ)$ *we have*

$$\alpha_{MC}(\mathbf{H}(\mathsf{LTS}((E, M_0)))) \sqsubseteq_{mc}^\circ \mathbf{H}^\circ(\mathsf{LTS}^\circ((E, M_0^\circ))).$$

The proof of Theorems 6.3, 6.4 and 6.5 can be found in AppendixB.

Moreover, Theorem 5.9, Proposition 5.11 and Theorem 6.5 guarantee that the approach is sound for probabilistic termination meaning that the abstract probabilistic model gives conservative lower and upper bounds for probabilistic termination. More in detail, the lower and upper bounds for probabilistic termination calculated over the IMC $\mathbf{H}^\circ(\mathsf{LTS}^\circ((E, M_0^\circ)))$ include the value for probabilistic termination calculated over the DTMC $\mathbf{H}(\mathsf{LTS}((E, M_0)))$, for each multiset M_0 represented by M_0° (that is $M_0 \in \gamma(M_0^\circ)$).

It is worth discussing the complexity of the IMC that models the abstract probabilistic semantics of abstract CGF systems. For each environment E and abstract state M_0°, the IMC $\mathbf{H}^\circ(\mathsf{LTS}^\circ((E, M_0^\circ)))$ has the same number of states than the corresponding abstract LTS $\mathsf{LTS}^\circ((E, M_0^\circ))$. The dimension of $\mathsf{LTS}^\circ((E, M_0^\circ))$ is discussed in Section 4.4 considering both the number of abstract states and the number of transitions. Moreover, in the IMC for each abstract state there is exactly one move into any another state that is decorated by the union of labels associated to the corresponding LTS transitions. Finally,

for each abstract state M° the cost of computing the intervals of probability for each move is linear in the dimension of $\mathsf{Ts}(M^\circ)$. Hence, the main source of complexity of the derivation and of the dimension of the IMC resides in the dimension of the corresponding abstract LTS $\mathsf{LTS}^\circ((E, M_0^\circ))$.

Notice that, in general, for computing the upper (resp. lower) bound for probabilistic termination, we have to consider the computations reaching a $\exists$-terminated state (resp. $\forall$-terminated state). However, by construction, the IMC modeling the semantics of CGF has no hybrid abstract states, hence, in our case, $\exists$-terminated and $\forall$-terminated states coincide. Therefore, in the following we will call a $\forall - \exists$-terminated state simply terminated state.

Example 6.6. *We consider the environment E, introduced in Example 3.1 which models the reaction $R_1 : X + Y \to X + X$ and $R_2 : X + Y \to Y + Y$ of the the 2-way oscillator,*

$$E \triangleq \quad X = a_r^\lambda.X + \bar{b}_r^\delta.Y, \quad Y = \bar{a}_r^\mu.X + b_r^\eta.Y.$$

Fig. 9 shows the IMC $\mathbf{H}^\circ(\mathsf{LTS}^\circ((E, M_5^\circ)))$, called here mc°, modeling the abstract probabilistic semantics of the biological system for the initial abstract state $M_5^\circ = \{([1,3], X), ([1,3], Y)\}$, where

$$\begin{array}{ll} M_0{}^\circ = \{([0,0], X), ([2,4], Y)\} & M_6{}^\circ = \{([2,4], X), ([0,0], Y)\} \\ M_4{}^\circ = \{([1,2], X), ([2,4], Y)\} & M_1{}^\circ = \{([0,0], X), ([3,5], Y)\} \\ M_3{}^\circ = \{([1,1], X), ([3,5], Y)\} & M_2{}^\circ = \{([0,0], X), ([4,6], Y)\} \\ M_7{}^\circ = \{([2,4], X), ([1,2], Y)\} & M_8{}^\circ = \{([3,5], X), ([0,0], Y)\} \\ M_9{}^\circ = \{([3,5], X), ([1,1], Y)\} & M_{10}{}^\circ = \{([4,6], X), ([0,0], Y)\} \end{array}$$

The IMC mc° is derived from the corresponding abstract LTS $\mathsf{LTS}^\circ((E, M_5^\circ))$ which is shown in Fig. 6 and commented in Example 4.15.

In the IMC of Fig. 9 the intervals of probability are exact. Thus, the admissible distributions associated to each abstract state correspond precisely to the combinations of moves with non conflicting labels. More in detail, mc° reports: for the initial state M_5° four admissible distribution, for the abstract states M_4° and M_7° two admissible distributions and for any other abstract state exactly one admissible distribution. In particular, the abstract states M_0°, M_1°, M_2°,M_6°, M_8° and M_{10}° are terminated.

The abstract model mc° does not introduce any loss of information for probabilistic termination w.r.t. the concrete behavior. In fact, we have for the lower and upper bound of probabilistic termination $\mathsf{Reach}^-_{mc^\circ}(M_5^\circ) = \mathsf{Reach}^+_{mc^\circ}(M_5^\circ) = 1$. This says that each system with initial concentrations of reagents X and Y varying inside interval [1,3] universally terminates.

Notice that in the IMC mc° the intervals of probability (and thus the corresponding set of admissible distributions) not only over-approximates *the concrete behavior but they are also the* most precise. *As an example, let us discuss the case of the initial abstract state M_5°, similar arguments can be applied to any other abstract state. The IMC mc° reports for M_5° the same situation of the*

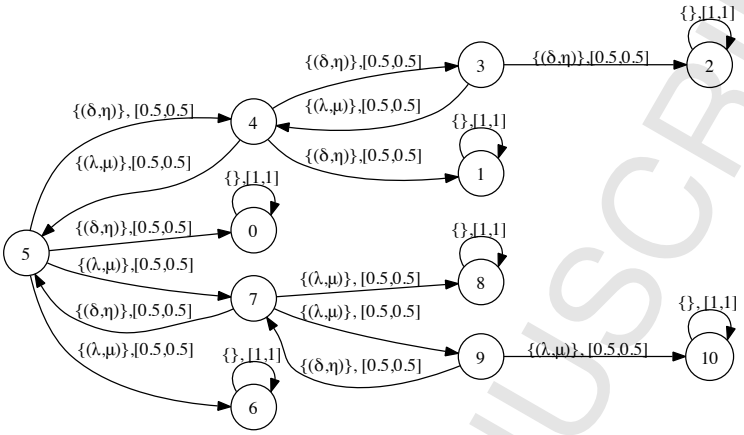


Figure 9: The IMC mc° for the 2-way oscillator

IMC which is illustrated in Fig. 7(c) and commented in Example 5.5. As it is discussed in Examples 5.1 and 5.5, the IMC gives for M_5° four admissible distributions, corresponding to the combinations of moves with non conflicting labels, which are precisely the probability distributions ρ_1, ρ_2, ρ_3 and ρ_4. Such probability distributions represent the most precise representation of the concrete probability distributions, corresponding to each exact concentration of reagents X and Y, varying into the intervals $[1, 3]$.

In this case, however, the intervals of probability of the IMC of Fig. 9 are calculated in an effective way *from the information reported on abstract transition labels. Nonetheless, the result obtained is the same that we would obtain by building the concrete probability distributions from the rates corresponding to reactions R_1 and R_2, for each concentration of reagents X and Y, varying into the corresponding intervals.* □

Example 6.7. *We modify the biological system modeling the 2-way oscillator, commented in Example 6.6 , by introducing a new "doping" reaction for reactant Y (in the style of [11]) : $R_3 : X + D_Y \to Y + Y$.*

The reaction R_3 is called a doping reaction *since it allows the production of a molecule Y even in absence of reactant Y, indeed now a new molecule of Y can be produced also from one molecule X and a new doping substance D_Y. The environment E_1 models the new system,*

$$E_1 \triangleq \quad X = a_r^\lambda.X + \bar{b}_r^\delta.Y + \bar{c}_r^\nu.Y \quad Y = \bar{a}_r^\mu.X + b_r^\eta.Y, \quad D_Y = c_r^\gamma.D_Y.$$

Fig. 11 describes the IMC $\mathbf{H}^\circ(\mathsf{LTS}^\circ((E_1, M_5^\circ)))$, called here mcd°, obtained from

the corresponding abstract LTS $\mathsf{LTS}^\circ((E_1, M_5^\circ))$ *of Fig. 10, for the initial abstract state*

$$M_5^\circ = \{([1,3], X), ([1,3], Y), ([1,1], D_Y)\}$$

where

$$\begin{aligned}
M_4{}^\circ &= \{([1,2], X), ([2,4], Y), ([1,1], D_Y)\}\\
M_0{}^\circ &= \{([0,0], X), ([2,4], Y), ([1,1], D_Y)\}\\
M_6{}^\circ &= \{([2,4], X), ([0,2], Y), ([1,1], D_Y)\}\\
M_1{}^\circ &= \{([0,0], X), ([3,5], Y), ([1,1], D_Y)\}\\
M_3{}^\circ &= \{([1,1], X), ([3,5], Y), ([1,1], D_Y)\}\\
M_7{}^\circ &= \{([3,5], X), ([0,1], Y)), ([1,1], D_Y)\}\\
M_2{}^\circ &= \{([0,0], X), ([4,6], Y), ([1,1], D_Y)\}\\
M_8{}^\circ &= \{([4,6], X), ([0,0], Y)), ([1,1], D_Y)
\end{aligned}$$

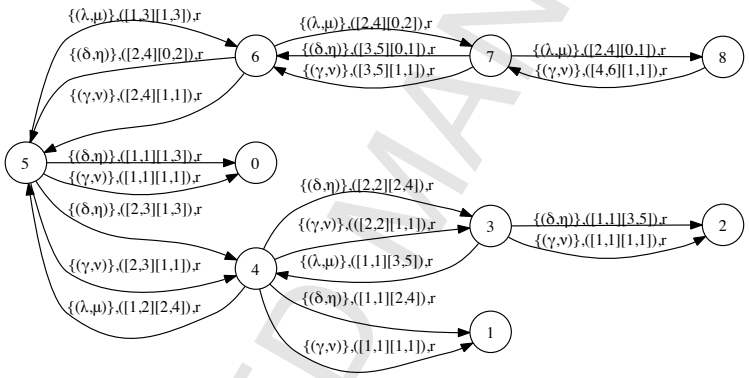


Figure 10: The LTS for the doping of Y

The abstract LTS for the biological system modeled by environment E_1 *is quite different w.r.t. the abstract LTS for the standard 2-way oscillator which is depicted in Fig. 6 and commented in Example 4.15. Specifically, in this case, much less abstract states are hybrid and need to be partitioned, since reaction* R_3 *(labeled by* (γ, ν)*) is enabled also when reactant* Y *is not available.*

Similarly as in Example 6.6, the IMC of Fig. 11 approximates the set of DTMCs modeling the same biological system with respect to different initial concentrations. In this case, however, the probability of reactions depends on concentrations of reagents X*,* Y *and* D_Y*. As a consequence, the intervals of probability of the IMC* mcd° *are not exact and represent for each move a possible range for the probability of that move, for all concentrations of reagents* X *and* Y *included in the corresponding intervals of multiplicity. Therefore, to each combination of moves with non conflicting labels is associated here a set of*

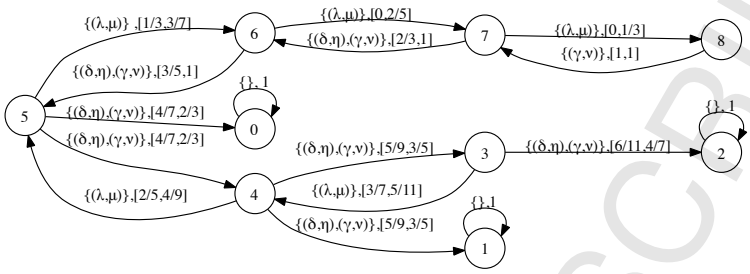


Figure 11: The IMC mcd° for the doping of Y

admissible distributions rather than a unique admissible distribution (as it is the case in the IMC of Example 6.6).

Nonetheless, similarly as in Example 6.6, the intervals of probability of mcd° *and thus also the associated set of admissible distributions are the* most precise *w.r.t. the concrete behavior. In this case, the lower and upper bounds for the probability of a move coincide with the minimum and maximum probability for that move for all concentrations of reagents* X *and* Y *varying in the corresponding intervals of multiplicities.*

Even if the intervals of probability of mcd° *are not exact, the abstract model does not introduce any loss of information for probabilistic termination: we have* $\mathsf{Reach}^-_{mcd^\circ}(M_5^\circ) = \mathsf{Reach}^+_{mcd^\circ}(M_5^\circ) = 1$*. Analogously as in Example 6.6, this shows that also for the version with the doping* Y*, for each initial concentrations of reagents* X *and* Y *varying inside interval [1,3], the system universally terminates.* □

7. Abstract Probabilistic Model Checking

In this section we illustrate the application of the proposed abstract probabilistic model checking technique. We revisit the standard and partially doped versions of the 2-ways oscillator already presented in Examples 6.6 and 6.7, considering wider intervals of concentrations in the initial abstract state. Moreover, we introduce a new fully doped version in the style of [11, 3]. For these systems we investigate probabilistic termination and some probabilistic reachability properties (the IMC is also sound w.r.t. simple reachability properties, as it is proved in [15]). In this section, the PRISM model checker is used to formally prove probabilistic properties on the MDPs derived from the corresponding IMCs. The translation of an IMC into an MDP is realized as already discussed in Section 5.1 by computing the extreme distributions from the intervals of probability.

7.1. The standard 2-way oscillator

The 2-way oscillator, commented in Examples 3.1, 4.15 and 6.6 is modeled by the following environment,

$$E \triangleq \quad X = a_r^{\lambda}.X + \bar{b}_r^{\delta}.Y, \qquad Y = \bar{a}_r^{\mu}.X + b_r^{\eta}.Y.$$

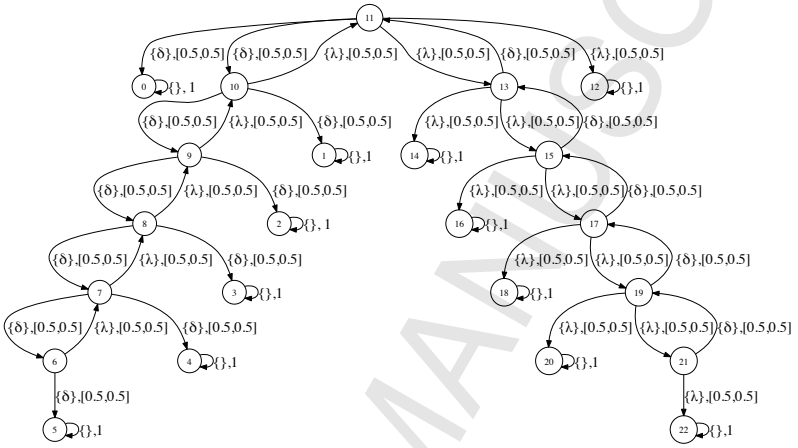


Figure 12: The IMC for the 2-ways oscillator

Fig. 12[7] shows the IMC modeling the abstract probabilistic semantics for the initial abstract state which has wider intervals of concentrations w.r.t. Example 6.6,

$$M_{11}^{\circ} = \{([1,6],X),([1,6],Y)\}.$$

Here, we have chosen to consider the IMC approximating 36 DTMCs, because the abstract model obtained is still manageable, easy to depict. However note that analogous results can be obtained for IMCs approximating a bigger number of DTMC, as we will discuss later in Section 7.3.

The abstract model checking of the previous IMC can be realized by translating it into a MDP, as explained in Section 5. Thus, the MDP (depicted in Fig. 14) is obtained by calculating, for each abstract state, the set of extreme distributions corresponding to each combination of non conflicting labels. Then, the PRISM model checker is used to verify the resulting MDP.

The encoding of the MDP in PRISM consists in encoding the states, the transitions between states and the information on the concentration of reagents

[7] To improve the reading, the label (λ,μ) is abbreviated simply by λ and the label (δ,η) by δ.

```
mdp

const int N=12;
const int M= 6;

module oscillator

        s : [0..22] init 11;
        minX:[0..N] init 1;
        maxX:[0..N] init M;
        minY: [0..N] init 1;
        maxY: [0..N] init M;
```

Figure 13: The PRISM code

in each state. In more detail, using variable definitions (see Fig. 13 for the PRISM code), we record for each state:

- information about the abstract state, specifically the variable $s \in [0...22]$ identifies the abstract state;
- information on the concentration of the reagents, in particular the variables $minX$ and $maxX$ are used to define the interval of concentration for reagent X, while $minY$ and $maxY$ are used to define the interval of concentration for Y.

It is worth noting that information on the abstract state (i.e. variable s) is redundant and could be omitted: any property can be expressed just in terms of the variables describing the concentrations of reagents X and Y. However, it is convenient to maintain this information in order to more easily address some termination properties.

We first verify if there are in our model *some reachable terminated states*. For this purpose we verify the following formula for $k = [0, 22]$,

$$Pmax =?[F(P >= 1[G(s = k)])] \tag{9}$$

That is, we ask for the maximum probability to reach a state where there is a self- loop with probability 1 . The result of verification of Formula (9) referred to the initial state M_{11}° is shown in Fig. 15.

This shows that there are 12 reachable terminated states, i.e. the states reachable with probability greater than 0 and in which the system loops forever.

Using the information about the terminated states we could verify the following formula to calculate the lower bound for probabilistic termination

$$Pmin =?[F((s = 0)|...|(s = 5)|(s = 12)|(s = 14)|(s = 16)|(s = 18)|(s = 20)|(s = 22)] \tag{10}$$

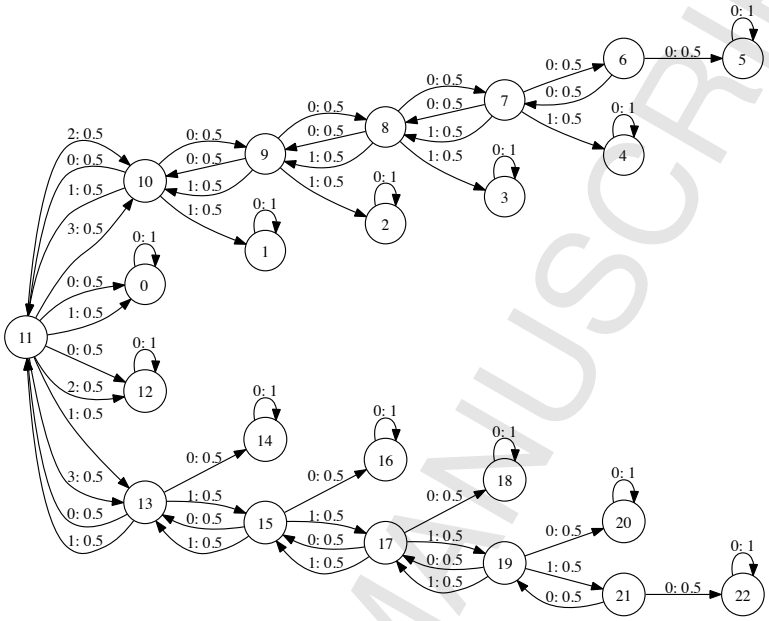


Figure 14: The MDP for the 2-ways oscillator

The result for the minimum probability being 1 assures us that the 2-ways oscillator system with any initial concentration of reagents $X \in [1, ..., 6], Y \in [1, ..., 6]$ universally terminates.

Probabilistic termination can also be observed using a simpler formulation: we ask for the abstract states where either the concentration of reagent X or the concentration of reagent Y is 0. This, for this version of the 2-ways oscillator, guarantees that the oscillation has finished. Formally, the lower and upper bound for probabilistic termination can be formalized as follows,

$$Pmin = ?[F(maxX = 0 | maxY = 0)] \tag{11}$$

$$Pmax = ?[F(maxX = 0 | maxY = 0)] \tag{12}$$

In both cases, the computed result is exactly 1.

Finally, we consider the following probabilistic reachability property (commented in Section 3): what is the probability that the oscillation terminates in a state which contains all reagents Y? Or analogously in a state which contains all reagents X?.

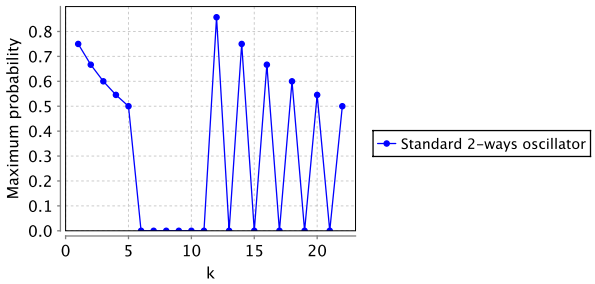


Figure 15: The terminated states of the 2-ways oscillator

In order to guarantee that an abstract state contains reagent X only it is enough to ask whether $maxY = 0$ holds. Thus, the lower and upper bound for the probabilistic property can be expressed by

$$Pmin = ?[F(maxY = 0)] \tag{13}$$

$$Pmax = ?[F(maxY = 0)] \tag{14}$$

In this case, the probability that the oscillation terminates in a state, which contains reagent X only, strictly depends on the initial concentrations of reagents X and Y. Since our abstract model approximate 36 experiments that differ for the initial concentration of X and Y, it should be clear that we will not obtain the same result for Formulas (13) and (14). In particular, the result of the verification of Formula (13) will give the lower bound by considering the worst case scenario for the probability to terminate in a state which contains reagent X only. Symmetrically, the result of the verification of Formula (14) will give the upper bound on the probability to terminate in a state containing reagent X only, by considering the best case scenario. Calculating the probabilities of (13) and (14) for the abstract state M_{11}° we obtain $Pmin = 0.142856$ and $Pmax = 0.185714$.

Note that these results are the *most precise* w.r.t. the set of DTMCs that are approximated by the IMC of Fig. 12. Indeed, the values of $Pmin$ and $Pmax$ computed on our abstract model exactly correspond to the results of the verification of formula $P = ?[F(Y = 0)]$ for particular DTMCs that the IMC of Fig. 12 approximates.

In particular, $Pmin = 0.142856$ is precisely the result of the verification of formula $P = ?[F(Y = 0)]$ for the DTMC related to the experiment with initial concentration $1X$ and $6Y$. Such system is depicted in Fig. 16[8], where the state formula $(Y = 0)$ is satisfied by state $M_7 = \{(7, X), (0, Y)\}$ only. On the other hand, $Pmax = 0.185714$ is precisely the result of the verification of formula $P = ?[F(Y = 0)]$ for the DTMC with initial concentration $6X$ and $1Y$.

[8] As before, (λ, μ) is abbreviated by λ and (δ, η) by δ.

Such DTMC can be obtained from the DTMC of Fig. 16 exchanging the role of variable X with variable Y, thus, model checking formula $P =?[F(Y = 0)]$ on the DTMC with initial concentrations $6X$ and $1Y$ is equivalent to model checking $P =?[F(X = 0)]$ on the DTMC of Fig. 16, where, in this case, the state formula $(X = 0)$ is satisfied by state $M_0 = \{(0, X), (7, Y)\}$ only.

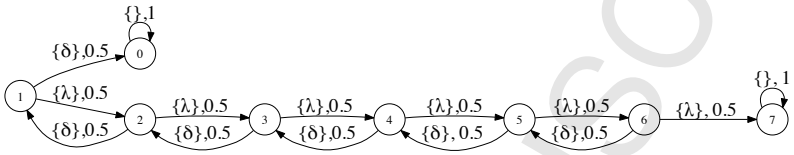


Figure 16: The DTMC for the initial state $\{(1, X), (6, Y)\}$

7.2. Adding doping reactions

In this section we investigate the effects of adding *doping* reactions to the previously illustrated system.

We first consider the partially doped system (already introduced in Example 6.7) obtained by adding the doping for reagent Y only. Thus, we consider again environment E_1 of Example 6.7,

$$E_1 \triangleq \quad X = a_r^{\lambda}.X + \bar{b}_r^{\delta}.Y + \bar{c}_r^{\nu}.Y \quad Y = \bar{a}_r^{\mu}.X + b_r^{\eta}.Y, \quad D_Y = c_r^{\gamma}.D_Y$$

Fig. 17[9] shows the IMC which describes the probabilistic abstract semantics for the abstract initial state which has wider intervals of concentrations w.r.t. Example 6.7,

$$M_{11}^{\circ} = \{([1, 6], X), ([1, 6], Y), ([1, 1], D_Y)\}.$$

The Fig. 18[10] depicts the corresponding MDP, whose encoding in PRISM is analogous to the one of the 2-ways oscillator.

As before, we first verify if there are some reachable terminated states, by verifying Formula (9). The results, shown in Fig. 19, confirms that the system still has 5 (states $0, ..., 5$) terminated states.

Then, we verify Formulas (11) and (12) in order to establish the lower and upper bounds of probabilistic termination. Also for the environment E_1 we obtain both for Formulas (11) and (12) exactly 1. This proves that each concrete

[9] As before, labels (λ, μ) and (δ, η) are abbreviated by λ and δ, respectively, and, analogously, label (γ, ν) is abbreviated by γ.

[10] To improve the reading, the values of the probabilities are cut to the third decimal digit.

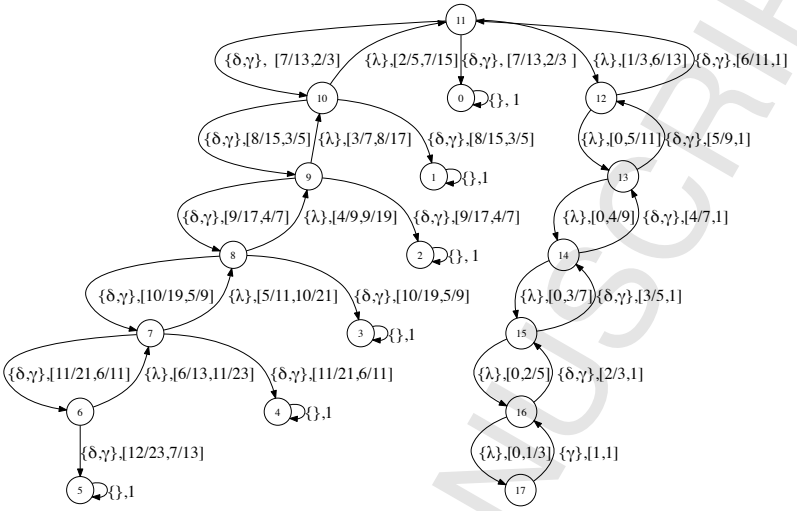


Figure 17: The IMC for the doping of Y

system, represented by the abstract system in Fig. 18, still universally terminates in spite of the presence of the doping reaction for Y.

Then, we consider a fully doped version by introducing in the previous system a doping reaction also for reagent X. Analogously to the case for Y, a doping reaction for X allows the production of a new molecule X from one of Y and a new doping substance D_X. This is modeled by the following environment E_2,

$$E_2 \triangleq \quad X = a_r^{\lambda}.X + \bar{b}_r^{\delta}.Y + \bar{c}_r^{\nu}.Y, \quad Y = \bar{a}_r^{\mu}.X + b_r^{\eta}.Y. + \bar{d}_r^{\psi}.X$$
$$D_Y = c_r^{\gamma}.D_Y, \quad D_X = d_r^{\theta}.D_X.$$

Fig.20[11] shows the IMC which describes the abstract probabilistic semantics for the initial abstract state

$$M_6^{\circ} = \{([1,6],X),([1,6],Y),([1,1],D_Y)\}.$$

The abstract probabilistic model, in this case, has even less states w.r.t. the one for the standard 2-ways oscillator since none of them is hybrid. Fig. 21[12]

[11] As before, labels (λ,μ), (δ,η), (γ,ν) are abbreviated by λ, δ, γ, respectively, and label (θ,ψ) is abbreviated by θ.

[12] To improve the reading, the values of the probabilities are cut to the third decimal digit.

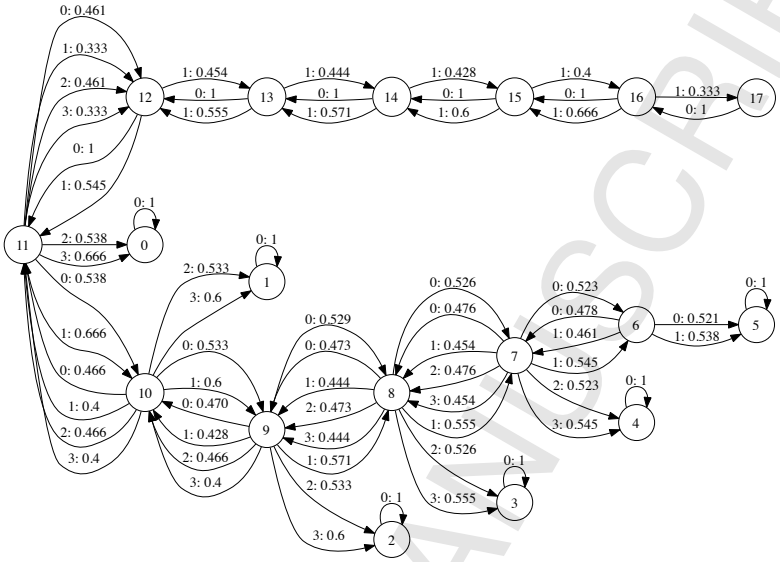


Figure 18: The MDP for the doping of Y

depicts the corresponding MDP, whose encoding in PRISM is analogous to the one of the 2-ways oscillator.

The addition of a doping reaction for X deeply modifies the behavior of the system w.r.t. probabilistic termination. Indeed, by verifying Formula (9), we derive that this abstract model no longer has terminated states (as it is shown in Fig. 22). As suggested by the previous result, for the environment E_2 we obtain both for Formulas (11) and (12) exactly 0. This proves that each concrete system, represented by the abstract system in Fig. 20, oscillates forever.

7.3. Addressing precision and complexity issues

We discuss the advantages of abstract probabilistic model checking w.r.t. probabilistic model checking each DTMC, separately. In particular we examine the biological systems commented in Sections 7.1 and 7.2. The MDPs of Fig. 14, 18 and 21 approximate the behavior of the three biological systems having non exact initial concentrations of reagents X and Y, indeed, $X, Y \in [1, 6]$. Thus, each abstract probabilistic model approximates 36 different DTMCs corresponding to exact initial concentrations of reagents X and Y.

In all examples, the validation over the abstract probabilistic model (MDP) gives the same result for probabilistic termination that one would obtain by model checking each DTMC corresponding to exact values for reagents X and

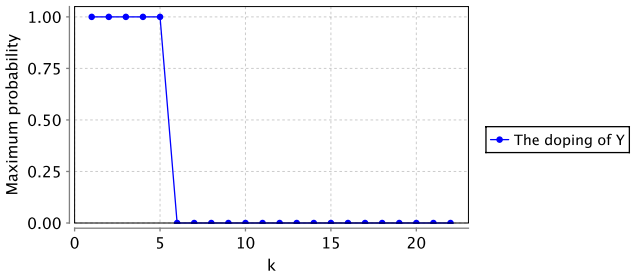


Figure 19: The terminated states of the standard 2-ways oscillator with doping of Y

Y. Therefore, in these cases, the abstraction does not introduce any loss of information and the value for probabilistic termination is exact. In particular, we are able to prove that for all 36 different initial concentrations for reagents X and Y: both the 2-ways oscillator and the partially doped version universally terminate, while the fully doped version oscillates forever.

Moreover, in all examples the abstract probabilistic model provides an efficient representation of the corresponding set of DTMCs in terms of number of abstract states and of associated probability distributions. Actually, the number of the abstract states of the MDPs is substantially reduced w.r.t. the number of states of all DTMCs and the probability distributions associated to each abstract state represents in a very efficient way the set of probability distributions associated to concrete states. Note that, in the concrete validation, it is necessary to calculate the probability distributions associated to each multiset. This requires to extract the rates of all reactions (that depend on the concentrations of reagents X and Y) and then to calculate the corresponding probability, for each exact concentrations of reagents X and Y with $X, Y \in [1, 6]$.

We recall that the MDPs of Fig. 14, 18 and 21 are derived from the corresponding IMCs, by computing for each abstract state a set of probability distributions that represents in an effective way the set of *all admissible distributions* of the corresponding IMC. More in detail, the probability distributions associated to an abstract state are precisely the set of *extreme distributions*, corresponding to each combination of moves with non conflicting labels. For each combination of moves with non conflicting labels, the extreme distributions are the ones that take the values on one of the two bounds of the interval of probability and can be calculated starting from the two bounds of the intervals of probability, as it is explained in Section 5.1.

The IMC of Fig. 12 generalizes the 2-ways oscillator examined in Example 6.6, while, in analogous way, the IMC of the Fig. 17 generalizes the partially doped system examined in Example 6.7. Note that these more complex models still maintain the main features of the smaller corresponding ones. Moreover, the IMC of Fig. 21 models the probabilistic behavior of the fully doped system. In all three cases, the intervals of probability associated to each abstract state in the IMC are the most precise w.r.t. the set of concrete probability distributions

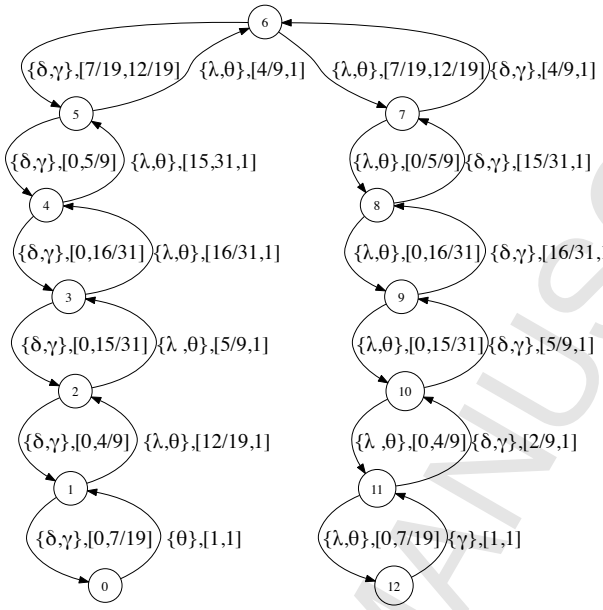


Figure 20: The IMC for the doping of Y and X

of the DTMCs which are represented.

In more detail, in the IMC for the 2-ways oscillator of Fig. 12 (similarly as for the smaller IMC of Example 6.6), for each abstract state, the intervals of probability are exact and there are at most 4 different combinations of non conflicting labels. This yields an MDP (see Fig. 14) that has, for each abstract state, at most 4 probability distributions. In the IMC for the partially doped system of Fig. 17 (similarly as for the smaller IMC of Example 6.7), the intervals of probability are not exact and there are at most 2 different combinations of non conflicting labels. Therefore, the corresponding MDP (see Fig. 18) has, for each abstract state, at most 4 probability distributions. In the IMC for the fully doped system of Fig. 21, the intervals of probability are not exact and there is just 1 possible combination of non conflicting labels. This yields an MDP (see Fig. 20) that has, for each abstract state, at most 2 probability distributions.

Finally, it is worth noting that the previously discussed complexity and precision issues for the biological systems considered in Sections 7.1 and 7.2., do not depend on the initial concentrations of reagents X and Y. Therefore, we could consider the 2-ways oscillator system, its partially doped and fully doped version with wider intervals for reagents X and Y, let us say $[1, m]$ and $[1, n]$ for a generic m and n, thus modeling more experiments. Also in that case we

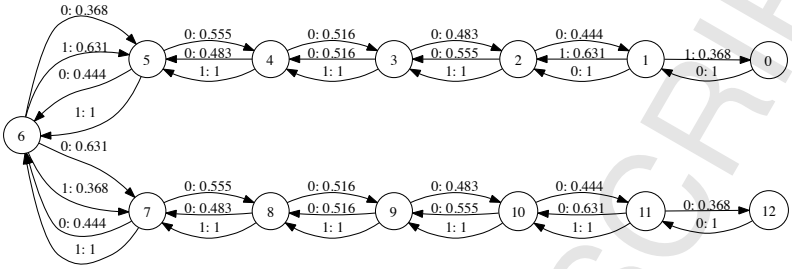


Figure 21: The MDP for the doping of Y and of X.

would obtain analogous results. In particular, the IMC for the standard and partially doped version, modeling, in that case, $m \times n$ experiments will have at most $2 \times (m+n)+1$ states and about $4 \times (m+n+1)$ transitions, $m+n+1$ being the number of states of the biggest DTMC that it represents and $2 \times (m+n+1)$ being its number of transitions.

While the IMC for the fully doped version will have exactly $m + n + 1$ states and $2 \times (m+n+1)$ transitions, the same number of states and transition than the biggest DTMC that it represents. Moreover, for each abstract state, the number of combinations of non conflicting labels as well as the number of probability distributions of the related MDP do not vary w.r.t. the ones of the corresponding smaller abstract system previously commented.

In all these more general cases, the validation of probabilistic termination would give the same precise results, as for the abstract systems with intervals $[1, 6]$ for reagents X and Y. Note that to prove analogous results on termination for the previous systems using a concrete approach would have required to construct $m \times n$ DTMCs, each one modeling the selected system with a different combination of initial concentrations for reagents X and Y and then model check

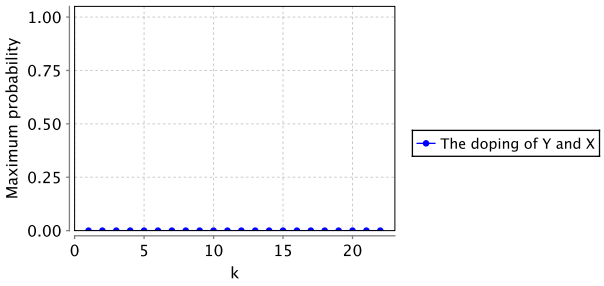


Figure 22: The terminated states of the standard 2-ways oscillator with doping of Y and X

each obtained DTMC separately.

The previous discussion shows that for these classes of systems our method can scale up quite well as long as the dimension of the concrete $DTMC$ modeling the biggest experiment (i.e., the one with concentrations $X = m, Y = n$) can be managed.

For the biological examples commented in Sections 7.1 and 7.2, the cost of the derivation of the MDP from the corresponding IMC, its dimension and therefore the complexity of abstract probabilistic model checking the obtained MDP are very efficient. In order to discuss these aspects in general, it is convenient to describe the number of states and the number of probability distributions for an MDP that represents the probabilistic semantics of an abstract CGF system. The number of states of the derived MDP will be the same as the one of the corresponding IMC $\mathbf{H}^{\circ}(\mathsf{LTS}^{\circ}((E, M_0^{\circ})))$ (and, therefore, of the corresponding abstract LTS $\mathsf{LTS}^{\circ}((E, M_0^{\circ}))$).

Moreover, in the MDP, an abstract state has associated a set of probability distributions that are precisely the set of extreme distributions, corresponding to each combination of moves with non conflicting labels. The extreme distributions are computed starting from the two bounds of the intervals of probability. We recall that $(3)^{n_1} \times (2)^{n_2}$[13], is the maximum number of different transitions with the same label exiting from an abstract state M° in the abstract LTS $\mathsf{LTS}^{\circ}((E, M_0^{\circ}))$. Therefore, this is also the maximum number of moves with the same label from the abstract state M° in the corresponding IMC. From the discussion of Section 4.4 it follows that the maximum number of different combinations of moves with non conflicting labels is $((3)^{n_1} \times (2)^{n_2})^n$, where n is the number of different reactions in the environment E. Since the maximum number of extreme distributions related to each combination is 2^n, then, the number of probability distributions associated to each abstract state of the MDP is, at most, $2^n \times ((3)^{n_1} \times (2)^{n_2})^n = (2 \times (3)^{n_1} \times (2)^{n_2})^n$, in the worst case. It is worth noting that such number is exponential in n as in the case of standard Interval Markov Chains [24]. More in detail, the number of extreme distributions $(2 \times (3)^{n_1} \times (2)^{n_2})^n$ is smaller than the number of extreme distributions $(2)^{(3)^{n_1} \times (2)^{n_2} \times n}$ we would have deriving an MDP from a standard Interval Markov Chain with the same number of states and transitions.

In conclusion, the complexity of deriving an MDP from the IMC and the dimension of such MDP is comparable to (actually is even smaller than) the complexity of deriving the MDP from a standard Interval Markov Chain with the same number of states and transitions. Hence, once again, the main source of complexity resides in the dimensions of the abstract model. As we have already discussed in Section 6.2, an IMC $\mathbf{H}^{\circ}(\mathsf{LTS}^{\circ}((E, M_0^{\circ})))$ has the same number of states and (even less) transitions of the corresponding abstract LTS, $\mathsf{LTS}^{\circ}((E, M_0^{\circ}))$. Therefore, an upper bound for the number of states (and of

[13]Here, n_1 was the number of variables appearing in homeo reactions enabled in M° and whose interval of multiplicity is actually split, n_2 was the number of variables appearing just in unary or binary reactions enabled in M°.

transitions) of the IMC can be found in the discussion of Section 4.4.

We believe that such complexity issues together with a careful analysis of the set of experiments that one wants to validate (e.g., weather it is convenient to express the different concentrations of reagents in the experiments by means of intervals) can guide the application of the abstract model checking technique to more complex biological systems.

8. Related Work

The design of abstractions for probabilistic or stochastic models has been widely investigated over the last few years.

Most of the proposals study abstractions able to deal with the traditional state-explosion problem, which limits the practical application of probabilistic model checking. The proposals of [22, 23, 24, 51] present similar approaches for approximating probabilistic models, by means of MDP and standard Interval Markov Chains, respectively. In this methodology the abstract probabilistic model is derived from the probabilistic model which has to be approximated, by considering a partition of the concrete state space. The abstract probabilistic model is constructed by computing, for each abstract state, the abstract probabilities from the concrete probabilities. The proposal of [37] extends the approaches of [22, 23] in order to better approximate MDP. The abstract model is based on two-player stochastic games that are able to separate the non-determinism introduced by the abstraction from the non-determinism present in the concrete MDP. De Alfaro [1] proposes an original method for the abstraction of finite state MDP, based on regions. Katoen et al. [33] proposes approximation techniques for CTMC along the lines of [24]. The key idea is to apply the abstraction to uniform CTMC and to abstract transition probabilities by means of intervals.

The drawback of these approaches is that they require to compute the full concrete model which is then reduced to the abstract model. Consequently, these techniques can only be applied to (finite) concrete models with a limited number of states.

The proposals of [52, 34] investigate the implementation of the abstraction techniques for MDP, proposed by [22, 23, 37] respectively. The approach applies predicate abstraction to PRISM models and supports the effective construction of an abstract model, using an extension of the PRISM-language.

Huth [32] proposes a framework for approximation based on standard Interval Markov Chains, where the abstraction of states is formalized using a sort of abstract interpretation. The framework is quite general and applies also to infinite DTMC; however, the method is not effectively applied to any real specification language.

An interesting application of abstract interpretation to biological system models, specifically signaling pathways, is presented in [21]. The proposed analysis calculates information about the reachable complexes which could be generated at run-time. Monnieux [40] proposes an approximation method, based

on abstract interpretation, for the validation of trace properties of probabilistic and non-deterministic concurrent programs.

9. Conclusions

In this paper we have applied abstract interpretation techniques in order to analyze probabilistic termination of CGF systems. The methodology proposed supports probabilistic model checking of a *set of experiments* that represent a biological system w.r.t. different initial concentrations of reagents. The set of experiments is represented by an abstract GCF system having initial concentrations of reagents which are not exact but vary in intervals. The abstract probabilistic model of an abstract CGF system, modeled as an IMC, *safely approximates* the set of DTMCs, describing the probabilistic semantics of each concrete CGF system. The validation of probabilistic termination (and also of probabilistic reachability properties) over the abstract probabilistic model reports *conservative lower and upper bounds* with respect to the set of CGF systems which are approximated.

The main novelty of the proposed technique is that the abstract probabilistic model (IMC) is derived through an approximation of the semantics following the approach based on abstract interpretation [17, 18]. In this application, the abstract probabilistic semantics is obtained from an abstract LTS semantics, by calculating the intervals of probability associated to each move from the information recorded on abstract transition labels. The method is *systematic* and *effective* given that: (i) the state space of the IMC is constructed without building the state space of the DTMCs which are approximated; (ii) the intervals of probability associated to each move are calculated from abstract rates (that is intervals of rates), without computing all the corresponding concrete probability distributions.

In this approach, the design of the abstract LTS semantics is critical. We have proposed a semantics where hybrid states, representing both terminated and non terminated states, are properly partitioned in order to more precisely address probabilistic termination properties. Moreover, the abstract transition labels record information about the reaction, which is realized by the move, and about the abstract rate of the move. The former is represented by a label which identifies the reaction and allows us to observe possible cases of conflict between abstract transitions. The latter uses a representation of the interval of rates corresponding to a move by means of the rate of the reaction and of the intervals of multiplicity of the reagent variables, which participate to the reaction.

The information maintained on abstract transition labels is profitably used in the derivation of the corresponding IMC in order to limit the non-determinism introduced by the abstraction over the state space. Specifically, they are exploited in the calculation of the abstract probability distributions, which are assigned to each abstract state. Not only the labels expressing conflict are translated into the corresponding IMC but also they are used in the calculation of the interval of probability, corresponding to each move. Moreover, the

derivation of the intervals of probability from the abstract rates is based on symbolic approach which permits to maintain more precise information about the possible multiplicity of reagent variables.

It should be clear that the choice of Labeled Interval Markov Chains (IMC), a variant of standard Interval Markov Chains [51, 24], is essential in this approach. As we have discussed in Section 5, the labels representing conflict provide more accurate information about the set of probability distributions, represented by the corresponding intervals of probability.

To illustrate the interest of the proposed technique we have investigated the property of probabilistic termination for a simple 2-way oscillator in standard and doped versions (in the style of [11, 3]). The IMC obtained for each of the three abstract experiments approximates a set of DTMCs, corresponding to all combinations of concentrations for reagent variables, which are included in the corresponding intervals of multiplicity. In order to realize abstract probabilistic model checking of the abstract systems we have used PRISM by encoding the IMC into a corresponding MDP, in which each abstract state has associated a set of probability distributions, the so called extreme distributions. The extreme distributions are extracted from the intervals of probability of the IMC by generalizing the methodology proposed [51, 24, 32] for standard Interval Markov Chains. In these three examples, the obtained MDP provides an efficient representation of the corresponding set of DTMCs, considering both the number of abstract states and the number of probability distributions, which are associated to each abstract state. Moreover, the abstract validation of probabilistic termination does not introduce any loss of information w.r.t. the concrete validation. Actually, probabilistic model checking of the abstract model gives an *exact value*, showing that for all the concentrations of reagent variables included in the intervals of multiplicity: both the standard 2-way oscillator and the partially doped version universally terminate while the fully doped version oscillates forever. As we have commented in Section 7 these results for probabilistic termination can be easily extended to more complex versions of the systems, by considering abstract systems with wider intervals of multiplicity for reagent variables.

In our opinion the design of techniques able to deal with uncertainty is fundamental in the analysis of biological systems. The framework, based on abstract interpretation, is rather flexible and can easily be adapted to similar applications. Barbuti et al. [4] propose an adaptation of the approach presented in [15] which supports probabilistic model checking of biological models with uncertain rates, e.g. where rates may vary over intervals. In this case, standard Interval Markov Chains are adequate for approximating the infinite set of DTMCs, corresponding to all the possible choices of rates. The abstract model is derived, in a fully automatic way, from an abstract LTS semantics. A related tool has been implemented using a translation from standard Interval Markov Chain into MDP, based on the calculation of extreme distributions. The technique has been successfully applied to detect probabilistic reachability properties of a model of tumor growth.

In the future work, we intend to investigate the implementation of the abstract probabilistic model checking methodology. The approach illustrated for

the examples in Section 7 is based on PRISM and could be implemented, in a natural way, along the lines of [4]. More efficient algorithms which construct the extreme distributions *on-the-fly* could also be developed for model checking an IMC (following the ideas discussed in [51, 24]). It is not clear whether our abstraction could be formalized using predicate abstraction and therefore whether related tools could be applied, such as the one proposed in [34].

Moreover, future work will involve studying how the efficiency and scalability of the approach can be improved. To this aim, it seems fundamental to investigate more efficient techniques to partition hybrid states and new widening operators that would allow the technique to scale up to much more complex systems. Note that the definition of a new abstract LTS semantics would not change the overall construction presented in this paper. Hence, we could re-use all theoretical concepts: the abstraction functions, the model IMC, the approximation orders on abstract LTS and IMC as well as the definition of the probabilistic translation function, mapping an abstract LTS into an IMC.

We also would like to apply the proposed abstract model checking technique to more complex biological systems and to further investigate the advantages/disadvantages w.r.t. the application of stochastic simulation techniques.

Furthermore, in this paper we have focused on the validation of probabilistic termination for finite systems. In the future work, we intend to investigate the extension of the technique to infinite CGF systems by considering an approach based on widening operators similarly as [15]. We also intend to study whether other probabilistic properties, expressible in the logic PCTL, could be validated by applying the proposed abstract model checking technique. In particular, it would be interesting to consider the properties of oscillators, concerning the periodicity and amplitude of oscillations, which are discussed in [3, 2].

Moreover, we would like to investigate the extension of the proposed approach to continuos-time, that is to the abstraction of the CTMC modeling the behavior of a CGF system. The adaption of existing techniques, such as [33], is not trivial, given that it requires to develop methods which are able to derive an approximated uniform CTMC from an abstract LTS. We also leave for future work the extension of the framework to the full calculus with communication [44].

AppendixA. Proofs of Section 4

Proof of [Theorem 4.5] We have to prove that the pair of functions (α, γ) of Definition 4.4 is a Galois connection.

- $\alpha : \mathcal{P}(\mathcal{M}) \to \mathcal{M}^\circ$ and $\gamma : \mathcal{M}^\circ \to \mathcal{P}(\mathcal{M})$ are obviously monotone.
- for each $S \in \mathcal{P}(\mathcal{M})$, $\gamma(\alpha(S)) \supseteq S$. We have $\alpha(S) = \bigsqcup^\circ_{M \in S} M^\bullet$ and $\gamma(\alpha(S)) = \{M' \mid M'^\bullet \sqsubseteq^\circ \bigsqcup^\circ_{M \in S} M^\bullet\}$. Now it is worth noting that $\{M' \mid M'^\bullet \sqsubseteq^\circ \bigsqcup^\circ_{M \in S} M^\bullet\} \supseteq \{M' \mid M' \in S\}$.

- for each $M^\circ \in \mathcal{M}^\circ$, $\alpha(\gamma(M^\circ)) \sqsubseteq^\circ M^\circ$. We have $\gamma(M^\circ) = \{M' \mid M'^\bullet \sqsubseteq^\circ M^\circ\}$ and $\alpha(\gamma(M^\circ)) = \bigsqcup^\circ_{M \in \{M' \mid M'^\bullet \sqsubseteq^\circ M^\circ\}} M^\bullet$. Now it is easy to see that $\bigsqcup^\circ_{M \in \{M' \mid M'^\bullet \sqsubseteq^\circ M^\circ\}} M^\bullet \sqsubseteq^\circ M^\circ$. □

Lemma AppendixA.1. *Let $op \in \{\ominus, \oplus\}$. For each $M, N \in \mathcal{M}$, we have $\alpha(M\ op\ N) = M^\bullet\ op^\circ\ \alpha(N)$.*

Proof of For all $X \in \mathcal{X}$,$\alpha(M \ominus N)(X) = [M(X)\widehat{-}N(X), M(X)\widehat{-}N(X)]$, by definition of $\ominus$ and α. Moreover, by definition of $\ominus^\circ$ and α, for all $X \in \mathcal{X}$, $M^\bullet \ominus^\circ N^\bullet(X) = [M(X)\widehat{-}N(X), M(X)\widehat{-}N(X)]$. We can reason analogously for $\oplus$. □

Proof of [Theorem 4.9] Assume, by contradiction, that there exists an $M'^\circ \in \bigtriangledown^{\mathcal{M}}_E(M^\circ)$ that is hybrid. Then, by Definition 4.8, there exists a $v \in \mathbb{S}_E(M'^\circ)$ such that $M'^\circ \models v$ and $M'^\circ \models \neg v$. We have two cases.

- $v = X \geq 2$, for some $X \in \mathcal{X}$. By definition of $\bigtriangledown^{\mathcal{I}}_E(M^\circ, X)$ the interval for X was partitioned so that either $M'^\circ \models v$ or $M'^\circ \models \neg v$. This gives a contradiction.

- $v = X \geq 1$ or $v = X \geq 1 \wedge Y \geq 1$ and $M'^\circ \models \neg(X \geq 1)$, for some $X, Y \in \mathcal{X}$. In this case if also $X \geq 2 \in \mathbb{S}_E(M'^\circ)$ then the interval for X was partitioned so that either $M'^\circ \models (X \geq 1)$ or $M'^\circ \models \neg(X \geq 1)$. Moreover, if $X \geq 2 \notin \mathbb{S}_E(M'^\circ)$, by definition of $\bigtriangledown^{\mathcal{I}}_E(M^\circ, X)$, the interval for X was partitioned in a different way but always guaranteeing that either $M'^\circ \models (X \geq 1)$ or $M'^\circ \models \neg(X \geq 1)$. This gives a contradiction.

Proof of [Theorem 4.14] We have to prove that, for each $M^\circ \in \mathcal{M}^\circ$ and $M' \in \gamma(M^\circ)$,

$$\alpha_{lts}(\mathsf{LTS}((E, M'))) \sqsubseteq^\circ_{lts} \mathsf{LTS}^\circ((E, M^\circ)).$$

Let $\mathsf{LTS}((E, M')) = (S, \rightarrow, M', E)$, then, by definition of α_{lts},

$$\alpha_{lts}(\mathsf{LTS}((E, M'))) = (\{M^\bullet\}_{M \in S}, \alpha(\rightarrow), M'^\bullet, E)$$

where $\alpha(\rightarrow) = \{M_1{}^\bullet \xrightarrow[\circ]{\Theta, \Delta^\bullet, r} M_2{}^\bullet \mid M_1 \xrightarrow{\Theta, \Delta, r} M_2 \in \rightarrow\}$.

Let $\mathsf{LTS}^\circ((E, M^\circ)) = (S^\circ, \rightarrow^\circ, M^\circ, E)$. Hence, by definition of $\sqsubseteq^\circ_{lts}$ we have to prove $M'^\bullet \preccurlyeq_{lts} M^\circ$. Note that, since $M' \in \gamma(M^\circ)$, by definition of γ, we have $M'^\bullet \sqsubseteq^\circ M^\circ$. Therefore, it is convenient to prove a more general property: if $M'^\bullet \sqsubseteq^\circ M^\circ$, then we have $M'^\bullet \preccurlyeq_{lts} M^\circ$, for each $M' \in S$ and $M^\circ \in S^\circ$.

According to Definition 4.12, we have condition (i) by hypothesis, e.g. $M'^\bullet \sqsubseteq^\circ M^\circ$. In order to prove condition (ii) we have to find a surjective function $H_t : \mathsf{Ts}(M'^\bullet) \rightarrow \mathsf{Ts}(M^\circ)$, such that, for each $t^\circ_1 \in \mathsf{Ts}(M'^\bullet)$, $t^\circ_1 = M'^\bullet \xrightarrow[\circ]{\Theta, \Delta_1{}^\bullet, r} N_1{}^\bullet$, $H_t(t^\circ_1) = t^\circ_2$, where $t^\circ_2 = M^\circ \xrightarrow[\circ]{\Theta, \Delta^\circ_2, r} N^\circ_2$, $\Delta_1^\bullet \leq_I \Delta^\circ_2$ and $N_1{}^\bullet \preccurlyeq_{lts} N^\circ_2$.

First, we show that, for each $t^\circ_1 \in \mathsf{Ts}(M'^\bullet)$ there exists a corresponding transition $t^\circ_2 \in \mathsf{Ts}(M^\circ)$. We observe that transition t°_1 is the abstraction of a

concrete transition t_1 so that $t_1 \in \mathsf{Ts}(M')$. Hence, transition t_1 could have been obtained either by applying rule **Sync** or rule **Delay**. We discuss the case of **Sync**, the other is analogous.

Since rule **Sync** has been applied, it must be the case that: (a) $\Theta = (\lambda, \mu)$, (b) $\Delta_1 = (M'(X), M'(Y))$, (c) $a_r{}^{\lambda}.Q_1 \in E(X)$ and $\bar{a_r}^{\mu}.Q_2 \in E(Y)$, and (d) $N_1 = (M' \ominus (1, X) \ominus (1, Y)) \oplus [\![Q_1]\!] \oplus [\![Q_2]\!]$.

Given (c), we can apply rule **Sync-a** for M° and derive a set of transitions t_2° with the same label Θ. More in detail, we have $t_2^\circ = M^\circ \xrightarrow{\Theta,(I_x,I_y),r}{}^{\circ} N^\circ \in \bigtriangledown_E^{\mathcal{M}}(N_2^\circ)$ where: $N_2^\circ = (M^\circ \ominus^\circ \{(1^\bullet, X)\}) \ominus^\circ \{(1^\bullet, Y)\}) \oplus^\circ [\![Q_1]\!]^\bullet \oplus^\circ [\![Q_2]\!]^\bullet$, $I_x = \bigtriangledown^{\mathcal{T}}(M'^\circ(X), ((1^\bullet, X) + (1^\bullet, Y))(X), ([\![Q]\!]_1^\bullet + [\![Q]\!]_2^\bullet)(X), N_2^\circ(X))$ and $I_y = \bigtriangledown^{\mathcal{T}}(M'^\circ(Y), ((1^\bullet, X) + (1^\bullet, Y))(Y), ([\![Q]\!]_1^\bullet + [\![Q]\!]_2^\bullet)(Y), N_2^\circ(Y))$.

Using (d) and Lemma AppendixA.1, we have that ${N_1}^\bullet \sqsubseteq^\circ N_2^\circ$. Moreover, note that the multiplicities of variables in ${N_1}^\bullet$ are represented by exact intervals, i.e., $n^\bullet$ for some $n \geq 0$. If $\bigtriangledown_E^{\mathcal{M}}$ splits state N_2° it does it, partitioning the intervals of some variables of N_2°. However, by definition of $\bigtriangledown_E^{\mathcal{T}}$, there will exist a $N'^\circ \in \bigtriangledown_E^{\mathcal{M}}(N_2^\circ)$ such that ${N_1}^\bullet \sqsubseteq^\circ N'^\circ$. Moreover, we recall that ${M'}^\bullet \sqsubseteq^\circ M^\circ$, thus we have ${M'}^\bullet(X) \leq_I M^\circ(X)$ as well as ${M'}^\bullet(Y) \leq_I M^\circ(Y)$. Since also the intervals in ${M'}^\bullet(X)$ and ${M'}^\bullet(Y)$ are exact, by definition of $\bigtriangledown^{\mathcal{T}}$, reasoning as before, we have that ${\Delta_1}^\bullet \leq_I (I_1, I_2)$ with $I_1 = \bigtriangledown^{\mathcal{T}}(M^\circ(X), ((1^\bullet, X) + (1^\bullet, Y))(X), ([\![Q]\!]_1^\bullet + [\![Q]\!]_2^\bullet)(X), N'^\circ(X))$ and $I_2 = \bigtriangledown^{\mathcal{T}}(M^\circ(Y), ((1^\bullet, X) + (1^\bullet, Y))(Y), ([\![Q]\!]_1^\bullet + [\![Q]\!]_2^\bullet)(Y), N'^\circ(Y))$. Moreover, note that if $N_1 = (M' \ominus (1, X) \ominus (1, Y)) \oplus [\![Q_1]\!] \oplus [\![Q_2]\!] \neq M'$, then by definition of $\ominus^\circ$ and $\ominus^\circ$ also $N_2^\circ = (M^\circ \ominus^\circ \{(1^\bullet, X)\}) \ominus^\circ \{(1^\bullet, Y)\}) \oplus^\circ [\![Q_1]\!]^\bullet \oplus^\circ [\![Q_2]\!]^\bullet \neq M^\circ$. As a consequence, also $N'^\circ \in \bigtriangledown^{\mathcal{T}}(N_2^\circ) \neq M^\circ$.

Finally, note that the transitions of both $\mathsf{Ts}({M'}^\bullet)$ and $\mathsf{Ts}(M^\circ)$ are dictated by the common environment which determine univocally the label o f the transitions and that the refinement operator does not change transition labels. Indeed, every label of transitions in $\mathsf{Ts}(M^\circ)$ has a corresponding labeled transition in $\mathsf{Ts}({M'}^\bullet)$ eventually with some multiplicities equal to zero. □

AppendixB. Proofs of Sections 5 and 6

Proof of [Theorem 5.9] Let $mc_i^\circ = (S_i{}^\circ, \mathbf{P}_i^-, \mathbf{P}_i^+, \mathbf{L}_i, M_{0,i}^\circ)$ be two IMC and let $M_i{}^\circ \in S_i{}^\circ$, for $i \in \{1, 2\}$. We have to show that $M_1^\circ \preccurlyeq_{mc} M_2^\circ$ implies

$$\mathsf{Reach}^-_{mc_2^\circ}(M_2^\circ) \leq \mathsf{Reach}^-_{mc_1^\circ}(M_1^\circ) \leq \mathsf{Reach}^+_{mc_1^\circ}(M_1^\circ) \leq \mathsf{Reach}^+_{mc_2^\circ}(M_2^\circ).$$

In particular, we examine the case of $\mathsf{Reach}^-_{mc_2^\circ}(M_2^\circ) \leq \mathsf{Reach}^-_{mc_1^\circ}(M_1^\circ)$. The case of $\mathsf{Reach}^+_{mc_1^\circ}(M_1^\circ) \leq \mathsf{Reach}^+_{mc_2^\circ}(M_2^\circ)$ can be proved by applying similar arguments. We recall that, for $j \in \{1, 2\}$,

$$\mathsf{Reach}^-_{mc_j^\circ}(M_j{}^\circ) = \bigcup_{i \in \{0,\infty\}} \rho^{-,i}_{mc_j^\circ}(M_j^\circ)$$

where

$$\rho^{-,i}_{mc^\circ_j}(M^\circ_j) = \begin{cases} 1 & \text{if } M^\circ_j \models^\forall A, \\ 0 & \text{if } i = 0 \wedge M^\circ_j \not\models^\forall A, \\ \inf\limits_{\rho_j \in \mathsf{ADistr}_{mc^\circ_j}(M_j{}^\circ)} \sum\limits_{N^\circ_j \in S^\circ_j} \rho_j(N^\circ_j) \cdot \rho^{-,i-1}_{mc^\circ_j}(N^\circ_j) & \text{otherwise.} \end{cases}$$

Therefore, it is enough to show that $\rho^{-,i}_{mc^\circ_2}(M^\circ_2) \leq \rho^{-,i}_{mc^\circ_1}(M^\circ_1)$, for each $i \geq 0$. The proof proceeds by induction.

($i = 0$) There are two possibilities for $\rho^{-,0}_{mc^\circ_2}(M^\circ_2)$. Either M°_2 is $\forall$-terminated and the result is 1 or M°_2 is non $\forall$-terminated and the result is 0.

Since we want to prove that $\rho^{-,0}_{mc^\circ_2}(M^\circ_2) \leq \rho^{-,0}_{mc^\circ_1}(M^\circ_1)$, the latter case is trivial.

For the former case, we will prove that M°_1 is non $\forall$-terminated implies that also M°_2 is non $\forall$-terminated. Assume then that M°_1 is non $\forall$-terminated. This means, by definition, that there exists a a $\rho^1 \in \mathsf{ADistr}_{mc^\circ}(M^\circ_1)$ such that $\rho^1(N_1{}^\circ) > 0$ with $N_1 \neq M^\circ_1$. Since $M^\circ_1 \preccurlyeq_{mc} M^\circ_2$, by Definition 5.8, there exists a corresponding $\rho^2 \in \mathsf{ADistr}_{mc^\circ}(M^\circ_2)$ and $\delta \in \mathsf{Distr}(S^\circ_1 \times S^\circ_2)$ such that $\rho_1(N^\circ_1) = \sum_{N^\circ_2 \in S^\circ_2} \delta(N^\circ_1, N^\circ_2)$. By hypothesis, $\rho^1(N_1{}^\circ) > 0$ then $\rho_1(N^\circ_1) = \sum_{N^\circ_2 \in S^\circ_2} \delta(N^\circ_1, N^\circ_2) > 0$. Let us choose a particular N°_2 so that $\delta(N^\circ_1, N^\circ_2) > 0$. For such abstract state N°_2, also $\sum_{N^\circ_1 \in S^\circ_1} \delta(N^\circ_1, N^\circ_2)$ is greater than 0 since at least one of its addend is indeed $\delta(N^\circ_1, N^\circ_2)$ which was greater than 0. Then, by definition, also $\rho_2(N^\circ_2) = \sum_{N^\circ_1 \in S^\circ_1} \delta(N^\circ_1, N^\circ_2) > 0$. Moreover, since $\delta(N^\circ_1, N^\circ_2) > 0$ and $N_1 \neq M^\circ_1$, by (a) of Definition 5.8, we know that $N^\circ_1 \neq M^\circ_2$. But this implies that M°_2 is non $\forall$-terminated.

($i > 0$) There are two possibilities for $\rho^{-,i}_{mc^\circ_2}(M^\circ_2)$. Either $M^\circ_2 \models^\forall A$ and result is 1 or the result is computed by

$$\rho^{-,i}_{mc^\circ_2}(M^\circ_2) = \inf_{\rho_2 \in \mathsf{ADistr}_{mc^\circ_2}(M_2{}^\circ)} \sum_{N^\circ_2 \in S^\circ_2} \rho_2(N^\circ_2) \cdot \rho^{-,i-1}_{mc^\circ_2}(N^\circ_2) \tag{B.1}$$

The case of $M^\circ_2 \models^\forall A$ is trivial, because we have $M^\circ_1 \models^\forall A$, as we have explained in the case of $i = 0$. In case (B.1), we observe that for $\rho^{-,i}_{mc^\circ_1}(M^\circ_1)$ there are two possibilities. Either $M^\circ_1 \models^\forall A$ and result is 1 or the result is

$$\rho^{-,i}_{mc^\circ_1}(M^\circ_1) = \inf_{\rho_1 \in \mathsf{ADistr}_{mc^\circ_1}(M_1{}^\circ)} \sum_{N^\circ_1 \in S^\circ_1} \rho_1(N^\circ_1) \cdot \rho^{-,i-1}_{mc^\circ_1}(N^\circ_1) \tag{B.2}$$

The case of $M^\circ_1 \models^\forall A$ is trivial. By contrast, in the other case we have to compare (B.1) and (B.2). For these purposes, we recall that $M^\circ_1 \preccurlyeq_{mc} M^\circ_2$ guarantees a correspondence between the distributions $\mathsf{ADistr}_{mc^\circ_1}(M_1{}^\circ)$ and $\mathsf{ADistr}_{mc^\circ_2}(M_2{}^\circ)$.

More in detail, by applying Definition 5.8, for each distribution $\rho_1 \in \mathsf{ADistr}(M_1^\circ)$, there exist distributions $\delta \in \mathsf{Distr}(S_1^\circ \times S_2^\circ)$ and $\rho_2 \in \mathsf{ADistr}(M_2^\circ)$ such that, for any $N_1^\circ \in S_1^\circ$ and $N_2^\circ \in S_2^\circ$: (a) $\rho_1(N_1^\circ) = \sum_{N_2{}^\circ \in S_2{}^\circ} \delta(N_1{}^\circ, N_2^\circ)$; (b) $\rho_2(N_2^\circ) = \sum_{N_1{}^\circ \in S_1{}^\circ} \delta(N_1{}^\circ, N_2^\circ)$; and (c) if $\delta(N_1^\circ, N_2^\circ) > 0$ then $N_1^\circ \preccurlyeq_{mc} N_2^\circ$.

We show that, for distributions $\rho_1 \in \mathsf{ADistr}_{mc_1^\circ}(M_1{}^\circ)$ and $\rho_2 \in \mathsf{ADistr}_{mc_2^\circ}(M_2{}^\circ)$, we have

$$\sum_{N_2^\circ \in S_2^\circ} \rho_2(N_2^\circ) \cdot \rho^{-,i-1}_{mc_2^\circ}(N_2^\circ) \leq \sum_{N_1^\circ \in S_1^\circ} \rho_1(N_1^\circ) \cdot \rho^{-,i-1}_{mc_1^\circ}(N_1^\circ)$$

This obviously guarantees that (B.1) $\leq$ (B.2). By exploiting (a), we obtain

$$\begin{array}{l} \sum_{N_1^\circ \in S_1^\circ} \rho_1(N_1^\circ) \cdot \rho^{-,i-1}_{mc_1^\circ}(N_1^\circ) \\ = \sum_{N_1^\circ \in S_1^\circ} (\sum_{N_2^\circ \in S_2^\circ} \delta(N_1^\circ, N_2^\circ)) \cdot \rho^{-,i-1}_{mc_1^\circ}(N_1^\circ) \end{array}$$

Moreover, by exploiting (c) we have that $\delta(N_1^\circ, N_2^\circ) > 0$ ensures $N_1 \preccurlyeq_{mc} N_2^\circ$. Then, by inductive hypothesis, we have also $\rho^{-,i-1}_{mc_2^\circ}(N_2^\circ) \leq \rho^{-,i-1}_{mc_1^\circ}(N_1^\circ)$. Hence, by exploiting also (b), we obtain

$$\begin{array}{l} \sum_{N_1^\circ \in S_1^\circ} (\sum_{N_2^\circ \in S_2^\circ} \delta(N_1^\circ, N_2^\circ)) \cdot \rho^{-,i-1}_{mc_1^\circ}(N_1^\circ) \geq \\ \sum_{N_1^\circ \in S_1^\circ} (\sum_{N_2^\circ \in S_2^\circ} \delta(N_1^\circ, N_2^\circ)) \cdot \rho^{-,i-1}_{mc_2^\circ}(N_2^\circ) = \\ \sum_{N_2^\circ \in S_2^\circ} \sum_{N_1^\circ \in S_1^\circ} \delta(N_1^\circ, N_2^\circ) \cdot \rho^{-,i-1}_{mc_2^\circ}(N_2^\circ) = \\ \sum_{N_2^\circ \in S_2^\circ} \rho_2(N_2) \cdot \rho^{-,i-1}_{mc_2^\circ}(N_2^\circ). \end{array}$$

□

In order to incrementally construct the proof of Theorem 6.3 we proceed as follows. We first present a simplified method (Definition AppendixB.1) for deriving an IMC for a particular subset of LTS's. Once we have introduced the method and prove it correct (see Theorem AppendixB.3) for such subset, we consider the more general case of LTS's satisfying Condition 8. Finally, the extension to function $\mathbf{H}^\circ$ to all LTS is discussed at the end of this section.

Consider first $\overline{\mathcal{LTS}^\circ} \subset \mathcal{LTS}^\circ$ the domain of $LTS = (S^\circ, \rightarrow^\circ, M_0^\circ, E)$ such that $\forall M^\circ \in S^\circ$, $|\mathsf{label}(\mathsf{Ts}(M^\circ))| = |\mathsf{Ts}(M^\circ)|$.

We introduce the functions $\mathbf{R}^\circ : S^\circ \times S^\circ \rightarrow \mathcal{E}$, and $\mathbf{E}^\circ : S^\circ \rightarrow \mathcal{E}$,

$$\mathbf{R}^\circ(M^\circ, M'^\circ) = \sum^\circ_{t^\circ \in \mathsf{Ts}(M^\circ, M'^\circ)} \mathsf{rate}^\circ(t^\circ) \quad \mathbf{E}^\circ(M^\circ) = \sum^\circ_{M'^\circ \in S^\circ} \mathbf{R}^\circ(M^\circ, M'^\circ)$$

Definition AppendixB.1 (Derivation of IMC - The simple case). *We define an* abstract probabilistic translation *function* $\mathbf{H}^\circ : \overline{\mathcal{LTS}^\circ} \rightarrow \mathcal{IMC}^\circ$ *such that* $\mathbf{H}^\circ((S^\circ, \rightarrow^\circ, M_0{}^\circ, E)) = (S^\circ, \mathbf{P}^-, \mathbf{P}^+, \mathbf{L}, M_0^\circ)$ *and* $\mathbf{P}^-, \mathbf{P}^+ \colon S^\circ \rightarrow \mathsf{SDistr}(S^\circ)$ *are the* lower *and* upper *probability functions, such that for all* $M_1{}^\circ \in S^\circ$

1. *if* $max(\mathbf{E}^\circ(M_1^\circ)) = 0$, *then* $\mathbf{P}^+(M_1^\circ)(M_2^\circ) = \mathbf{P}^-(M_1^\circ)(M_2^\circ) = 0$, *for each* $M_1^\circ \neq M_2^\circ$, *and* $\mathbf{P}^+(M_1^\circ)(M_1^\circ) = \mathbf{P}^-(M_1^\circ)(M_1^\circ) = 1$;

2. *if* $max(\mathbf{E}^\circ(M_1^\circ)) > 0$ *then*
   (a) *if* $min(\mathbf{E}^\circ(M_1^\circ)) = 0$ *then* $\mathbf{P}^+(M_1^\circ)(M_1^\circ) = 1$ *and* $\mathbf{P}^-(M_1^\circ)(M_1^\circ) = 0$,
   (b) *for each* M_2°, *if* $min(\mathbf{R}^\circ(M_1^\circ, M_2^\circ)) = 0$ *then* $\mathbf{P}^-(M_1^\circ)(M_2^\circ) = 0$ *else* $\mathbf{P}^-(M_1^\circ)(M_2^\circ) = min(\mathbf{R}^\circ(M_1^\circ, M_2^\circ)/^\circ\mathbf{E}^\circ(M_1^\circ))$,
   (c) *for each* M_2°, *if* $max(\mathbf{R}^\circ(M_1^\circ, M_2^\circ)) = 0$ *then* $\mathbf{P}^+(M_1^\circ)(M_2^\circ) = 0$ *else* $\mathbf{P}^+(M_1^\circ)(M_2^\circ) = max(\mathbf{R}^\circ(M_1^\circ, M_2^\circ)/^\circ\mathbf{E}^\circ(M_1^\circ))$.

$\mathbf{L} : S^\circ \to (S^\circ \to \wp(\widehat{\mathcal{L}}))$ *is a labeling function defined as* $\forall M_1^\circ, M_2^\circ \in S^\circ$, $\mathbf{L}(M_1^\circ, M_2^\circ) = \mathsf{label}(\{t^\circ \in \mathsf{Ts}(M_1^\circ, M_2^\circ) \mid max(\mathsf{rate}^\circ(t^\circ)) > 0\})$.

Before proving the correctness of the previous method we prove some properties which compare the abstract rates of transitions leaving from state M_1° with the abstract rates of transitions leaving from state M_2° when $M_1^\circ \preccurlyeq_{lts} M_2^\circ$. For this reasons, we recall that an abstract rate is expressed by a pair (z, c), where e is a symbolic expression and c is a membership constraint. In the following, with an abuse of notation, we say that (z_1, c_1) is an approximation of (z_2, c_2), $(z_1, c_1) \leq_I (z_2, c_2)$, iff $e_1 = e_2$ and $c_1 \leq c_2$ (e.g. for each $X \in I_1 \in c_1$, there exists $X \in I_2 \in c_2$ such that $I_1 \leq_I I_2$).

Lemma AppendixB.2. *Let* $lts_i^\circ = ({S_i}^\circ, {\to_i}^\circ, {M_{0,i}}^\circ) \in \overline{\mathcal{LTS}}$ *for* $i \in \{1, 2\}$, *such that* $lts_1^\circ \sqsubseteq_{lts} lts_2^\circ$, *and let* $M_1^\circ \in S_1^\circ, M_2^\circ \in S_2^\circ$. *If* $M_1^\circ \preccurlyeq_{lts} M_2^\circ$, *then there exists a bijective function* $H_t : \mathsf{Ts}(M_1^\circ) \to \mathsf{Ts}(M_2^\circ)$ *and*

1. $min(\mathbf{E}(M_2^\circ)) \leq min(\mathbf{E}(M_1^\circ)) \leq max(\mathbf{E}(M_1^\circ)) \leq max(\mathbf{E}(M_2^\circ))$;
2.

$$\begin{array}{ll} \forall N_2^\circ \in S_2^\circ & \sum^\circ_{N_1^\circ \in S_1^\circ} \mathbf{R}^\circ_{|(M_2^\circ, N_2^\circ)}(M_1^\circ, N_1^\circ) \leq_I \sum^\circ_{t_2^\circ \in \mathsf{Ts}(M_2^\circ, N_2^\circ)} \mathsf{rate}^\circ(t_2^\circ) \\ \forall N_1^\circ \in S_1^\circ & \mathbf{R}^\circ(M_1^\circ, N_1^\circ) = \sum^\circ_{N_2^\circ \in S_2^\circ} \mathbf{R}^\circ_{|(M_2^\circ, N_2^\circ)}(M_1^\circ, N_1^\circ) \end{array}$$

where $\mathbf{R}^\circ_{|(M_2^\circ, N_2^\circ)}(M_1^\circ, N_1^\circ) = \sum^\circ_{\{t_1^\circ \in \mathsf{Ts}(M_1^\circ, N_1^\circ) \mid H_t(t_1^\circ) \in \mathsf{Ts}(M_2^\circ, N_2^\circ)\}} \mathsf{rate}^\circ(t_1^\circ)$.

Proof of [Lemma AppendixB.2]

Since $M_1^\circ \preccurlyeq_{lts} M_2^\circ$, by Definition 4.12, there exists a function $H_t : \mathsf{Ts}(M_1^\circ) \to \mathsf{Ts}(M_2^\circ)$ such that, for each $t_1^\circ \in \mathsf{Ts}(M_1^\circ)$, $t_1^\circ = M_1^\circ \xrightarrow[\circ]{\Theta, \Delta_1^\circ, r} N_1^\circ$, $H_t(t_1^\circ) = t_2^\circ$ with $t_2^\circ \in \mathsf{Ts}(M_2^\circ), t_2^\circ = M_2^\circ \xrightarrow[\circ]{\Theta, \Delta_2^\circ, r} N_2^\circ$, $\Delta_1^\circ \leq_I \Delta_2^\circ$, $N_1^\circ \neq M_1^\circ$ implies that $N_2^\circ \neq M_2^\circ$, $N_1^\circ R N_2^\circ$ and $\mathsf{label}(\mathsf{Ts}({M_1}^\circ)) = \mathsf{label}(\mathsf{Ts}({M_2}^\circ))$.

Observation 1:

Note that $\mathsf{label}(\mathsf{Ts}({M_1}^\circ)) = \mathsf{label}(\mathsf{Ts}({M_2}^\circ))$ together with the restriction that $lts_i^\circ \in \overline{\mathcal{LTS}}$ implies that the function H_t defined above is indeed a bijective function.

In order to prove 1. and 2. we have to calculate the abstract rates of the transitions in $\mathsf{Ts}(M_1^\circ)$ and $\mathsf{Ts}(M_2^\circ)$.

Let us consider $t_1^\circ \in \mathsf{Ts}(M_1^\circ)$ and its image $t_2^\circ \in \mathsf{Ts}(M_2^\circ)$, such that $H_t(t_1^\circ) = t_2^\circ$. It must be the case that $t_1^\circ = M_1^\circ \xrightarrow[\circ]{\Theta, \Delta_1^\circ, r} N_1^\circ$ and $t_2^\circ = M_2^\circ \xrightarrow[\circ]{\Theta, \Delta_2^\circ, r} N_2^\circ$

with $\Delta_1^\circ \leq_I \Delta_2^\circ$. Since t_1° and t_2° are decorated by the same label Θ, there is an important relation between $\mathsf{rate}^\circ(t_1^\circ)$ and $\mathsf{rate}^\circ(t_2^\circ)$. More in detail, we have $\mathsf{rate}^\circ(t_1^\circ) = (z_{t_1^\circ}, c_{t_1^\circ})$ and $\mathsf{rate}^\circ(t_2^\circ) = (z_{t_1^\circ}, c_{t_2^\circ})$, e.g. the abstract rates share the same symbolic expression and differ only for the membership constraints. By exploiting $\Delta_1^\circ \leq_I \Delta_2^\circ$, we derive also an approximation between the membership constraints; indeed, we have $c_{t_1^\circ} \leq_I c_{t_2^\circ}$, and thus $\mathsf{rate}^\circ(t_1^\circ) \leq_I \mathsf{rate}^\circ(t_2^\circ)$.

Then, we examine the abstract rates of M_1° and M_2°, namely

$$\mathbf{R}^\circ(M_i^\circ, N_i^\circ) = \sum^\circ_{t_i^\circ \in \mathsf{Ts}(M_i^\circ, N_i^\circ)} \mathsf{rate}^\circ(t_i^\circ)$$
$$\mathbf{E}^\circ(M_i^\circ) = \sum^\circ_{N_i^\circ \in S_i^\circ} \mathbf{R}^\circ(M_i^\circ, N_i^\circ).$$

Since there is a one to one correspondence between the transitions of $\mathsf{Ts}(M_2^\circ)$ and the ones of $\mathsf{Ts}(M_1^\circ)$, it should be clear that, for each $i \in \{1, 2\}$, we have

$$\mathbf{E}^\circ(M_i^\circ) = (\sum^\circ_{t_i^\circ \in \mathsf{Ts}(M_i^\circ)} e_{t_i^\circ}, \sum^\circ_{t_i^\circ \in \mathsf{Ts}(M_i^\circ)} c_{t_i^\circ}) = (z_i, c_i)$$

where the symbolic expressions coincide and the constraints are approximated, that is $e_1 = e_2$ and $c_1 \leq_I c_2$. Hence, we can conclude that $min(\mathbf{E}(M_2^\circ)) \leq min(\mathbf{E}(M_1^\circ)) \leq max(\mathbf{E}(M_1^\circ)) \leq max(\mathbf{E}(M_2^\circ))$.

In order to prove 2. we have to focus on the abstract rate of a move from M_2° and N_2°, for $N_2^\circ \in S_2^\circ$. Using again the correspondence between the abstract rates of the transitions of $\mathsf{Ts}(M_2^\circ)$ and of $\mathsf{Ts}(M_1^\circ)$, we have

$$\mathbf{R}^\circ(M_2^\circ, N_2^\circ) = \sum^\circ_{t_2^\circ \in \mathsf{Ts}(M_2^\circ, N_2^\circ)} \mathsf{rate}^\circ(t_2^\circ) \geq^I \sum^\circ_{t_2^\circ \in \mathsf{Ts}(M_2^\circ, N_2^\circ)} \mathsf{rate}^\circ(H_t^{-1}(t_2^\circ))$$

We recall that H_t is bijective and that, for each $t_2^\circ \in \mathsf{Ts}(M_2^\circ, N_2^\circ)$, we have $H_t^{-1}(t_2^\circ) \in \mathsf{Ts}(M_1^\circ, N_1^{\circ\prime})$ for some $N_1^{\circ\prime} \in S_1^\circ$ (possibly different from N_1°). As a consequence, we obtain

$$\sum^\circ_{t_2^\circ \in \mathsf{Ts}(M_2^\circ, N_2^\circ)} \mathsf{rate}^\circ(H_t^{-1}(t_2^\circ)) = \sum^\circ_{N_1^\circ \in S_1^\circ} \mathbf{R}^\circ_{|(M_2^\circ, N_2^\circ)}(M_1^\circ, N_1^\circ) \text{ with}$$
$$\mathbf{R}^\circ_{|(M_2^\circ, N_2^\circ)}(M_1^\circ, N_1^\circ) = \sum^\circ_{\{t_1^\circ \in \mathsf{Ts}(M_1^\circ, N_1^\circ) \mid H_t(t_1^\circ) \in \mathsf{Ts}(M_2^\circ, N_2^\circ)\}} \mathsf{rate}^\circ(t_1^\circ).$$

Finally, we note that $\mathbf{R}^\circ_{|(M_2^\circ, N_2^\circ)}(M_1^\circ, N_1^\circ)$ sum up the rates of transitions from state M_1° to state N_1°, *which are mapped through H_t into transition going from M_2° to N_2°*. Since H_t is an injective function, it should be clear that

$$\sum^\circ_{N_2^\circ \in S_2^\circ} \mathbf{R}^\circ_{|(M_2^\circ, N_2^\circ)}(M_1^\circ, N_1^\circ) = \mathbf{R}^\circ(M_1^\circ, N_1^\circ)$$

□

Theorem AppendixB.3. *Let $lts_i^\circ = (S_i{}^\circ, \rightarrow_i{}^\circ, M_{0,i}{}^\circ) \in \overline{\mathcal{LTS}}$ be two abstract LTS, for $i \in \{1, 2\}$. If $lts_1^\circ \sqsubseteq^\circ_{lts} lts_2^\circ$, then also $\mathbf{H}^\circ(lts_1^\circ) \sqsubseteq^\circ_{mc} \mathbf{H}^\circ(lts_2^\circ)$.*

Proof of [Theorem AppendixB.3] Let $lts_i^\circ = (S_i^\circ, M_{0,i}^\circ, E) \in \overline{\mathcal{LTS}}$, for $i \in \{1, 2\}$, such that $lts_1^\circ \sqsubseteq^\circ_{lts} lts_2^\circ$. We have to prove that $mc_1^\circ \sqsubseteq^\circ_{mc} mc_2^\circ$, where $mc_i^\circ = \mathbf{H}^\circ(lts_i^\circ) = (S_i^\circ, \mathbf{P}_i^-, \mathbf{P}_i^+, \mathbf{L}, M_{0,i}^\circ)$; thus, we have to prove that $M_{0,1}^\circ \preccurlyeq_{mc} M_{0,2}^\circ$, according to Definition 5.8. We recall that, by Definition 4.12, $lts_1^\circ \sqsubseteq^\circ_{lts} lts_2^\circ$ ensures that $M_{0,1}^\circ \preccurlyeq_{lts} M_{0,2}^\circ$. Therefore, it is convenient to show that: for each $M_1^\circ \in S_1^\circ$ and $M_2^\circ \in S_2^\circ$, if $M_1^\circ \preccurlyeq_{lts} M_2^\circ$, then also $M_1^\circ \preccurlyeq_{mc} M_2^\circ$.

In order to obtain $M_1^\circ \preccurlyeq_{mc} M_2^\circ$ we have to demonstrate that: (i) $M_1^\circ \sqsubseteq^\circ M_2^\circ$; and (ii) for each distribution $\rho_1 \in \mathsf{ADistr}(M_1^\circ)$ there exist distributions $\delta \in \mathsf{Distr}(S_1^\circ \times S_2^\circ)$ and $\rho_2 \in \mathsf{ADistr}(M_2^\circ)$ such that, for any ${N_1}^\circ \in {S_1}^\circ$ and ${N_2}^\circ \in {S_2}^\circ$:

1. $\rho_1(N_1^\circ) = \sum_{N_2^\circ \in S_2^\circ} \delta(N_1^\circ, N_2^\circ)$ and $\rho_2(N_2^\circ) = \sum_{N_1^\circ \in S_1^\circ} \delta(N_1^\circ, N_2^\circ)$.
2. if $\delta(N_1^\circ, N_2^\circ) > 0$ then
   (a) $M_1^\circ \neq N_1^\circ$ implies that $M_2^\circ \neq N_2^\circ$;
   (b) $N_1^\circ \preccurlyeq_{mc} N_2^\circ$.

It should be clear that (i) follows immediately from $M_1^\circ \preccurlyeq_{lts} M_2^\circ$ by definition of the approximation order (see Definition 4.12). For (ii) we observe that an admissible distribution $\rho_i \in \mathsf{ADistr}(M_i^\circ)$, for $i \in \{1,2\}$, satisfies, for each $N_i^\circ \in S_i^\circ$, $\mathbf{P}_i^-(M_i^\circ)(N_i^\circ) \leq \rho_i(N_i^\circ) \leq \mathbf{P}_i^+(M_i^\circ)(N_i^\circ)$. Note indeed that if $lts_1^\circ = ({S_1}^\circ, {\rightarrow_1}^\circ, {M_{0,1}}^\circ) \in \overline{\mathcal{LTS}}$, then all the outgoing transitions from M_1° have different distinct labels, therefore the set of no-conflict states coincides with $\mathsf{Ts}(M_1^\circ)$. Analogously, $\mathsf{Ts}(M_2^\circ)$ is the set of no-conflict states for M_2°. Moreover, for each $i \in \{1,2\}$ the lower bound $\mathbf{P}_i^-(M_i^\circ)(N_i^\circ)$ and the upper bound $\mathbf{P}_i^+(M_i^\circ)(N_i^\circ)$ are derived from the abstract rates of the transitions in $\mathsf{Ts}(M_i^\circ)$. More in detail, according to the probabilistic translation function of Definition AppendixB.1, for most of the cases, the lower and upper bound probabilities for the move from M_i° to N_i° are computed by minimizing and maximizing the solution of $\mathbf{R}^\circ(M_i^\circ, {N_i}^\circ)/^\circ\mathbf{E}^\circ(M_i^\circ)$, respectively.

Let us consider an admissible distribution $\rho_1 \in \mathsf{ADistr}({M_1}^\circ)$. Since $M_1^\circ \preccurlyeq_{lts} M_2^\circ$ we can use the properties of Lemma AppendixB.2 in order to properly relate $\mathsf{Ts}(M_1^\circ)$ and $\mathsf{Ts}(M_2^\circ)$. In particular, we recall that there exists a one to one function $H_t : \mathsf{Ts}(M_1^\circ) \rightarrow \mathsf{Ts}(M_2^\circ)$ (see **Observation 1** of proof of LemmaAppendixB.2).

Our goal is to find distributions $\delta \in \mathsf{Distr}(S_1^\circ \times S_2^\circ)$ and $\rho_2 \in \mathsf{ADistr}(M_2^\circ)$, which satisfy conditions 1. and 2. Intuitively, for each $N_i^\circ \in S_i^\circ$ with $i \in \{1,2\}$, $\delta(N_1^\circ, N_2^\circ)$ says how much N_2° approximates N_1°. In order to compute δ, we have to consider the rate of the transitions from M_1° to N_1° which are mapped through H_t into transitions from M_2° to N_2°. Using Lemma AppendixB.2, this rate is $\mathbf{R}^\circ_{|(M_2^\circ, N_2^\circ)}(M_1^\circ, N_1^\circ) = \sum^\circ_{\{t_1^\circ \in \mathsf{Ts}(M_1^\circ, N_1^\circ) | H_t(t_1^\circ) \in \mathsf{Ts}(M_2^\circ, N_2^\circ)\}} \mathsf{rate}^\circ(t_1^\circ)$.

Based on $\mathbf{R}^\circ_{|(M_2^\circ, N_2^\circ)}(M_1^\circ, N_1^\circ)$ we define corresponding distributions $\sigma_{N_1^\circ} \in \mathsf{Distr}(S_2^\circ)$ such that $L(N_1^\circ, N_2^\circ) \leq \sigma_{N_1^\circ}(N_2^\circ) \leq U(N_1^\circ, N_2^\circ)$, where

$$L(N_1^\circ, N_2^\circ) = \begin{cases} 0 & \text{if } min(\mathbf{R}^\circ_{|(M_2^\circ, N_2^\circ)}(M_1^\circ, N_1^\circ)) = 0 \\ min(\frac{\mathbf{R}^\circ_{|(M_2^\circ, N_2^\circ)}(M_1^\circ, N_1^\circ)}{\mathbf{R}^\circ(M_1^\circ, N_1^\circ)}) & \text{otherwise} \end{cases}$$

$$U(N_1^\circ, N_2^\circ) = \begin{cases} 0 & \text{if } max(\mathbf{R}^\circ_{|(M_2^\circ, N_2^\circ)}(M_1^\circ, N_1^\circ)) = 0 \\ max(\frac{\mathbf{R}^\circ_{|(M_2^\circ, N_2^\circ)}(M_1^\circ, N_1^\circ)}{\mathbf{R}^\circ(M_1^\circ, N_1^\circ)}) & \text{otherwise} \end{cases}$$

Any distribution $\sigma_{N_1^\circ} \in \mathsf{Distr}(S_2^\circ)$ tells us at what extent N_2° approximates N_1° (regarding the set of transitions starting from M_1°, only). This is the ratio between the rates of the set of transitions of $\mathsf{Ts}(M_1^\circ, N_1^\circ)$ which have a corresponding transition in $\mathsf{Ts}(M_2^\circ, N_2^\circ)$ on the rates of *all* transitions of $\mathsf{Ts}(M_1^\circ, N_1^\circ)$.

Now, the proof proceeds by considering three different cases for $E^\circ(M_1^\circ)$. This is because $\mathbf{P}_1^-(M_1^\circ)(N_1^\circ)$ and $\mathbf{P}_1^+(M_1^\circ)(N_1^\circ)$ are set to 0 or1 or computed using $\mathbf{R}^\circ(M_1^\circ, {N_1}^\circ)/^\circ\mathbf{E}^\circ(M_1^\circ)$ depending on $E^\circ(M_1^\circ)$.

- Assume that $min(E^\circ(M_1^\circ)) \neq 0$. We define distributions $\delta \in \mathsf{Distr}(S_1^\circ \times S_2^\circ)$ and $\rho_2 \in \mathsf{Distr}(S_2^\circ)$, such that

$$\delta(N_1^\circ, N_2^\circ) = \rho_1(N_1^\circ) \cdot \sigma_{N_1^\circ}(N_2^\circ)$$
$$\rho_2(N_2^\circ) = \textstyle\sum_{N_1^\circ \in S_1^\circ} \delta(N_1^\circ, N_2^\circ)$$

  We have to show that δ and ρ_2 satisfy conditions 1. and 2. For 2. we observe that, by definition of δ, if $\delta(N_1^\circ, N_2^\circ) > 0$, it must be the case that $\sigma_{N_1^\circ}(N_2^\circ) > 0$. This means that $max(\mathbf{R}^\circ_{|(M_2^\circ, N_2^\circ)}(M_1^\circ, N_1^\circ)) \neq 0$, e.g. there exists a transition $t_1^\circ \in \mathsf{Ts}(M_1^\circ, N_1^\circ)$ such that $H_t(t_1^\circ) \in \mathsf{Ts}(M_2^\circ, N_2^\circ)$. By definition of $\preccurlyeq_{lts}$, we have $N_1^\circ \preccurlyeq_{lts} N_2^\circ$, and thus $N_1^\circ \preccurlyeq_{mc} N_2^\circ$ by inductive hypothesis.

  For 1. we have that

$$\sum_{N_2^\circ \in S_2^\circ} \delta(N_1^\circ, N_2^\circ) = \sum_{N_2^\circ \in S_2^\circ} \rho_1(N_1^\circ) \cdot \sigma_{N_1^\circ}(N_2^\circ) = \rho_1(N_1^\circ) \cdot \sum_{N_2^\circ \in S_2^\circ} \sigma_{N_1^\circ}(N_2^\circ) = \rho_1(N_1^\circ)$$

  Thus, we are left to prove that ρ_2 is an admissible distribution for ${M_2}^\circ$ i.e for each $N_2^\circ \in S_2^\circ$, $\mathbf{P}_2^-(M_2^\circ)(N_2^\circ) \leq \rho_2(N_2^\circ) \leq \mathbf{P}_2^+(M_2^\circ)(N_2^\circ)$.

  For simplicity, we examine the case of $\rho_2(N_2^\circ) \leq \mathbf{P}_2^+(M_2^\circ)(N_2^\circ)$; the other is analogous. We have:

$$\rho_2(N_2^\circ) = \sum_{N_1^\circ \in S_1^\circ} \delta(N_1^\circ, N_2^\circ) = \sum_{N_1^\circ \in S_1^\circ} \rho_1(N_1^\circ) \cdot \sigma_{N_1^\circ}(N_2^\circ)$$

  Since $\sigma_{N_1^\circ}(N_2^\circ)$ may be equal to 0, by definition of U, we have

$$\textstyle\sum_{N_1^\circ \in S_1^\circ} \rho_1(N_1^\circ) \cdot \sigma_{N_1^\circ}(N_2^\circ) = \sum_{\{N_1^\circ \in S_1^\circ | \sigma_{N_1^\circ}(N_2^\circ) > 0\}} \rho_1(N_1^\circ) \cdot \sigma_{N_1^\circ}(N_2^\circ) \leq$$
$$\textstyle\sum_{\{N_1^\circ \in S_1^\circ | \sigma_{N_1^\circ}(N_2^\circ) > 0\}} \rho_1(N_1^\circ) \cdot max(\frac{\mathbf{R}^\circ_{|(M_2^\circ, N_2^\circ)}(M_1^\circ, N_1^\circ)}{\mathbf{R}^\circ(M_1^\circ, N_1^\circ)^\circ})$$

  Since $\rho_1(N_1^\circ)$ may be equal to 0, we have

$$\textstyle\sum_{\{N_1^\circ \in S_1^\circ | \sigma_{N_1^\circ}(N_2^\circ) > 0\}} \rho_1(N_1^\circ) \cdot max(\frac{\mathbf{R}^\circ_{|(M_2^\circ, N_2^\circ)}(M_1^\circ, N_1^\circ)}{\mathbf{R}^\circ(M_1^\circ, N_1^\circ)^\circ}) =$$
$$\textstyle\sum_{\{N_1^\circ \in S_1^\circ | \sigma_{N_1^\circ}(N_2^\circ) > 0 \text{ and } \rho_1(N_1^\circ) > 0\}} \rho_1(N_1^\circ) \cdot \frac{max(\mathbf{R}^\circ_{|(M_2^\circ, N_2^\circ)}(M_1^\circ, N_1^\circ)}{\mathbf{R}^\circ(M_1^\circ, N_1^\circ)^\circ}$$

  We have assumed that, in this case, $min(\mathbf{E}^\circ(M_1^\circ)) \neq 0$, then, by definition of the translation function $\mathbf{H}^\circ$, and by Lemma AppendixB.2,

$$\begin{aligned}
&\rho_1(N_1^\circ) \cdot max(\tfrac{\mathbf{R}^\circ_{|(M_2^\circ, N_2^\circ)}(M_1^\circ, N_1^\circ)}{\mathbf{R}^\circ(M_1^\circ, N_1^\circ)^\circ}) \\
&= max(\tfrac{\mathbf{R}^\circ(M_1^\circ, N_1^\circ)}{\mathbf{E}^\circ(M_1^\circ)^\circ}) \cdot max(\tfrac{\mathbf{R}^\circ_{|(M_2^\circ, N_2^\circ)}(M_1^\circ, N_1^\circ)}{\mathbf{R}^\circ(M_1^\circ, N_1^\circ)^\circ}) \\
&\leq max(\tfrac{\mathbf{R}^\circ_{|(M_2^\circ, N_2^\circ)}(M_1^\circ, N_1^\circ)}{\mathbf{E}^\circ(M_1^\circ)^\circ}) \\
&\leq max(\tfrac{\mathbf{R}^\circ_{|(M_2^\circ, N_2^\circ)}(M_1^\circ, N_1^\circ)}{\mathbf{E}^\circ(M_2^\circ)^\circ})
\end{aligned}$$

By definition of $\mathbf{R}^{\circ}_{|(M_2^{\circ},N_2^{\circ})}(M_1^{\circ},N_1^{\circ})$, and by Lemma AppendixB.2,

$$\begin{array}{l}\sum_{\{N_1^{\circ}\in S_1^{\circ}|\sigma_{N_1^{\circ}}(N_2^{\circ})>0,\rho_1(N_1^{\circ})>0\}} max(\frac{\mathbf{R}^{\circ}_{|(M_2^{\circ},N_2^{\circ})}(M_1^{\circ},N_1^{\circ})}{\mathbf{E}^{\circ}(M_2^{\circ})^{\circ}})\\ = max(\frac{\mathbf{R}^{\circ}(M_2^{\circ},N_2^{\circ})}{\mathbf{E}^{\circ}(M_2^{\circ})^{\circ}})\\ = \mathbf{P}^{+}(M_2^{\circ})(N_2^{\circ}).\end{array}$$

- Assume that $min(E^{\circ}(M_1^{\circ}))=0$ but $max(E^{\circ}(M_1^{\circ}))>0$. We define distributions $\delta\in\mathsf{Distr}(S_1^{\circ}\times S_2^{\circ})$ and $\rho_2\in\mathsf{Distr}(S_2^{\circ})$, such that

$$\begin{array}{l}\delta(N_1^{\circ},N_2^{\circ})=\left\{\begin{array}{ll}\rho_1(N_1^{\circ})\cdot\sigma_{N_1^{\circ}}(N_2^{\circ}) & \text{if } N_1^{\circ}\neq M_1^{\circ}\\ \rho_1(M_1^{\circ}) & \text{if } N_1^{\circ}=M_1^{\circ} \text{ and } N_2^{\circ}=M_2^{\circ}\\ 0 & \text{otherwise}\end{array}\right.\\ \rho_2(N_2^{\circ})=\sum_{N_1^{\circ}\in S_1^{\circ}}\delta(N_1^{\circ},N_2^{\circ})\end{array}$$

  Note that the only difference w.r.t. the previous case is when $N_1^{\circ}=M_1^{\circ}$. Indeed, in this case, by definition of the translation function $\mathbf{H}^{\circ}$, $\mathbf{P}^{+}(M_1^{\circ})(M_1^{\circ})$=1. Then, $\rho_1(M_1^{\circ})\leq 1$ assumes, in general a value which is not strictly related to $\mathbf{R}^{\circ}_{|(M_2^{\circ},N_2^{\circ})}(M_1^{\circ},M_1^{\circ})$. This could lead to a ρ_2 which is not admissible, i.e., $\rho_2(N_2^{\circ})\not\leq\mathbf{P}^{+}(M_2^{\circ})(N_2^{\circ})$.

  We have to show that new δ and ρ_2 satisfy conditions 1. and 2. The reasoning showing that $\delta\in\mathsf{Distr}(S_1^{\circ}\times S_2^{\circ})$ satisfies also 2. is similar as in the previous case for each $N_1^{\circ}\neq M_1^{\circ}$. Instead, when $N_1^{\circ}=M_1^{\circ}$, we exploit the fact that $M_1^{\circ}\preccurlyeq_{lts}M_2^{\circ}$.

  For 1. we observe that

$$\begin{array}{l}\forall N_1^{\circ}\neq M_1^{\circ},\sum_{N_2^{\circ}\in S_2^{\circ}}\delta(N_1^{\circ},N_2^{\circ})=\sum_{N_2^{\circ}\in S_2^{\circ}}\rho_1(N_1^{\circ})\cdot\sigma_{N_1^{\circ}}(,N_2^{\circ})=\rho_1(N_1^{\circ})\\ \text{for } N_1^{\circ}=M_1^{\circ},\sum_{N_2^{\circ}\in S_2^{\circ}}\delta(M_1^{\circ},N_2^{\circ})=\delta(M_1^{\circ},M_2^{\circ})=\rho_1(N_1^{\circ})\end{array}$$

  Thus, we are left to prove that ρ_2 is an admissible distribution for $M_2{}^{\circ}$, i.e. for each $N_2^{\circ}\in S_2^{\circ}$ $\mathbf{P}_2^{-}(M_2^{\circ})(N_2^{\circ})\leq\rho_2(N_2^{\circ})\leq\mathbf{P}_1^{+}(M_2^{\circ})(N_2^{\circ})$. It is convenient to distinguish two cases.

$$\text{For } N_2^{\circ},N_2^{\circ}\neq M_2^{\circ},\rho_2(N_2^{\circ})=\sum_{N_1^{\circ}\in S_1^{\circ}}\delta(N_1^{\circ},N_2^{\circ})=\sum_{N_1^{\circ}\in S_1^{\circ},N_1^{\circ}\neq M_1^{\circ}}\delta(N_1^{\circ},N_2^{\circ})$$

  Hence, we can follow the guidelines of the proof in the previous case.

  Consider now N_2°, such that $N_2^{\circ}=M_2^{\circ}$, since $min(E^{\circ}(M_1^{\circ}))=0$ then, by Lemma AppendixB.2, also $min(E^{\circ}(M_2^{\circ}))=0$. Therefore, by definition of $\mathbf{H}^{\circ}$, $\mathbf{P}^{-}(M_2^{\circ})(M_2^{\circ})=0$ and $\mathbf{P}^{+}(M_2^{\circ})(M_2^{\circ})=1$.

- Assume that $max(E^{\circ}(M_1^{\circ}))=0$. We define distributions $\delta\in\mathsf{Distr}(S_1^{\circ}\times S_2^{\circ})$ and $\rho_2\in\mathsf{Distr}(S_2^{\circ})$, such that

$$\begin{array}{l}\delta(N_1^{\circ},N_2^{\circ})=\left\{\begin{array}{ll}1 & \text{if } N_1^{\circ}=M_1^{\circ} \text{ and } N_2^{\circ}=M_2^{\circ}\\ 0 & \text{otherwise}\end{array}\right.\\ \rho_2(M_2^{\circ})=1 \text{ and } \forall N_2^{\circ}\neq M_2^{\circ},\rho_2(N_2^{\circ})=0\end{array}$$

  We have to show that new δ and ρ_2 satisfy conditions 1. and 2. For proving $\delta\in\mathsf{Distr}(S_1^{\circ}\times S_2^{\circ})$ satisfies 2. we exploit the fact that $M_1^{\circ}\preccurlyeq_{lts}M_2^{\circ}$. Moreover,

it is easy to verify that the previously defined δ and ρ_2 satisfy 1, recalling that $max(E^\circ(M_1^\circ)) = 0$ implies, by definition of $\mathbf{H}^\circ$, $\rho_1(M_1^\circ) = 1$ and $\forall N_1^\circ \neq M_1^\circ, \rho_1(N_1^\circ) = 0$.

Thus, we are left to prove that ρ_2 is an admissible distribution for ${M_2}^\circ$. $max(E^\circ(M_1^\circ)) = 0$ implies that also $min(E^\circ(M_1^\circ)) = 0$. Hence, by Lemma AppendixB.2, $min(E^\circ(M_2^\circ)) = 0$. Then, by definition of $\mathbf{H}^\circ$, $\mathbf{P}^+(M_2^\circ)(M_2^\circ) = 1$. Moreover, $min(E^\circ(M_2^\circ)) = 0$ implies that $min(\mathbf{R}^\circ(M_2^\circ, N_2^\circ)) = 0$, for all N_2°. Hence, by definition of the translation function $\mathbf{H}^\circ$, for all N_2°, $\mathbf{P}^-(M_2^\circ)(N_2^\circ) = 0$. □

Finally, $M_1^\circ \neq N_1^\circ$ implies that $M_2^\circ \neq N_2^\circ$ follows directly from the definition of order on $\mathcal{LTS}$ and therefore on $\overline{\mathcal{LTS}}$.

We now extend the previous results to LTS's satisfying Condition 8.

Lemma AppendixB.4. *Let $lts_i^\circ = ({S_i}^\circ, {\rightarrow_i}^\circ, {M_{0,i}}^\circ) \in \mathcal{LTS}$ for $i \in \{1,2\}$, such that $lts_1^\circ \sqsubseteq_{lts} lts_2^\circ$, and let $M_1^\circ \in S_1^\circ, M_2^\circ \in S_2^\circ$. If $M_1^\circ \preccurlyeq_{lts} M_2^\circ$, then there exists a function $H_t : \mathsf{Ts}(M_1^\circ) \rightarrow \mathsf{Ts}(M_2^\circ)$ and*

1. *$min(\mathbf{E}_{N_2^\circ}(M_2^\circ)) \leq min(\mathbf{E}_{N_1^\circ}(M_1^\circ)) \leq max(\mathbf{E}_{N_1^\circ}(M_1^\circ)) \leq max(\mathbf{E}_{N_2^\circ}(M_2^\circ))$ where N_1° and N_2° are such that $t^\circ \in \mathsf{Ts}(M_1^\circ, N_1^\circ)$ and $H_t(t^\circ) \in \mathsf{Ts}(M_2^\circ, N_2^\circ)$;*
2. *Let $\overline{S^\circ}_1$ a be a maximal set of states such that $\forall N^\circ \in \overline{S_1^\circ}$, it does not exist $N_1^\circ \in \overline{S^\circ}_1, N^\circ \neq N_1^\circ$ such that $\mathsf{label}(\mathsf{Ts}(M_1^\circ, N^\circ)$ is in conflict with $\mathsf{label}(\mathsf{Ts}(M_1^\circ, N_1^\circ)$. Let $\overline{S^\circ}_2 = \bigcup_{\{t^\circ \mid t^\circ \in (\mathsf{Ts}(M_1^\circ, N^\circ), N^\circ \in \overline{S^\circ}_1\}} \mathsf{target}(H_t(t^\circ))$. Then*

$$\begin{array}{ll} \forall N_2^\circ \in \overline{S^\circ}_2 & \sum^\circ_{N_1^\circ \in \overline{S^\circ}_1} \mathbf{R}^\circ_{|(M_2^\circ, N_2^\circ)}(M_1^\circ, N_1^\circ) \leq_I \sum^\circ_{t_2^\circ \in \mathsf{Ts}(M_2^\circ, N_2^\circ)} \mathsf{rate}^\circ(t_2^\circ) \\ \forall N_1^\circ \in \overline{S^\circ}_1 & \mathbf{R}^\circ(M_1^\circ, N_1^\circ) = \sum^\circ_{N_2^\circ \in \overline{S^\circ}_2} \mathbf{R}^\circ_{|(M_2^\circ, N_2^\circ)}(M_1^\circ, N_1^\circ) \end{array}$$

where $\mathbf{R}^\circ_{|(M_2^\circ, N_2^\circ)}(M_1^\circ, N_1^\circ)$ is defined as in Lemma AppendixB.2.

Proof of [Lemma AppendixB.4] Since $M_1^\circ \preccurlyeq_{lts} M_2^\circ$, by Definition 4.12, there exists a function $H_t : \mathsf{Ts}(M_1^\circ) \rightarrow \mathsf{Ts}(M_2^\circ)$ such that, for each $t_1^\circ \in \mathsf{Ts}(M_1^\circ)$, $t_1^\circ = M_1^\circ \xrightarrow[\circ]{\Theta, \Delta_1^\circ, r} N_1^\circ$, $H_t(t_1^\circ) = t_2^\circ$ with $t_2^\circ \in \mathsf{Ts}(M_2^\circ), t_2^\circ = M_2^\circ \xrightarrow[\circ]{\Theta, \Delta_2^\circ, r} N_2^\circ$, $\Delta_1^\circ \leq_I \Delta_2^\circ$, $N_1^\circ \neq M_1^\circ$ implies that $N_2^\circ \neq M_2^\circ$, $N_1^\circ R N_2^\circ$ and $\mathsf{label}(\mathsf{Ts}({M_1}^\circ)) = \mathsf{label}(\mathsf{Ts}({M_2}^\circ))$.

In order to prove 1. and 2. we have to calculate the abstract rates of the transitions in $\mathsf{Ts}(M_1^\circ)$ and $\mathsf{Ts}(M_2^\circ)$.

Let us consider $t_1^\circ \in \mathsf{Ts}(M_1^\circ)$ and its image $t_2^\circ \in \mathsf{Ts}(M_2^\circ)$, such that $H_t(t_1^\circ) = t_2^\circ$. It must be the case that $t_1^\circ = M_1^\circ \xrightarrow[\circ]{\Theta, \Delta_1^\circ, r} N_1^\circ$ and $t_2^\circ = M_2^\circ \xrightarrow[\circ]{\Theta, \Delta_2^\circ, r} N_2^\circ$ with $\Delta_1^\circ \leq_I \Delta_2^\circ$. Since t_1° and t_2° are decorated by the same label Θ, there is an important relation between $\mathsf{rate}^\circ(t_1^\circ)$ and $\mathsf{rate}^\circ(t_2^\circ)$. More in detail, we have $\mathsf{rate}^\circ(t_1^\circ) = (z_{t_1^\circ}, c_{t_1^\circ})$ and $\mathsf{rate}^\circ(t_2^\circ) = (z_{t_1^\circ}, c_{t_2^\circ})$, e.g. the abstract rates share the same symbolic expression and differ only for the membership constraints. By exploiting $\Delta_1^\circ \leq_I \Delta_2^\circ$, we derive also an approximation between the membership constraints; indeed, we have $c_{t_1^\circ} \leq_I c_{t_2^\circ}$, and thus $\mathsf{rate}^\circ(t_1^\circ) \leq_I \mathsf{rate}^\circ(t_2^\circ)$.

Then, we examine the abstract exit rates of M_1° and M_2°, namely

$$\mathbf{E}^\circ_{N_i^\circ}(M_i^\circ) = \sum^\circ_{(z,c)\in \mathsf{rate}(\mathsf{Ts}_{\setminus N_i^\circ}(M_i^\circ)\cup \mathsf{Ts}(M_i^\circ,N_i^\circ))}(z,c).$$

Since there is the function H_t which relates (as described before) $t_1^\circ \in \mathsf{Ts}(M_1^\circ, N_1^\circ)$ with its image $t_2^\circ \in \mathsf{Ts}(M_2^\circ, N_2^\circ)$ and we have the condition that $\mathsf{label}(\mathsf{Ts}(M_1{}^\circ)) = \mathsf{label}(\mathsf{Ts}(M_2{}^\circ))$, we can conclude that

$$\mathsf{label}(\mathsf{Ts}_{\setminus N_1^\circ}(M_1^\circ)) = \mathsf{label}(\mathsf{Ts}_{\setminus N_2^\circ}(M_2^\circ))$$

Then, let $\Theta \in \widehat{\mathcal{L}}$ and $i \in \{1,2\}$, let

$$r^i_\Theta = \bigcup^\circ_{\{t^\circ \in \mathsf{Ts}_{\setminus N_i^\circ}(M_i^\circ)\cup \mathsf{Ts}(M_i^\circ,N_i^\circ), \mathsf{label}(t^\circ)=\Theta\}} \mathsf{rate}(t^\circ) = (z_i^\Theta, c_i^\Theta)$$

then the symbolic expression e_1^Θ and e_2^Θ coincide while the constraints are approximated, i.e., $c_1^\Theta \leq_I c_2^\Theta$.

Recall that $\mathsf{label}(\mathsf{Ts}(M_1{}^\circ)) = \mathsf{label}(\mathsf{Ts}(M_2{}^\circ))$, as a consequence, also in

$$\mathbf{E}^\circ_{N_i^\circ}(M_i^\circ) = \sum^\circ_{(z,c)\in \mathsf{rate}(\mathsf{Ts}_{\setminus N_i^\circ}(M_i^\circ)\cup \mathsf{Ts}(M_i^\circ,N_i^\circ))}(z,c) = (z_i, c_i)$$

the symbolic expression e_1 and e_2 coincide while the constraints $c_1 \leq_I c_2$. Hence, we can conclude that $min(\mathbf{E}_{N_2^\circ}(M_2^\circ)) \leq min(\mathbf{E}_{N_1^\circ}(M_1^\circ)) \leq max(\mathbf{E}_{N_1^\circ}(M_1^\circ)) \leq max(\mathbf{E}_{N_2^\circ}(M_2^\circ))$.

Before proving 2. observe that, by definition, $\overline{S^\circ}_1$ will be a set of non-conflict states w.r.t. M_1° in the derived IMC, while $\overline{S^\circ}_2$ will be a set of non-conflict states w.r.t. M_2°. Then, we focus on the abstract rate of a move from M_2° to N_2°, for $N_2^\circ \in \overline{S^\circ}_2$. Once again, we use the correspondence between the abstract rates of the transitions of $\mathsf{Ts}(M_2^\circ)$ and of $\mathsf{Ts}(M_1^\circ)$. Moreover, note that while H_t is not in general a bijective function, it becomes bijective when we restrict the function to the domain $\bigcup_{N_1^\circ \in \overline{S^\circ}_1} \mathsf{Ts}(M_1^\circ, N_1^\circ) \rightarrow \bigcup_{N_2^\circ \in \overline{S^\circ}_2} \mathsf{Ts}(M_2^\circ, N_2^\circ)$ once that Condition 8 holds. Therefore, we can reason as in the proof of Lemma AppendixB.2, once we recall that we have supposed that $N_1^\circ \in \overline{S^\circ}_1$ and $N_2^\circ \in \overline{S^\circ}_2$. we have

$$\mathbf{R}^\circ(M_2^\circ, N_2^\circ) = \sum^\circ_{t_2^\circ \in \mathsf{Ts}(M_2^\circ,N_2^\circ)} \mathsf{rate}^\circ(t_2^\circ) \geq^I \sum^\circ_{t_2^\circ \in \mathsf{Ts}(M_2^\circ,N_2^\circ)} \mathsf{rate}^\circ(H_t^{-1}(t_2^\circ))$$

As a consequence, we obtain

$$\sum^\circ_{t_2^\circ \in \mathsf{Ts}(M_2^\circ,N_2^\circ)} \mathsf{rate}^\circ(H_t^{-1}(t_2^\circ)) = \sum^\circ_{N_1^\circ \in \overline{S^\circ}_1} \mathbf{R}^\circ_{|(M_2^\circ,N_2^\circ)}(M_1^\circ, N_1^\circ) \text{ with}$$
$$\mathbf{R}^\circ_{|(M_2^\circ,N_2^\circ)}(M_1^\circ, N_1^\circ) = \sum^\circ_{\{t_1^\circ \in \mathsf{Ts}(M_1^\circ,N_1^\circ) | H_t(t_1^\circ) \in \mathsf{Ts}(M_2^\circ,N_2^\circ)\}} \mathsf{rate}^\circ(t_1^\circ).$$

Finally, we note that $\mathbf{R}^\circ_{|(M_2^\circ,N_2^\circ)}(M_1^\circ, N_1^\circ)$ sum up the rates of transitions from state M_1° to state N_1°, *which are mapped through H_t into transition going from M_2° to N_2°*. Since H_t is an injective function, it should be clear that

$$\sum^\circ_{N_2^\circ \in \overline{S_2^\circ}} \mathbf{R}^\circ_{|(M_2^\circ,N_2^\circ)}(M_1^\circ, N_1^\circ) = \mathbf{R}^\circ(M_1^\circ, N_1^\circ)$$

□

Proof of [Theorem 6.3] Let $lts_i^\circ = (S_i^\circ, M_{0,i}^\circ, E)$, for $i \in \{1,2\}$, such that $lts_1^\circ \sqsubseteq_{lts}^\circ lts_2^\circ$. We have to prove that $mc_1^\circ \sqsubseteq_{mc}^\circ mc_2^\circ$, where $mc_i^\circ = \mathbf{H}^\circ(lts_i^\circ) = (S_i^\circ, \mathbf{P}_i^-, \mathbf{P}_i^+, \mathbf{L}, M_{0,i}^\circ)$; thus, we have to prove that $M_{0,1}^\circ \preccurlyeq_{mc} M_{0,2}^\circ$, according to Definition 5.8.

Reasoning as in the proof of Theorem AppendixB.3, we have to show that for each $M_1^\circ \in S_1^\circ$ and $M_2^\circ \in S_2^\circ$, if $M_1^\circ \preccurlyeq_{lts} M_2^\circ$, then also $M_1^\circ \preccurlyeq_{mc} M_2^\circ$.

In order to obtain $M_1^\circ \preccurlyeq_{mc} M_2^\circ$ we have to demonstrate that: (i) $M_1^\circ \sqsubseteq^\circ M_2^\circ$; and (ii) for each distribution $\rho_1 \in \mathsf{ADistr}(M_1^\circ)$ there exist distributions $\delta \in \mathsf{Distr}(S_1^\circ \times S_2^\circ)$ and $\rho_2 \in \mathsf{ADistr}(M_2^\circ)$ such that, for any ${N_1}^\circ \in {S_1}^\circ$ and ${N_2}^\circ \in {S_2}^\circ$:

1. $\rho_1(N_1^\circ) = \sum_{N_2^\circ \in S_2^\circ} \delta(N_1^\circ, N_2^\circ)$ and $\rho_2(N_2^\circ) = \sum_{N_1^\circ \in S_1^\circ} \delta(N_1^\circ, N_2^\circ)$.
2. if $\delta(N_1^\circ, N_2^\circ) > 0$ then
   (a) $M_1^\circ \neq N_1^\circ$ implies that $M_2^\circ \neq N_2^\circ$;
   (b) $N_1^\circ \preccurlyeq_{mc} N_2^\circ$.

As before, (i) follows immediately from $M_1^\circ \preccurlyeq_{lts} M_2^\circ$ by definition of the approximation order (see Definition 4.12). For (ii) let us choose a an admissible distribution $\rho_1 \in \mathsf{ADistr}(M_1^\circ)$, such that for all $N_1 \in \overline{S^\circ}_1$, $\overline{S^\circ}_1$ a given set of no-conflict states, $\mathbf{P}_1^-(M_1^\circ)(N_1^\circ) \leq \rho_1(N_1^\circ) \leq \mathbf{P}_1^+(M_1^\circ)(N_1^\circ)$ and $(\rho_1(N^\circ)) = 0$, otherwise. By Definition 4.12, it is easy to see that there exists a corresponding set of no-coflict states $\overline{S^\circ}_2$ such that for all $N_2 \in \overline{S^\circ}_2$, $\mathbf{P}_2^-(M_2^\circ)(N_2^\circ) \leq \rho_2(N_2^\circ) \leq \mathbf{P}_2^+(M_2^\circ)(N_2^\circ)$ and $(\rho_2(N^\circ)) = 0$, otherwise. Hence, in the following we restrict ourself to consider $N_1 \in \overline{S^\circ}_1$ and $N_2 \in \overline{S^\circ}_2$.

More in detail, according to the probabilistic translation function of Definition 6.1, for most of the cases, the lower and upper bound probabilities for the move from M_i° to N_i° are computed by minimizing and maximizing the solution of $\mathbf{R}^\circ(M_i^\circ, {N_i}^\circ)/^\circ \mathbf{E}_{N_i^\circ}^\circ(M_i^\circ)$, respectively.

Let us consider then the admissible distribution $\rho_1 \in \mathsf{ADistr}({M_1}^\circ)$. Since $M_1^\circ \preccurlyeq_{lts} M_2^\circ$ we can use the properties of Lemma AppendixB.4 in order to properly relate $\mathsf{Ts}(M_1^\circ)$ and $\mathsf{Ts}(M_2^\circ)$. In particular, we recall that there exists a function $H_t : \mathsf{Ts}(M_1^\circ) \to \mathsf{Ts}(M_2^\circ)$.

Our goal is to find distributions $\delta \in \mathsf{Distr}(S_1^\circ \times S_2^\circ)$ and $\rho_2 \in \mathsf{ADistr}(M_2^\circ)$, which satisfy conditions 1. and 2. As before, for each $N_i^\circ \in \overline{S^\circ}_i$ with $i \in \{1,2\}$, $\delta(N_1^\circ, N_2^\circ)$ says how much N_2° approximates N_1°, if $N_1^\circ \notin \overline{S^\circ}_1$ or $N_2^\circ \notin \overline{S^\circ}_2$ then $\delta(N_1^\circ, N_2^\circ) = 0$. Therefore, here, we look for a $\delta \in \mathsf{Distr}(\overline{S^\circ}_1 \times \overline{S^\circ}_2)$ which can be easily extended to a $\delta \in \mathsf{Distr}(S_1^\circ \times S_2^\circ)$ as described before. In order to compute δ, we have to consider the rate of the transitions from M_1° to N_1° which are mapped through H_t into transitions from M_2° to N_2°. From Lemma AppendixB.2, this rate is denoted by $\mathbf{R}^\circ_{|(M_2^\circ, N_2^\circ)}(M_1^\circ, N_1^\circ) = \sum^\circ_{\{t_1^\circ \in \mathsf{Ts}(M_1^\circ, N_1^\circ) | H_t(t_1^\circ) \in \mathsf{Ts}(M_2^\circ, N_2^\circ)\}} \mathsf{rate}^\circ(t_1^\circ)$.

Based on $\mathbf{R}^\circ_{|(M_2^\circ, N_2^\circ)}(M_1^\circ, N_1^\circ)$ we define corresponding distributions $\sigma_{N_1^\circ} \in$

$\mathsf{Distr}(\overline{S^\circ}_2)$ such that $L(N_1^\circ, N_2^\circ) \leq \sigma_{N_1^\circ}(N_2^\circ) \leq U(N_1^\circ, N_2^\circ)$, where

$$L(N_1^\circ, N_2^\circ) = \begin{cases} 0 & \text{if } min(\mathbf{R}^\circ_{|(M_2^\circ, N_2^\circ)}(M_1^\circ, N_1^\circ)) = 0 \\ min(\frac{\mathbf{R}^\circ_{|(M_2^\circ, N_2^\circ)}(M_1^\circ, N_1^\circ)}{\mathbf{R}^\circ(M_1^\circ, N_1^\circ)}) & \text{otherwise} \end{cases}$$

$$U(N_1^\circ, N_2^\circ) = \begin{cases} 0 & \text{if } max(\mathbf{R}^\circ_{|(M_2^\circ, N_2^\circ)}(M_1^\circ, N_1^\circ)) = 0 \\ max(\frac{\mathbf{R}^\circ_{|(M_2^\circ, N_2^\circ)}(M_1^\circ, N_1^\circ)}{\mathbf{R}^\circ(M_1^\circ, N_1^\circ)}) & \text{otherwise} \end{cases}$$

As before, any distribution $\sigma_{N_1^\circ} \in \mathsf{Distr}(\overline{S^\circ}_2)$ tells us at what extent N_2° approximates N_1°.

Now, the proof proceeds by considering several different cases for $E^\circ_{\_}(M_1^\circ)$. The proofs of such cases is very similar to proof of Theorem AppendixB.3, once Lemma AppendixB.2 have been generalized as Lemma AppendixB.4. We prove the first case as an example.

Assume that $min(E^\circ_{N_1^\circ}(M_1^\circ)) \neq 0$. We define distributions $\delta \in \mathsf{Distr}(\overline{S^\circ}_1 \times \overline{S^\circ}_2)$ and $\rho_2 \in \mathsf{Distr}(\overline{S^\circ}_2)$, such that

$$\delta(N_1^\circ, N_2^\circ) = \rho_1(N_1^\circ) \cdot \sigma_{N_1^\circ}(N_2^\circ)$$
$$\rho_2(N_2^\circ) = \textstyle\sum_{N_1^\circ \in \overline{S^\circ}_1} \delta(N_1^\circ, N_2^\circ)$$

We have to show that δ and ρ_2 satisfy conditions 1. and 2. For 2. we observe that, by definition of δ, if $\delta(N_1^\circ, N_2^\circ) > 0$, it must be the case that $\sigma_{N_1^\circ}(N_2^\circ) > 0$. This means that $max(\mathbf{R}^\circ_{|(M_2^\circ, N_2^\circ)}(M_1^\circ, N_1^\circ)) \neq 0$, e.g. there exists a transition $t_1^\circ \in \mathsf{Ts}(M_1^\circ, N_1^\circ)$ such that $H_t(t_1^\circ) \in \mathsf{Ts}(M_2^\circ, N_2^\circ)$. By definition of $\preccurlyeq_{lts}$, we have $N_1^\circ \preccurlyeq_{lts} N_2^\circ$, and thus $N_1^\circ \preccurlyeq_{mc} N_2^\circ$ by inductive hypothesis.

For 1. we have that

$$\sum_{N_2^\circ \in \overline{S^\circ}_2} \delta(N_1^\circ, N_2^\circ) = \sum_{N_2^\circ \in \overline{S^\circ}_2} \rho_1(N_1^\circ) \cdot \sigma_{N_1^\circ}(N_2^\circ) = \rho_1(N_1^\circ) \cdot \sum_{N_2^\circ \in \overline{S^\circ}_2} \sigma_{N_1^\circ}(N_2^\circ) = \rho_1(N_1^\circ)$$

Thus, we are left to prove that ρ_2 is an admissible distribution for $M_2{}^\circ$ i.e for each $N_2^\circ \in \overline{\overline{S^\circ}_2}$, $\mathbf{P}_2^-(M_2^\circ)(N_2^\circ) \leq \rho_2(N_2^\circ) \leq \mathbf{P}_2^+(M_2^\circ)(N_2^\circ)$.

For simplicity, we examine the case of $\rho_2(N_2^\circ) \leq \mathbf{P}_2^+(M_2^\circ)(N_2^\circ)$; the other is analogous. We have:

$$\rho_2(N_2^\circ) = \sum_{N_1^\circ \in \overline{S^\circ}_1} \delta(N_1^\circ, N_2^\circ) = \sum_{N_1^\circ \in \overline{S^\circ}_1} \rho_1(N_1^\circ) \cdot \sigma_{N_1^\circ}(N_2^\circ)$$

Since $\sigma_{N_1^\circ}(N_2^\circ)$ may be equal to 0, by definition of U, we have

$$\textstyle\sum_{N_1^\circ \in \overline{S^\circ}_1} \rho_1(N_1^\circ) \cdot \sigma_{N_1^\circ}(N_2^\circ) = \sum_{\{N_1^\circ \in \overline{S^\circ}_1 | \sigma_{N_1^\circ}(N_2^\circ) > 0\}} \rho_1(N_1^\circ) \cdot \sigma_{N_1^\circ}(N_2^\circ) \leq$$
$$\textstyle\sum_{\{N_1^\circ \in \overline{S^\circ}_1 | \sigma_{N_1^\circ}(N_2^\circ) > 0\}} \rho_1(N_1^\circ) \cdot max(\frac{\mathbf{R}^\circ_{|(M_2^\circ, N_2^\circ)}(M_1^\circ, N_1^\circ)}{\mathbf{R}^\circ(M_1^\circ, N_1^\circ)^\circ})$$

Since $\rho_1(N_1^\circ)$ may be equal to 0, we have

$$\textstyle\sum_{\{N_1^\circ \in \overline{S^\circ}_1 | \sigma_{N_1^\circ}(N_2^\circ) > 0\}} \rho_1(N_1^\circ) \cdot max(\frac{\mathbf{R}^\circ_{|(M_2^\circ, N_2^\circ)}(M_1^\circ, N_1^\circ)}{\mathbf{R}^\circ(M_1^\circ, N_1^\circ)^\circ}) =$$
$$\textstyle\sum_{\{N_1^\circ \in \overline{S^\circ}_1 | \sigma_{N_1^\circ}(N_2^\circ) > 0 \text{ and } \rho_1(N_1^\circ) > 0\}} \rho_1(N_1^\circ) \cdot \frac{max(\mathbf{R}^\circ_{|(M_2^\circ, N_2^\circ)}(M_1^\circ, N_1^\circ)}{\mathbf{R}^\circ(M_1^\circ, N_1^\circ))^\circ}$$

We have assumed that, in this case, $min(\mathbf{E}^{\circ}_{N_1^{\circ}}(M_1^{\circ})) \neq 0$, then, by definition of the translation function $\mathbf{H}^{\circ}$, and by Lemma AppendixB.4,

$$\rho_1(N_1^{\circ}) \cdot max(\frac{\mathbf{R}^{\circ}_{|(M_2^{\circ},N_2^{\circ})}(M_1^{\circ},N_1^{\circ})}{\mathbf{R}^{\circ}(M_1^{\circ},N_1^{\circ})^{\circ}}) = max(\frac{\mathbf{R}^{\circ}(M_1^{\circ},N_1^{\circ})}{\mathbf{E}^{\circ}(M_1^{\circ})^{\circ}})\cdot$$
$$max(\frac{\mathbf{R}^{\circ}_{|(M_2^{\circ},N_2^{\circ})}(M_1^{\circ},N_1^{\circ})}{\mathbf{R}^{\circ}(M_1^{\circ},N_1^{\circ})^{\circ}}) \leq max(\frac{\mathbf{R}^{\circ}_{|(M_2^{\circ},N_2^{\circ})}(M_1^{\circ},N_1^{\circ})}{\mathbf{E}^{\circ}_{N_1^{\circ}}(M_1^{\circ})^{\circ}}) \leq max(\frac{\mathbf{R}^{\circ}_{|(M_2^{\circ},N_2^{\circ})}(M_1^{\circ},N_1^{\circ})}{\mathbf{E}^{\circ}_{N_2^{\circ}}(M_2^{\circ})^{\circ}})$$

By definition of $\mathbf{R}^{\circ}_{|(M_2^{\circ},N_2^{\circ})}(M_1^{\circ},N_1^{\circ})$, and by Lemma AppendixB.4,

$$\sum_{\{N_1^{\circ}\in\overline{S^{\circ}}_1 | \sigma_{N_1^{\circ}}(N_2^{\circ})>0, \rho_1(N_1^{\circ})>0\}} max(\frac{\mathbf{R}^{\circ}_{|(M_2^{\circ},N_2^{\circ})}(M_1^{\circ},N_1^{\circ})}{\mathbf{E}^{\circ}_{N_2^{\circ}}(M_2^{\circ})^{\circ}}) = max(\frac{\mathbf{R}^{\circ}_{(}M_2^{\circ},N_2^{\circ})}{\mathbf{E}^{\circ}_{N_2^{\circ}}(M_2^{\circ})^{\circ}}) = \mathbf{P}^{+}(M_2^{\circ})(N_2^{\circ}).$$

Proof of [Theorem 6.4] We have to show that

$$\alpha_{MC}(\mathbf{H}(\mathsf{LTS}((E,M_0)))) = \mathbf{H}^{\circ}(\alpha_{lts}(\mathsf{LTS}((E,M_0)))).$$

Let $lts = \mathsf{LTS}((E,M_0) = (S,\rightarrow,M_0,E)$. On the one hand, by Definition 4.13, we have $\alpha_{lts}(lts) = (\{M^{\bullet}\}_{M\in S}, \alpha(\rightarrow), {M_0}^{\bullet}, E)$ where $\alpha(\rightarrow) = \{M^{\bullet} \xrightarrow[\circ]{\Theta,\Delta^{\bullet},r} M'^{\bullet} \mid M \xrightarrow{\Theta,\Delta,r} M' \in \rightarrow\}$ and $\Delta^{\bullet}$ is the best abstraction of Δ. Note that $\alpha_{lts}(\mathsf{LTS}((E,M_0))) \in \overline{\mathcal{LTS}}$, then, by applying the abstract probabilistic function (see Definition 6.1 which coincides with Definition AppendixB.1, in this case) we obtain

$$\mathbf{H}^{\circ}(\alpha_{lts}(lts)) = (\{M^{\bullet}\}_{M\in S}, \mathbf{P}_1^{-}, \mathbf{P}_1^{+}, \mathbf{L}, {M_0}^{\bullet})$$

where $\mathbf{P}_1^{-}, \mathbf{P}_1^{+}$ are the lower and upper probability functions. We recall that, for each $M \in S$, both $\mathbf{P}_1^{-}(M^{\bullet})$ and $\mathbf{P}_1^{+}(M^{\bullet})$ are calculated from the abstract rate of the transitions in $\mathsf{Ts}(M^{\bullet})$.

On the other hand, by applying the probabilistic function (see Definition 2.6), we obtain $\mathbf{H}(lts) = (S,\mathbf{P},\mathbf{L},M_0)$ where $\mathbf{P}$ is the probability transition function which is calculated, for each $M \in S$, from the rate of the transitions in $\mathsf{Ts}(M)$. Then, by Definition 5.10 we have,

$$\alpha_{MC}(\mathbf{H}(lts)) = (\{M^{\bullet}\}_{M\in S}, {\mathbf{P}_2}^{-}, {\mathbf{P}_2}^{+}, \mathbf{L}, {M_0}^{\bullet})$$

where ${\mathbf{P}_2}^{-}(M^{\bullet},M'^{\bullet}) = {\mathbf{P}_2}^{+}(M^{\bullet},M'^{\bullet}) = \mathbf{P}(M_1)(M_2)$, for each $M_1, M_2 \in S$.

It should be clear that, for each $M \in S$, and for each transition $\alpha(t) \in \mathsf{Ts}(M^{\bullet})$, the solution of $\mathsf{rate}^{\circ}(\alpha(t))$ is an exact value which is equal to $\mathsf{rate}(t)$, where $t \in \mathsf{Ts}(M)$ is the corresponding concrete transition. As a consequence, for each $M, M' \in S$, we have ${\mathbf{P}_1}^{-}(M^{\bullet},M'^{\bullet}) = {\mathbf{P}_1}^{+}(M^{\bullet},M'^{\bullet}) = {\mathbf{P}_2}^{-}(M^{\bullet},M'^{\bullet}) = {\mathbf{P}_2}^{+}(M^{\bullet},M'^{\bullet})$. □

Proof of [Theorem 6.5] By Theorem 6.4, we have that $\alpha_{MC}(\mathbf{H}(\mathsf{LTS}((E,M_0)))) \sqsubseteq^{\circ}_{mc} \mathbf{H}^{\circ}(\alpha_{lts}(\mathsf{LTS}((E,M_0))))$. Hence we have to prove that $\mathbf{H}^{\circ}(\alpha_{lts}(\mathsf{LTS}((E,M_0)))) \sqsubseteq^{\circ}_{mc} \mathbf{H}^{\circ}(\mathsf{LTS}^{\circ}((E,M_0^{\circ})))$.
By Theorem 4.14 , we have that $\alpha_{lts}(\mathsf{LTS}((E,M_0))) \sqsubseteq_{lts}{}^{\circ} \mathsf{LTS}^{\circ}((E,M_0^{\circ}))$, therefore, by Theorem 6.3, we can conclude that $\mathbf{H}^{\circ}(\alpha_{lts}(\mathsf{LTS}((E,M_0)))) \sqsubseteq^{\circ}_{mc} \mathbf{H}^{\circ}(\mathsf{LTS}^{\circ}((E,M_0^{\circ})))$.

We are left now with the generalization of the function $\mathbf{H}^\circ$ also to LTSs which do not satisfy Condition 8. As we have already pointed out the difficulty in this case resides in summing up rates of transitions, one of which shares the same label with some other transition leaving from the same M°. Formally the problem arises when (i) $|\mathsf{label}(\{t^\circ \in \mathsf{Ts}(M^\circ, N_1^\circ) \mid max(\mathsf{rate}^\circ(t^\circ)) > 0\})| > 1$ and (ii) there exists a transition $t^\circ \in \mathsf{Ts}(M^\circ, N_1^\circ)$ such that $\mathsf{label}(t^\circ) \in \mathsf{label}(\mathsf{Ts}_{\setminus N_1^\circ}(M^\circ))$. Indeed, note that if (i) holds, by definition, we are not able to represent in the derived IMC the notion of conflict between the transition t° and the other transitions of $\mathsf{Ts}_{\setminus M^\circ}(N_1^\circ)$ with label $\mathsf{label}(t^\circ)$, therefore, the minimum of and the maximum probability to reach N_1° has to be adjusted consequently exploiting the *worst and best case scenario*.

Let us consider the LTS in Figure AppendixB, where $\mathsf{label}(t_2^\circ) = \mathsf{label}(t_3^\circ) = (\lambda, \mu)$ and $\mathsf{label}(t_1^\circ) = (\delta, \eta)$.

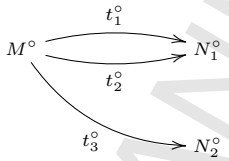


Figure B.23: An LTS not satisfying Condition 8

Notice that label of the transition from M° to N_1°, i.e., $\{(\lambda, \mu), (\delta, \eta)\}$ will not be in conflict with $\{(\lambda, \mu)\}$ in the derived IMC. Therefore, looking for a safe approximation of the probabilities to reach N_1° we have to consider the worst case scenario for the minimum probability and the best case scenario for the maximum probability. Since t_2° and t_3° share the same label, this means that either one or the other transition is taken. Therefore, for the minimum probability to reach N_1° we consider transition t_3° (which does not reach N_1°) while for the maximum probability we consider transition t_2°. In other words the *abstract probabilistic translation* function $\mathbf{H}^\circ$ of Definition 6.1 has to be applied to *two different LTS's*. The *abstract probabilistic translation* function $\mathbf{H}^\circ$ of Definition 6.1 have to be applied to the LTS of Figure AppendixB when considering $\mathbf{P}^-(M^\circ, N_1^\circ)$ while it has to be applied to the LTS of Figure AppendixB

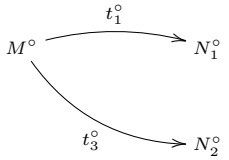


Figure B.24: The worst case scenario

when considering $\mathbf{P}^+(M^\circ, N_1^\circ)$. Note that the previous reasoning applies even when t_2° share the same label with more than one other transition leaving

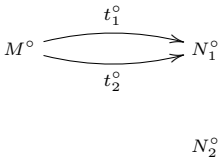


Figure B.25: The best case scenario

from M°.

Here, we briefly discuss the correctness of this approach. Intuitively the first point of Lemma AppendixB.4 can easily be extended since it does not require Condition 8 to hold. In the second part such Condition is instead used to assure that the function H_t is bijective. Note however, that using two different LTS for the best and worst case scenario, allows us to prove that the function H_t restricted to a set a non-conflict states is indeed bijective.

[1] L. de Alfaro and P. Roy. *Magnifying-Lens Abstraction for Markov decision Process.* Proc. of CAV '07, LNCS 4590, 325–338, 2007.

[2] P. Ballarini and M.L. Guerriero. *Query-based Verification of Qualitative Trends and Oscillations in Biochemical Systems.* Theoretical Computer Science, 411, 2019–2036, 2010.

[3] P. Ballarini, R. Mardare and I. Mura. *Analysing Biochemical Oscillation through Probabilistic Model Checking.* Proc. of FBTC '08, ENTCS 229 (1), 3–19, 2009.

[4] R. Barbuti, F. Levi, P. Milazzo and G. Scatena. *Probabilistic Model Checking of Biological Systems with Uncertain Kinetic Rates.* Proc. of RP '09, LNCS 5797, 68–74, 2009.

[5] A. Bianco and L. de Alfaro. *Model Checking of Probabilistic and Nondeterministic Systems.* Proc. of FSTTCS '95, LNCS 1026, 499–513, 1995.

[6] C. Bodei. *A Control Flow Analysis for Beta-binders with and without static compartments.* Theoretical Computer Science, 410 (33-34), 3110–3127, 2009.

[7] C. Bodei, P. Degano, F. Nielson and H.R. Nielson. *Static Analysis for the Pi-Calculus with Applications to Security.* Information and Computation, 168, 68–92, 2001.

[8] M. Calder, V. Vyshemirsky, D. Gilbert and R. Orton. *Analysis of signalling pathways using the PRISM model checker.* Proc. of CMSB '05, LNCS 3901, 179–190, 2005.

[9] M. Calder, V. Vyshemirsky, D. Gilbert, and R. Orton. *Analysis of Signalling Pathways using Continuous Time Markov Chains.* Transactions on Computational Systems Biology VI, 4220, 44–67, 2006.

[10] L. Cardelli. *Brane Calculi.* Proc. of CMSB '04, LNCS 3082, 257–278, 2004.

[11] L. Cardelli. *Artificial Biochemestry.* Thecnical report, The Microsoft Research-CoSBi, 2006.

[12] L. Cardelli. *On Process Rate Semantics.* Theoretical Computer Science, 391 190–215, 2008.

[13] L. Cardelli. *Algorithmic Bioprocesses.* In A.Condon, D.Harel, J.N.Kok, A.Salomaa, E.Winfree (Eds.), Springer, 2009

[14] N. Chabrier, M. Chiaverini, V. Danos and F. Fages. *Modeling and Querying Biomolecular Interaction Networks.* Theoretical Computer Science, 325(1), 25-44, 2004.

[15] A. Coletta, R. Gori and F. Levi. *Approximating probabilistic behaviours of biological systems using abstract interpretation.* Proc. of FBTC '08, ENTCS 229 (1), 165–182, 2009.

[16] P. Cousot and R. Cousot. *Static Determination of Dynamic Properties of Programs.* Proc. of POPL'76, 106–130, 1976.

[17] 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.

[18] P. Cousot and R. Cousot. *Systematic Design of Program Analysis Frameworks.* Proc. of POPL'79 , 269–282, 1979.

[19] 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.

[20] D. Dams, R. Gerth and O. Grumberg. *Abstract Interpretation of Reactive Systems.* TOPLAS, 19(2), 253-291, 1997.

[21] V. Danos, J. Feret, W. Fontana and J. Krivine. *Abstract interpretation of cellular signalling networks.* Proc. of VMCAI'08, LNCS 4905, 83–97, 2008.

[22] P. D'Argenio, B. Jeannet, H. Jensen and K. Larsen. *Reachability Analysis of Probabilistic Systems by Successive Refinements.* Proc. of PAPM-PROBMIV'01, LNCS 2165, 39–56, 2001.

[23] P. D'Argenio, B. Jeannet, H. Jensen and K. Larsen. *Reduction and Refinement Strategies for Probabilistic Analysis.* Proc. of PAPM-PROBMIV'02, LNCS 2399, 57–76, 2002.

[24] H. Fecher, M. Leucker and V. Wolf. *Don't Know in Probabilistic Systems.* Proc. of SPIN'06, LNCS 3925, 71–88, 2006.

[25] J. Feret. *Abstract Interpretation-Based Static Analysis of Mobile Ambients.* Proc. of SAS'01, LNCS 2126, 412-430, Springer Verlag, 2001.

[26] D. Gillespie. *Exact Stochastic Simulation of Coupled Chemical Reactions.* Journal of Physical Chemistry, 81(25), 2340–2361, 1977.

[27] R. Gori and F. Levi. *Abstract interpretation based verification of temporal properties for BioAmbients.* Information and Computation, 208(8), 869–921, 2010.

[28] R. Gori and F. Levi. *Abstract Interpretation for Probabilistic Termination of Biological Systems.* Proc. of MeCBIC'09, EPTCS 11, 137–153, 2009.

[29] H.Hansson and B. Jonsson. *A Logic for Reasoning about Time and Probability.* Formal Aspects of Computing, 6(5), 512–535, 1994.

[30] J. Heat, M. Kwiatkowska, G. Norman, D. Parker and O. Tymchyshyn. *Probabilistic Model Checking of Complex Biological Pathways.* Theoretical Computer Science 319(3), 239–257, 2008.

[31] A. Hinton, M. Kwiatkowska, G. Norman and D. Parker. *PRISM: a tool for automatic verification of probabilistic systems.* Proc. of TACAS'06, LNCS 3920, 441-444, Springer-Verlag, 2006.

[32] M. Huth. *On finite-state approximants for probabilistic computation tree logic.* Theoretical Computer Science, 346(1), 113–134, 2005.

[33] J.P. Katoen, D. Klink, M. Leucker and V. Wolf. *Three-Valued Abstraction for Continuous-Time Markov Chains*, Proc. of CAV '07, LNCS 4590, 311–324, 2007.

[34] M. Kattenbelt, M. Kwiatkowska, G. Norman, D. Parker. *Game-Based Probabilistic Predicate Abstraction in PRISM.* Proc. of QAPL'08, ENTCS 220(3),5–21, 2008.

[35] J.G. Kemeny, J. L. Snell and A. W. Knapp *Denumerable Markov Chains.* Springer-Verlag, 1976.

[36] M. Kwiatkowska. *Model checking for probability and time: from theory to practice.* Proc. of LICS' 03, 351–360, 2003.

[37] M. Kwiatkowska, G. Norman and D. Parker. *Game-based Abstraction for Markov Decision Processes.* Proc. of QEST'06, 157–166, 2006.

[38] M. Kwiatkowska, G. Norman and D. Parker *Stochastic Model Checking.* SFM 2007, 220–270, 2007.

[39] F. Levi and S. Maffeis. *On Abstract Interpretation of Mobile Ambients.* Information and Computation, 188, 179–240, 2004.

[40] D. Monniaux. *Abstract interpretation of programs as Markov Decision Processes.* Science of Computer Programming, 58(1-2), 179–205, 2005.

[41] F. Nielson, H.R. Nielson and R.R. Hansen. *Validating firewalls using flow logics.* Theoretical Computer Science, 283(2), 381-418, 2002.

[42] F. Nielson, H.R. Nielson and H. Pilegaard. *Spatial Analysis of BioAmbients.* Proc. of SAS'04, LNCS 3148, pp. 69–83, Springer-Verlag, 2004.

[43] A. Phillips and L. Cardelli. *A Correct Abstract Machine for the Stochastic Pi-calculus.* Proc. of BioCONCUR '04, ENTCS, 2004.

[44] A. Phillips and L. Cardelli. *Efficient, Correct Simulation of Biological Processes in the Stochastic Pi-calculus.* Proc. of CMSB '07, LNCS 4695, 184–199, 2007.

[45] H. Pilegaard, F. Nielson and H.R. Nielson. *Pathway analysis for BioAmbients.* The Journal of Logic and Algebraic Programming, 77, 92–130, 2008.

[46] C.Priami. *Stochastic π-calculus.* The Computer Journal, 38, 578–589,1995.

[47] C.Priami and P. Quaglia. *Beta binders for biological interactions.* Proc. of CMSB'04, LNCS 3082,20–33,2005.

[48] 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.

[49] 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.

[50] 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.

[51] K. Sen, M. Viswanathan and G. Agha. *Model Checking Markov Chains in the Presence of Uncertainties.* Proc. of TACAS'06, LNCS 3920, 394-410, 2006.

[52] B. Wachter, L. Zhang and H. Hermanns. *Probabilistic model checking modulo theories.* Proc. of QEST'07, 119–128, 2007.

[53] G. Zavattaro and L. Cardelli. *Termination Problems in Chemical Kinetics.* Proc. of CONCUR'08, LNCS 5201, 477-491, 2008.