IMT Institute for Advanced Studies, Lucca

Lucca, Italy

Abstract Probabilistic Semantics for the Analysis of Biological Systems Models

PhD Program in Computer Science and Engineering

XXIII Cycle

By

Guido Scatena

2011

The dissertation of Guido Scatena is approved.

Program Coordinator:

Ugo Montanari, University of Pisa

Supervisors:

Roberto Barbuti, University of Pisa
Francesca Levi, University of Pisa

The dissertation of Guido Scatena has been reviewed by:

Damas Gruska, University of Bratislava (Slovakia)
Francisco J. Romero-Campero, University of Seville (Spain)

IMT Institute for Advanced Studies, Lucca

2011

Contents

1 Introduction **1**
- 1.1 Motivations . . . 3
- 1.2 Related Works . . . 4
- 1.3 Contributions . . . 6
- 1.4 Structure of the thesis . . . 7
- 1.5 Published Material . . . 8

2 Background **9**
- 2.1 Introduction to Biological Systems Modelling . . . 9
- 2.2 Notions of Biochemical Reactions Kinetics . . . 14
- 2.3 Probabilistic Semantics and Analysis . . . 18
  - 2.3.1 Notions of Probability . . . 19
  - 2.3.2 Kripke Structures, Markov Chains and Markov Decision Processes . . . 21
  - 2.3.3 Model Checking . . . 25
- 2.4 Abstraction Techniques . . . 31
  - 2.4.1 Abstract Interpretation . . . 32
  - 2.4.2 Predicate Abstraction . . . 35

3 Abstract Semantics for Models with Uncertainty on Kinetic Rates **39**
- 3.1 Introduction . . . 39
- 3.2 Probabilistic Model Checking of Biological Systems . . . 41
  - 3.2.1 Labeled Transition System Semantics . . . 42
  - 3.2.2 Derivation of Probabilistic Semantics . . . 43
  - 3.2.3 Probabilistic Model Checking . . . 44
- 3.3 Abstract Systems Modelling and Model Checking . . . 45
  - 3.3.1 Abstraction and Concretization . . . 46

3.3.2 Abstract LTS Semantics . . . 47
3.3.3 Interval Markov Chains . . . 50
3.3.4 Derivation of Abstract Probabilistic Semantics . . . 53
3.4 Case Study: Tumor Cell Growth . . . 58
3.5 Comparison with Related Works . . . 63
3.6 Conclusions . . . 63

4 Maximally Parallel Probabilistic Semantics for Multiset Rewriting 65
4.1 Introduction . . . 65
4.2 Maximally Parallel Multiset Rewriting Models . . . 67
4.3 Maximally Parallel Labeled Transition System Semantics . . . 69
4.4 Maximally Parallel Probabilistic Semantics . . . 72
4.5 Max. Parallel Multiset Rewriting Branching Complexity . . . 74
4.6 Case Study: *C. elegans* Vulval Development . . . 77
4.7 Comparison with Related Works . . . 81
4.8 Conclusions . . . 82

5 Interval Valued Abstract Maximally Parallel Semantics for Multiset Rewriting 85
5.1 Introduction . . . 86
5.2 Interval Valued Abstract Models . . . 87
5.3 Abstract Labelled Transition System Semantics . . . 91
5.3.1 Computation of Reachable Abstract States . . . 92
5.3.2 Computation of Abstract Max. Parallel Rule Applications 95
5.3.3 Computation of Abstract Transition Rates . . . 100
5.3.4 Soundness of abstract LTS semantics . . . 104
5.4 Abstract Probabilistic Semantics . . . 106
5.4.1 Abstract Probabilistic Semantics . . . 108
5.4.2 Soundness with respect to Probabilistic Reachability . . 109
5.5 Case study: Seasonal Reproduction Model . . . 111
5.6 Discussion . . . 117
5.7 Comparison with Related Works . . . 118
5.8 Conclusions . . . 120
5.9 Proofs . . . 121

6 Conclusions 137

Bibliography 141

VITA

April 2, 1982	Born, Pisa, Italy
2007	Degree Computer Science Final marks: 106/110 Università di Pisa Pisa, Italy

PUBLICATIONS AND PRESENTATIONS

R. Barbuti, F. Levi, P. Milazzo, G. Scatena (2009) *Probabilistic Model Checking of Biological Systems with Uncertain Kinetic Rates*. In: Reachability Problems, RP09, Palaiseau, France, LNCS 5797. pp.64-78.

P. Drabick, G. Scatena (2010) *An Application of Model Checking to Epidemiology*. In: Applications of Membrane computing, Concurrency and Agent-based modelling in POPulation biology, AMCA-POP 2010, Jena, Germany. pp. 90-97.

R. Barbuti, F. Levi, P. Milazzo, G. Scatena (2010) *Maximally Parallel Probabilistic Semantics for Multiset Rewriting*. In: CS&P, Informatik-Bericht of Humboldt-Universitat zu Berlin , Berlin, Genrmany. pp.25-36.

Abstract

This Thesis concerns the development of probabilistic semantics tailored to model the dynamic behavior of biological systems in order to formally analyze them. More specifically, it attempts to overcome problems, related to uncertainty and to the state space explosion, inherent to models describing biological systems.

Recently, many formalisms originated from Computer Science have been successfully applied to describe biological systems. Many of these formalisms include probabilistic aspects, and techniques like *stochastic simulation* and *probabilistic model checking* have been proposed to study biological systems properties. However, the practical application of formal analysis tools in this context is still limited.

The size of state space associated with models is often prohibitively large. Moreover, the knowledge of biological processes is often incomplete, resulting in models with uncertain parameters. For these reasons the application of available Computer Science tools is often difficult. In addition, usual tools deal with models in which concurrency is described by interleaving semantics. However, interleaving is not suitable for modelling certain classes of biological systems.

To overcome these problems, in this Thesis, we propose to apply abstraction techniques to probabilistic semantics of biological systems models. The application of such techniques presents several advantages. On one hand, these techniques can help in reducing the state space associated to models. On the other hand, they can help in handling models with uncertainty.

About the management of uncertainty in models, we consider the uncertainty in stochastic parameters. Often, having incomplete knowledge of the kinetics of a system, we are not able to choose among models differing only for parameters. Hence, we define a framework to study models with parameters expressed as

intervals, obtaining results that hold for all models with parameters included in the specified intervals. In more detail, probabilistic model checking can be performed on biochemical reactions systems models when kinetic rates, expressing the propensity of the interaction events, are not expressed precisely as point values, but as intervals. We define an effective method to derive an abstract semantics for such models and to obtain conservative bounds on probability of reachability properties. The abstract semantics, given in terms of *Interval Markov Chain* (IMC), is derived from a *Labeled Transition System* (LTS) semantics. It is proven to be correct, by means of abstract interpretation techniques, with respect to the *Discrete Time Markov Chain* (DTMC) semantics, usually associated with these systems. As example of application, we study how the behavior of a model of tumor cell growth changes when different intervals of kinetic rates are used.

Subsequently, we face the problems related to the use of interleaving semantics and to the size of state space size of models. In particular, we define the probabilistic semantics for systems evolving in a maximally parallel way: in each step of the system evolution, as many interactions happen synchronously. Using the proposed semantics we are able to reproduce *in vivo* experiments outcomes on a model of *C. elegans* vulval development.

Moreover, we develop an abstraction framework for the proposed maximally parallel probabilistic semantics. The framework is based on a form of predicate abstraction computing an abstract semantics in terms of IMC. Since the abstraction is parametric on a set of predicates, the abstract probabilistic model can be refined until a right compromise between dimension and precision is reached. We prove that conservative bounds on probabilities of reachability properties of systems evolving in a maximally parallel way can be computed on the abstract semantics. We show the efficacy of the approach, in terms of state and transition number reduction, by analysis probabilistic reachability on a simple model of seasonal animal reproduction.

Chapter 1

Introduction

Nowadays, the study of biological systems is evolving from a *reductionist* approach toward a *systemic* approach. Molecular Biology and other "omics" sciences produce a huge amount of data concerning the behavior of single constituents or single aspects of living organisms. Nevertheless, a detailed knowledge of biological systems components is not sufficient to gain a deep comprehension of how such components interact together at the system level, generating the set of complex behavior we observe in nature. This is the main motivation of the rising of *Systems Biology* [Kit02], a science integrating experimental activity and mathematical modelling to study the organizational principles and the dynamic behavior of biological systems. Mathematical and computational techniques are central in this approach to Biology, as they provide the capability of formally describing living systems and studying their properties.

The base of this approach is to view living systems components as computing entities and biological systems as concurrent systems: objects able to change their state as result of biochemical interactions [RS02].

Successful attempts have been made in formal modelling of biological systems. Formalisms originated in Computer Science to describe concurrent interactive systems, such as stochastic π–calculus [PRSS01] (a stochastic extension of π–calculus [Mil99]) or (stochastic) Petri Nets [Pet62, Rei85, ST05, SKSW04, BC89], have been used. Also biologically inspired formalisms such as κ–calculus [DL04], BioAmbients [RPS$^+$04], Brane Calculi [Car05], P Systems [Pău02], Stochastic Calculus of Looping Sequences [BCMS$^+$08, Mil07] have

been proposed. As far as the latter class of languages is concerned, they are based on different theories – namely process algebras theory, concurrent systems theory, rewriting systems theory – but they offer primitives to easily express biological features, such as arbitrary nested membranes, complex biological components and interactions.

The formalization of the knowledge about a biological system by using one of the previous formalisms, instead of using one of ambiguous notations commonly used in Biology, gives the opportunity to realize several analyses. In this way biologists can perform verification of models and simulate them, obtaining information and predictions on the possible results of *"in vitro"*/*"in vivo"* experiments. These analyses can be classified as *qualitative*, in the case they consider only possible interactions and reachable configurations, abstracting from probability and time aspects, or as *quantitative*, otherwise.

Among the qualitative analyses, *model checking* [CGL94] is one of most popular approaches. This technique allows properties to be checked by exploiting the Kripke structure defined by a formal semantics and describing the dynamic behavior of a system. The properties of interest, expressed as formulas of appropriate logics (as for instance *Computation Tree Logic* (CTL) [Eme90]), are verified by exhaustively exploring all the possible reachable configurations of the system (i.e. the associated state space). This approach is useful both to validate models against known properties, and to test certain hypotheses on validated models.

Among quantitative analyses, techniques of *simulation* or *probabilistic model checking* are commonly used. *Simulation* techniques trace possible time evolutions of system models, offering to biologist a framework to perform *"in silico"* experiments.

Probabilistic model checking consists in performing model checking considering events probabilities [Kwi03]. The model checking techniques are extended both to probabilistic systems and stochastic systems, whose semantics is modelled either as *Discrete Time Markov Chains* (DTMCs) or as *Continuous Time Markov Chains* (CTMCs) or as *Markov Decision Processes* (MDPs). Indeed, for certain biological properties, like the ones associated with very unlikely events, the use of stochastic simulation only is not enough to deeply understand the system dynamics. In fact, sporadic events require a huge number of simulations to be observed, and any number of simulations cannot give any formal guarantees on event probabilities. Thus, studying such systems in a quantitative way requires to exhaustively evaluate the probability of every possible system behavior.

1.1 Motivations

In the last years many formalisms with probabilistic semantics have been successfully applied to describe biological systems and stochastic simulation have been proposed to study properties of such systems, obtaining results that are more precise than those obtained by deterministic models.

Despite of the great amount of work done in biological systems research, formal modelling tools are not very diffused in biology research current practice, and their application is limited to certain type of small and well known models. Within the reasons for this limitations, we focus our attention on the following aspects.

First, the semantics traditionally used in Computer Science systems to model concurrent systems are typically interleaving, i.e. each component of a system can evolve asynchronous. Instead, in the context of biological systems modelling, there exist scenarios for which the standard interleaving semantics seems to be not adequate. Indeed, asynchrony semantics may not mimic real-life biological behavior properly (e.g. cellular or animal population dynamics) as it allows a part of the systems (e.g. a single cell or individual) to evolve indefinitely while other system components may stall. Hence, for certain kind of synchronized behavior the interleaving semantics may be not the best choice. For these modelling scenarios a *parallel* (i.e. on a single transitions many components can evolve) and *maximal* (i.e. no components can remain blocked) *semantics* is required.

Another cause of the limited application of formal tools in biological systems modelling is that, since biological systems are composed by a huge number of elements, the state space of such systems is often prohibitively large and both the approaches based on model checking and simulation suffer from complexity issues. Model checking tools, such as PRISM [PRI], suffer from *state explosion problems* when applied to biochemical model: as the number of elements in the system increases, the range of possible behaviors grows exponentially. For instance Gilbert et al. [GHL07] experienced this problem just when systems consisting of few tens of molecules are considered. The same problem arises in the case of stochastic simulation due to the slowness of the algorithm moving on the same (huge) state space.

Finally, formal frameworks need to be extended in order to deal with uncertainty in models. Indeed, classical formal tools require a complete description of the system under study and this requirement is in contrast with the typical knowledge of biological processes. In Biology the knowledge

is often extracted from wet lab experiments that give semi–quantitative and incomplete information about the system in exam, resulting, as discussed in [IM07], in models that are often incomplete and containing uncertainty. In fact, it is often impossible to assign precise probability to each interaction of an intricate biological pathway; even if probabilities are given, they are often estimated through statistical experiments, which only provide bounds on the actual ones. Thus, an important challenge is to be able to model and analyze systems having incomplete knowledge of them. However, since uncertainty differs qualitatively from the randomness of biological systems, and arises from different causes, probabilistic methods should not be expected to model also uncertainty [MHS90].

Having in mind these problems, we focus our attention on Multiset Rewriting (MSR) as modelling language; such a language is, indeed, simple but expressive enough to describe a wide range of scenarios. For such a formalism we discuss the definition of a maximally parallel probabilistic semantics and the use of abstraction both to manage uncertainty in models, and to reduce the size associated state-space. To this aim we investigate the use of *Interval Markov Chains* (IMCs) to abstract probabilistic semantics (i.e. DTMCs).

1.2 Related Works

MSR has been used as modelling formalism for describing, for instance, chemical reactions and network protocols, using interleaving semantics, both in a qualitative and quantitative fashion [BCL$^+$03, CS06, CDL$^+$99]. The formalism has the same expressing power of Petri Nets [Pet62], also used in this context [HGD08].

The abstraction of probabilistic semantics has been widely studied over the last few years, but few approaches are aimed in supporting uncertain models. For instance, infinite state abstraction [HHWZ10], predicate abstraction [WZH07, KKNP08], symmetry reduction [DMP07], counter example driven abstraction refinement [HWZ08] has been recently proposed to address the traditional state explosion problem . The approaches of [FLW06, DJJL01, SVA, Hut05, Šku06, Šku09] present abstractions of probabilistic semantics, using MDP or IMC. In particular, the abstract semantics is derived from the concrete one (a DTMC), by partitioning the concrete state space and by calculating the abstract probability distributions directly from the concrete ones. The approaches presented in [CGL09, GL09] compute an abstract semantics to validate probabilistic temporal properties of biological systems. The analysis

computes an IMC by approximating the multiplicity of individuals, present in a state, using intervals of integers. Namely these abstractions are designed for approximating the multiplicity of individuals, present in a state, using intervals of integers. The proposal of [DFF+08, DFFK08] applies abstract interpretation techniques, in the context of formal studies of biological systems, in order to compute efficiently a superset of reachable complexes, and to generates smaller systems of differential equations from the concrete one. Finally, [Mon05, DPW00] investigate the application of abstract interpretation into the context of standard concurrent probabilistic programming languages.

The need of a maximally parallel semantics to describe certain kind of biological systems has been advocated by many (as, for instance [FHMP07, FHMP08]). The maximally parallel semantics proposed, in the qualitative case, for instance for Petri Nets [Bur80] (when firing is under Maximal Strategy), has received great attention in the context of P Systems [Pău02]. P Systems are a biologically inspired formalism, based on the maximally parallel rewriting of atomic objects spread across different compartments.

Apart from the qualitative, non-deterministic, semantics originally proposed, for P Systems, different probabilistic and stochastic semantics have been proposed [PBMZ06, CC07, AC03, Mad03, Obt02, OP03]. Nevertheless, each approach faces the problem under particular assumptions and, hence, in the probabilistic setting, an affirmed general interpretation of maximally parallel semantics still lacks. The Dynamical P Systems, by Pescini et al. [PBMZ06], are presented with a stochastic simulation algorithm, but lack of a formal probabilistic semantics. The definition of probabilistic transitions proposed by Ciobanu and Cormacel [CC07] uses a hyper-geometric distribution. The approaches proposed by Aderlean and Cavaliere [AC03] and by Madhu [Mad03] give a probabilistic semantics for P Systems modifying the basic framework with additional rule probabilities. Obtulowicz [Obt02] proposes a stochastic and a randomized semantics, while Obtulowicz and Paun [OP03] discuss in general terms how to add probability to P Systems semantics.

While the abstraction of probabilistic semantics has been widely studied over the last few years, to our knowledge there are not any work dealing with abstraction of a maximally parallel probabilistic semantics for MSR.

1.3 Contributions

The contribution of this thesis is twofold: a part of the thesis is devoted to handle uncertainty in stochastic models, while the other part defines a probabilistic maximally parallel semantics and describes a state space reduction abstraction technique.

As modelling language we choose MSR as it is simple and, at the same time, expressive enough to model a wide range of biological systems.

Concerning the management of uncertainty in models, we consider the uncertainty in stochastic parameters. Often, having incomplete knowledge of the kinetics of a system, we are not able to choose among models differing only for parameters. Hence, we define a framework to study models where kinetic parameters are expressed as intervals, obtaining results that holds for all models with parameters included in the specified intervals. In more detail, probabilistic model checking can be performed on biochemical reactions systems models when kinetic rates, expressing the propensity of the interaction events, are not expressed precisely as point values, but as intervals. We define an effective method to derive an abstract semantics for such models and to obtain bounds on probability of reachability properties that are, not only conservative but, exactly the most precise values which are correct. Indeed, they corresponds to the minimum and the maximum of the probabilistic reachability corresponding to each concrete system represented by an abstract one.

Subsequently, we face the problems related to the use of interleaving semantics and to the size of the state space size of models. In particular, we define the probabilistic semantics for systems evolving in a maximally parallel way: in each step of the system evolution, as many interactions happen synchronously. The choice of a maximally parallel semantics is tailored to study systems with a synchronous behavior. Indeed, interleaving may not mimic real-life biological behavior properly, especially cellular population behavior, as it allows a part of the systems (e.g. a single cell) to evolve indefinitely while other system components may stall. Such kind of semantics is not adequate also for modelling phase-wise populations dynamics. Indeed, in such systems populations evolve in phases, often related to environmental conditions (e.g. seasonality). Within a phase, each individual makes a choice about the action to be taken among those possible. The set of choices made by individuals identifies a single step of the whole population evolution. Moreover, in such cases the use of the standard interleaving semantics build bigger and more imprecise transitions systems than the one computed considering maximally

parallelism: big, as they containing additional configurations and transitions not actually realizable, and imprecise, as less close to real system behavior. For these reasons we define a probabilistic semantics tailored to describe the behavior of systems evolving in a maximally parallel way, where transitions have an associated probability depending on the state and on the propensity of maximally parallel rewriting events.

Using the proposed semantics we are able to reproduce *in vivo* experiments outcomes on a model of *C. elegans* vulval development.

Subsequently, for the proposed semantics we develop an abstraction framework. The framework is based on a form of predicate abstraction and is able to drastically reduce the number of state and transitions of a system semantics, and to finitely represents the behavior of possibly infinite maximally parallel rewriting systems. We prove that conservative bounds on probabilities of reachability properties of systems evolving in a maximally parallel way can be computed on the abstract semantics. Being the abstraction parametric on a set of predicates, we are able to refine the abstract probabilistic model until a right compromise between dimension and precision is reached. We show the efficacy of the approach, in terms of state and transition number reduction, on a simple model of seasonal animal reproduction.

All proposed semantics are computed by the construction of appropriate Labeled Transition Systems. Subsequently, from such structures are derived the corresponding probabilistic structures, given in terms of DTMC or IMC in the concrete or abstract case respectively. The proposed abstract semantics are proved, by means of abstract interpretation techniques and through the definition of suitable approximation orders, to offer sound approximations.

1.4 Structure of the thesis

The thesis is structured as follows.

- In Chapter 2, we recall some background notions of Biology and Computer Science that will be assumed in the rest of the thesis. In particular, we review some approaches in Biology systems modelling and we present some notion of biochemical reactions kinetics. We recall some models to describe probabilistic dynamics and how to perform their analysis through model checking. Finally, we present the concepts of abstraction, abstract interpretation and of predicate abstraction.

- In Chapter 3, we present an abstract framework for modelling and performing discrete-time probabilistic model checking of biochemical systems of reactions with uncertain kinetic rates (expressed by intervals). We discuss the soundness of the approach and we shown its efficacy in the study of the different outcomes exhibited by a model of tumor cell growth dynamic, when different intervals of reaction rates are considered.

- In Chapter 4, we present a maximally parallel probabilistic semantics for MSR. We describe by a model the vulval development process of *C. Elegans*. Performing probabilistic simulations of such a model, we are able to mime the in vivo observed behavior.

- In Chapter 5, we define an abstract maximally semantics for MSR based on interval-valued predicates evaluation, and we prove the soundness with respect to probabilistic reachability. Using such a framework we are able to obtain an approximated probabilistic semantics with a reduced number of states and transitions, and to get bounds on probability of reachability properties, as we show on a simple example of seasonally animal reproduction model.

Finally, we conclude and discuss further work in Chapter 6.

1.5 Published Material

Part of the material presented in this thesis has appeared in some publications or has been submitted for publication, in particular:

- The definitions of the abstract semantics for MSR to perform reachability analysis on models of biochemical reactions with uncertain kinetic rates presented in Chapter 3 have appeared, in a preliminary form, in [BLMS09] and submitted to *Theoretical Computer Science*.

- The definition of the probabilistic maximally parallel semantics for MSR presented in Chapter 4 have appeared in [BLMS10] and submitted to *Fundamenta Informaticae*.

All the published material is presented in this thesis in revised and extended form.

Chapter 2

Background

This Chapter presents the basic concept on which biological systems modelling is constituted, that will be assumed in the rest of the thesis. In particular:

- Section 2.1 gives an overview of the approaches, the formalisms and the tools used in *Systems Biology*;
- Section 2.2 gives the an introduction to *biochemical systems dynamics* as it is used as reference for biochemical systems interaction;
- Section 2.3 introduces the main notions of *probability* and of the *formal models* traditionally used to describe the semantics of *probabilistic systems*. Moreover, it introduces standard techniques for studying systems dynamic behaviors by *model checking*.
- Section 2.4 introduces some notion of *abstraction* and *abstract interpretation*.

2.1 Introduction to Biological Systems Modelling

A detailed knowledge of biological systems components is not sufficient to gain a deep comprehension of how such components interact together at the system level, generating the set of complex behavior we observe in nature. This is the main motivation of the rising of *Systems Biology* [Kit02], a science integrating

experimental activity and mathematical modelling to study the organizational principles and the dynamic behavior of biological systems.

Mathematical and computational techniques are central in this approach to Biology, as they provide the capability of formally describing living systems and studying their properties.

Successful attempts have been made in formal modelling of biological systems. The base of this approach is to view living systems components as computing entities and biological systems as concurrent systems: objects able to change their state as result of biochemical interactions [RS02].

Formalisms originated in Computer Science to describe generic systems of concurrent interacting processes, such as stochastic π–calculus [PRSS01] (a stochastic extension of π–calculus [Mil99]) or (stochastic) Petri Nets [Pet62, Rei85, ST05, SKSW04, BC89], have been used. Also biologically inspired formalisms such as κ–calculus [DL04], BioAmbients [RPS+04], Brane Calculi [Car05], P Systems [Pău02], Stochastic Calculus of Looping Sequences [BCMS+08, Mil07] have been proposed. As regards of the latter class of languages, they are based on different theories – namely process algebras theory, concurrent systems theory, rewriting systems theory – but they offer primitives to easily express biological features, such as arbitrary nested membranes, complex biological components and interactions.

The formalization of the knowledge about a biological system by using one of the previous formalisms, instead of using one of ambiguous notations commonly used in Biology, gives the opportunity to realize several analyses. In this way biologists can perform verification of models and simulate them, obtaining information and predictions on the possible results of *"in vitro"*/*"in vivo"* experiments. These analyses can be classified as *qualitative*, in the case they consider only possible interactions and reachable configurations, abstracting from probability and time aspects, or as *quantitative*, otherwise.

Among the qualitative analyses, *model checking* [CGL94] is one of most popular approaches. The technique allows properties to be checked by exploiting the Kripke structure (see Section 2.3.2) defined by a formal semantics and describing the dynamic behavior of a system (see Section 2.3.3). The properties of interest, expressed as formulas of appropriate logics (as for instance *Computation Tree Logic* (CTL) [Eme90], described in Section 2.3.3), are verified by exhaustively exploring all the possible reachable configurations of the system (the state space). This approach is useful both to validate models against known properties, and to test certain hypotheses on validated models.

For instance, in the context of biochemical systems example of properties

that can be formalized in CTL, and verified against models, are the following:

- Given an initial configuration s, is there a pathway for synthesizing a molecule Y ?
- Which are the initial configurations for which a molecule Y can be produced ?
- Can the system reach a configuration s while passing by another configuration s' ?
- Can the system reach a configuration s without violating certain constraints c ?
- Is a certain (partially described) system configuration stable ?
- Which stable configurations are reachable from the initial configuration s ?
- Can / must the system reach a stable state starting from the initial configuration s ?

Another traditional approach for qualitative analysis is based on testing the *behavioral equivalence* of different models. For example, it is possible to model a pathway and test if it has the same observable behavior of (if it is *bisimilar* with) the same model specified at an higher level of abstraction, or in which certain perturbing factors (i.e drugs or viruses) are added [BMSMT08, APP+04]

As regards quantitative analysis, techniques of *probabilistic model checking* or *simulation* are commonly used.

Simulation techniques trace possible time evolutions of system models, offering to the biologist a framework to perform *"in silico"* experiments. These virtual experiments have advantages with respect to real experiments in terms of feasibility and cost, allowing the testing hypotheses and guide *"in vitro"*/*"in vivo"* experiments. For many formalisms a stochastic semantics is defined and specific software simulators have been developed (SPiM [SPI] for the Stochastic π–calculus, CytoSim and PSym [PSY] for P Systems, BAM for BioAmbients [MPV], CLSm [CLS, Sca07] for Stochastic Calculus of Looping Sequences). These simulators permit to get some traces of the time–evolution of the modelled systems according to the *Stochastic Simulation Algorithm* (SSA) [Gil77] (see Section 2.2).

In the case of probabilistic model checking, we perform model checking considering events probability [Kwi03]. Traditional model checking techniques are extended both to probabilistic and stochastic systems, whose semantics is modelled either as *Discrete Time Markov Chains* (DTMCs) or as *Continuous Time Markov Chains* (CTMCs) or as *Markov Decision Processes* (MDPs) (see Section 2.3.2). Indeed, certain biological properties, such as the ones associated with very unlikely events, cannot be observed using stochastic simulation. In fact, sporadic events require a huge number of simulations to be observed, and any number of simulations cannot give any formal guarantees on event probabilities. Thus, studying such a properties requires to exhaustively evaluate the probability of possible evolutions of the system by model checking techniques. For example, by using logics as *Probabilistic Temporal Logic* (PCTL) (see Section 2.3.3), the following quantitative properties can be checked:

- Which is the probability to reach configurations in which the concentration of molecule X exceeds c (by avoiding that concentration of molecule Y exceeds d) ?
- Which is the probability that the concentration of a certain molecule always stays between x and y ?

Probabilistic model checking has been applied to validate a model with respect to temporal specification, to complete it, and to search for kinetic parameter value in models expressed by Biochemical Abstract Machine [FS08a]. Also oscillations can be verified by probabilistic model checking [BMM08]. Moreover, queries regarding timed properties (i.e. the property is satisfied within a time limit or a time interval) can be verified with time–aware probabilistic model checking, verifying CTMCs against properties expressed in logics such as *Continuous Stochastic Logic* (CSL) [ASSB96].

A reference software for probabilistic model checking is PRISM [PRI]: it supports models as DTMCs, CTMCs and MDPs, temporal logics as PCTL, CSL and incorporates state-of-the-art data structures and algorithms.

Current Limitations Unfortunately, despite of the great amount of work done in biological systems research, formal modelling tools are not very spread in biology research and their application is limited to small well known models. Two reasons for this limitations are the following.

Since biological systems are composed by an huge number of elements, the state space of such systems is often very large (and even infinite) so that both

the approaches based on model checking and simulation suffer from complexity issues. Model checking tools, such as PRISM [PRI], suffer from *state explosion problems* when applied to biochemical models: as the number of elements in the system increases, the range of possible behaviors grows exponentially. For instance Gilbert et al. [GHL07] experienced this problem and are able to check only systems with less than ten molecules. The same limitations arises in the case of stochastic simulation due to the slowness of the algorithm which also explores the same (huge) state space. In fact, more are the events enabled, smaller is the time consumed by each simulation step, making the computation slow.

Another limitation of current tools is related to the presence of uncertainty in the knowledge of studied systems. Indeed, classical formal tools require a complete description of the system under study and this requirement is in contrast with the typical description of biological processes. In biology the knowledge is often extracted from wet lab experiments that give semi–quantitative and incomplete information about the system in exam. An example of such description is

> *"The concentration of the protein peaks within 2 and 5 minutes and then falls to less than 50% of the peak value within about 60 minutes".*

As discussed in [IM07], biological models are often incomplete. In fact, it is often impossible to assign precise probability to each interaction of an intricate biological pathway; even if probabilities are given, they are often estimated through statistical experiments, which only provide bounds on the actual ones. Thus, an important challenge is to be able to model incomplete systems. However, since uncertainty differs qualitatively from the randomness of biological systems, and arises from different causes, probabilistic methods should not be expected to model also uncertainty [MHS90].

Finally, as discussed in [FS08], the need of developing an abstraction framework dealing with uncertainty in models comes from the fact that models of biological systems are built with two different perspectives. The first is a perspective of knowledge representation: here "the more concrete the better" as models aim at gathering in a consistent way current knowledge on a particular system, representing the interactions with the maximum detail. The second perspective for building models is to make predictions and to answer to particular questions about a system. In this perspective "the more abstract the better" as models for making prediction should get rid of useless details and

should represent the minimum information that is sufficient for answering the considered question. In this perspective the aim is not to model a single precise system setting (i.e. a single "experiment"), but to describe a range of system setting, expressing parameters that may vary through uncertainty. These two different modelling perspectives require not only to develop models but also to formalize the relationship between models at different levels of abstraction.

2.2 Notions of Biochemical Reactions Kinetics

Biological systems are constituted by cells, that are regulated by coupled chemical reactions at the molecular level. Thus the specification of chemical reactions is essential in all modelling approaches.

In the description of systems of biological reactions the fundamental rules are given by stoichiometric equations, defining which molecular species may react in order to result in a certain product, and how many molecules are involved in reaction.

We consider $n \in \mathbb{N}$ molecular species $\{S_1, S_2, \ldots, S_n\}$ and $m \in \mathbb{N}$ reaction types $\{R_1, R_2, \ldots, R_m\}$. Each reaction $R_i, 1 \leq i \leq m$ is usually represented by a *reaction equation* denoted as

$$l_1^i S_1 + l_2^i S_2 + \ldots + l_n^i S_n \xrightarrow{k_i} r_1^i S_1 + r_2^i S_2 + \ldots + r_n^i S_n.$$

The stoichiometric coefficients $l_1^i, l_2^i, \ldots, l_n^i \in \mathbb{N}$ describe, for each species, the number of molecules which are consumed by a reaction of type R_i. Similarly, the stoichiometric coefficients $r_1^i, r_2^i, \ldots, r_n^i \in \mathbb{N}$ describe how many molecules of each species are produced by R_i . The reaction rate constants $k_i \in \mathbb{R}^{\geq 0}$ are related to the kinetic model adopted; they represent its basic expected frequency and determine the "speed" of R_i, as explained below. Note that the population of species S_j is unaffected by R_i if $l_j^i - r_j^i = 0$. The species for which $l_j > 0$ are called *reactants*, the species for which $r_j > 0$ are called *products* of the reaction. The previous equation states that combining an appropriate number of reactants we can obtain the products. The use of the symbol $\rightleftharpoons$ denotes that the reaction is *reversible* (i.e. it can occur in both directions). Irreversible reactions are denoted by the single arrow $\rightarrow$.

Quantitative probability and timing aspects are specified by reaction rates assigned to each reaction. The most popular law for computing rates is the *law of mass action*: for a reaction in a homogeneous medium, the reaction rate will be proportional to the concentrations of the individual involved reactants. Other

kinetic law, as for instance *Hill kinetic* [Hil10] or *Michaelis–Menten kinetics* [MM13], can also be used.

Models of biochemical reactions may be state–continuous or state–discrete and their dynamical behavior may be deterministic or stochastic. In any case, it is assumed that the system is well stirred[1] and thermally equilibrated. This means that a well stirred mixture of molecules inside some fixed volume interact at constant temperature.

Deterministic Approach

The deterministic approach to biochemical reaction kinetics modelling is based on the generalized *law of mass action*. The system state at any time is given by the concentrations (measured in mol per liter) of each molecular species. Expressing the system dynamics in terms of deterministic rate equations yields a system of *ordinary differential equations* (ODEs) for the concentrations.

In more detail, in the differential semantics of reaction models a set of reaction rules $\{R_i = (l_i, r_i, k_i) \forall i = 1, \ldots, n\}$ over molecular concentration variables $\{x_1, \ldots, x_m\}$ is interpreted by the following system of ODE:

$$\delta x_k / \delta t = \sum_{i=1}^{n} r_i(x_k) * k_i - \sum_{j=1}^{n} l_j(x_k) * k_j.$$

This approach assumes continuous, deterministic changes in concentrations of molecular species and can be suitable for reaction networks involving large populations. Thanks to its wide range of mathematical tools, this approach is the most commonly used in mathematical biology [Seg84]. The major drawback of this approach is that it neither properly models the discreteness of molecular quantities nor the inherent randomness in chemical reactions. In particular, for gene expression and signal transduction processes it has been extensively demonstrated that stochastic noise plays a major role and should be taken into account. Many examples and studies elucidate the stochastic nature of biological systems such that stochastic models are well established in systems biology [Wil06, TSB04, SES02, Pau04, MA99].

The study of the relationship between the differential and the stochastic semantics dates back to the seminal work of Boltzmann in the XIXth century. In this setting, the differential semantics is obtained from the stochastic semantics

[1] Meaning that the mixture is *spatially homogeneous*: such that the concentration or the number of molecules does not depend on positions in space.

by limit operations where the number of molecules tends to the infinity and the time steps tend to zero, under several assumptions such as perfect diffusion.

Stochastic Approach

In the stochastic approach, that we focus on, the system state at any time is given by the number of molecules, for each species, and the system is modelled by a *Continuous Time Markov Chain* (CTMC) (see Section 2.3.2). The system dynamics are described by a system of *first–order differential equations* (ODEs) called the *chemical master equation* (CME).

In more detail, the stochastic process that represents the temporal evolution of the species populations is given by a family $(X(t))_{t\geq 0}$ of random vectors

$$X(t) = (X_1(t), X_2(t), \ldots, X_n(t))$$

taking values in a discrete set $\{\mathcal{X} \subset \mathbb{N}^n\}$. The random variable $X_i(t)$, $1 \leq i \leq n$, describes the number of molecules of species S_i at time instant t. We fix the initial conditions of the process by taking that $P(X(0) = x_0) = 1$ for an initial population vector $x_0 \in \mathcal{X}$.

The *transient state probability* that, at time $t \geq 0$, the system is in state $x = (x_1, x_2, \ldots, x_n)$, given $X(0) = x_0$, is denoted by

$$p^t(x) = P(X(t) = x \,|\, X(0) = x_0)\,.$$

Here $P(E)$ stands for the *probability of the event E* (i.e. the value of a *probability distribution* over possible events, see Section 2.3.1), and $P(E_1 \,|\, E_2)$ denotes the probability of event E_1 when it is known that event E_2 happened (this is called *conditional probability*).

State changes are triggered by chemical reactions. For an infinitesimal time interval $[t, t + \delta t)$,

$$P(R_i \text{ occurs in } [t, t + \delta t) \,|\, X(t) = x) = \alpha_i(x)\delta t$$

where $\alpha_i(x) : \mathcal{X} \mapsto \mathbb{R}_{\geq 0}$ is called *propensity function* of R_i. This probability is proportional to the number of distinct combination of R_i's reactants[2]. Hence, $\alpha_i(x)$ is computed as

$$\alpha_i(x) = k_i \prod_{j=1}^{n} \binom{x_j}{l^i_j}.$$

[2]This interpretation is based on the *law of mass action* kinetics. Other possible formulation can be based on other kinetic laws as for instance *Hill kinetic* [Hil10] or *Michaelis–Menten kinetics* [MM13].

The probability $P(R_i \text{ occurs in } [t, t+\delta t) \,|\, X(t) = x)$ only depends on the length of the time interval which means that the propensity functions are time-independent. Besides, the next time of state in the system evolution only depends on the current state, and neither on the specific time nor on the history of reactions that led to the current state. Hence, the system is modelled as a CTMC $(X(t))_t \geq 0$ with n-dimensional state space $\mathcal{X} \subseteq \mathbb{N}^n$. This gives rise to a state-transition graph representation in which outgoing transitions of x are labeled by *transition rates* $\alpha_i(x)$. The successor state according to a transition from x triggered by a reaction of type R_i is the state $x + v_i$ where vector v_i, the *state change vector* of R_i, equals the i^{th} row of the *stoichiometric matrix* V, $M \times N$, is defined as follows: for R_i, $v_i = (v_{i1}, \ldots, v_{in})$ where $v_{ij} = h^i_j - l^i_j$. The system dynamics, in terms of the state probabilities time derivatives, are given by the *chemical master equation* (CME)

$$\frac{\delta p^t(x)}{\delta t} = \sum_{i=1}^{m} (\alpha_i(x - v_i) p^t(x - v_i) - \alpha_i(x) p^t(x)).$$

The CME is a set of first–order differential equations (ODEs) describing the time evolution of the probability of a system to occupy each one of a discrete set of states. As shown in [Gil77], this ODE is generally difficult to solve, in particular it can be solved analytically only for a very few simple systems and, furthermore, numerical solutions may be prohibitively difficult. These difficulties justified the definition of the *stochastic simulation algorithm* (SSA) by Gillespie [Gil77]. This algorithm addresses the following problem: given the system in state x at time t, computes the time instant at which the next reaction fires and chooses, accordingly to some policy, the reaction to fire. As regards the former problem, it is shown in [Gil77] how the putative time for the next reaction can be chosen by sampling an *exponentially distributed random variable* with mean $\alpha_0(x) = \sum_{j=1}^{m} \alpha_j(x)$. The sampling of such variable can be obtained by inverse Monte Carlo algorithm for generating exponentially distributed values. Similarly, the reaction to fire is chosen accordingly to the following inequalities, $\sum_{i=1}^{j-1} \alpha_i(x) < r_2 \alpha_0(x) \leq \sum_{i=1}^{j} \alpha_i(x)$, where r_2 is a random real number uniformly distributed in $[0, 1]$. For a proof of correctness of these choices see [Gil77].

Gillespie Stochastic Simulation Algorithm (SSA).

1. Initialize the time $t = t_0$ and the system state $x = x_0$.

2. With the system in state x at time t, evaluate all the $\alpha_j(x)$ and their sum $\alpha_0(x) = \sum_{j=1}^{m} \alpha_j(x)$.

3. Given two random numbers r_1 and r_2 uniformly distributed in $[0; 1]$, generate values for τ and j accordingly to

$$\tau = \frac{1}{\alpha_0(x)} \ln(\frac{1}{r_1}) \qquad \sum_{i=1}^{j-1} \alpha_i(x) < r_2 \alpha_0(x) \leq \sum_{i=1}^{j} \alpha_i(x)$$

then update $x := x + v_j$ and $t = t + \tau$, go to step 2.

Notice that this algorithm is exact in the sense that produces one exact trajectory in the state space of the system. Furthermore, it is worth mentioning that many equivalent variants of the SSA exist; in particular they differ from the way in which they compute the putative time for next reaction and on the way in which they choose the reaction to fire. The variant we presented here is named *Direct Method* [Gil77]. Other algorithms for the stochastic simulation of biological systems can be found in [GB00, CLP04, Gil07, GW].

Stochastic simulation is in widespread use for analyzing stochastic models of biological networks. It can be applied to arbitrarily large models but it also has a couple of major drawbacks. Stochastically exact trajectory generation by Gillespie algorithm is computationally expensive and is exceedingly slow. Moreover stochastic simulations can only provide statistical estimates. In fact, rather than directly solving the CME, trajectories (sample paths) of the CTMC are generated, and, even with approximate methods for accelerated trajectory generation, a large number of trajectories is required in order to obtain reliable and meaningful results with acceptable statistical accuracy.

2.3 Probabilistic Semantics and Analysis

When we are interested in studying the dynamic behavior of a system in a formal way, the first step is to model it using a formal language and to describe its formal semantics.

Here, we introduce the formal models traditionally used to describe the semantics of probabilistic and stochastic systems; that is, systems where the behavior is not deterministic, but where actions are performed somehow in according to certain probabilities.

In Section 2.3.1 we introduce basic probability concepts, then in Sections 2.3.2 we introduce *Kripke Systems*, *Discrete* and *Continuous time Markov chains* and *Markov Decision Processes*.

We refer to [RKNP04] for a more detailed discussion.

Given a formal description of the dynamic behavior of a system in terms of a probabilistic semantics, system can be automatically analyzed using *simulation* and *model checking* techniques (see Section 2.3.3). In the case of simulation one is interested in sampling a set of trajectories in the systems state space. Conversely, model checking consists of exhaustively exploring state space looking for the satisfaction of certain properties of interest. In other words, the simulation approach can be considered equivalent to test systems behaviors by performing experiments, while the model checking approach can be considered similar to analyze all possible systems behaviors in a systematic way.

2.3.1 Notions of Probability

Probability Distributions

A *probability distribution* over reals is a function which assigns to every interval of the real numbers a probability $P(I)$, so that Kolmogorov axioms are satisfied, namely:

- for any interval I it holds $P(I) \geq 0$
- $P(\mathbb{R}) = 1$
- for any set of pairwise disjoint intervals $I_1, I_2, \ldots$ it holds $P(I_1 \cup I_2 \cup \ldots) = \sum P(I_i)$

A *probability pseudo–distribution* is a probability distribution for which the second axiom is relaxed. It is not required that $P(\mathbb{R}) = 1$.

Given a finite set of events S we denote with

$$Distr(S) = \{\rho \,|\, \rho : S \rightarrow [0,1] \text{ and } \sum_{e \in S} \rho(e) = 1\}$$

the set of *(discrete) probability distribution* over S, and with

$$PDistr(S) = \{\rho \,|\, \rho : S \rightarrow [0,1]\}$$

the set of *(discrete) probability pseudo–distribution* over S.

A *random variable* on a real domain is a variable whose value is randomly determined. Every random variable gives rise to a probability distribution, and this distribution contains most of the important information about the variable. If X is a random variable, the corresponding probability distribution assigns to

the interval $[a, b]$ the probability $P(a \leq X \leq b)$, i.e. the probability that the variable X will take a value in the interval $[a, b]$. The probability distribution of the variable X can be uniquely described by its *cumulative distribution function* $F(x)$, which is defined by

$$F(x) = P(X \leq x)$$

for any $x \in \mathbb{R}$.

A distribution is called *discrete* if its cumulative distribution function consists of a sequence of finite jumps, which means that it belongs to a discrete random variable X: a variable which can only attain values from a certain finite or countable set.

A distribution is called *continuous* if its cumulative distribution function is continuous.

Most of the continuous distribution functions can be expressed by a *probability density function*: a non-negative Lebesgue integrable function f defined on the real numbers such that

$$P(a \leq X \leq b) = \int_a^b f(x)\,dx$$

for all a and b.

The *support* of a distribution is the smallest closed set whose complement has probability zero.

An important continuous probability distribution function is the *exponential distribution*, which is often used to model the time between independent events that happen at a constant average rate. The distribution is supported on the interval $[0, \infty)$. The probability density function of an exponential distribution has the form

$$f(x, \lambda) = \begin{cases} \lambda e^{-\lambda x} & x \geq 0 \\ 0 & x < 0 \end{cases}$$

where $\lambda > 0$ is a parameter of the distribution, often called the rate parameter. Its cumulative distribution function, instead, is given by

$$F(x, \lambda) = \begin{cases} 1 - e^{-\lambda x} & x \geq 0 \\ 0 & x < 0 \end{cases}$$

The exponential distribution is used to model *Poisson processes*, situations where an object initially in state A can change to state B with constant probability per unit time λ. The time at which the state actually changes is described by an

exponential random variable with parameter λ. Therefore, the integral from 0 to T over f is the probability that the object is in state B at time T.

Given a set X, a *σ–algebra* (sigma–algebra) F is a non-empty collection of subsets of X (subset F of the power set of a set X) such that the following hold:

1. X is in F.
2. F is closed under complements: if A is in F, then so is the complement of A ($X \setminus A \in F$).
3. F is closed under countable unions: if A_n is a sequence of elements of F, then the union of the A_n is in F.

From these axioms, it follows that X and the empty set are in F, and that the σ–algebra is also closed under countable intersections (via De Morgan's laws). If S is any collection of subsets of X, then we can always find a sigma-algebra containing S, namely the power set of X. By taking the intersection of all σ–algebras containing S, we obtain the smallest such σ–algebra. We call the smallest σ–algebra containing S the sigma-algebra generated by S.

A *measure* on X is a function which assigns a real number to subsets of X; this can be thought of as making precise a notion of "size" or "volume" for sets.

Elements of the σ–algebra are called *measurable sets*. An ordered pair (X, F), where X is a set and F is a σ–algebra over X, is called a *measurable space*. A function between two measurable spaces is called measurable if the preimage of every measurable set is measurable. The collection of measurable spaces forms a category with the measurable functions as morphisms. Measures are defined as certain types of functions from a σ–algebra to $[0, \infty]$.

A *probability space* is a measure space such that the measure of the whole space is equal to 1. In other words: a probability space is a triple (X, F, P) consisting of a set X (called the *sample space*), a σ–algebra F of subsets of X (these subsets are called *events*), and a measure P on (X, F) such that $P(X) = 1$ (called the *probability measure*).

2.3.2 Kripke Structures, Markov Chains and Markov Decision Processes

Kripke Structure To describe the semantics of non-deterministic systems we use *Kripke Structure*, a.k.a. non-deterministic transition systems. It is basically a graph whose nodes represent the reachable states of the system and whose edges represent possible state transitions.

Definition 1 (Kripke Structure)**.** *A Kripke Structure is a tuple* (S, R, s_0)*, where:* S *is the set of states,* s_0 *is a starting state,* $R \subseteq S \times S$ *is the* transition relation*.*

A *path* π is a non-empty (finite or infinite) ordered succession of states $s', s'', \ldots$ of S. We denote the i^{th} state of the path π by $\pi[i]$, starting from 1, and the length of π by $|\pi|$, where $|\pi| = \infty$ if π is infinite. The set of paths over S is denoted by $Paths(S)$ and its subset of finite paths is denoted as $FPaths(S)$. For a finite path π we use π_{last} for the last state of the path. The *cylinder* corresponding to a path π is the set of all paths prefixed by π. Formally, for $\pi \in Paths(s)$, $C(\pi) = \{\pi\pi' \,|\, \pi' \in Paths(S)\}$ and $C(s)$ denotes the set of paths starting from the state s.

On Kripke structure is possible to verify qualitative temporal properties, expressed by CTL (see Section 2.3.3).

Discrete Time Markov Chain To describe the probabilistic semantics of a system we use *Discrete Time Markov Chain* (DTMC). DTMCs are similar to transition systems with the difference that non-deterministic choices among successor states are replaced by probabilistic ones. That is, the successor of a state s is chosen according to a probability distribution (see Figure 2.1.(a)). The probability distribution only depends on the current state s and not on the path fragment, leading to state s from the initial state. Accordingly, the system evolution does not depends on the history (i.e., the path fragment that has been executed so far), but only depend on the current state s. This is know as the *memoryless property*.

Definition 2 (Discrete Time Markov Chain)**.** *A DTMC is a tuple* (S, P, s_0)*, where:* S *is the set of states,* s_0 *is the starting state;* $P : S \times S \mapsto \mathbb{R}^{\geq 0}$ *is the* transition probability function*, satisfying* $\forall s \in S \sum_{s' \in S} P(s, s') = 1$ *(or equivalently* $P : S \mapsto Distr(S)$*).*

Here, $P(s, s')$ gives the (time–independent) probability to move from state s to state s'.

We say that a DTMC (S, P, s_0) is *finite* if S is finite. When a DTMC is finite its probabilistic transition function can be expressed by a $|S| \times |S|$ matrix with elements ≤ 1.

Markov chains, as in Definition 2, are called *discrete-time* as they are adequate only when the underlying time domain is discrete and each transition is assumed to take a single time unit. On DTMC it is possible to verify both

qualitative and (time-abstract) *quantitative* properties expressed in CTL and PCTL formulae (see Section 2.3.3).

On a DTMC to each path has an associated probability, defined as follows.

Definition 3 (Probability of Paths)**.** *Let* (S, s_0, P) *be a DTMC.*
Let $\Pi = \bigcup_{\pi \in FPaths(s)} C(\pi)$ *be the* set of all cylinders*,* $\mathcal{B}$ *be the smallest* σ–algebra *containing* Π*, and* $s \in S$ *a* state*. The tuple* $(Paths(S), \mathcal{B}, P_s)$ *is a* probability space*, where* P_s *is the unique measure satisfying, for all path* $s_0 \dots s_n$*,*

$$P_s(C(s_0 \dots s_n)) = \begin{cases} 1 & \text{if } s_0 = s \wedge n = 0 \\ P(s_0, s_1) \times \dots \times P(s_{n-1}, s_n) & \text{if } s_0 = s \wedge n > 0 \\ 0 & \text{otherwise.} \end{cases}$$

Continuous Time Markov Chain To describe the semantics of a stochastic system we use *Continuous Time Markov Chain* (CTMC). A DTMC is time–abstract, conversely, CTMCs are time–aware as they have an explicit reference to time in the form of exit rates which determine, together with the transition probabilities, the stochastic evolution of the system. Roughly speaking, a CTMC is a DTMC where each state has a residence time that is governed by negative exponential distributions [Ros83].

A CTMC corresponds to a family of random variables $\{X(t) \mid t \geq 0\}$, where $X(t)$ is an observation made at time instant t and t varies over non-negative reals. The state space, namely the set of all possible values taken by $X(t)$, is a discrete set. Moreover, a CTMC must satisfy the *Markov (memoryless) property*: for any integer $k \geq 0$, sequence of time instances $t_0 < t_1 < \dots < t_k$ and states $s_0, \dots, s_k$ it holds

$$P(X(t_k) = s_k \mid X(t_{k-1}) = s_{k-1}, \dots, X(t_1) = s_1) = P(X(t_k) = s_k \mid X(t_{k-1}) = s_{k-1}).$$

Intuitively, the memoryless property means that the probability of making a transition to a particular state at a particular time depends only on the current state, and not on the previous history of states passed through. The exponential distribution is the only continuous probability distribution which exhibits this memoryless property, hence it is the only one that can be used in the definition of CTMCs.

Formally, a CTMC is defined as follows.

Definition 4 (Continuous Time Markov Chain)**.** *A CTMC is a tuple* (S, s_0, R)*, where:* S *is the set of states;* $s_0 \in S$ *is the starting state;* $R : S \times S \mapsto \mathbb{R}^{\geq 0}$ *is the* transition rate function*.*

To a CTMC is usually associated an *exit rate function* $E : S \mapsto \mathbb{R}^{\geq 0}$ such that $\forall s \in S\ E(s) := \sum_{s' \in S} R(s, s')$. The exit rate $E(s)$ determines the random, exponentially distributed residence time of state s. That is, $(1 - e^{-E(s)t})$ is the probability to take a transition emanating from s within the next t time units. Note that self-loops are admitted. We also say that a transition in state s occurs with an average pace of $E(s)$. The time-dependent transition probability to move from s to s' within t time units is now given by $P(s, s', t) := R(s, s')(1 - e^{-E(s)t})$.

The system is assumed to pass from a configuration, modelled by a state s, to another one, modelled by a state s', by consuming an exponentially distributed quantity of time, in which the parameter of the exponential distribution is the rate $R(s, s')$. If the set of states of the CTMC is finite ($S = \{s_1, \ldots, s_n\}$), then the transition function R can be represented as a square matrix of size n in which the element at position (i, j) is equal to $R(s_i, s_j)$. On CTMC is possible to verify *Continuous Stochastic Logics* properties, a continuous-time variant of PCTL proposed by Aziz et al. [ASB95] and Baier et al. [BHHK03], (i.e. basically, PCTL properties extended with continuous time bounds).

The time–abstract probabilistic behavior of CTMC M is described by its *embedded* DTMC. The embedded DTMC of CTMC $M = (S, s_0, R)$ is simply given by $emb(M) = (S, s_0, P)$ with,

$$\forall s, s' \in S\ ,\ P(s, s') = \begin{cases} R(s, s')/E(s) & \text{if} E(s) \geq 0 \\ 1 & \text{if} E(s) = 0 \text{ and } s = s' \\ 0 & \text{otherwise.} \end{cases}$$

The probability to move from a state s to a state s', $P(s, s')$, is calculated normalizing the rate of the move $R(s, s')$ with respect to the exit rate of the state s, $E(s)$.

Markov Decision Process To model both probabilistic and *non-deterministic* behaviors we use *Markov Decision Processes* (MDP).

Definition 5 (Markov Decision Process)**.** *A MDP is a tuple* (S, A, P)*, where:* S *is the set of states;* A *is a non-empty finite alphabet of actions;* $P : S \times A \mapsto S \mapsto \mathbb{R}^{\geq 0}$ *is the* transition function*, satisfying* $\forall s \in S, \forall a \in A, \sum_{s' \in S} P(s, a)(s') = 1$ *(or equivalently* $P : S \times A \rightharpoonup Distr(S)$*).*

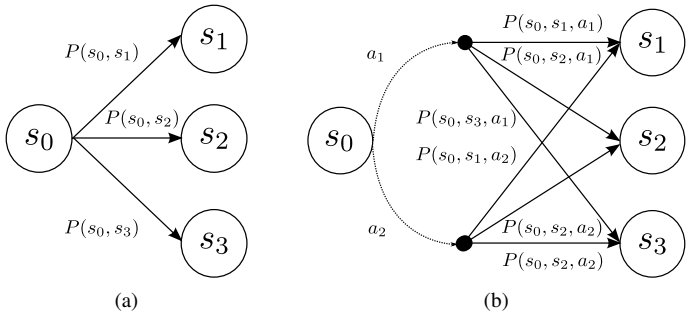


Figure 2.1: Examples of DTMC (a) and of MDP (b).

Notice that the function P associates to each state s and to each action a a distribution $Distr(S)$.

In a MDP each move from a state $s \in S$ is done performing firstly a *non-deterministic* choice of an action $a \in A$ and then doing a *probabilistic* choice of the next state according to the probability $P(s,a)$ given by the distribution $P(s,a)$ (see Figure 2.1).

In other words, to trace a path through an MDP, both the non-deterministic and probabilistic choices have to be resolved. Usually, it is assumed that the non-deterministic choices are made by an *scheduler* (also known as *adversary*).

On a MDP is possible to obtain lower and upper bounds on probabilistic temporal properties, or compute it precisely once a give scheduler is fixed. In fact, the behavior of an MDP under a given adversary is purely probabilistic.

2.3.3 Model Checking

Model checking is an automated technique which, given a finite-state model of a system and a formal property, systematically checks whether this property holds for that model, starting from a certain state [CE81]. Such a verification techniques explores all possible system states in a brute-force manner, and can discover subtle behaviors which cannot be observed by simulation.

Model checking has been successful applied to several ICT systems and their applications, both software and hardware, from network protocols to from spacecraft controllers, both for systems *verification* (i.e. “are we build the thing right ?”) and for systems *validation* (i.e. “are we build the right thing ?”) . We

refer to [BGC09] for a detailed analysis of model checking techniques history and bibliography.

While the earlier techniques were restricted to checking the absence of deadlock or livelocks, model checking allows for examination of broader classes of properties using modal logics.

Modal Logics

To make a rigorous verification possible, properties should be described in a precise and unambiguous manner. This is typically done using a property specification language. We focus in particular on *temporal logic* as property specification language, a form of modal logics. In terms of mathematical logic, one check that the system description is a model of a temporal logic formula. Temporal logic is basically an extension of traditional propositional logic with operators that refer to the behavior of the system over time

In the following a set AP of atomic propositions are used to formalize properties of states. Intuitively, atomic propositions express simple facts about the states of the system under consideration, while temporal properties are expressed by operators of certain logics, as for instance *Computation Tree Logic*.

CTL *Computation Tree Logic* (CTL), is a branching-time temporal logic based on propositional logic with a discrete notion of time, and only future modalities. CTL is an important branching temporal logic that is sufficiently expressive for the formulation of an important set of system properties. It was originally used by Clarke and Emerson [CE81] and (in a slightly different form) by Queille and Sifakis [QS82] for model checking.

CTL has a two-stage syntax where formulae in CTL are classified into *state and path formulae*. The former are assertions about the atomic propositions in the states and their branching structure, while path formulae express temporal properties of paths.

Syntax of CTL CTL *state formulae* over the set AP of atomic proposition are formed according to the following grammar:

$$\Phi ::= true \mid a \mid \Phi_1 \wedge \Phi_2 \mid \neg\Phi \mid \exists\varphi \mid \forall\varphi$$

where $a \in AP$ and φ is a path formula. CTL *path formulae* are formed according to the following grammar:

$$\varphi ::= \bigcirc\Phi \mid \Phi_1 U \Phi_2$$

where and Φ, Φ_1, and Φ_2 are state formulae.

CTL distinguishes between state formulae and path formulae. Intuitively, state formulae express a property of a state, while path formulae express a property of a path, i.e., an infinite sequence of states. The temporal operators $\bigcirc$ and U are path operators with the following meaning. Formula $\bigcirc\Phi$ holds for a path if Φ holds at the next state in the path, and $\Phi U \Psi$ holds for a path if there is some state along the path for which Ψ holds, and Φ holds in all states prior to that state. Path formulae can be turned into state formulae by prefixing them with either the path quantifier $\exists$ (pronounced for some path) or the path quantifier $\forall$ (pronounced for all paths). Note that the linear temporal operators $\bigcirc$ and U are required to be immediately preceded by $\exists$ or $\forall$ to obtain a legal state formula. Formula $\exists\Phi$ holds in a state if there exists some path satisfying Φ that starts in that state. Dually, $\forall\Phi$ holds in a state if all paths that start in that state satisfy Φ.

Satisfaction Relation for CTL CTL formulae are interpreted over the states and paths of a transition system TS. Formally, given a Kripke Structure TS, the semantics of CTL formulae is defined by two satisfaction relations (both denoted by $\models_{TS}$, or briefly $\models$): one for the state formulae and one for the path formulae. For the state formulae, $\models$ is a relation between the states in TS and state formulae. We write $s \models \Phi$ rather than $(s, \Phi) \in \models$. The intended interpretation is: $s| = \Phi$ if and only if state formula Φ holds in state s. For the path formulae, $\models$ is a relation between maximal path fragments in TS and path formulae. We write $\pi \models \Phi$ rather than $(\pi, \Phi) \in \models$. The intended interpretation is: $\pi \models \Phi$ if and only if path π satisfies path formula Φ.

Let $a \in AP$ be an atomic proposition, $TS = (S, R, s_0)$ be a Kripke Structure, state $s \in S$, Φ,Ψ be CTL state formulae, and φ be a CTL path formula. The satisfaction relation $\models$ is defined for state formulae by

$$\begin{array}{lrll}
s \models & \neg\Phi & iff & s \not\models \Phi \\
s \models & \Phi \wedge \Psi & iff & s \models \Phi \text{ and } s \models \Psi \\
s \models & \exists\varphi & iff & \pi \models \varphi \text{ for some } \pi \in Paths(s) \\
s \models & \forall\varphi & iff & \pi \models \varphi \text{ for all } \pi \in Paths(s)
\end{array}$$

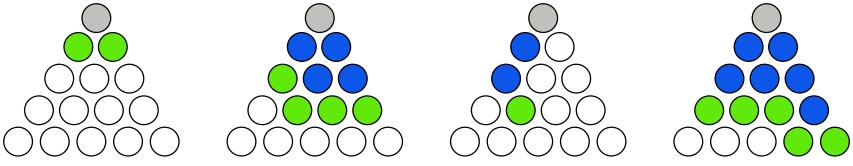


Figure 2.2: Examples of satisfaction of CTL formulae.

For path π, the satisfaction relation $\vDash$ for path formulae is defined by

$$\pi \vDash \bigcirc\Phi \quad iff \quad \pi[1] \vDash \Phi$$
$$\pi \vDash \Phi U \Psi \quad iff \quad \exists j \geq 0\, s.t.\, (\pi[j] \vDash \Psi \wedge (\forall 0 \leq k < j : \pi[k] \vDash \Phi))$$

where for path $\pi = s_0\, s_1\, s2 \ldots$ and integer $i \geq 0$, $\pi[i]$ denotes the $(i+1)$th state of π, i.e., $\pi[i] = s_i$.

The interpretations for atomic propositions, negation, and conjunction are as usual, and are interpreted over states. State formula $\exists\varphi$ is valid in state s if and only if there exists some path starting in s that satisfies φ. Conversely, $\forall\varphi$ is valid in state s if and only if all paths starting in s satisfy φ. The semantics of the path formulae is as follows. $\exists \bigcirc \Phi$ is valid in state s if and only if there exists some path π starting in s such that in the next state of this path, state $\pi[1]$, the property Φ holds. This is equivalent to the existence of a direct successor s' of s such that $s' \vDash \Phi$. $\forall(\Phi U \Psi)$ is valid in state s if and only if every path starting in s has an initial finite prefix (possibly only containing s) such that Ψ holds in the last state of this prefix and Φ holds in all other states along the prefix. $\exists(\Phi U \Psi)$ is valid in s if and only if there exists a path starting in s that satisfies $\Phi U \Psi$. The semantics of CTL here is non strict in the sense that the path formula $\Phi U \Psi$ is valid if the initial state of the path satisfies Ψ (see Figure 2.2).

PCTL The logic *Probabilistic computation tree logic* (PCTL) is a branching-time temporal logic, based on CTL. The main difference of PCTL with respect to CTL is that universal and existential path quantifications are replaced by the probabilistic operator $P_J(\varphi)$, where φ is a path formula and J is an interval of

$[0, 1]$. The path formula φ imposes a condition on the set of paths, whereas J indicates a lower bound and/or upper bound on the probability.

As for CTL formulae, a PCTL formula formulates conditions on a state of a Markov chain and its interpretation is Boolean, i.e., a state either satisfies or violates a PCTL formula. The intuitive meaning of formula $P_J(\varphi)$ in state s is: the probability of the set of paths satisfying φ and starting in s meets the bounds given by J.

The path formulae φ are defined as for CTL, except that a bounded until operator is additionally incorporated. The intuitive meaning of the path formula $\Phi U^{\leq n}\Psi$ for a natural number n is that a Ψ state should be reached within n transitions, and that all the previous states satisfy Φ.

Syntax of PCTL PCTL *state formulae* over the set AP of atomic propositions are formed according to the following grammar

$$\Phi ::= true \mid a \mid \Phi_1 \wedge \Phi_2 \mid \neg\Phi \mid P_J(\varphi)$$

where $a \in AP$, Φ is a path formula and $J \subseteq [0, 1]$ is an interval with rational bounds. PCTL *path formulae* are formed according to the following grammar:

$$\varphi ::= \bigcirc\Phi \mid \Phi_1 U \Phi_2 \mid \Phi_1 U^{\leq n} \Phi_2$$

where Φ, Φ_1, and Φ_2 are state formulae and $n \in \mathbb{N}$. As in CTL, the linear temporal operators $\bigcirc$ and U (and its bounded variant) are required to be immediately preceded by P. Rather than writing the intervals explicitly, often abbreviations are used; e.g., $P_{\leq 0.5}(\Phi)$ denotes $P_{[0,0.5]}(\Phi)$, $P_{=1}(\Phi)$ stands for $P_{[1,1]}(\Phi)$, and $P_{\geq 0}(\Phi)$ denotes $P_{]0,1]}(\Phi)$.

The propositional logic fragment of PCTL, as well as the path formulae $\bigcirc\Phi$ and $\Phi_1 U \Phi_2$ has the same meaning as in CTL. Path formula $\Phi_1 U^{\leq n} \Phi_2$ is the *step-bounded* variant of $\Phi_1 U \Phi_2$. It asserts that the event specified by Φ_2 will hold within at most n steps, while Φ_1 holds in all states that are visited before a Φ_2-state has been reached. Other Boolean connectives are derived in the usual way. Also the eventually operator and the always operator can be derived using the U operator and the duality of eventually and always (as in CTL) and the duality of lower and upper bounds.

Satisfaction Relation for PCTL Let $a \in AP$ be an atomic proposition, $\mathcal{M} = (S, P, s_0)$ be a DTMC, $s \in S$ a state, Φ, Ψ be PCTL state formulae, and

φ be a PCTL path formula. The satisfaction relation $\models$ is defined, assuming the definition of $s \vDash a$, for state formulae by

$$\begin{array}{lrll} s \vDash & \neg\Phi & iff & s \nvDash \Phi \\ s \vDash & \Phi \wedge \Psi & iff & s \vDash \Phi \text{ and } s \vDash \Psi \\ s \vDash & P_J(\varphi) & iff & Pr(s \vDash \varphi) \in J \end{array}$$

Here, $Pr(s \vDash \varphi) = Pr_s\{\pi \in Paths(s) : \pi \vDash \varphi\}$.

Given a path π in $\mathcal{M}$, the satisfaction relation is defined (as for CTL):

$$\begin{array}{lrll} \pi \vDash & \bigcirc\Phi & iff & \pi[1] \vDash \Phi \\ \pi \vDash & \Phi U \Psi & iff & \exists j \geq 0\, s.t.\, (\pi[j] \vDash \Psi \wedge (\forall 0 \leq k < j : \pi[k] \vDash \Phi)) \\ \pi \vDash & \Phi U^{\leq n} \Psi & iff & \exists 0 \leq j \leq n\, s.t.\, (\pi[j] \vDash \Psi \wedge (\forall 0 \leq k < j : \pi[k] \vDash \Phi)) \end{array}$$

where for path $\pi = s_0\, s_1\, s_2\, \ldots$ and integer $i \geq 0$, $\pi[i]$ denotes the $(i+1)$-st state of π, i.e., $\pi[i] = s_i$.

The semantics of the probability operator P refers to the probability for the sets of paths for which a path formula holds. To ensure that this is well-defined, we need to establish that the event specified by PCTL path formulae are measurable; but, as the set $\{\pi \in Paths(s) s.t. \pi \vDash \varphi\}$ for PCTL path formula φ can be considered as a countable union of cylinder sets, its measurably is ensured.

Brief Bibliography on Quantitative Model Checking PCTL is introduced, with several model checking algorithms for its verification over DTMC in [HJ94], and is extended to PCTL* in [ASB95]. The initial work on model checking a DTMC against PCTL formulae symbolically is [BCHG+97]: it introduces the representation of the probability transition matrix by means of multi-terminal binary decision diagrams (MTBDDs). Such an approach has been then extended by [dAKN+00] and it is used by the state of the art model checker tool PRISM [PRI].

Works about the verification of MDP against PCTL properties are [Var85, CY95, BdA95, BK98]. Such approaches has been extended [dA99a] to consider also cost and rewards in the computation of minimum/maximum probability of reaching a set of states.

An extended and updated bibliography on quantitative model checking can be found at `http://www.prismmodelchecker.org/publications`.

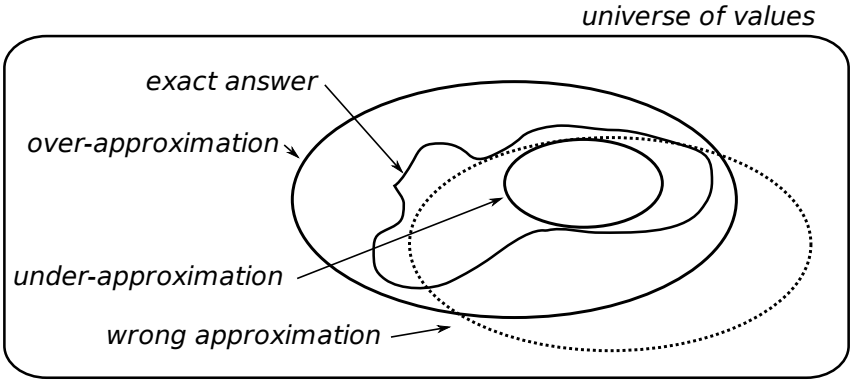


Figure 2.3: The nature of approximation.

2.4 Abstraction Techniques

We are often interested in reasoning about complex systems for which the exact study is not computable or is not practically feasible due to excessive requirement in term of computation. It is therefore reasonable to pursue approaches which simplify this task even if they contain some degrees of *imprecision* or *approximation*. For these reasons *abstraction techniques* have been developed.

The notion of approximation is crucial (See Figure 2.3). We may have an *over–approximation* to the exact result of the analysis. In this case we can guarantee that certain values cannot be result of the analysis, namely those not included in the analysis result (certain events will *never* happen). When we have an *under–approximation* we can guarantee that certain values are included in the analysis result, namely those included in the analysis result (certain events *will indeed happen*). Results that neither are over nor under–approximations are uninteresting as we cannot interpret them meaningfully.

When we have an analysis that always gives under– or over–approximations we talk about *conservative* or *safe abstraction*. Obviously, it is trivial to construct uninformative over– and under– approximations that actually give us useless information (i.e. return always the universe of values as over–approximation and the empty space as under–approximation), so the challenge is to obtain approximations striking the right balance between precision and

computational cost; the higher precision requires more costly analysis.

In this framework, we talk about the *best abstraction* if we have an analysis that is conservative and is the most accurate. The correctness and the precision of an abstraction is traditionally expressed in formal way by means of an *order over abstractions*.

By *abstract analyses* we refer to a variety of techniques which extract information about the dynamic behavior of systems without executing the systems themselves. This is typically done by systematically inspecting the studied system structure (syntax), or by executing the program using an *abstract semantics*, considering only the properties of interest. These analyses are typically designed for a particular set of properties of interest and a particular specification language, and are *systematic*, meaning that they can be applied to all programs of the language.

2.4.1 Abstract Interpretation

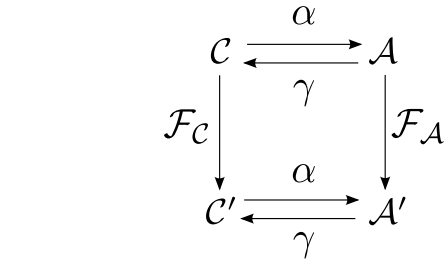
Abstract interpretation (AI) [CC77, CC79] is a very popular and general methodology for developing abstract analyses.

The theory is based on the idea of approximating the semantics of a programming or specification language. It formalizes the idea that the semantics can be more or less precise according to the considered level of observation. In more detail, abstract interpretation allows both to effectively construct conservative approximations of the semantics of a programming language, and to prove the corresponding analyses correct.

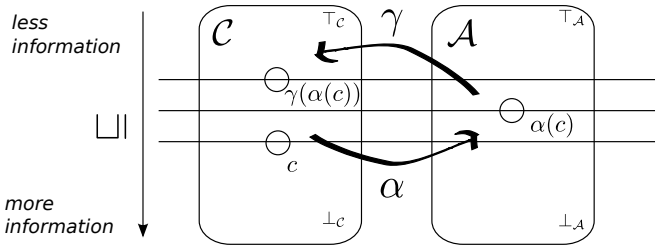
If the approximation is coarse enough, the abstraction of a semantics yields less precise but easier to compute analyses than the ones computed on the original semantics. Because of the corresponding loss of information, not all questions can be answered, but all answers given by the effective computation of the approximate semantics are always correct.

In mathematics, a *lattice* is a partially ordered set (also called a poset) in which any two elements have a unique supremum (the elements' least upper bound; called their join) and an infimum (greatest lower bound; called their meet). Lattices can also be characterized as algebraic structures satisfying certain axiomatic identities.

In the algebraic setting of abstract interpretation, a *domain* is a lattice $L(\sqsubseteq, \bot, \top, \sqcup, \sqcap)$ defined by a partial order $(L, \sqsubseteq)$, where $\bot$ and $\top$ are elements of L and $\sqcup$ and $\sqcap$ are binary operators on L, respectively denote the least element, the



(a)



(b)

Figure 2.4: Scheme of construction of abstract semantics function (a) and of Galois connection (b).

greatest element, the least upper bound and the greatest lower bound. Intuitively, the partial ordering represents the information loss.

In general, the abstract interpretation framework is used for constructing a non-standard (approximated) semantics $\mathcal{F}_{\mathcal{A}}$ obtained from the the standard (or concrete) one $\mathcal{F}_{C}$ by replacing the actual (concrete) domain of computation (C) and its basic (concrete) operators with an abstract domain ($\mathcal{A}$) and corresponding abstract semantic operations, respectively (see Figure 2.4).

An abstraction can be formalized by a *Galois connection* between a concrete domain C and an abstract domain $\mathcal{A}$, using an abstraction and a concretization functions, α and γ, as follows:

Definition 6 (Galois Connection)**.** *A Galois connection* $C \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \mathcal{A}$ *between two lattices* $(C, \sqsubseteq_C)$ *and* $(\mathcal{A}, \sqsubseteq_{\mathcal{A}})$ *is defined by an abstraction function* $\alpha : C \mapsto \mathcal{A}$*, and a concretization function* $\gamma : \mathcal{A} \mapsto C$*, that are both*

- *monotonic:*

- $\forall c, c' \in C : c \sqsubseteq_C c' \Rightarrow \alpha(c) \sqsubseteq_{\mathcal{A}} \alpha(c')$
- $\forall a, a' \in \mathcal{A} : a \sqsubseteq_C a' \Rightarrow \gamma(a) \sqsubseteq_C \gamma(a')$

- *adjoint:*
  - $\forall c \in C, \forall a \in \mathcal{A} : c \sqsubseteq_C \gamma(a) \Leftrightarrow \alpha(c) \sqsubseteq_{\mathcal{A}} a.$

Theorem 2.4.1 (Properties of Galois connection)**.** *For any Galois connection, the following properties hold*

1. $\gamma \circ \alpha$ *is* extensive *(i.e.* $c \sqsubseteq_C \gamma \circ \alpha(c)$*) and represents the* information lost by the abstraction
2. $\alpha \circ \gamma$ *is* contracting *(i.e.* $\alpha \circ \gamma(a) \sqsubseteq_C a$*)*
3. $\gamma \circ \alpha$ *is the* identity $\Leftrightarrow$ γ *is onto* $\Leftrightarrow$ α *is one–to–one*
4. α *preserves* $\top$*, and* γ *preserves* $\bot$
5. $\gamma(a) = max\ \alpha^{-1}(\downarrow a) = \top\alpha^{-1}(\downarrow a)$
6. $\alpha(c) = min\ \gamma^{-1}(\uparrow c) = \bot\gamma^{-1}(\uparrow c)$
7. *the composition of two Galois connections is a Galois connection.*

Where $f \circ g \equiv \lambda x.g(f(x))$ *and* $\downarrow a = \{b \,|\, b \sqsubseteq a\}$, $\uparrow a = \{b \,|\, a \sqsubseteq b\}$.

With *one–to–one function* we mean injective function; a function that associates distinct arguments with distinct values (information-preserving). With *onto function* we mean surjective function: its values span its whole codomain (for every y in the codomain, there is at least one x in the domain such that $f(x) = y$).

If $\gamma \circ \alpha$ is the *identity*, the abstraction α loses no information, and C and $\mathcal{A}$ are isomorphic from the information standpoint (although α may be not onto and γ not one–to–one). It is equivalent in the definition of Galois connections to replace the condition of adjointness by conditions 1 and 2, or by condition 5 which also entails the monotonicity of γ.

Once defined an abstraction function α and an order over the abstract domain $\sqsubseteq_{\mathcal{A}}$, the abstract analysis can be proved to be sound if, for each program $P \in C$ and the corresponding abstract program $P^\circ \in \mathcal{A}$, it holds that $\alpha(\mathcal{F}_C(P)) \sqsubseteq_{\mathcal{A}} \mathcal{F}_{\mathcal{A}}(P^\circ)$.

The theory of abstract interpretation provides several properties of abstract operators and of abstract domain to guarantee the soundness of abstract semantics and their fix-point. We refer the interested reader to [CC77, CC79]. Here, we are interested in a different application of abstract interpretation, that is in abstract probabilistic model checking. Therefore, we apply theory in the style of [CGL94, DGG97, Hut05].

2.4.2 Predicate Abstraction

Predicate abstraction has been introduced as a technique for reducing an infinite state system to a finite state in the work of Graf and Saidi [GS97]. In that work, a finite state system is obtained as an over-approximation of an infinite state system. This is a conservative abstraction, in the sense that for every execution in the concrete system there is a corresponding execution in the abstract system. The abstract version of the verification condition is model checked in this abstract system. If a property (typically expressed in some form of modal logic) is verified then it holds in the concrete system. Otherwise an abstract counter-example trace is generated. There could be a concrete counter-example corresponding to it, in which case there is a bug in the design, or the abstract counter-example is an artifact of the abstraction (for more detailed discussion on predicate abstraction we refer to [Das03]).

Formally, a predicate is a boolean condition over states. Given a state space S and a set of predicates P, an abstract state space is computed: each abstract state is equal to a conjunction of a possible evaluation all the predicates in P. The size of the abstract state space is top bound by $2^{|P|}$. An abstract state is identified by the subset of P of predicates that are true for the state.

The techniques has been lately applied also to probabilistic transition systems (see for instance [WZH07, KKNP08, KH09]). In this case the result of the predicate abstraction is an MDP: a transition system where probabilistic transitions are alternated to non-deterministic transitions (see Section 2.3.2). Practically, given an abstract state, to perform a move, it is necessary, first, to perform a non-deterministic choice, in order to identify a concrete state within the states abstracted by the current abstract state, and, then, to perform a probabilistic move corresponding to the probabilistic move of the concrete state selected.

By *safety property* we denote properties specifying that "something bad never happens". By *liveness property* we denote properties specifying that "something good will happen eventually" [Lam77, Kin94].

One of the main drawback of predicate abstraction is that, often, it cannot be used to prove *liveness* properties. Indeed, abstract transition systems usually contains cycles that do not correspond to concrete computations restricting useful results to *safety* properties only: according to the predicate abstracted semantics, there is the possibility to loop forever on certain states, while there are not any corresponding concrete computation. Actually, a sound but totally imprecise abstract semantics is computed (see the following Example). This problem is sometimes solved by imposing *fairness constraints* over transitions, but this is not always correct w.r.t. the concrete semantics of the system [BK98, dA99b, BGC09].

Example 1. *Let us consider a MSR system (see Section 3.2) where two populations* A, B *evolve, starting from a state consisting in* 3 *individuals of A. Each individual of the species A can disappear or become an individual of the species B. This behavior can be expressed by the following two rewriting rules:*

$$R1 : A \to B\,, \quad R2 : A \to \ .$$

Assuming an interleaving semantics, we can associate to such a system the transition system depicted in Figure 2.5.a).

If we perform predicate abstraction using the set of predicates (see Figure 2.5.b))

$$\{(A = 0)\,(A \in [1,2])\,(A \in [3,4])\,(A \geq 4)\,(B = 0)\,(B \in [1,2])\,(B \in [3,4])\,(B \geq 4)\,\}$$

we obtain the abstract states depicted in Figure 2.5.c), on which an abstract MDP semantics can be computed as shown in Figure 2.5.d).

The problem with such a semantics is that liveness properties cannot be verified without imposing a fairness constraint on some non-deterministic choice. Indeed, without fairness constraints, it is possible to remain forever on the starting state.

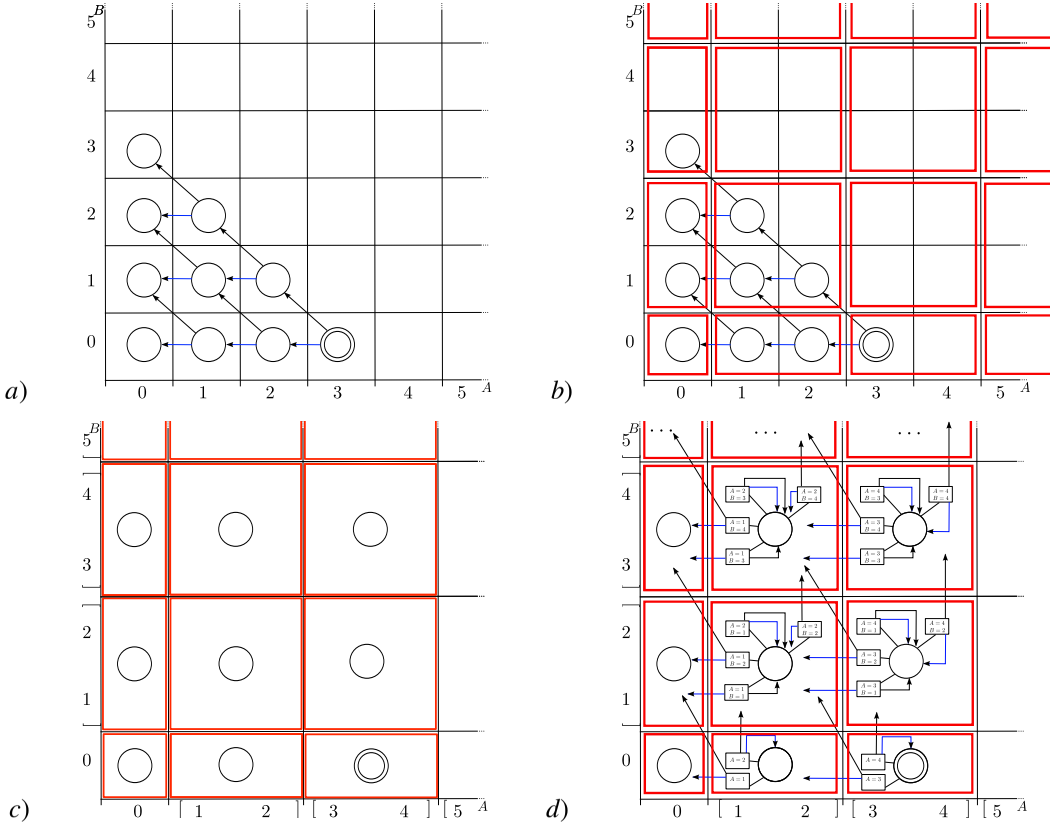


Figure 2.5: Illustration of predicate abstraction of model of Example 1. *a*) concrete semantics, *b*) partition by predicate evaluation, *c*) abstract states, *d*) abstract non-deterministic semantics: circles are abstract states, rectangles represents non-deterministic choices, arrows represents probabilistic transitions.

Chapter 3

Abstract Semantics for Models with Uncertainty on Kinetic Rates

In this chapter, we present a formalization of biological systems based on Multiset Rewriting systems and we investigate the use of abstract interpretation on their semantics. We consider a probabilistic semantics, which is well suited to represent the non-deterministic evolution of real biological systems. Abstract interpretation allows us to deal with systems in which the kinetic rates of the evolution rules are not precisely known. On the (abstract) systems we perform probabilistic model checking obtaining lower and upper bounds for the probabilities of reaching states satisfying given properties. We apply probabilistic model checking to verify reachability properties in a model of tumor growth.

3.1 Introduction

Modelling biological systems requires to represent the events (reactions) which guide the evolution of the systems together with their rates. Rates are often not precisely known, given the difficulty of measuring them for each single reaction. Thus, in many cases, it is necessary to construct models with some approximation which should not influence the overall behavior of the system

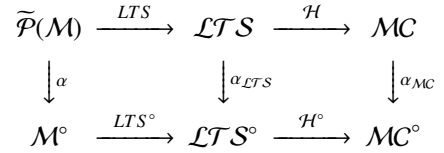


Figure 3.1: Schematics of the defined theory; with $\circ$ we indicate abstract structures, with α abstraction functions. $\widetilde{\mathcal{P}}$ denotes the power-set of isomorphic elements. Here, H and H° stand for the concrete and abstract probabilistic translation functions, while LTS and LTS° are the concrete and abstract LTS computation functions, respectively.

we are interested to analyze. In these cases we can predict the evolution of the system, although in a non-precise way.

In this chapter we present a formalization of biological systems based on *Multiset Rewriting* (MSR) [CDL+99], and we investigate the use of abstract interpretation [CC77] on its semantics. We consider a probabilistic semantics of MSR which is well suited to represent the non-deterministic evolution of real biological systems. We define an effective method to compute an approximation of the probabilistic semantics of MSR systems for which the exact kinetic rates are not precisely known, but they are supposed to lie in some intervals. We use an IMC [JL91, KU02] to abstract the set of DTMC describing the probabilistic semantics of a set of MSR systems with uncertain kinetic rates. IMC is a model, which combines non-deterministic and probabilistic steps, using intervals of probabilities. Probabilistic model checking on IMC, which can be realized following the approach of [FLW06], reports lower and upper bounds for probabilistic temporal properties. In particular, we are interested in the probability of reachability properties, that is in the probability to reach states satisfying given properties. The methodology is illustrated in Figure 3.1.

We start by recalling MSR. MSR is used as the formalism for constructing *concrete systems*, namely systems with exact kinetic rates. We give a *Labeled Transition System* (LTS) semantics to MSR and show how to derive, in standard way, a probabilistic semantics from it, in terms of a DTMC. On the DTMC it is possible to perform probabilistic model checking.

In order to deal with uncertainty we define *abstract systems*, in which the kinetic rates are given as intervals, we introduce an abstract LTS semantics and a systematic method to derive an IMC form abstract LTS. We relate the concrete

probabilistic semantics with the abstract one by means of abstract interpretation techniques [CC77]. We prove the soundness (and the precision) of abstract semantics, both LTS and probabilistic, with respect to their concrete versions. This guarantees that lower and upper bounds of probabilistic reachability, computed on the IMC of an abstract system, safely approximate the concrete probability values, for each corresponding concrete system.

To validate the usefulness of our approach in the context of biological systems modelling, we apply probabilistic model checking to verify reachability properties in an abstract system of tumor growth [VR03]. We conclude with a discussion about related works and we present some possible future direction of the research.

3.2 Probabilistic Model Checking of Biological Systems

To model biological systems we adopt MSR [CDL+99] where rewriting rules are enriched with non-negative real kinetic constants. In this model, multisets are states of computation and transitions between states are obtained by applying rewriting rules with a probability proportional to their kinetic constants.

We choose such a formalism because it is simple and expressive enough to describe many systems of interest. Moreover, as many formalisms used in the context of biological systems modelling are based on MSR, techniques developed for MSR may be further expanded to more complex languages.

Given a finite set of elements, X, a *multiset* is a function $s : X \to \mathbb{N}$ and $\mathcal{MS}(X)$ is the *universe of multisets over* X. Sum $\oplus$ and difference $\ominus$ of multisets are defined as follows: for $s', s'' \in \mathcal{MS}(X)$, we have $s' \oplus s''(x) = s'(x) + s''(x)$ and $s' \ominus s''(x) = max(s'(x) - s''(x), 0)$. In the following we shall often assume a set of *species names* Σ, of size n, to be given.

In the following, a multiset represents a configuration of a biological system, and possible events are modelled by rewriting rules. A *rewriting rule* is a pair (l, r), where l and r are multisets, called *reactants* and *products*, respectively. Each rule is associated to a *kinetic constant* that is, roughly, an indication of the likelihood of the represented event[1].

[1] In the context of chemical kinetics studies, kinetic constants are often used to express the speed of reactions, and the a continuous time semantics is used (i.e. a CTMC). Here we use kinetic constants just as an indication of the likelihood of events and we study systems in a probabilistic (time-abstract) setting.

Definition 7 (Concrete System)**.** *A* concrete system M *is a triple* $(\mathcal{R}, \mathcal{K}, s_0)$*:*

- $\mathcal{R} = \{R_1, \ldots, R_m\}$*, with* $R_i \in \mathcal{MS}(\Sigma) \times \mathcal{MS}(\Sigma)$*, is a vector of* rewriting rules*;*
- $\mathcal{K} = \{k_1, \ldots, k_m\}$*, with* $k_i \in \mathbb{R}_{\geqslant 0}$*, is a vector of* kinetic constants*;*
- $s_0 \in \mathcal{MS}(\Sigma)$ *is the* starting state*.*

In the following we refer to generic tuples components by name. For instance, given a system $M = (\mathcal{R}, \mathcal{K}, s_0)$, we use $\mathcal{R}(M), \mathcal{K}(M), s_0(M)$ to denote $\mathcal{R}, \mathcal{K}, s_0$ respectively. When M is clear from the context, for $i \in [1, m]$, we use l_i and r_i to denote the reactants and products multisets of rule $R[i]$, and we use k_i for the kinetic constant $\mathcal{K}[i]$.

The universe of concrete systems is denoted by $\mathcal{M}$. We also say that two concrete systems $M_i, i \in \{1, 2\}$, are *isomorphic* ($M_1 \sim M_2$) if and only if $\mathcal{R}(M_1) = \mathcal{R}(M_2) \wedge s_0(M_1) = s_0(M_2)$. Intuitively, $M_1 \sim M_2$ iff M_1 and M_2 share the initial state and the set of rewriting rules.

3.2.1 Labeled Transition System Semantics

To describe the semantics of a concrete systems we adopt a *Labeled Transition System* (LTS) semantics. Namely, we adopt a *transition* relation of the form $s' \xrightarrow{\eta, \beta} s''$, where η is the number of the applied rule and $\beta \in \mathbb{R}_{\geqslant 0}$ is the *transition rate*.

The application of a rule R_η to a state s' is modelled by the inference rule

$$\frac{(l_\eta, r_\eta) \in \mathcal{R} \qquad k_\eta \in \mathcal{K} \qquad l_\eta \subseteq s' \qquad \beta = rate(l_\eta, s', k_\eta) \qquad s'' = ((s' \ominus l_\eta) \oplus r_\eta)}{s' \xrightarrow{\eta, \beta} s''} \tag{3.1}$$

where $rate(l_\eta, s', k_\eta) = kin(l_\eta, s') \times k_\eta$ and $kin(l_\eta, s') = \prod_{x \in \Sigma} \binom{s'(x)}{l_\eta(x)}$.

To compute $kin(l_\eta, s')$ we take into account the number of possible distinct applications of the rule R_η to state s'. Actually, this requires to compute the number of distinct combinations of the reactants l_η in the multiset s'. Then, $rate(l_\eta, s', k_\eta)$ is obtained by multiplying the value of $kin(l_\eta, s')$ by the kinetic constant k_η associated with rule R_η.

In the following, we use $\mathcal{LTS}$ to denote the universe of LTSs and we define the function $LTS : \mathcal{M} \mapsto \mathcal{LTS}$, such that $LTS(M)$, with $M = (\mathcal{R}, \mathcal{K}, s_0)$, is the LTS $= (S, s_0, \rightarrow)$, obtained by transitive closure of (3.1) starting from s_0.

When the transition relation $\rightarrow$ is clear from the context, we use $Next(s)$ for the set of transitions exiting from the state s. In addition, we use $TS(s', s'') = \{s' \xrightarrow{\eta,\beta} s'' \text{ for some } \eta, \beta\}$ to denote the set of transitions from s' to s''. Given a transition $t = s' \xrightarrow{\eta,\beta} s''$, we also use $rate(t) = \beta$. Note that, $\forall R_\eta \in \mathcal{R}, s \in S$, there is at most one transition $s \xrightarrow{\eta,\beta} s' \in Next(s)$ corresponding to R_η.

3.2.2 Derivation of Probabilistic Semantics

We define the probabilistic semantics of a concrete system by means of a translation from its LTS into a DTMC (as defined in Section 2.3.2, Definition 2).

In the following, we restrict our attention to *finitely branching* DTMCs, meaning that for each s in the state space, the set $\{s' \mid P(s, s') > 0\}$ is finite. Since our systems have m–sized vector of rules, for each state, we have at most m outgoing transitions. Moreover, we use $\mathcal{MC}$ to denote the universe of (finitely branching) DTMCs.

To derive a DTMC from an LTS, we have to calculate, for each states s and s' of LTS , the probability of moving from s to s', by exploiting transition rates. Thus, we introduce two functions $R : S \times S \mapsto \mathbb{R}_{\geqslant 0}$ and $E : S \mapsto \mathbb{R}_{\geqslant 0}$, such that

$$R(s, s') = \sum_{t \in TS(s,s')} rate(t) \text{ and } E(s) = \sum_{s' \in S} R(s, s').$$

Intuitively, $R(s, s')$ gives the rate of the set of transitions from s to s', while $E(s)$ computes the exit rate of states. The probability of moving from s to s' is derived from $R(s, s')$ and $E(s)$, in the standard way.

Definition 8 (Probabilistic Translation Function)**.** *We define* $\mathcal{H} : \mathcal{LTS} \rightarrow \mathcal{MC}$ *as* $\mathcal{H}((S, s_0, \rightarrow)) = (S, s_0, P)$*, where* $P : S \rightarrow Distr(S)$ *is the* probability transition function*, s.t.* , $\forall s, s' \neq s \in S$ *: if* $E(s) = 0$*, then* $P(s, s') = 0$*, and* $P(s, s) = 1$*;* $P(s, s') = R(s, s')/E(s)$ *otherwise.*

Note that, traditionally, the semantics of a stochastic system is formalized as a *Continuous Time Markov Chain* (CTMC). The DTMC of Definition 8 is obviously the so called "embedded" DTMC (see Section 2.3.2). We consider the DTMC because we are interested in probability of reachability properties (see the following section).

3.2.3 Probabilistic Model Checking

In the context of probabilistic model checking [Kwi03, KNP02] we consider a fragment of the Probabilistic Temporal Logic CTL (PCTL) [HJ94], able to express probabilistic reachability properties (see Section 2.3.3 for more details). Probabilistic reachability captures the probability to reach a state which satisfies a given property. Formally, this requires to evaluate the probability of a set of paths in the DTMC. We briefly recall main concepts concerning PCTL model checking and we refer the interested reader to [Kwi03, BK08].

Our reachability properties are parametric w.r.t. a set AP of propositional symbols (ranged over by $\{A, B, \ldots\}$). A symbol $A \in AP$ denotes a set of conditions on multisets that are evaluated by a corresponding notion of satisfaction $\vDash$: $\mathcal{MS}(\Sigma) \times AP \mapsto \{true, false\}$. As usual, given $s \in \mathcal{MS}(\Sigma)$ and $A \in AP$, $s \vDash A$ says that s satisfies A.

Definition 9 (Concrete Reachability)**.** *Let $mc = (S, s_0, P)$ be a DTMC. The probability of reaching a state satisfying $A \in AP$, starting from $s \in S$, is*

$$Reach_{A,mc}(s) = P_s(\{\pi \in C(s) \,|\, \pi[i] \vDash A \text{ for some } i \geq 0\}) .$$

Model checking of reachability properties on a DTMC, from a state s, consists on computing $Reach_{A,mc}(s)$, and can be done using standard iterative methods [Kwi03, BK08].

We use $Reach(A)$ to denote $Reach_{A,mc}(s_0)$ where $mc = \mathcal{H}(LTS(M))$, for a system M clear from the context.

Example 2 (Concrete System Model Checking)**.** *We consider a simple system of chemical reactions, where, starting from a configuration consisting of two molecules of X, two of Y and ten of W, two molecules X and Y may bind, to form complex XY, and molecule X may be degraded, by molecule W. Using $\Sigma = \{X, Y, W, XY\}$, the system can be formalized as $M_{ex} = (\mathcal{R}, \mathcal{K}, s_0)$ where*

$$\begin{aligned} s_0 = \quad & \{(X, 2), (Y, 2), (W, 10)\}, \\ \mathcal{K} = \quad & \{k_1 = 3, k_2 = 1\}, \\ \mathcal{R} = \quad & \{(R_1 = \{X, Y\} \xrightarrow{k_1} \{XY\}), (R_2 = \{X, W\} \xrightarrow{k_2} \{W\})\}. \end{aligned}$$

Note that we assume that the complexation is three times faster than the

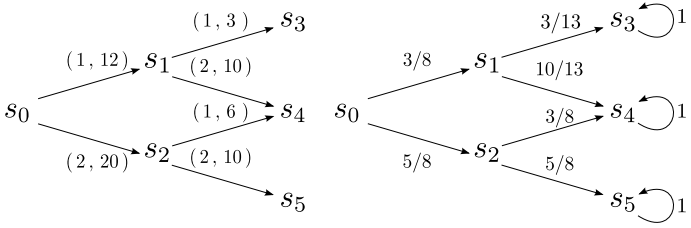


Figure 3.2: $LTS(M_{ex})$, and $\mathcal{H}(LTS(M_{ex}))$.

degradation. Figure 3.2 shows the derived $LTS(M_{ex})$ *and* $\mathcal{H}(LTS(M_{ex}))$ *where*

$$
\begin{aligned}
S = \{\quad & s_0 && = \{(X,2),(Y,2),(W,10),(XY,0)\} \\
& s_1 && = \{(X,1),(Y,1),(W,10),(XY,1)\} \\
& s_2 && = \{(X,1),(Y,2),(W,10),(XY,0)\} \\
& s_3 && = \{(X,0),(Y,0),(W,10),(XY,2)\} \\
& s_4 && = \{(X,0),(Y,1),(W,10),(XY,1)\} \\
& s_5 && = \{(X,0),(Y,2),(W,10),(XY,0)\} \qquad \}.
\end{aligned}
$$

The probability of obtaining at least two complexes XY corresponds to the probability to reach s_3*. That is,* $3/8 \times 3/13 = 9/104$*. This shows that, even if the rate of the complexation is (three times) greater that the one of the degradation, the concentration of reagent W makes the degradation more likely to happen than the binding of reagent X and Y.*

3.3 Abstract Systems Modelling and Model Checking

We introduce *abstract systems*, the *abstract LTS semantics*, and the corresponding *abstract probabilistic semantics* in terms of IMC. Moreover, we prove the soundness of the approach, using notions of the abstract interpretation theory.

In order to approximate the information about the kinetic rates of the reaction rules we adopt the domain of *intervals of (non-negative) reals* $\mathbb{I}$ (the real valued version of intervals of integers [CC77, Kea96, Wei99]).

Definition 10 (Intervals)**.** $\mathbb{I} = \{\,[m,n] \mid m \in \mathbb{R}_{\geq 0}, n \in \mathbb{R}_{\geq 0} \cup \{\infty\} \wedge m \leq n\}$.

Over intervals of reals $\mathbb{I}$ we use the operations and the order defined as follows.

$$\forall\, i, j \in \mathbb{I},\ i = [a\,,\, b],\ j = [c\,,\, d]\ : \qquad [i]^- = a\,, [i]^+ = b$$
$$i \times^{\mathbb{I}} j = [\, a \times c\,,\, b \times d\,]\,, \qquad i \cup^{\mathbb{I}} j = [\, \min(a\,,\, c)\,,\, \max(b\,,\, d)\,]\,,$$
$$i +^{\mathbb{I}} j = [\, a + c\,,\, b + d\,]\,, \qquad i \sqsubseteq_{\mathbb{I}} j \text{ iff } (i \cup_{\mathbb{I}} j \;=\; j)\ .$$

We consider both $\cup_{\mathbb{I}}$ and $\sqsubseteq_{\mathbb{I}}$ extended component-wise to m–sized vectors of intervals, and for simplicity we use the same symbols. For $x \in \mathbb{R}_{\geqslant 0}$ we use $x^\bullet = [x, x] \in \mathbb{I}$ for its *best abstraction* - i.e. the most precise abstraction - as interval, considered extended to vector of reals.

In *abstract systems* each reaction rule has associated an interval of reals ($\in \mathbb{I}$) rather than a precise kinetic constant ($\in \mathbb{R}$).

Definition 11 (Abstract Systems)**.** *An* abstract system M *is a triple* $(\mathcal{R}, \mathcal{K}^\circ, s_0)$ *with* $\mathcal{R}$ *and* s_0 *as in the concrete case, while* $\mathcal{K}^\circ = \{k_1^\circ, \ldots, k_m^\circ\}$, $k_i^\circ \in \mathbb{I}$, *is a* vector of interval values.

We denote the universe of abstract systems as $\mathcal{M}^\circ$. We assume the notations used for concrete systems extended, in the obvious way, to abstract systems. The order $\sqsubseteq_{\mathbb{I}}$ over intervals introduces a corresponding approximation order $\sqsubseteq_{\mathcal{M}^\circ}$ over abstract systems.

Definition 12 (Order on Abstract Systems)**.** *For all* $M_i^\circ, i \in \{1, 2\}$: $M_1^\circ \sqsubseteq_{\mathcal{M}^\circ} M_2^\circ$ *iff* $M_1^\circ \sim M_2^\circ \wedge \mathcal{K}(M_1^\circ) \sqsubseteq_{\mathbb{I}} \mathcal{K}(M_2^\circ)$.

3.3.1 Abstraction and Concretization

To formalize the relation between concrete and abstract systems we introduce a pair of functions, *abstraction* and a *concretization functions*, which form a Galois connection [CC77]. The abstraction function α reports the approximation of sets of concrete systems differing only for the kinetic part of the rules: *sets of isomorphic systems*. Its counterpart is the concretization function which reports the set of concrete systems abstracted by an abstract system.

Given that as abstract system represents infinite set of concrete systems differing only on the rates of reactions we introduce the domain of *isomorphic concrete systems*. Intuitively, they are sets of concrete systems that are identical except for the kinetic part of the rewriting rules.

Let $\widetilde{\mathcal{P}}(\mathcal{M}) = \{X \in \mathcal{P}(\mathcal{M})\,, \forall M, M' \in X\,, M \sim M'\}$ be the domain of *sets of isomorphic concrete systems*. Given $X \in \widetilde{\mathcal{P}}(\mathcal{M})$ we denote with $R(X)$

and $s_0(X)$ the shared components, e.g. the vector of rules and the starting state, respectively.

To define the concrete domain of the Galois connection we also have to define the order $\sqsubseteq_{\widetilde{\mathcal{P}}(\mathcal{M})}$ on sets of isomorphic concrete systems.

Definition 13 (Order on Set of Isomorphic Concrete Systems)**.**
Given two set of isomorphic concrete systems $X_i \in \widetilde{\mathcal{P}}(\mathcal{M})$, $i \in \{1,2\}$:
$X_1 \sqsubseteq_{\widetilde{\mathcal{P}}(\mathcal{M})} X_2$ *iff* $\overline{\mathcal{K}_1} \sqsubseteq_{\mathbb{I}} \overline{\mathcal{K}_2}$ *where* $\overline{\mathcal{K}_i} = \cup^{\mathbb{I}}_{M \in X_i}(\mathcal{K}(M))^{\bullet}$.

Definition 14 (Abstraction and Concretization Functions)**.** *Let* $\alpha : \widetilde{\mathcal{P}}(\mathcal{M}) \mapsto \mathcal{M}^{\circ}$ *and* $\gamma : \mathcal{M}^{\circ} \mapsto \widetilde{\mathcal{P}}(\mathcal{M})$ *be s.t.* $\forall X \in \widetilde{\mathcal{P}}(\mathcal{M})$, $\forall M^{\circ} \in \mathcal{M}^{\circ}$:

- $\alpha(X) = (\, R(X)\,,\, \overline{\mathcal{K}^{\circ}}\,,\, s_0(X)\,)$ *where* $\overline{\mathcal{K}^{\circ}} \equiv \bigcup^{\mathbb{I}}_{M \in X}(\mathcal{K}(M))^{\bullet}$;
- $\gamma(M^{\circ}) = \{M \,|\, \alpha(M) \sqsubseteq_{\mathcal{M}^{\circ}} M^{\circ}\}$.

Theorem 3.3.1. *The pair* (α, γ) *is a Galois connection between* $(\widetilde{\mathcal{P}}(\mathcal{M}), \sqsubseteq_{\widetilde{\mathcal{P}}(\mathcal{M})})$ *and* $(\mathcal{M}^{\circ}, \sqsubseteq_{\mathcal{M}^{\circ}})$*;* α *and* γ *are* a) monotonic *and* b) adjoint.

Proof. a) Is trivial given the definition of α and γ.
b) We have to show: $\forall X \in \widetilde{\mathcal{P}}(\mathcal{M}), M^{\circ} \in \mathcal{M}^{\circ} : \alpha(X) \sqsubseteq_{\mathcal{M}^{\circ}} M^{\circ} \;\Leftrightarrow\; X \sqsubseteq_{\widetilde{\mathcal{P}}(\mathcal{M})} \gamma(M^{\circ})$.

Let us consider $M^{\circ} = (\mathcal{R}, \mathcal{K}^{\circ}_{M^{\circ}}, s_0)$ and $X = \{M_i = (\mathcal{R}', \mathcal{K}_i, s'_0), i \in I_X\}$.

By definition of α and γ, $\gamma(M^{\circ}) = \{M_j = (\mathcal{R}, \mathcal{K}_j, s_0), j \in J_{\gamma(M^{\circ})}\}$ and $\alpha(X) = (\mathcal{R}', \overline{\mathcal{K}^{\circ}}, s'_0)$, where $\overline{\mathcal{K}^{\circ}_X} \equiv \bigcup^{\mathbb{I}}_{i \in I_X}(\mathcal{K}(M_i))^{\bullet}$. Thus, by definition of $\sqsubseteq_{\widetilde{\mathcal{P}}(\mathcal{M})}$ and $\sqsubseteq_{\mathcal{M}^{\circ}}$, it must be the case that $\mathcal{R} = \mathcal{R}'$ and $s_0 = s'_0$, and, remains to show that

$$\overline{\mathcal{K}^{\circ}_X} \sqsubseteq_{\mathbb{I}} \mathcal{K}^{\circ}_{M^{\circ}} \;\Leftrightarrow\; \cup^{\mathbb{I}}_{i \in I_X}(\mathcal{K}(M_i))^{\bullet} \sqsubseteq_{\mathbb{I}} \cup^{\mathbb{I}}_{j \in J_{\gamma(M^{\circ})}}(\mathcal{K}(M_j))^{\bullet} .$$

This is evident as the dis-equations are side by side equal by def. of α and γ. □

This formalization shows that an abstract system M° represents a (possibly infinite) set of isomorphic concrete systems $\gamma(M^{\circ})$. Each model $M \in \gamma(M^{\circ})$ has the same vector of rules and the same starting state, while the kinetic rates may vary in the vector of intervals $K^{\circ}(M^{\circ})$.

3.3.2 Abstract LTS Semantics

We introduce the LTS semantics associated with abstract systems, adopting an *abstract transition* relation $s \xrightarrow{\eta, \beta^{\circ}}_{\circ} s'$, where η is as in the concrete case, while $\beta^{\circ} \in \mathbb{I}$ is an interval of rates.

The application of a rule R_η to a state s is modelled by the rule

$$\frac{(l_\eta\,,\,r_\eta)\in\mathcal{R}\qquad k^\circ_\eta\in\mathcal{K}^\circ\qquad l_\eta\subseteq s'\qquad \beta^\circ=rate^\circ(l_\eta,\,s,\,k^\circ_\eta,)\qquad s'=((s\ominus l_\eta)\oplus r_\eta)}{s\xrightarrow{\eta\,,\beta^\circ}_\circ s'} \tag{3.2}$$

where $rate^\circ(l_\eta, s, k^\circ_\eta) = kin(l_\eta, s) \times^{\mathbb{I}} k^\circ_\eta$. To compute $rate^\circ(l_\eta, s, k^\circ_\eta)$ we follow the same reasoning of the concrete case, replacing exact rates with intervals.

We define the function $LTS^\circ : M^\circ \mapsto LTS^\circ$ such that $LTS^\circ((\mathcal{R}, \mathcal{K}^\circ, s_0)) = (S, s_0, \rightarrow_\circ)$ is obtained by transitive closure of (3.2) starting from s_0. As in the concrete case the outgoing transitions from a state have distinct labels. In the following we use $\mathcal{LTS}^\circ$ to denote the universe of abstract LTSs and we assume that the notations, defined for LTSs, are adapted in the obvious way to the abstract case.

To relate an LTSs to its abstract counterpart, and to express the soundness and the precision of abstract LTSs, we introduce the concept of *best abstraction*, both for an LTS and for *sets of isomorphic LTSs*.

Two LTSs $lts_i = (S_i, s_{0,i}, \rightarrow_i), i \in [1, 2]$ are isomorphic ($lts_1 \sim lts_2$) iff $S_1 = S_2$ and $s_{0,1} = s_{0,2}$, that is if they share the same state space, included the initial state. We denote the universe of *isomorphic LTS* as $\widetilde{\mathcal{P}}(\mathcal{LTS})$.

Definition 15 (Best Abstraction of LTSs)**.** *We define*

- $\alpha_{\mathcal{LTS}} : \mathcal{LTS} \mapsto \mathcal{LTS}^\circ$ *such that* $\alpha_{\mathcal{LTS}}((S, s_0, \rightarrow)) = ((S, s_0, \rightarrow^\alpha_\circ))$ *with* $\rightarrow^\alpha_\circ = \{s \xrightarrow{\eta,\beta^\bullet}_{\circ^\alpha} s' | s \xrightarrow{\eta,\beta} s' \in \rightarrow\}$;
- $\widehat{\alpha}_{\mathcal{LTS}} : \widetilde{\mathcal{P}}(\mathcal{LTS}) \rightarrow \mathcal{LTS}^\circ$ *such that* $\widehat{\alpha}_{\mathcal{LTS}}(X) \equiv (S(X), s_0(X), \rightarrow^\wedge_\circ)$ *with*
$$\rightarrow^\wedge_\circ = \{s \xrightarrow{\eta,\widehat{\beta^\circ}}_{\circ^\wedge} s' \,|(S, s_0, \rightarrow) \in X_{LTS}\,, \widehat{\beta^\circ} = \bigcup^{\mathbb{I}}_{s\xrightarrow{\eta,\beta^\circ}_\circ s',(S,s_0,\rightarrow_\circ)\in X_{LTS}} \beta^\circ\,,$$
$$X_{LTS} = \{\alpha_{\mathcal{LTS}}(LTS(M))|M \in X\}\}\,.$$

The most precise abstraction of an LTS is obviously obtained by replacing the rate β of each transition with $\beta^\bullet = [\beta, \beta]$. Note that $\alpha_{\mathcal{LTS}}$ does not effectively introduce any approximation. The abstraction of a set of isomorphic LTSs use as rates the union of rates of the abstract LTSs, obtained by computing the most precise abstraction of each LTS in the set.

Function $\alpha_{\mathcal{LTS}}$ can be suitably used to relate concrete and abstract LTSs. To express soundness, however, we need to introduce an approximation order

$\sqsubseteq_{\mathcal{LTS}^\circ}$ over abstract LTSs, in the style of [DGG97]. In this way, we can say that an abstract LTS $lts^\circ \in \mathcal{LTS}^\circ$ is a *sound approximation* of an LTS $lts \in \mathcal{LTS}$, if it approximates the best abstraction of lts. That is $\alpha_{\mathcal{LTS}^\circ}(lts) \sqsubseteq_{\mathcal{LTS}^\circ} lts^\circ$.

Definition 16 (Order on Abstract LTSs)**.** *Let* $lts_i^\circ = (S, s_0, \rightarrow_\circ^i), i \in \{1,2\}$. *We say that* $lts_1^\circ \sqsubseteq_{\mathcal{LTS}^\circ} lts_2^\circ$ *iff,* $\forall s, s' \in S$

$$\forall t_1^\circ = (s \xrightarrow{\eta,\beta_1^\circ}_\circ s') \in \rightarrow_\circ^1,\ \exists\, t_2^\circ = (s \xrightarrow{\eta,\beta_2^\circ}_\circ s') \in \rightarrow_\circ^2 \ \textit{such that}\ \beta_1^\circ \sqsubseteq_{\mathbb{I}} \beta_2^\circ.$$

Intuitively, the definition of $\sqsubseteq_{\mathcal{LTS}^\circ}$, requires that, if $lts_1 \sqsubseteq_{\mathcal{LTS}^\circ} lts_2^\circ$, each pair of states, in $\rightarrow_\circ^1$ relation, are in $\rightarrow_\circ^2$ relation with a coarser transition rate interval.

Function $\widehat{\alpha}_{\mathcal{LTS}}$ can suitably be used to relate a set of isomorphic LTS with abstract LTS. In more detail, the following theorem shows that $LTS^\circ(M^\circ)$, for an abstract system M°, coincides with the best abstraction of the set of isomorphic LTS $\{(LTS(M))|M \in \gamma(M^\circ)\}$. This demonstrates the precision of the abstract LTS semantics of an abstract system M° with respect to the set of LTS describing the behavior of the concrete system M approximated by M° (i.e. $M \in \gamma(M^\circ)$).

Theorem 3.3.2 (Precision of LTS°)**.**
$\forall M^\circ \in \mathcal{M}^\circ : \widehat{\alpha}_{\mathcal{LTS}}(\{(LTS(M))|M \in \gamma(M^\circ)\}) = LTS^\circ(M^\circ)$.

Proof. Let $M^\circ = (\mathcal{R}, \mathcal{K}^\circ, s_0)$ and $\widehat{LTS}(M^\circ) = \{LTS(M)|M \in \gamma(M^\circ)\}$. Moreover, let $LTS^\circ(M^\circ) = (S, s_0, \rightarrow_{M^\circ}^\circ)$. For each $M \in \gamma(M^\circ)$ we have $M = (\mathcal{R}, \mathcal{K}, s_0)$ for some vector of kinetic constants $\mathcal{K}$, and $LTS(M) = (S, s_0, \rightarrow)$ for some transition relation $\rightarrow$; consequently $\widehat{\alpha}_{\mathcal{LTS}}(\widehat{LTS}(M^\circ)) = (S, s_0, \rightarrow_\circ^\wedge)$ for some transition relation $\rightarrow_\circ^\wedge$. Hence, we have only to prove that $\rightarrow_\circ^\wedge = \rightarrow_\circ^{M^\circ}$.

Since the vector of rules $\mathcal{R}$ in M° is the same as in any $M \in \gamma(M^\circ)$, we have that each transition in $LTS^\circ(M^\circ)$ has a corresponding transition in $LTS(M)$, namely

$\forall s, s' \in S, \forall\, t_1 = s \xrightarrow{\eta,\beta} s'$, $\exists\, t_2 = s \xrightarrow{\eta,\beta^\circ}_\circ{}^{M^\circ} s'$, and consequently, $\forall\, t_1 = s \xrightarrow{\eta,\beta_1^\circ}_\wedge s'$, $\exists\, t_2 = s \xrightarrow{\eta,\beta_2^\circ}_{M^\circ} s'$. Now, also $\beta_1^\circ = \beta_2^\circ$ holds as, by def. of $\bigcup^{\mathbb{I}}$, LTS, and γ,

$$\beta_1^\circ = \bigcup^{\mathbb{I}}_{\substack{s \xrightarrow{\eta,\beta^\circ}_\circ s', \\ (S,s_0,\to_\circ)\in\alpha_{\mathcal{LTS}}(\widehat{LTS}(M^\circ))}} \beta^\circ = \left[\min_{\substack{s \xrightarrow{\eta,\beta} s', \\ (S,s_0,\to)\in\widehat{LTS}(M^\circ)}} \beta, \max_{\substack{s \xrightarrow{\eta,\beta} s', \\ (S,s_0,\to)\in\widehat{LTS}(M^\circ)}} \beta\right]$$

$$= \left[\min_{(\mathcal{R},\mathcal{K},s_0)\in\gamma(M^\circ)} k_\eta \times kin(l_\eta, s), \max_{(\mathcal{R},\mathcal{K},s_0)\in\gamma(M^\circ)} k_\eta \times kin(l_\eta, s)\right] = k_\eta^\circ \times kin(l_\eta, s)$$
$$= \beta_2^\circ$$

□

A consequence of the previous Theorem is that $LTS^\circ(M^\circ)$ is a sound approximation of $LTS(M)$, for each M represented by M° (i.e. such that $M \in \gamma(M^\circ)$).

Corollary 3.3.3 (Soundness of LTS°)**.**
$\forall M^\circ \in \mathcal{M}^\circ, \forall M \in \gamma(M^\circ) : \alpha_{\mathcal{LTS}}(LTS(M)) \sqsubseteq_{\mathcal{LTS}^\circ} LTS^\circ(M^\circ)$.

Proof. Follows from $\alpha_{\mathcal{LTS}}(LTS(M)) \sqsubseteq_{\mathcal{LTS}^\circ} \widehat{\alpha}_{\mathcal{LTS}}(\{(LTS(M))|M \in \gamma(M^\circ)\})$.
□

3.3.3 Interval Markov Chains

We use *Interval Discrete-Time Markov Chains* [JL91, KU02] (IMC) to define the probabilistic semantics of abstract systems. We briefly recall the main concepts concerning the validation of probabilistic temporal properties on IMC and we refer the interested reader to [JL91, KU02, FLW06].

Definition 17 (Interval Markov Chain)**.** *An* IMC *is a tuple* (S, s_0, P^-, P^+)*, where:* S *is the* set of states *and* $s_0 \in S$ *the* starting state*;* $P^-, P^+ : S \to PDistr(S)$ *are the* lower and upper probability transition functions *such that* $\forall s, s' \in S$*,* $P^-(s, s') \leq P^+(s, s')$ *and* $\sum_{s''\in S} P^-(s, s'') \leq 1 \leq \sum_{s''\in S} P^+(s, s'')$.

Here, $P^-(s, s')$ and $P^+(s, s')$ define intervals of probabilities, that represent *lower and upper bounds for the transition probabilities* of moving from s to s'. In the following we use $\mathcal{MC}^\circ$ to denote the universe of IMCs.

In an IMC, for any state s, there is a choice for an *admissible distribution* yielding the probabilities to reach successor states. A distribution $\sigma \in Distr(S)$ is admissible for an IMC $mc^\circ = (S, s_0, P^-, P^+)$ and a state $s \in S$, iff, $\forall\, s' \in S$:

$P^-(s,s') \leq \rho(s') \leq P^+(s,s')$. We use $ADistr_{mc^\circ}(s)$ for denoting the admissible distributions for s and mc°. As in *Markov Decision Processes* (MDP), the non-determinism is resolved by schedulers. The notion of path for IMCs is analogous to that presented for DTMCs, and therefore it is convenient to use the same notation.

Definition 18 (Scheduler)**.** *Let $mc^\circ = (S, s_0, P^-, P^+)$ be an IMC. A* scheduler *is a function $\mathbb{S} : FPaths(S) \mapsto ADistr_{mc^\circ}(\pi_{last})$ for each path $\pi \in FPaths(S)$. We use $Adm(mc^\circ)$ for the* set of schedulers on mc°.

Given a scheduler $\mathbb{S} \in Adm(mc^\circ)$ a probability space over paths can be defined analogously as for DTMCs (see Definition 3); $P_s^{\mathbb{S}}$ stands for the probability starting from the state s w.r.t. the scheduler $\mathbb{S}$.

On IMCs, probabilistic reachability properties gives *lower* and *upper bounds*, obtained considering the minimum and maximum probabilities w.r.t. all schedulers.

Definition 19 (Abstract Reachability)**.** *Let $mc^\circ = (S, s_0, P^-, P^+)$ be an IMC. The* lower *and* upper bound *of the probability of reaching a state satisfying a propositional symbol $A \in AP$, starting from $s \in S$, are defined as follows:*

$$Reach^\circ_{A,mc^\circ}(s) = \Big[\inf_{\mathbb{S}\in Adm(mc^\circ)} P_s^{\mathbb{S}}(\{\pi \in C(s) \,|\, \pi[i] \vDash A \text{ for some } i \geq 0\}), \sup_{\mathbb{S}\in Adm(mc^\circ)} P_s^{\mathbb{S}}(\{\pi \in C(s) \,|\, \pi[i] \vDash A \text{ for some } i \geq 0\}) \Big].$$

Similarly as for LTSs, we introduce the concepts necessary to state the soundness and the precision of IMCs.

To relate DTMCs to IMCs, their abstract counterparts, we introduce the *best abstraction* of a DTMC and of *sets of isomorphic DTMCs*.

Two IMCs $mc_i = (S_i, s_{0,i}, P_i), i \in [1,2]$ are isomorphic ($mc_1 \sim mc_2$) iff $S_1 = S_2$ and $s_{0,1} = s_{0,2}$. We denote the universe of *isomorphic DTMC* with $\widetilde{\mathcal{P}}(\mathcal{MC})$.

Definition 20 (Best Abstraction of DTMCs)**.** *We define*

- $\alpha_{\mathcal{MC}} : \mathcal{MC} \mapsto \mathcal{MC}^\circ$ *such that* $\alpha_{\mathcal{MC}}((S, s_0, P)) = (S, s_0, P, P)$
- $\widehat{\alpha}_{\mathcal{MC}} : \widetilde{\mathcal{P}}(\mathcal{MC}) \to \mathcal{MC}^\circ$ *such that* $\widehat{\alpha}_{\mathcal{MC}}(X) \equiv (S(X), s_0(X), P^-_\wedge, P^+_\wedge)$ *and* $\forall s, s' \in S(X)$, $P^+_\wedge(s,s') \equiv \max_{(S,P,s_0)\in X} P(s,s')$, $P^-_\wedge(s,s') \equiv \min_{(S,P,s_0)\in X} P(s,s')$.

As for LTS with $\alpha_{\mathcal{LTS}}$, $\alpha_{\mathcal{MC}}$ does not introduce any approximation. Thus, the probabilities derived by $\alpha_{\mathcal{MC}}$ are exact: $\forall A \in AP, mc \in \mathcal{MC} : [Reach_{A,mc}(s_0)]^\bullet = Reach^\circ_{A,\alpha_{\mathcal{MC}}(mc)}(s_0)$. Conversely, $\widehat{\alpha}_{\mathcal{MC}}$, given a set of isomorphic DTMC, reports, for each pair of states in the shared state space, the minimum and the maximum transition probability with respect to all the DTMC.

Moreover, we introduce an approximation order $\sqsubseteq_{\mathcal{MC}^\circ}$, similar to [CGL09, DJJL01].

Definition 21 (Order on IMCs)**.** *Let $mc_i^\circ = (S, s_0, P_i^-, P_i^+), i \in \{1,2\}$, two IMCs. We say that $mc_1^\circ \sqsubseteq_{\mathcal{MC}^\circ} mc_2^\circ$ iff $\forall s \in S$, $ADistr_{mc_1^\circ}(s) \subseteq ADistr_{mc_2^\circ}(s)$.*

Intuitively, we say that $mc_1^\circ \sqsubseteq_{\mathcal{MC}^\circ} mc_2^\circ$ iff, for each state, the set of admissible distributions of the state in ${mc_1}^\circ$ is included in the set of admissible distributions of the state in ${mc_2}^\circ$.

The following theorem states the soundness of the order on IMCs for probabilistic reachability. In particular, $mc_1^\circ \sqsubseteq_{\mathcal{MC}^\circ} mc_2^\circ$ guarantees that the lower and upper bounds for probabilistic reachability obtained for mc_1 are included in the ones obtained for mc_2.

Theorem 3.3.4. *Let $mc_i^\circ = (S, s_0, P_i^-, P_i^+), i \in \{1,2\}$, two IMCs. If $mc_1^\circ \sqsubseteq_{\mathcal{MC}^\circ} mc_2^\circ$ then $\forall A \in AP$, $s \in S : Reach^\circ_{A,mc_2^\circ}(s) \sqsubseteq_{\mathbb{I}} Reach^\circ_{A,mc_1^\circ}(s)$.*

Proof. We examine only the case $[Reach_{A,mc_2^\circ}(s)]^- \leq [Reach_{A,mc_1^\circ}(s)]^-$.
From $mc_1^\circ \sqsubseteq_{\mathcal{MC}^\circ} mc_2^\circ$ it follows that $ADistr_{mc_1^\circ}(s) \subseteq ADistr_{mc_2^\circ}(s)$.

In order to simplify the proof it is convenient to exploit the fact that $Reach^-_{A,mc^\circ}(s)$ can be specified as a linear equations system [CGL09, DJJL01, Kwi03, FLW06]. In particular, for $h \in \{1,2\}$, $[Reach_{A,mc_h^\circ}(s)]^- = \bigcup_{i \in \{0,\infty\}} \rho^{-,i}_{A,mc_h^\circ}(s)$ where

$$\rho^{-,i}_{A,mc_h^\circ}(s) = \begin{cases} 1 & \text{if } s \vDash A, \\ 0 & \text{if } i = 0 \wedge s \nvDash A, \\ \inf\limits_{\rho_{j_h} \in ADistr_{mc_h^\circ}(s)} \sum\limits_{s' \in S} \rho_{j_h}(s') \times \rho^{-,i-1}_{A,mc_h^\circ}(s') & \text{otherwise.} \end{cases}$$

and where $\bigcup$ stands for the least upper bound with respect to the underlying order on pseudo-distributions, e.g. $\rho_1 \subseteq \rho_2$ iff for each s, $\rho_1(s) \leq \rho_2(s)$.

Intuitively, $\rho^{-,i}_{A,mc_h^\circ}(s)$ reports the minimum probability to reach a state satisfying A, starting from s, after i-iterates.

Therefore, it is enough to show that $\rho^{-,i}_{A,mc_2^\circ}(s) \leq \rho^{-,i}_{A,mc_1^\circ}(s)$, for every $i \geq 0$. The proof proceeds by induction.

($i = 0$) There are two possibilities for $\rho^{-,0}_{A,mc^\circ_2}(s)$. Either $s \vDash A$ and result is 1 or $s \nvDash A$ and the result is zero. Both the cases are trivial as $\rho^{-,0}_{A,mc^\circ_2}(s) = \rho^{-,0}_{A,mc^\circ_1}(s)$.

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

$$\rho^{-,i}_{A,mc^\circ_2}(s) = \inf_{\rho_{j_2} \in ADistr_{mc^\circ_2}(s)} \sum_{s' \in S} \rho_{j_2}(s') \times \rho^{-,i-1}_{A,mc^\circ_2}(s') \tag{3.3}$$

The case of $s \vDash A$ is trivial, as we have explained in the case of $i = 0$. In case (3.3), we observe that for $\rho^{-,i}_{A,mc^\circ_1}(s)$ the result is

$$\rho^{-,i}_{A,mc^\circ_1}(s) = \inf_{\rho_{j_1} \in ADistr_{mc^\circ_1}(s)} \sum_{s' \in S} \rho_{j_1}(s') \times \rho^{-,i-1}_{A,mc^\circ_1}(s') \tag{3.4}$$

In this case we have to compare (3.3) and (3.4). By inductive hypothesis we have that $\rho^{-,i-1}_{A,mc^\circ_2}(s') \leq \rho^{-,i-1}_{A,mc^\circ_1}(s')$, so that we reduce to show

$$\inf_{\rho_{j_2} \in ADistr_{mc^\circ_2}(s)} \sum_{s' \in S} \rho_{j_2}(s') \leq \inf_{\rho_{j_1} \in ADistr_{mc^\circ_1}(s)} \sum_{s' \in S} \rho_{j_1}(s') \,.$$

This is guaranteed by the fact that $ADistr_{mc^\circ_1}(s) \subseteq ADistr_{mc^\circ_2}(s)$.

□

3.3.4 Derivation of Abstract Probabilistic Semantics

We define the abstract probabilistic translation function $\mathcal{H}^\circ : \mathcal{LTS}^\circ \to \mathcal{MC}^\circ$. Moreover, we prove the soundness and precision of the abstract probabilistic semantics using the notions of Section 3.3.3.

The abstract LTS reports on transitions the number of the rule which is applied and the interval representing a possible range for its rate. From this information, both lower and upper bounds for the probabilities of moving from a state to another can be calculated. Following the guidelines of the derivation of the DTMC from the concrete LTS, we introduce $R^\circ : S \times S \mapsto \mathbb{I}$, and $E^\circ : S \mapsto \mathbb{I}$ s.t. $\forall s, s' \in S$

$$R^\circ(s, s') = \sum_{t \in TS(s,s')}^{\mathbb{I}} rate^\circ(t) \text{ and } E^\circ(s) = \sum_{s' \in S}^{\mathbb{I}} R^\circ(s, s').$$

Intuitively, $R^\circ(s, s')$ reports the interval of rates corresponding to the move from s to s', while $E^\circ(s)$ is the abstract exit rate.

For all states s and $s' \in S$, both lower and upper bounds of the probability of moving from s to s' can be determined by exploiting $R^\circ(s, s')$ and $E^\circ(s)$. For these purposes we need to consider the *worst case* and *best case* scenario, respectively. That is, the transition to be maximized (minimized) takes as rate value its upper (lower) bound and all the others take their lower (upper) bound. This reasoning has to be properly combined with the special cases when $[E^\circ(s)]^+ = 0$ (the state s is stable) or $[E^\circ(s)]^- = 0$ (the state s is stable for some values of kinetic constant of some rules).

Definition 22 (Abstract Probabilistic Translation Function)**.** *We define* $\mathcal{H}^\circ : \mathcal{LTS}^\circ \to \mathcal{MC}^\circ$ *such that* $\mathcal{H}^\circ((S, s_0, \to^\circ)) = (S, s_0, P^-, P^+)$*, where* $P^-, P^+ : S \to PDistr(S)$ *are obtained, for each* $s, s' \in S$, $s \neq s'$*, as follows:*

- *if* $[E^\circ(s)]^+ = 0$*,*
  then $P^+(s, s') = P^-(s, s') = 0$*,* $P^+(s, s) = P^-(s, s) = 1$*;*
- *if* $[E^\circ(s)]^+ > 0$*,*
  then
  - *(a) if* $[E^\circ(s)]^- = 0$*, then* $P^+(s, s) = 1$*,* $P^-(s, s) = 0$
  - *(b) if* $[R^\circ(s, s')]^- = 0$*, then* $P^-(s, s') = 0$ *else*
    $P^-(s, s') = [R^\circ(s, s')]^- / ([R^\circ(s, s')]^- + \sum_{s'' \in S, s'' \neq s'} [R^\circ(s, s'')]^+)$
  - *(c) if* $[R^\circ(s, s')]^+ = 0$*, then* $P^+(s, s') = 0$ *else*
    $P^+(s, s') = [R^\circ(s, s')]^+ / ([R^\circ(s, s')]^+ + \sum_{s'' \in S, s'' \neq s'} [R^\circ(s, s'')]^-)$.

The following theorem states that the approximation order over abstract LTSs is preserved by the translation to IMCs.

Theorem 3.3.5. *Let* $lts_i^\circ = (S, s_0, \to_\circ^i), i \in \{1, 2\}$*, be s.t.* $lts_1^\circ \sqsubseteq_{\mathcal{LTS}^\circ} lts_2^\circ$*. We have that* $\mathcal{H}^\circ(lts_1^\circ) \sqsubseteq_{\mathcal{MC}^\circ} \mathcal{H}^\circ(lts_2^\circ)$*.*

Proof. From $lts_1^\circ \sqsubseteq_{\mathcal{LTS}^\circ} lts_2^\circ$ we have that $\forall s, s' \in S$

$$\forall t_1^\circ = (s \xrightarrow{\eta, \beta_1^\circ}_\circ s') \in \to_\circ^1, \ \exists\, t_2^\circ = (s \xrightarrow{\eta, \beta_2^\circ}_\circ s') \in \to_\circ^2 \text{ such that } \beta_1^\circ \sqsubseteq_{\mathbb{I}} \beta_2^\circ . \quad (3.5)$$

We have to prove that (3.5) $\Rightarrow ADistr_{\mathcal{H}^\circ(lts_1^\circ)}(s) \subseteq ADistr_{\mathcal{H}^\circ(lts_2^\circ)}(s)$.

By Def. 22 of $\mathcal{H}^\circ$, for $i \in \{1, 2\}$, $\mathcal{H}^\circ(lts_i^\circ) = (S, s_0, P_i^-, P_i^+,)$. Moreover, $ADistr_{\mathcal{H}^\circ(lts_i^\circ)}(s) = \rho_i$ s.t. $\forall s' \in Next(s) : P_i^-(s, s') \leq \rho_i(s') \leq P_i^+(s, s')$.

We have that P_i^+, P_i^-, are defined, according to $\mathcal{H}^\circ$, maximizing and minimizing $R^\circ(s,s')/E^\circ(s)$. Namely, for the general case we have that,
$P_i^-(s,s') = [R^\circ(s,s')]^- / ([R^\circ(s,s')]^- + \sum_{s'' \in S, s'' \neq s'} [R^\circ(s,s'')]^+) =$
$[\sum^{\mathbb{I}}_{s \xrightarrow{\eta,\beta^\circ}_\circ \in \to^i_\circ s'} \beta^\circ]^+ / ([\sum^{\mathbb{I}}_{s \xrightarrow{\eta,\beta^\circ}_\circ \in \to^i_\circ s'} \beta^\circ]^+ + \sum_{s'' \in S, s'' \neq s'} [\sum_{s \xrightarrow{\eta',\beta^\circ}_\circ s'' \in \to^i_\circ} \beta^\circ]^-)$.
By (3.5), we have that $P_1^-(s,s') \leq P_2^-(s,s')$ and, for the same reasoning on P_1^+, $P_1^+(s,s') \geq P_2^+(s,s')$. Similarly, for the special cases, when $[E^\circ(s)]^+ = 0$ or $[E^\circ(s')]^- = 0$, by (3.5) we have that $P_1^- = P_2^-$ and $P_1^+ = P_2^+$.

Thus $\forall s \in S$, $ADistr_{\mathcal{H}^\circ(lts_1^\circ)}(s) \subseteq ADistr_{\mathcal{H}^\circ(lts_2^\circ)}(s)$. □

The following theorems show the soundness and the precision of the IMC obtained by our approach. Specifically, we relate the IMC $\mathcal{H}^\circ(LTS^\circ(M^\circ))$ with the DTMC $\mathcal{H}(LTS(M))$ for each M represented by M°. Following the same reasoning done for LTSs, we exploit the abstraction functions $\alpha_{\mathcal{MC}}$ and $\widehat{\alpha}_{\mathcal{MC}}$, reporting the best abstraction of a DTMC and of a set of isomorphic DTMC, respectively.

To prove the main theorem, we introduce the following lemma, stating that $\alpha_{\mathcal{MC}} \circ \mathcal{H} = \mathcal{H}^\circ \circ \alpha_{\mathcal{LTS}}$.

Lemma 3.3.6. $\forall M \in \mathcal{M}$, $\alpha_{\mathcal{MC}}(\mathcal{H}(LTS(M))) = \mathcal{H}^\circ(\alpha_{\mathcal{LTS}}(LTS(M)))$.

Proof. Let $M = (\mathcal{R}, \mathcal{K}, s_0)$, $LTS(M) = (S, s_0, \to)$. We have $\mathcal{H}(LTS(M)) = (S, s_0, P)$ and $\alpha_{\mathcal{MC}}(\mathcal{H}(LTS(M))) = (S, s_0, P, P)$.

On the other hand we have $\alpha_{\mathcal{LTS}}(LTS(M)) = (S, s_0, \to^\alpha_\circ)$ where
$\to^\alpha_\circ = \{s' \xrightarrow{\eta,\beta^\bullet}_\circ s'' \mid s' \xrightarrow{\eta,\beta} s'' \in \to\}$ and $\mathcal{H}^\circ(\alpha_{\mathcal{LTS}}(LTS(M))) = (S, s_0, P, P)$. □

The following theorem shows that $\mathcal{H}^\circ(LTS^\circ(M^\circ))$ coincides with the best abstraction, obtained by means of $\widehat{\alpha}_{\mathcal{MC}}$, of the set of isomorphic DTMCs $\{\mathcal{H}(LTS(M)) | M \in \gamma(M^\circ)\}$. As a consequence, $\mathcal{H}^\circ(LTS^\circ(M^\circ))$ is also a sound approximation of each DTMC $\mathcal{H}(LTS(M))$ such that $M \in \gamma(M^\circ)$ (as stated by Corollary 3.3.8).

Theorem 3.3.7 (Precision of $\mathcal{H}^\circ$)**.**
$\forall M^\circ \in \mathcal{M}^\circ : \widehat{\alpha}_{\mathcal{MC}}(\{\mathcal{H}(LTS(M)) | M \in \gamma(M^\circ)\}) = \mathcal{H}^\circ(LTS^\circ(M^\circ))$.

Proof. Let $\widehat{\mathcal{H}}(M^\circ) = \{\mathcal{H}(LTS(M)) | M \in \gamma(M^\circ)\}$ and $\widehat{LTS}(M^\circ) = \{LTS(M) | M \in \gamma(M^\circ)\}$. By Theorem 3.3.2 it is enough to prove $\widehat{\alpha}_{\mathcal{MC}}(\widehat{\mathcal{H}}(M^\circ)) = \mathcal{H}^\circ(\widehat{\alpha}_{\mathcal{LTS}}(\widehat{LTS}(M^\circ)))$.
Here $\widehat{\alpha}_{\mathcal{MC}}(\widehat{\mathcal{H}}(M^\circ)) = (S, s_0, P^-_\wedge, P^+_\wedge)$ and $\mathcal{H}^\circ(\widehat{\alpha}_{\mathcal{LTS}}(\widehat{LTS}(M^\circ))) = (S, s_0, P^-, P^+)$.

We show that $P^+_\wedge = P^+$; the same reasoning applies to $P^-_\wedge = P^-$.

By definition of $\widehat{\alpha}_{\mathcal{MC}}$ and $\mathcal{H}$, we have for the general case that, $\forall s, s' \in S$,

$$
\begin{aligned}
P^{+}_{\wedge}(s,s') &\equiv \max_{(S,P,s_0)\in\widehat{\mathcal{H}}(M^\circ)} P(s,s') \\
&= \max_{(S,s_0,\rightarrow)\in\widehat{LTS}(M^\circ)} R(s,s')/(R(s,s') + \sum_{s''\neq s'} R(s,s'')) \\
&= \max_{(S,s_0,\rightarrow)\in\widehat{LTS}(M^\circ)} \Big(\sum_{(s\xrightarrow{\eta,\beta}s')\in\rightarrow} \beta\Big)/\Big(\sum_{(s\xrightarrow{\eta,\beta}s')\in\rightarrow} \beta + \sum_{(s\xrightarrow{\eta',\beta}s'')\in\rightarrow,\, s'\neq s''} \beta\Big). \quad (3.6)
\end{aligned}
$$

Moreover, by definition of $\mathcal{H}^\circ$, we have for the general case that, $\forall s, s' \in S$,

$$
\begin{aligned}
&P^{+}(s,s') \equiv [R^\circ(s,s')]^{+}/([R^\circ(s,s')]^{+} + \textstyle\sum_{s''\in S,\, s''\neq s'} [R^\circ(s,s'')]^{-}) = \\
&\quad \Big[\sum^{\mathbb{I}}_{s\xrightarrow{\eta,\beta^\circ}_{\wedge_\circ} s'} \beta^\circ\Big]^{+}/\Big(\Big[\sum^{\mathbb{I}}_{s\xrightarrow{\eta,\beta^\circ}_{\wedge_\circ} s'} \beta^\circ\Big]^{+} + \textstyle\sum_{s''\in S,\, s''\neq s'} \Big[\sum_{s\xrightarrow{\eta',\beta^\circ}_{\wedge_\circ} s''} \beta^\circ\Big]^{-}\Big) = \\
&\qquad \sum_{s\xrightarrow{\eta,\beta^\circ}_{\wedge_\circ} s'} [\beta^\circ]^{+}/\Big(\sum_{s\xrightarrow{\eta,\beta^\circ}_{\wedge_\circ} s'} [\beta^\circ]^{+} + \sum_{s\xrightarrow{\eta',\beta^\circ}_{\wedge_\circ} s'',\, s'\neq s''} [\beta^\circ]^{-}\Big). \quad (3.7)
\end{aligned}
$$

For the general case, it remains to prove that (3.6) = (3.7), that is true by the fact that maximizing $a/(a+b)$ corresponds to maximize a and minimize b, and by definition of γ, which ensures that the maximum in $\widehat{LTS}(M^\circ)$ of $\sum_{(s\xrightarrow{\eta,\beta}s')\in\rightarrow} \beta$ is equal to $\sum_{s\xrightarrow{\eta,\beta^\circ}_{\wedge_\circ} s'} [\beta^\circ]^{+}$ and the minimum $\widehat{LTS}(M^\circ)$ of $\sum_{(s\xrightarrow{\eta',\beta}s'')\in\rightarrow, s'\neq s''} \beta$ is equal to $\sum_{s''\in S, s''\neq s'}$ of $\big[\sum_{s\xrightarrow{\eta',\beta^\circ}_{\wedge_\circ} s''} \beta^\circ\big]^{-}$) . The special cases in which either $P^{+}(s,s') = 1$ and $s = s'$ or $P^{+}(s,s') = 0$ and $s \neq s'$ are trivial. □

Corollary 3.3.8 (Soundness of $\mathcal{H}^\circ$)**.**
$\forall M^\circ \in \mathcal{M}^\circ,\ M \in \gamma(M^\circ) :\ \alpha_{\mathcal{MC}}(\mathcal{H}(LTS(M))) \sqsubseteq_{\mathcal{MC}^\circ} \mathcal{H}^\circ(LTS^\circ(M^\circ))$.

Proof. Follows from $\alpha_{\mathcal{MC}}(\mathcal{H}(LTS(M))) \sqsubseteq_{\mathcal{MC}^\circ} \widehat{\alpha}_{\mathcal{MC}}(\{\mathcal{H}(LTS(M))|M \in \gamma(M^\circ)\})$. □

The following theorem states our main result: the soundness and precision results on IMC are lifted to probabilistic reachability, that is the lower and upper bounds of probabilistic reachability we obtain on $\mathcal{H}^\circ(LTS^\circ(M^\circ))$ are exactly the most precise values which are correct. Indeed, they correspond to the minimum and the maximum of the concrete probabilities corresponding to each concrete system M represented by M°.

Theorem 3.3.9.
$\bigcup^{\mathbb{I}}_{mc\in\{\mathcal{H}(LTS(M))|M\in\gamma(M^\circ)\}}[Reach_{A,mc}(s)]^\bullet = Reach^\circ_{A,\mathcal{H}^\circ(LTS^\circ(M^\circ))}(s)$.

Sketch of proof. In the definition of $Reach^\circ_{A,mc^\circ}(s)$ the probability of a path is computed by associating each step from a state s to a state s' in the path with a probability taken form one of the admissible distributions for s and mc°. The proof reduces to show that for each state s of both $\widehat{\alpha}_{\mathcal{MC}}$ and $\mathcal{H}^\circ(LTS^\circ(M^\circ))$, we have that
$(\exists M \in \gamma(M^\circ)$ s.t. $(\mathcal{H}(LTS(M)) = (S, s_0, P) \wedge P(s) = \rho)) \Leftrightarrow \rho \in ADistr_{\mathcal{H}^\circ(LTS^\circ(M^\circ))}(s)$. The implication $\Rightarrow$ follows from $M \in \gamma(M^\circ)$ and Theorem 3.3.7. The implication $\Leftarrow$ follows from the definition of γ, $\gamma(M^\circ)$ contains a concrete model M for each possible combination of values chosen from the intervals of M°, and from the fact that LTS° and $\mathcal{H}^\circ$ do not introduce admissible distribution that are not present in any $\mathcal{H}(LTS(M))$. □

Finally, we conclude that the IMC, derived from the abstract LTS of an abstract system M°, gives *conservative bounds* for probability of reachability properties for each concrete system $M \in \gamma(M^\circ)$.

Theorem 3.3.10. $\forall M \in \gamma(M^\circ), A \in AP, s \in S(\mathcal{LTS}(M))$,

$$[Reach_{A,\mathcal{H}(\mathcal{LTS}(M))}(s)]^\bullet \sqsubseteq_{\mathbb{I}} Reach^\circ_{A,\mathcal{H}^\circ(\mathcal{LTS}^\circ(M^\circ))}(s)\,.$$

Proof.
From Theorem 3.3.2 and 3.3.5, $\mathcal{H}^\circ(\alpha_{\mathcal{LTS}^\circ}(\mathcal{LTS}(M))) \sqsubseteq_{\mathcal{MC}^\circ} \mathcal{H}^\circ(\mathcal{LTS}^\circ(M^\circ))$.
From Lemma 3.3.6, $\alpha_{\mathcal{MC}}(\mathcal{H}(\mathcal{LTS}(M))) \sqsubseteq_{\mathcal{MC}^\circ} \mathcal{H}^\circ(\mathcal{LTS}^\circ(M^\circ))$.
By Theorem 3.3.4, $Reach^\circ_{A,\alpha_{\mathcal{MC}}(\mathcal{H}(\mathcal{LTS}(M)))}(s) \sqsubseteq_{\mathbb{I}} Reach^\circ_{A,\mathcal{H}^\circ(\mathcal{LTS}^\circ(M^\circ))}(s)$ and finally, by Definition 20, $[Reach_{A,\mathcal{H}(\mathcal{LTS}(M)))}(s)]^\bullet \sqsubseteq_{\mathbb{I}} Reach_{A,\mathcal{H}^\circ(\mathcal{LTS}^\circ(M^\circ))}(s)$. □

Example 3 (Abstract System Model Checking)**.** *We consider the system of reactions introduced in Example 2. In this case, we assume that the kinetic rates of the rules are not exact, but described by intervals. For instance, we consider the abstract system* $M^\circ_{ex} = (\mathcal{R}, \mathcal{K}^\circ, s_0)$ *where* $\mathcal{R}$ *and* s_0 *are the same of Example 2, while* $\mathcal{K}^\circ = \{k^\circ_1 = [1,5], k^\circ_2 = [1,5]\}$*. Note that the concrete system* M_{ex} *of Example 2 is one of the systems represented by* M°_{ex}*, i.e.* $M_{ex} \in \gamma(M^\circ_{ex})$*.*

Figure 3.3 shows $LTS^\circ(M^\circ_{ex})$ *and* $\mathcal{H}^\circ(LTS^\circ(M^\circ_{ex}))$*, where the state space S is the same of Example 2. By computing the probability of obtaining at least two complexes XY, we obtain* $[4/104, 1/2] \times^{\mathbb{I}} [1/51, 1/3] = [1/1326, 1/6]$*: the concentration of reagent W makes the degradation more likely to happen than the binding of reagent X and Y. This result shows that the abstraction is precise*

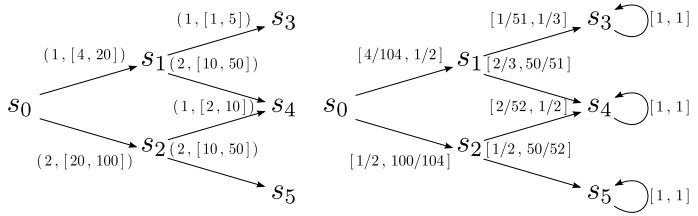


Figure 3.3: $LTS^{\circ}(M^{\circ}_{ex})$ and $\mathcal{H}^{\circ}(LTS^{\circ}(M^{\circ}_{ex}))$.

enough to observe the same behavior of Example 2, even with imprecise reaction rates.

3.4 Case Study: Tumor Cell Growth

We briefly present the application of the proposed approach to a model of tumor growth, proposed by Villasana and Radunskaya and studied with Delay Differential Equations (DDEs) in [VR03].

Tumor growth is based on cell divisions (or *mitosis*). The cell cycle is the process between two mitosis, and it consists of four phases: the G_1 phase (a resting phase or gap period), the S phase where the replication of DNA occurs, the G_2 gap period, and the mitosis phase M in which the cells segregate the duplicated sets of chromosomes between daughter cells. The three phases G_1, S, and G_2 constitute the pre-mitotic phase, also called *inter-phase*.

The simplest model proposed in [VR03] considers two populations of tumor cells: the population of tumor cells during cell cycle inter-phase, and the population of tumor cells during mitosis. Such a model can be expressed as the following reactions:

$$\mathcal{R} = \{R_1 : T_I \xrightarrow{a_1} T_M\,, \quad R_2 : T_M \xrightarrow{a_4} 2T_I\,, \quad R_3 : T_I \xrightarrow{d_2}, \quad R_4 : T_M \xrightarrow{d_3} \quad \}$$

where T_I and T_M are tumor cells in inter-phase and in mitosis, respectively. Reaction R_1 represents the passage of a tumor cell from the inter-phase to the mitosis phase, R_2 represents the mitosis, whereas R_3 and R_4 represent tumor cell death.

Let d be the rate at which mitotic cells disappear, namely $d = d_3 + a_4$. Figure 3.4 shows the results of the analytical study of the DDEs model, by setting the parameters a_4 and d_2 to 0.5 and 0.3, respectively, and by varying a_1 and d.

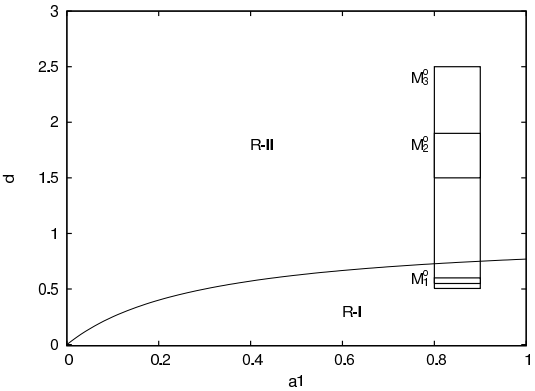


Figure 3.4: The regions which describe the different behaviors of the DDEs model by varying parameters a_1 and d.

There are two regions. The region in which the tumor grows is R-I, while in R-II both kinds of tumor cells disappear. A concrete probabilistic model of tumor growth could be trivially obtained from reactions $\mathcal{R}$. We have constructed three abstract systems of tumor growth, M_1°, M_2° and M_3°, by replacing rates in the reactions with intervals. Actually, in all the three systems we have replaced a_1 with $[0.8, 0.9]$, a_4 with $0.5^\bullet$, d_2 with $0.3^\bullet$. Concerning d_3, we have replaced it with $[0.05, 0.1], [1, 1.4]$ and $[0.005, 2]$ in M_1°, M_2° and M_3°, respectively. This corresponds to considering a region in R-I, a region in R-II and a region across the line separating R-I and R-II (see Figure 3.4). Moreover, we have considered an initial population consisting of 10 tumor cells in inter-phase and 10 tumor cells in mitosis.

Formally, $M_i^\circ = (\mathcal{R}, \mathcal{K}_i^\circ, s_0)$, with $i \in \{1, 2, 3\}$, where $s_0 = \{(T_I, 10), (T_M, 10)\}$,

$$\mathcal{K}_i^\circ = [[0.8, 0.9]; 0, 5^\bullet; 0, 3^\bullet; d_3^i],$$

$$\text{where } d_3^1 = [0.05, 0.1], d_3^2 = [1, 1.4], d_3^3 = [0.005, 2].$$

In order to perform model checking on the abstract systems we have developed a translator [AMS] of abstract MSR semantics into equivalent MDP by following the extreme distribution approach of [FLW06]. In particular, it computes in effective way the extreme distributions from intervals of probability reported by the IMC probabilistic semantics of the system. The tool invokes PRISM [PRI] for the verification of the properties on the corresponding MDP

model. Moreover, in order to obtain a finite MDP, we have, heuristically, limited the number of states of the model to 10^4. Specifically, we generate states with a breadth-first approach, starting with s_0 and we put a deadlock loop on states when we reached a number of states equal to 10^4. As states on this border correspond to system configurations with a very big number of individuals, even if this artifact affects the behavior of the system, its effect on probability of studied reachability properties, where we test states with at most 20 individuals, is minimal.

In Figure 3.5 we show the results of model checking of property $Reach^{\circ}(T_M = x)$ in M_1°, M_2° and M_3° by varying x. In M_1° both the minimum and the maximum probabilities tend to zero for small values of x while they are both equal to 1 for values greater than or equal to 10 (the initial value of T_M). In M_2° it holds the opposite. In M_3° we have that both probabilities are equal to 1 when x is 10, but they tend to the interval $[0, 1]$, namely to complete uncertainty, both for greater and smaller values of x. A more immediate representation of systems dynamic behavior can be obtained plotting $Reach(T_M = y \wedge time = x)$, where *time* is the number of steps of the path that reaches a state satisfying $T_M = y$ (Figure 3.6).

The obtained results agree with the analytic ones: the results on M_1° describe tumor growth, those on M_2° describe tumor decay, those on M_3° leave uncertainty.

Our approach is more precise with respect to analytic studies, as it looks at all possible behaviors of the modelled system, rather than a single average behavior. Moreover, a more realistic discrete probabilistic semantics is considered, instead of a continuous deterministic one.

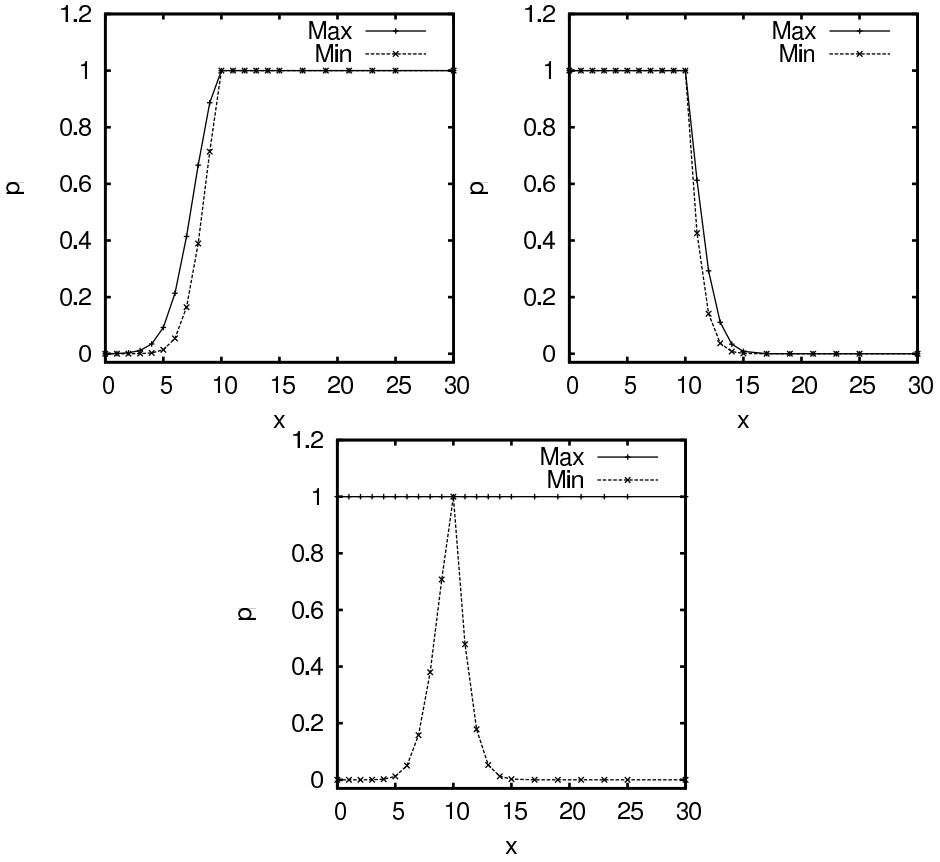


Figure 3.5: Model checking of $Reach^{\circ}(T_M = x)$ in, M_1° (top left), M_2° (top right), M_3° (bottom).

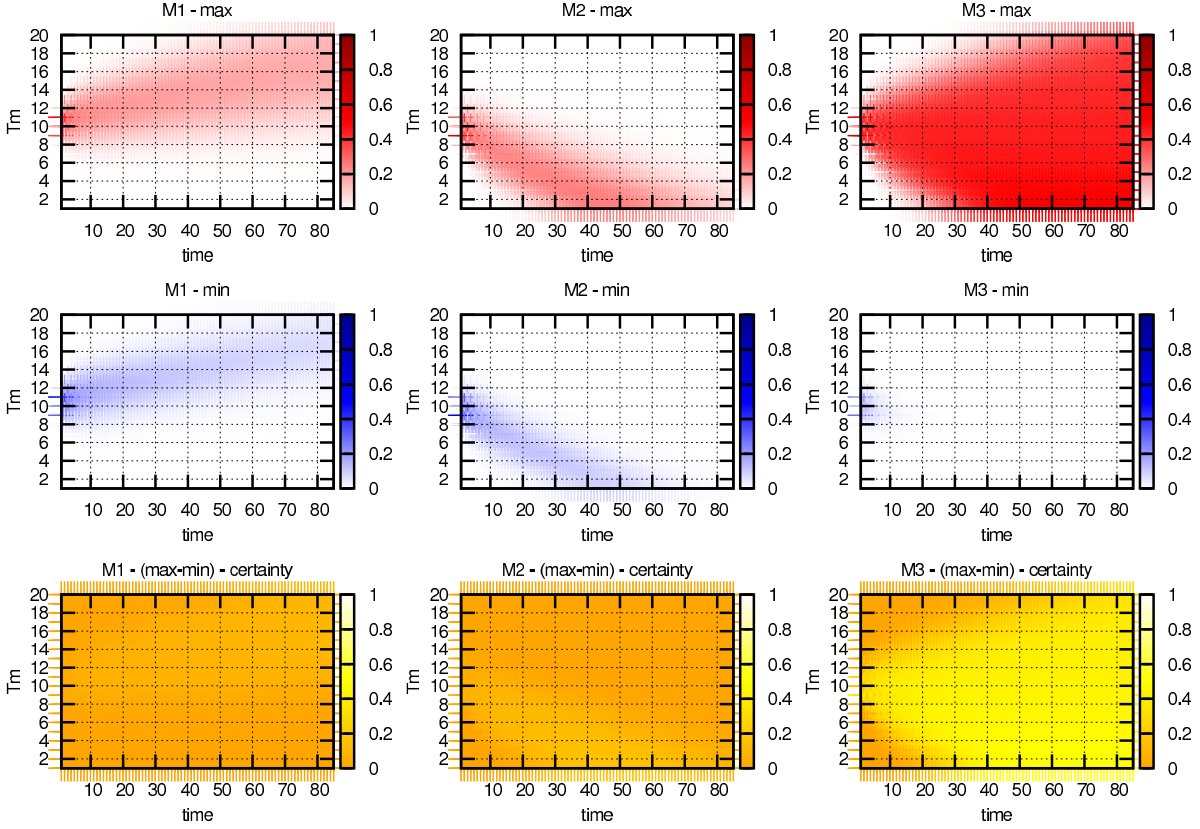


Figure 3.6: Model checking of $Reach(T_M = y \wedge time = x)$ in, from left to right, $M_1^\circ, M_2^\circ, M_3^\circ$. The probability is expressed by color intensity. The plots of $[Reach]^+$, $[Reach]^-$ and $[Reach]^+ - [Reach]^-$ are shown from top to down.

3.5 Comparison with Related Works

The abstraction of probabilistic semantics has been widely studied over the last few years.

The approaches of [FLW06, DJJL01, SVA, Hut05, Šku06, Šku09] present similar abstractions of probabilistic systems, using MDP or IMC. The abstractions are designed for dealing with the traditional state explosion problem. In particular, the abstract model is derived from the concrete one (a DTMC), by partitioning the concrete state space and by calculating the abstract probability distributions directly from the concrete ones. Others approaches aimed to fight state explosion problem are those based on infinite state abstraction [HHWZ10], predicate abstraction [WZH07, KKNP08], symmetry reduction [DMP07] or counter example driven abstraction refinement [HWZ08]. We refer to [KKLW07a, KKLW07b, Kli10] for a more detailed discussion of abstraction of probabilistic and stochastic systems.

We use abstraction techniques in a different way in order to deal with the uncertainty about kinetic rates, typical of biological system modelling. In our context the abstract probabilistic model (IMC), representing an infinite set of concrete models with different kinetic rates, is calculated in effective way from an LTS semantics.

A similar approach, is presented in [CGL09, GL09] to validate probabilistic temporal properties of biological systems. The analysis computes an IMC by approximating the multiplicity of individuals, present in a state, using intervals of integers.

The proposal of [DFF$^+$08, DFFK08] applies abstract interpretation techniques, in the context of formal studies of biological systems, to compute efficiently a superset of reachable complexes, and to generates smaller systems of differential equations from the concrete one.

Finally, [Mon05, DPW00] investigate the application of abstract interpretation into the context of standard concurrent probabilistic programming languages.

3.6 Conclusions

In this Chapter we have considered biological systems modelled by MSR, where rewriting rules, corresponding to reactions, are enriched by real valued kinetic constraints. Our framework supports probabilistic model checking of MSR

systems with uncertain kinetic rates. Model checking an abstract system gives conservative probabilistic bounds with respect to the (infinite) set of concrete models which are abstracted. This approach allows us to safely and effectively manage in a finite way the semantics of an infinite set of (finite) systems. Moreover results obtained on an abstract system are exactly the most precise values which are correct. Indeed, they corresponds to the minimum and the maximum of the concrete probability values corresponding to each concrete system represented by an abstract one.

We have developed an automatic verifier of abstract systems [AMS]: the tool, based on PRISM [PRI], uses a translation (similar to that of [FLW06]) of an abstract probabilistic model (IMC) into a MDP. This translation has exponential complexity as it requires the computation of all the extreme distributions whose number grows exponentially with the number of uncertain parameters. More efficient algorithms, which calculate the extreme distributions on-the-fly, could be applied (see [FLW06, SVA]). Also the use of approximated verification approach presented by [HP09] can be used.

We apply the presented approach to a model of tumor growth [VR03], obtaining more precise results than the ones obtained with analytical studies.

With regard to future development of our work, since in the presented case study we made use of an ad-hoc techniques to deal with infinite state space, would be interesting to combine the proposed approach, dealing with uncertainty of kinetic rates, with abstraction approaches dealing with infinite systems with infinite state space [BLO98, CK01, MP08, HHWZ09].

Moreover, we plan to investigate the extension of our methodology to the abstraction of Continuous-Time Markov Chains (CTMC), for example by following the approach of [KKLW07a], based on uniform CTMC [BKHW05]. In particular, from transition rates of LTSs it is possible to derive uniform CTMC of the form $(S, s_0, P^-, P^+, E_{unif})$. On such a structure, the *uniform exit rate* E_{unif} can be computed as $E_{unif} \geq \max_{s \in S} [E(s)]^+$ and, consequently, continuous time rates can be defined as $P(s, s') = [[R^\circ(s, s')]^- / E_{unif}\ ,\ [R^\circ(s, s')]^+ / E_{unif}]$ and $P(s, s) = [1 - \sum_{s' \in S} P^-(s, s')\ ,\ 1 - \sum_{s' \in S} P^+(s, s')]$.

Special cases are when: (a) $[E(s)]^+ = 0$ and then $P(s, s) = [1, 1]$ and $P(s, s') = [0, 0]$; (b) $[E(s)]^- = 0$ and then $[P(s, s)]^+ = 1$; (c) $[R(s, s')]^+ = 0$ and then $P(s, s') = [0, 0]$; (d) $[R(s, s')]^- = 0$ and then $[P(s, s')]^- = 0$.

Chapter 4

Maximally Parallel Probabilistic Semantics for Multiset Rewriting

Maximally parallel semantics have been proposed for many formalisms as an alternative to the standard interleaving semantics for some modelling scenarios. Nevertheless, in the probabilistic setting an affirmed interpretation of maximal parallelism still lacks.

In this chapter, we define a synchronous maximally parallel probabilistic semantics for Multiset Rewriting tailored to describe, simulate and verify systems evolving with maximally parallel steps. Each step of the proposed semantics is *parallel*: each reaction can happen multiple times; and it is *maximal* as it leaves no enabled reaction i.e. as many reactions as possible are executed. We define a maximally parallel probabilistic semantics in terms of *Discrete Time Markov Chain* for systems described by stochastic Multiset Rewriting. We propose a simple, maximally parallel, model of *Caenorhabditis elegans* vulval development on which we show probabilistic simulations results.

4.1 Introduction

Multiset Rewriting is used to model the dynamic behavior of systems composed by unstructured objects, each of which may come in contact with each other,

taking part in interactions described by rewriting rules. Typically, for such systems an *interleaving semantics* is given: a step of the computation occurs each time a single reaction happens, resulting in a totally asynchronous behavior, i.e. all possible interleaving of transitions are possible. Probabilistic or stochastic interleaving semantics, has been successfully used, for instance, to describe the dynamics of chemical reactions [BCL$^+$03, CS06] or network protocols [CDL$^+$99].

Nevertheless, there exist modelling scenarios for which the standard interleaving semantics seems to be not adequate. Fisher et al. [FHMP07, FHMP08] argue that (unbounded) asynchrony semantics may not mimic real-life biological behavior properly, especially cellular population behavior, as it allows a part of the systems (e.g. a single cell) to evolve indefinitely while other system components may stall. The interleaving semantics is not adequate also for modelling phase-wise populations dynamics. Indeed, in such systems populations evolve in phases, often related to environmental conditions (e.g. seasonality). Within a phase, each individual makes a choice about the action to be taken among those possible. The set of choices made by individuals identifies a single step of the whole population evolution. For this kind of synchronized behavior the interleaving semantics may be not the best choice.

For these modelling scenarios a *parallel* (i.e. on a single transitions many components can evolve) and *maximal* (i.e. no components can remain blocked) *semantics* is required. A synchronous semantics has been proposed, for instance, for P-systems [Pău02] and Petri nets with firing under Maximal Strategy [Bur80].

Here we present a maximally parallel probabilistic semantics for MSR, which extends the standard interleaving probabilistic semantics of MSR. In particular, the MSR formalism used here is analogous to the one presented in Section 3.2, where also its interleaving semantics is given. Such a semantics is computed in terms of *Discrete Time Markov Chain* (DTMC), via the construction of a *Labeled Transition System* (LTS). This allows the dynamics of biological systems with maximally parallel evolution to be described, and such systems to be analyzed through both probabilistic simulation and model checking tools.

In Section 4.2 we formalize maximally parallel MSR models; in Section 4.3 we define their semantics in terms of LTS and in Section 4.4 we describe the derivation of a probabilistic semantics in terms of DTMC. Some results about branching complexity in maximally parallel MSR are discussed in Section 4.5. In Section 4.6 we present a case study: the modelling and analysis, through

probabilistic simulation, of a simple model of *Caenorhabditis elegans* vulval development. We consider related works in Section 4.7 and we discuss future work directions and conclude in Section 4.8.

4.2 Maximally Parallel Multiset Rewriting Models

As in the previous section, to model biological systems we adopt *Multiset Rewriting* (MSR) [CDL+99] where rewriting rules are enriched with non negative real kinetic constants. In this model, multisets are states of the computation and transitions between states are obtained by applying rewriting rules.

Given a multiset $m \in \mathcal{MS}(X)$ we use $|m|$ to denote its cardinality, i.e. the number of elements contained in X. Assuming an arbitrary order on elements of X, with $X[i], i \in [1, |X|]$ we denote the i^{th} element of X.

A multiset can be used to represent a configuration of a biological system, while events may be modelled by multiset rewriting rules. A *rewriting rule* is a triple (l, r, k) where l and r are multisets, called *reactants* and *products*, respectively. Each rule has associated a *kinetic constant*, $k \in \mathbb{R}_{\geqslant 0}$, that is, roughly, an indication of the propensity of the group of individuals l to take part the represented event. In the following, given a set of rewriting rules $\mathcal{R}$, we use l_R, r_R and k_R to denote the components of $R = (l_R, r_R, k_R) \in \mathcal{R}$.

Each rewriting rule expresses a possible behavior for a certain group of individuals, with a numeric rate expressing the propensity to make such a choice when individuals can take part in different behaviors.

A system is a tuple $S = (\Sigma, \mathcal{R}, s_0)$ where Σ is an n-sized set of species interacting in the system through the rules in the m-sized set $\mathcal{R}$ of rewriting rules, and s_0 is a multiset representing the starting configuration of the system.

Definition 23 (System)**.** *A* system *M is a triple $(\Sigma, \mathcal{R}, s_0)$:*

- Σ *is a finite set of* species names *of size n;*
- $\mathcal{R} = \{R_1, \ldots, R_m\}$*,* $R_i \in \mathcal{MS}(\Sigma) \times \mathcal{MS}(\Sigma) \times \mathbb{R}_{\geqslant 0}$*, is a set of* rewriting rules*;*
- $s_0 \in \mathcal{MS}(\Sigma)$ *is the* starting state*.*

In the following we use $\mathcal{M}$ to denote the universe of systems.

Transitions correspond to the application of rules in a maximally parallel way: each individual takes part in a reaction, if possible, into the current step, and all individuals perform the actions in parallel. Each step is parallel as each reaction can happen multiple times, and it is maximal as it leaves no enabled reaction, i.e. as many reactions as possible are executed. Thus, each step is associated with a multiset $\mu \in \mathcal{MS}(\mathcal{R})$ expressing how many times each reaction is applied.

Given a system $(\Sigma, \mathcal{R}, s_0)$, a multiset $\mu \in \mathcal{MS}(\mathcal{R})$ is *applicable* to a state s, denoted as

$$IsApplicable(\mu, s, \mathcal{R}), \text{ iff } \forall a \in \Sigma : \sum_{R \in \mathcal{R}} l_R(a) * \mu(R) \leq s(a)$$

i.e. there are enough symbols in the configuration to perform all the rules in μ with the corresponding multiplicity.

The result of removing the reactants associated with the rules multiplicity, expressed by μ, from s', and the result of applying μ on s' are, respectively

$$Rem(\mu, s', \mathcal{R}) = s'' \text{ s.t. } \forall a \in \Sigma, s''(a) = s'(a) - \sum_{R \in \mathcal{R}} (l_R(a) * \mu(R)),$$

$$Apply(\mu, s', \mathcal{R}) = s'' \text{ s.t. } \forall a \in \Sigma, s''(a) = Rem(\mu, s', \mathcal{R}) + \sum_{R \in \mathcal{R}} (r_R(a) * \mu(R)).$$

The state s'', resulting from the parallel application of rules in $\mathcal{R}$ expressed by μ, is obtained from s' by removing, for each rule $R \in \mathcal{R}$, $\mu(R)$ times l_R and then by inserting $\mu(R)$ times r_R.

The multiset of rules represented by μ is *maximal* if $IsApplicable(\mu, s, \mathcal{R})$, and no rules $R \in \mathcal{R}$ can be applied to the remaining individuals in the same step, i.e. for any $R \in \mathcal{R}$: $Rem(\mu, s, \mathcal{R}) \not\geq l_R$. We denote this as $IsMaximal(\mu, s, \mathcal{R})$.

As a maximally parallel step should correspond to one time step in the evolution of the biological system, the value k associated with each reaction should be chosen carefully. The kinetic constants is particularly important when two or more reactions compete for reactants: two reactions competing for the same reactant should have a ratio between rates equal to the ratio between their propensity. On the other hand, it should be stressed that not competing reactions are always executed as many times as possible. If a species $A \in \Sigma$ could not be modified, a "null" rule should be included for such species e.g. $(\{A\}, \{A\}, k)$.

In the following we describe how to associate a maximally parallel probabilistic semantics to systems through the construction of a Labeled Transitions System semantics and their translation into a DTMC.

4.3 Maximally Parallel Labeled Transition System Semantics

To describe the evolution of a system we adopt a *Labeled Transition System* (LTS) semantics with a *transition* relation of the form $s' \xrightarrow{\mu, r} s''$. Here, s' and s'' are multisets describing the system configurations before and after a maximally parallel step; $\mu \in \mathcal{MS}(\mathcal{R})$ is a multiset, representing how many times each rule is applied; $r \in \mathbb{R}_{\geqslant 0}$ is the *transition rate*.

The application of a multiset of rules μ to a state s' is formalized by the inference rule

$$\boxed{\frac{IsMaximal(\mu, s', \mathcal{R}) \qquad r = Rate(\mu, s', \mathcal{R}) \quad s'' = Apply(\mu, s', \mathcal{R})}{s' \xrightarrow{\mu, r} s''}} \tag{4.1}$$

where

$$Rate(\mu, s, \mathcal{R}) = MUL(\mu, s, \mathcal{R}) * KIN(\mu, s, \mathcal{R}), \tag{4.2}$$

$$MUL(\mu, s, \mathcal{R}) = \prod_{a \in \Sigma} \prod_{\substack{i \in [1,m] \\ s.t.\, Applied(i,\mu)}} \binom{s(a) - \sum_{r=1}^{i} l_{\mathcal{R}[r]}(a) * \mu(\mathcal{R}[r])}{l_{\mathcal{R}[i]}(a) * \mu(\mathcal{R}[i])}, \tag{4.3}$$

$$KIN(\mu, s, \mathcal{R}) = \prod_{R \in \mathcal{R}} LRR(R, s, \mathcal{R})^{\mu(R)}, \tag{4.4}$$

$$LRR(R, s, \mathcal{R}) = \prod_{\substack{a \in \Sigma \\ s.t.\, l_R(a) > 0}} LIRP(R, s, a, \mathcal{R})^{l_R(a)}, \tag{4.5}$$

$$LIRP(R, s, a, \mathcal{R}) = \frac{P(R, s, a, \mathcal{R}) * k_R}{\sum_{\substack{R' \in \mathcal{R} \\ s.t.\, Enabled(R', s, \mathcal{R})}} P(R', s, a, \mathcal{R}) * k_{R'}}, \tag{4.6}$$

$$P(R, s, a, \mathcal{R}) = \binom{MaxReq(a, s, \mathcal{R})}{l_R(a)}, MaxReq(a, s, \mathcal{R}) = \max_{\substack{R \in \mathcal{R} \\ s.t.\, Enabled(R, s, \mathcal{R})}} l_R(a), \tag{4.7}$$

$$Enabled(R, s, \mathcal{R}) = (l_R \subseteq s) \text{ and } Applied(i, \mu) = \mu(\mathcal{R}[i]) > 0\,.$$

The rate associated with a maximally parallel transition expressed by μ, $Rate(\mu, s, \mathcal{R})$, is equal to the product of the kinetics of such an event, $KIN(\mu, s, \mathcal{R})$, by the multiplicity of the event, $MUL(\mu, s, \mathcal{R})$ (4.2).

The multiplicity $MUL(\mu, s, \mathcal{R})$ of a maximally parallel rewriting event μ is equal to the number of ways in which the event can be realized. This corresponds to the product, for each applied rule, for each species, of the number of way of applying the rule (4.3). Note that MUL yields the same results for every order of evaluation of the rules (that is every evaluation order of μ)[1].

The kinetics of the event expressed by μ, $KIN(\mu, s, \mathcal{R})$, is given by the product of the propensity that each reaction $R \in \mathcal{R}$ is applied in the state s, $LRR(R, s, \mathcal{R})$ (for Local Rule Rate), raised to the power of the number of times the rule is applied, as expressed by $\mu(R)$ (4.4).

The propensity that a reaction R_r is applied once from a configuration s is $LRR(R, s, \mathcal{R})$. This is equal to the product, for each species $a \in \Sigma$ involved (that is, s.t. $l_R(a) > 0$), of the probability that an individual of the species take part in the reaction, that is $LIRP(R, s, a, \mathcal{R})$ (for Local Individual Rule Probability), raised to the power of the number of individuals required for the species ($l_R(a)$).

To obtain the probability that an individual is involved in a certain reaction we need to "normalize" the rates associated with the rules, expressing the propensity of a group of individuals (defined by its left hand side) to take part in a reaction, into a probability distribution on each individual. Such a normalization depends on the state s of the system as it concerns only enabled rules. Actually, for each species $a \in \Sigma$, we consider $MaxReq(a, s, \mathcal{R})$, the maximum number of individuals of such species needed by an enabled rule; then, through $LIRP$ function, we spread the kinetic constants on each individual (4.6). We consider how many times the number of individuals of species $a \in \Sigma$ required by a rule R can be chosen in $MaxReq(a, s, \mathcal{R})$ individuals: that is the number of way in which the rule requirements $l_R(a)$ can be found in the requirements of the maximum demanding rule (4.7). Note that the co-domain of $LIRP$, and consequently of LRR, is $[0, 1]$.

An example of how kinetic rates are normalized is shown in Fig. 4.1. Note that the kinetic constants are not spread among different species.

We define the function $LTS : \mathcal{M} \mapsto \mathcal{LTS}$, such that $LTS(M)$, with $M = (\Sigma, \mathcal{R}, s_0)$, is the LTS $= (S, s_0, \rightarrow)$, obtained by transitive closure of inference rule (4.1) starting from s_0. We use $\mathcal{LTS}$ to denote the universe of LTSs.

[1] e.g. $\binom{N}{M}\binom{N-M}{T}\binom{N-M-T}{K} = \frac{N!}{M!T!K!(N-M-T-K)!} = \binom{N}{K}\binom{N-K}{T}\binom{N-K-T}{M}$

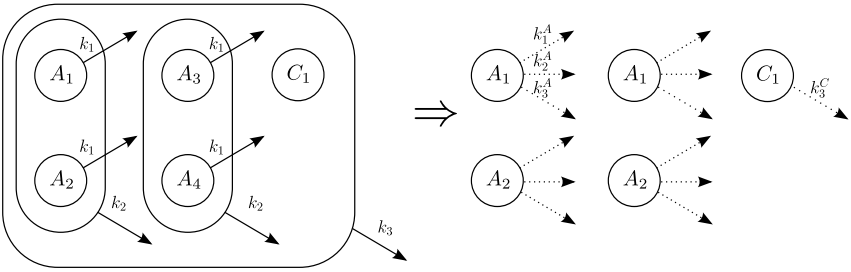


Figure 4.1: Example of kinetic rates normalization done by LIRP (4.6): the rates associated with the rules, expressing the propensity of a group of individuals, are normalized into a probability distribution for each individual.
Let $\mathcal{R} = \{R_1, R_2, R_3\}$ where

$$R_1 = \{A \xrightarrow{k_1} B\}, R_2 = \{2A \xrightarrow{k_2} C\}, R_3 = \{4A, C \xrightarrow{k_3} D\}$$

with

$$k_1 = 1,\ k_2 = 2,\ k_3 = 3 \text{ and } s = \{4A,\ C\}.$$

We have

- $LIRP(R_1, s, A, \mathcal{R}) = k_1^A = \dfrac{\binom{4}{1} * k_1}{\binom{4}{1} * k_1 + \binom{4}{2} * k_2 + \binom{4}{2} * k_3} = \dfrac{4}{19}$;
- $LIRP(R_2, s, A, \mathcal{R}) = k_2^A = \dfrac{12}{19}$;
- $LIRP(R_3, s, A, \mathcal{R}) = k_3^A = \dfrac{3}{19}$;
- $LIRP(R_3, s, C, \mathcal{R}) = k_3^C = 1$.

4.4 Maximally Parallel Probabilistic Semantics

The maximally parallel *probabilistic semantics* is formalized as a DTMC (as defined in Section 2.3.2, Definition 2) which is obtained for the LTS semantics.

As in the previous chapter, we restrict our attention to *finitely branching* DTMCs and We use $\mathcal{MC}$ to denote the universe of (finitely branching) DTMCs.

To derive a DTMC from an LTS, we have to compute, for each pair of states, s and s', the probability of moving from s to s', by exploiting transition rates. Thus, we introduce two functions $R : S \times S \mapsto \mathbb{R}_{\geqslant 0}$ and $E : S \mapsto \mathbb{R}_{\geqslant 0}$, such that

$$R(s, s') = \sum_{s \xrightarrow{\mu, r} s' \in \rightarrow} r \text{ and } E(s) = \sum_{s' \in S} R(s, s') .$$

Intuitively, $R(s, s')$ gives the rate of the set of transitions from s to s', while $E(s)$ computes the exit rate of the state s. The probability of moving from s to s' is derived from $R(s, s')$ and $E(s)$, in standard way, by the function $\mathcal{H}$.

Definition 24 (Probabilistic Semantics)**.** *We define a function $\mathcal{H} : \mathcal{LTS} \rightarrow \mathcal{MC}$ as $\mathcal{H}((S, s_0, \rightarrow)) = (S, s_0, P)$, where $P : S \rightarrow Distr(S)$ is the* probability transition function*, s.t. , $\forall s, s' \neq s \in S$: if $E(s) = 0$, then $P(s, s') = 0$, and $P(s, s) = 1$; $P(s, s') = R(s, s')/E(s)$ otherwise.*

We now explain the proposed probabilistic semantics by two examples.

Example 4. *Let $S_{ex} = (\Sigma_{ex}, \mathcal{R}_{ex}, s_{0_{ex}})$ with $\Sigma_{ex} = \{A, B, C\}$,*
$\mathcal{R}_{ex} = \{ R_1 = \{\{A\}, \{B\}, 1\} ; R_2 = \{\{A\}, \{C\}, 2\} \}$ and $s_{0_{ex}} = \{3A\}$.

The number of possible outcomes of such system corresponds to the number of success in three flips of an unfair coin, and their probabilities are described by a Bernoulli distribution where $p = 1/(1 + 2)$ and $1 - p = 2/(1 + 2)$. The same result can be obtained by the construction of the LTS of the system (see Fig. 4.2).

In more detail, the following events are possible:

- *3 times R_1, 0 times R_2, with multiplicity 1*
  has a probability of $1 * (1/3)^3 = 1/27$
- *2 times R_1, 1 time R_2, with multiplicity 3*
  has a probability of $3 * (1/3)^2 * (2/3) = 6/27$
- *1 time R_1, 2 times R_2, with multiplicity 3*
  has a probability of $3 * (1/3) * (2/3)^2 = 12/27$

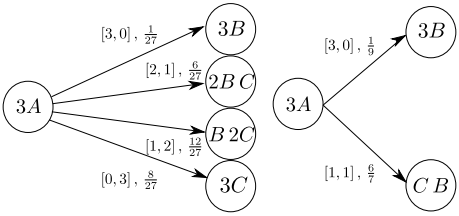


Figure 4.2: LTSs of Example 4 (left) and Example 5 (right).

- *0 times R_1, 3 times R_2, with multiplicity 1*
  has a probability of $1 * (2/3)^3 = 8/27.$

Note that this case does not require to use the translation function $\mathcal{H}$; the rates reported on the LTS are probability distributions on exit transitions and can be directly used in the DTMC. When all the rules are context free and they all compete for the same species, we have that $\forall s \in S : P(s) = R(s) \in Distr(S)$ and the normalization done by $\mathcal{H}$ is not needed.

Example 5. *Consider the previous example $S_{ex} = (\Sigma_{ex}, \mathcal{R}_{ex}, s_{0_{ex}})$, and replace R_2 with $\{\{2A\}, \{C\}, 2\}$ in $\mathcal{R}$. The main difference is that the second reaction can happen only if 2 individuals of species A are present. In this case through the LTS construction we assign to each transition a weight, expressing the propensity of the related maximally parallel step, which is proportional to the kinetic rates associated with the reactions and to the multiplicity of the events (the number of possible assignments of individuals to reactions). In this case, we obtain the LTS of Figure 4.2.*

Then, by applying the translation function $\mathcal{H}$ we get the following probability distribution of events:

- *3 times R_1, 0 times R_2, with multiplicity 1*
  has rate $1 * (1/3)^3 = 1/9$ *corr. to a probability of* $1/7$

- *1 time R_1, 1 time R_2, with multiplicity 3*
  has rate $3 * (1/3) * (2/3) = 6/9$ *corr. to a probability of* $6/7$.

(n, m)	1	2	3	4	5	6	...
1	1	2	3	4	5	6	...
2	1	3	6	10	15	21	...
3	1	4	10	20	35	46	...
4	1	5	15	35	70	116	...
5	1	6	21	46	116	232	...
...							

Figure 4.3: Number of transitions exiting from s_0 in S_{ex} of Example 6 where $n = s_0(A_0)$, $m = |\mathcal{R}|$.

4.5 Notes on the Maximally Parallel Multiset Rewriting Branching Complexity

A major drawback of the maximally parallel semantics is that the number of transitions exiting from a state (i.e. the *branching complexity*) grows with respect to the size of the population (i.e. the total number of individuals represented by the state). In the following we use $Tr(s, \mathcal{R})$ to denote the transitions exiting from a state s using the rules in $\mathcal{R}$.

Example 6. *Let* $S_{ex} = (\Sigma_{ex}, \mathcal{R}_{ex}, s_{0_{ex}})$ *with* $\Sigma_{ex} = \bigcup_{i=0}^{m} A_i$, $\mathcal{R}_{ex} = \bigcup_{i=1}^{m} \mathcal{R}[i] = ([A_0], [A_i], 1)$ *and* $s_{0_{ex}} = \{nA\}$. *The number of transitions exiting from* s_0 *are shown in Figure 4.3.*

In general, the number of transitions exiting from a state is difficult to obtain. If we focus on a particular case, namely systems using only *context free* rewriting rules, we are able to compute accurately such a number, while in general, with arbitrary rewriting rules, we can get an upper bound on it. We define a rewriting rule $R = (l, r, k)$ to be *context free* on the species a, $ContextFree(R, a)$, iff $l(a) = 1 \wedge \forall b \in \Sigma, b \neq a : l(b) = 0$. We define a set of rules to be context free iff it consists only of context free rules. Given a set of context free rewriting rules $\mathcal{R}$, $\forall a \in \Sigma$, it can be partitioned into disjoint subsets $(\mathcal{R})_a$ consisting only of rules with their left hand side requiring only an individual of the species a. Formally $\forall a \in \Sigma : (\mathcal{R})_a = \{R = (l, r, k) \in \mathcal{R} \,|\, ContextFree(R, a)\}$.

Theorem 4.5.1. *Given a system* $S = (\Sigma, \mathcal{R}, s_0)$ *and a state* $s \in \mathcal{MS}(\Sigma)$*, if* $\mathcal{R}$ *is context free, the number of exiting transitions from a state,* $|Tr(s, \mathcal{R})|$ *is* $(\prod_{a \in \Sigma,\, s(a)>0} \phi(|(\mathcal{R})_a|, s(a)))$ *where* $\phi(m, n) = \binom{m+n-1}{n} = \frac{(n+m-1)!}{(m-1)!n!}$.

Proof. Let us consider the case in which Σ consists of a single species a, i.e. $|\Sigma| = 1$. We have to prove that the number of transitions exiting from s, $|Tr(s, \mathcal{R})|$, is $\phi(|\mathcal{R}|, s(a))$. The proof proceeds by induction both on the number of rules, $|R|$, and on the number of individuals in the state, $s(a)$.

Base cases:

$|R| = 1$**:** there is a single exiting transition assigning all individuals to the single rule in the system;

$s(a) = 1$**:** the number of exiting transitions is $|\mathcal{R}|$: we have a transition for each way of assigning the only individual to one of the rules.

Inductive case: let us consider a rule $R \in \mathcal{R}$. The set of transitions exiting from s can be split into two disjoint sets: the set of transitions in which R is not applied, i.e. $\mu(R) = 0$, and the set of transitions in which R is applied at least once, i.e. $\mu(R) \geq 1$. In the first set we have transitions corresponding to $|\mathcal{R}| - 1$ rules competing for $s(a)$ objects; by inductive hypothesis their number is $\phi(|\mathcal{R}|-1, s(a)) = \binom{s(a)+|\mathcal{R}|-2}{s(a)}$. On the other set we have transitions corresponding to $|\mathcal{R}|$ rules competing for $n-1$ objects: an object is used to apply R once while the other objects are contended by the rules, including R. By inductive hypothesis the number of transitions in the second set is $\phi(|\mathcal{R}|, s(a) - 1) = \binom{s(a)+|\mathcal{R}|-2}{s(a)-1}$. Summarizing we have $\binom{s(a)+|\mathcal{R}|-2}{s(a)} + \binom{s(a)+|\mathcal{R}|-2}{s(a)-1}$ transitions, and by the fact that $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$, this is equal to $\binom{s(a)+|\mathcal{R}|-1}{s(a)} = \phi(|\mathcal{R}|, s(a))$.

Let us consider the case in which $|\Sigma| > 1$. Given the fact that rules are context free, they do not compete on different species. Hence the set of possible transitions corresponds to the Cartesian product of the possible transitions of each partition of rules with respect to a species. Their number is thus

$$|Tr(s, \mathcal{R})| = \left(\prod_{a \in \Sigma,\, s(a) > 0} \phi(|(\mathcal{R})_a|, s(a)) \right).$$

□

We now explain the previous theorem by means of two examples.

Example 7. *Let* $S_{ex} = (\Sigma_{ex}, \mathcal{R}_{ex}, s_{0_{ex}})$ *with* $\Sigma_{ex} = \{A, B, C, D\}$, $\mathcal{R}_{ex} = \{R_1 = (\{A\}, \{B\}, 1)\,,\ R_2 = (\{A\}, \{C\}, 1)\,,\ R_3 = (\{A\}, \{D\}, 1)\}$ *and* $s_{0_{ex}} = \{3A\}$ *the number of transitions exiting from* s_0 *are* $\phi(3, 3) = 10$*. In more detail, such a number is equal to the sum of :*

- *the number of transitions in which* R_1 , R_2 *compete for* $3a$*:* $\phi(2,3) = 4$*. Namely they correspond to the set of maximally parallel application of rules,* $\{\{3,0,0\}, \{2,1,0\}, \{1,2,0\}, \{0,3,0\}\}$*;*

- *the number of transitions in which* R_1 , R_2 , R_3 *compete for* $2a$ *(considering at least an object assigned to* R_3*):* $\phi(3,2) = 6$*. Namely they correspond to the set of maximally parallel application of rules,* $\{\{2,0,1\}, \{1,1,1\}, \{0,2,1\}, \{1,0,2\}, \{0,1,2\}, \{0,0,3\}\}$.

Example 8. *Let* $S_{ex} = (\Sigma_{ex}, \mathcal{R}_{ex}, s_{0_{ex}})$ *with* $\Sigma_{ex} = \{A, B, C, D\}$*,* $\mathcal{R}_{ex} = \{R_1 = (\{A\}, \{B\}, 1), R_2 = (\{A\}, \{C\}, 1), R_3 = (\{B\}, \{C\}, 1), R_4 = (\{B\}, \{D\}, 1)\}$ *and* $s_{0_{ex}} = \{2A, 2B\}$ *the number of transitions exiting from* s_0 *are* $\phi(2,2) \times \phi(2,2) = 9$*. In more detail, such a number is equal to the Cartesian product of*

- *the transitions in which* R_1 , R_2 *compete for* $2a$ *(that are* $\phi(2,2) = 3$*) and*

- *the transitions in which* R_3 , R_4 *compete for* $2b$ *(that are* $\phi(2,2) = 3$*).*

Namely they correspond to the set of maximally parallel application of rules

$$\{\{2,0,2,0\}, \{2,0,1,1\}, \{2,0,0,2\}, \{1,1,2,0\}, \{1,1,1,1\}, \{1,1,0,2\}, \{0,2,2,0\}, \{0,2,1,1\}, \{0,2,0,2\}\}.$$

We have seen how to compute the number of transitions exiting from a state using only context free rules. In general, when the rules are not constrained to be context free, we are able to get an upper bound on the number of transitions exiting from a state, and to this aim, we introduce an encoding of rules, from the general form, into context free rules.

Assuming an arbitrary order on Σ, the encoding of a rewriting rule, and of a set of rewriting rules, into context free form is defined as:

- given a rewriting rule $R = (l, r, k)$, and being a the minimum species such that $l(a) > 0$: $\|R\| = \{(\{a\}, r, k)\} \cup \{(\{b\}, \ , k) \,|\, l(b) > 0\,,\ b \neq a\}$,

- $\|\mathcal{R}\| = \bigcup_{R \in \mathcal{R}} \|R\| \cup \{(\{a\}, \{a\}, k) \,|\, a \in \Sigma\}$.

The encoding of a rule creates a rule for each species required in its left hand side: these rules produce nothing, except one that produces the effect of the original rule. The encoding of a set of rules is equal to the union of the encoding of the single rules plus a "null" rule, rewriting an element in itself, for each species.

The following lemma states that by replacing the rules of a system with a context free encoding of them we obtain a system which is able to perform more transitions than the original one, from any given state.

Lemma 4.5.2. *Given a system $M = (\Sigma, \mathcal{R}, s_0)$, its context free encoding $M' = (\Sigma, ||\mathcal{R}||, s_0)$ and a state $s \in \mathcal{MS}(\Sigma)$, it holds that $|Tr(s, \mathcal{R})| \leq |Tr(s, ||\mathcal{R}||)|$.*

Proof. It is easy to see that M' can simulate the behavior of M: each maximal application of rules in $\mathcal{R}$ corresponds to a different maximal application of rules in $||\mathcal{R}||$, being $||\mathcal{R}||$ composed of context free rules plus additional "null" rules. Moreover M' can perform transitions that M cannot perform. □

The following lemma states that we can get an upper bound on the number of transitions a system can perform from a given state. To this aim we consider the number of transitions a system using a context free encoded version of the original rules can perform from the same state.

Theorem 4.5.3. *Given a system $M = (\Sigma, \mathcal{R}, s_0)$, and a state $s \in \mathcal{MS}(\Sigma)$, it holds that*

$$|Tr(s, \mathcal{R})| \leq \prod_{a \in \Sigma,\, s(a)>0} \phi(||(\mathcal{R})_a||, s(a)) \,.$$

Proof. Follows from the Lemma 4.5.2 and the Theorem 4.5.1. □

Related aspects of are discussed in [AV08, CPPJ06, GNPJRN07].

4.6 Case Study: *C. elegans* Vulval Development

We present the application of our framework to a model of *Caenorhabditis elegans* vulval development, a system already studied with different formalisms at different levels of detail [FPHH07, FPH+05, SFB+08, BKF+09, LNUM09]. Here, our purpose is a demonstration of the usability of maximally parallel probabilistic semantics for modelling inter-cellular dynamics, rather than an accurate modelling of the biological process.

C. elegans is a hermaphrodite round worm, about 1 mm in length, which lives in soil. In order to lay eggs, the *C. elegans* grows an organ called vulva. The biological mechanisms underlying the vulval development has been object of research in the last 20 years and include cell-cell interactions, cell differentiation, cross-talk between pathways and gene regulation.

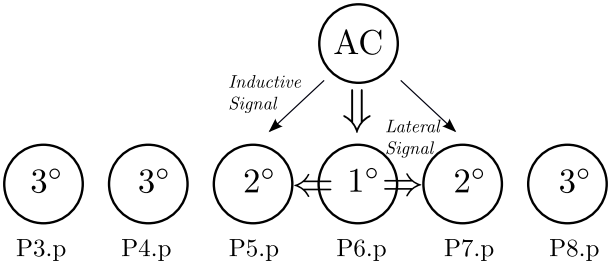


Figure 4.4: Inter-cellular signaling events involved in VPCs fate specification.

The *C. elegans* vulva normally derives from three vulval precursor cells (VPCs) that are members of a larger set of six VPCs, P3.p-P8.p. Each of the six VPCs is multi-potent, capable of adopting one of three fates, called primary (1°), secondary (2°), tertiary (3°) [SH86, SH89, Ste05]. The actual fate that each cell adopts depends on inter-cellular signals: an inductive signal emanating from the gonad anchor cell (AC) and a later signal between VPCs originated form presumptive 1° fate cell (see Fig. 4.4). In response to inductive signal the VPCs produce lateral signal that counteracts the inductive AC signal in the neighboring VPCs by inducing the expression of a set of inhibitions and causing the cells to assume 2° fate cell. Despite the ability of each cell to adopt any of the three fates, the pattern of fates adopted by P3.p-P8.p in wild-type animals is always [3°3°2°1°2°3°], respectively. VPCs fates in wild-type animals are influenced by their distance from the AC: the cell closest to the AC (P6.p) becomes 1°, the next closest (P5.p and P7.p) become 2°, and the most distant cells (P3.p,P4.p and P8.p) become 3°.

The considerable amount of descriptive biological knowledge and the large number of genetic perturbations tested in vivo, welcome the research of alternative modelling procedures. Among the others, the process has been modelled with Reactive Modules [FPHH07], with StateCharts [FPH+05], with a combination of Live Sequence Charts and StateCharts [SFB+08], with Petri net with firing under Maximal Strategy and overshooting [BKF+09], with hybrid functional Petri nets [LNUM09].

Here we present a simple maximally parallel Multiset Rewriting model in of *C. elegans* and we show that different behaviors, corresponding to different in vivo perturbations, can be observed by probabilistic simulation. The different behaviors can be realized altering the rate associated with reactions.

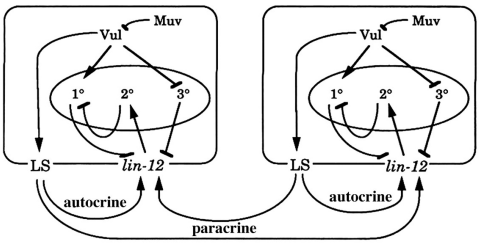


Figure 4.5: Diagrammatic model of VPCs from [SH89].

Using our approach we are able to consider a probabilistic semantics without extending the MSR framework. Conversely, [FPHH07, FPH+05, SFB+08, BKF+09] study the system with non-deterministic models, while [LNUM09], in order to include quantitative information about the system dynamics, extends the Petri nets framework with continuous processes.

We propose a formal dynamics model of vulval fate specification based on the diagrammatic model proposed by Sternberg and Horvitz [SH89, Ste05] (see Fig. 4.5), where the process is expressed as a set of simple production or inhibition reactions.

We encode an inhibitory relation *A inhibits B*, as $A\,B \to A$; an activation *A activates B*, as $A \to B$. The resulting model of a single VPC is shown in Figure 4.6. It consists of the following eight reactions (that are parametric to the VPC identifier $i \in [3, 8]$).

$$Vul_i \xrightarrow{10} G1_i \quad (R_{1,i}) \qquad Vul_i \quad G3_i \xrightarrow{100} Vul_i \quad (R_{2,i})$$

$$Vul_i \xrightarrow{1} LS_i \quad (R_{3,i}) \qquad G1_i \quad Lin12_i \xrightarrow{1000} G1_i \quad (R_{4,i})$$

$$Lin12_i \xrightarrow{1} G2_i \quad (R_{5,i}) \qquad G2_i \quad G1_i \xrightarrow{1} G2_i \quad (R_{6,i})$$

$$G3_i \quad Lin12_i \xrightarrow{1} G3_i \quad (R_{7,i}) \qquad LS_i \xrightarrow{1} Lin12_i \quad (R_{8,i})$$

The connection between neighboring cells is modelled as follows.

$$LS_i \xrightarrow{1} Lin12_{i+1} \qquad (Rconn_{i,i+1}) \qquad LS_i \xrightarrow{1} Lin12_{i-1} \qquad (Rconn_{i,i-1})$$

The inductive signal by *AC* is modelled as follows.

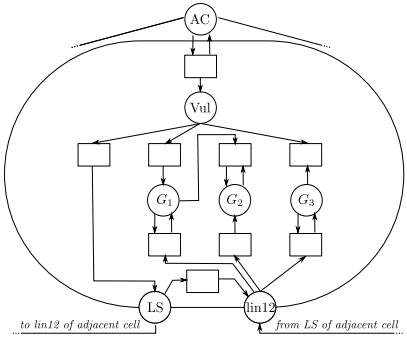


Figure 4.6: Single VPC maximally parallel Multiset Rewriting model.

$$AC \xrightarrow{K_{Rac_i}} Vul_i \qquad (Rac_i)$$

The different amount of signal received by each VPC, according to the distance from the AC, is modelled by the use of different kinetic rates: K_{Rac_i} is equal to 100 for $i = 6$, equal to 1 for $i \in \{7, 5\}$ and equal to 0,001 for $i = \{3, 4, 8\}$.

A rule is used to keep track of the time elapsed (i.e. the number of maximally parallel steps). The final fate of cells, whose determination is described in details in [LNUM09], is determined by three rules, activated after a certain number of steps, on the base of concentration of fate specific proteins, $G1_i, G2_i, G3_i$.

$$t \xrightarrow{1} \qquad t \quad time \qquad (Rtime)$$

$$mark_i \quad G1_i \quad time * 100 \xrightarrow{1} \quad G1_i \quad time * 100 \quad CellFate1_i \qquad (Rfate_{1,i})$$

$$mark_i \quad G2_i * 3 \quad time * 100 \xrightarrow{1} \quad G2_i * 3 \quad time * 100 \quad CellFate2_i \qquad (Rfate_{2,i})$$

$$mark_i \quad G3_i \quad time * 100 \xrightarrow{1} \quad G3_i \quad time * 100 \quad CellFate3_i \qquad (Rfate_{3,i})$$

The whole studied system is shown in Figure 4.7: the six VPCs and the AC.

We considered three different scenarios: *a*) the wild-type, *b*) a mutant where the AC sends equal signals to all the VPCs, and *c*) a mutant in which cells do not respond to lateral signals. The two mutants are obtained modifying the rates associated to AC signals and suppressing the reaction in charge of replying to

lateral signal $Rconn_{i,i+1}$ and $Rconn_{i,i-1}$. Namely, in *b*), $K_{Rac_i} = 100$ for each $i \in [3, 8]$, in *c*) the rates associated with $Rconn_{i,i+1}$ and $Rconn_{i,i-1}$ are set to 0.

By performing probabilistic simulation runs, for each case, we are able to reproduce the pattern formations observed *in vivo*: wild-type *a*) yields [3°3°2°1°2°3°] pattern[2], mutant *b*) yields patterns where 1° and 2° are random distributed among cells, and, similarly, mutant *c*) yields patterns where some cells adopt 1° and some others 3°.

To perform simulations we developed a probabilistic simulator that, at each step, computes the probability distribution over the possible maximally parallel events, and then selects one of them probabilistically. The computation of the multiset of maximally parallel rule applications is done using an algorithm similar to [AV08]. A more efficient algorithm, as one described in [MPPRS11], can be used.

4.7 Comparison with Related Works

Multiset rewriting has been used as modelling formalism for describing, for instance, chemical reactions and network protocols, using interleaving semantics, both in a qualitative and quantitative fashion [BCL$^+$03, CA06, CDL$^+$99]. The formalism has the same expressing power of Petri Nets [Pet62], also used in this context [HGD08].

The maximally parallel semantics proposed, in the qualitative case, for instance for Petri Nets [Bur80], has received great attention in the context of P Systems [Pău02]. P Systems are a biologically inspired formalism, based on the maximally parallel rewriting of atomic objects spread across different compartments, that recently have been successfully applied to many modelling scenarios (see, for instance, [CA06, BCPM08, RCPJ08, RC08a, BMMG10]). Apart from the qualitative semantics originally proposed, for P Systems, several probabilistic and stochastic semantics have been proposed [PBMZ06, CC07, AC03, Mad03, Obt02, OP03].

Multiset rewriting with a maximally parallelism semantics is Turing-complete (see [Pău02] where this is proved for one-membrane P Systems). Turing-completeness of different semantics of Multiset Rewriting is discussed also in [CZ08].

The approaches more similar to our are [PBMZ06, CC07]. The Dynamical P Systems, by Pescini et al. [PBMZ06], are presented with a stochastic

[2] On 10^3 simulation runs, all yielded such a pattern.

simulation algorithm, but lack of a formal probabilistic semantics. The definition of probabilistic transitions proposed by Ciobanu and Cormacel [CC07] uses an hyper-geometric distribution. In both cases, the rates assigned to a parallel step are different from those obtained with our methodology. In particular, in [PBMZ06] the rate computation, bone by splitting one parallel step into several sequential sub-steps, depends on the order in which reactions are considered. In [CC07] the rates may be influenced by the presence of extraneous reactions (i.e. rules never applicable to the system).

The approaches proposed by Aderlean and Cavaliere [AC03] and by Madhu [Mad03] give a probabilistic semantics for P Systems but they modify the basic framework with additional rule probabilities. Obtulowicz [Obt02] proposes a stochastic and a randomized semantics, while Obtulowicz and Paun [OP03] discuss how to add probability to P Systems semantics.

Finally, many are the approaches [SMC+08, RCPJ08, BRCG+05, RCGB+06] where the requirement for maximal parallelism of P Systems is relaxed in favor of a stochastic interleaving semantics, realized by the Gillespie Stochastic Simulation Algorithm (SSA) [Gil77].

4.8 Conclusions

In this Chapter we have defined a probabilistic semantics for maximally parallel Multiset Rewriting systems which corresponds to P systems with one membrane or Petri nets where promoter arcs are added and the parallelism is maximal. The need of such a semantics is motivated by the fact that most of the semantics/simulators of P systems (i.e. maximally parallel MSR into membranes) either resolve the non-determinism in the random way or use the interleaving semantics to simulate via Gillespie SSA the studied system.

We defined a maximally parallel probabilistic semantics in term of DTMC, built via LTS construction, and we have shown an application to *C. elegans* vulval development modelling. Here we have shown probabilistic simulation results; as it would be interesting to study maximally parallel systems through probabilistic model checking, we plan to realize on a translator from MPMRS to DTMC allowing to use existing model checking tools.

We think that the proposed semantics can be easily adapted to describe a (maximally parallel) probabilistic semantics for P Systems and Petri nets with firing under Maximal Strategy, and can also be considered as an alternative semantics for other formalisms proposed for Systems Biology (e.g. [Phi07]).

A major drawback of the maximally parallel semantics is that the number of transitions exiting from a state grows with respect to the size of the population represented by the state (see Section 4.5). This represents the main computational cost of the proposed semantics and can be a serious problem, depending on the system under study, to run simulations or to perform model checking. For this reason in Chapter 5 we define an abstract semantics to reduce the number of transitions exiting from a state, still obtaining bounds on transitions probabilities and conservative results about probabilistic reachability.

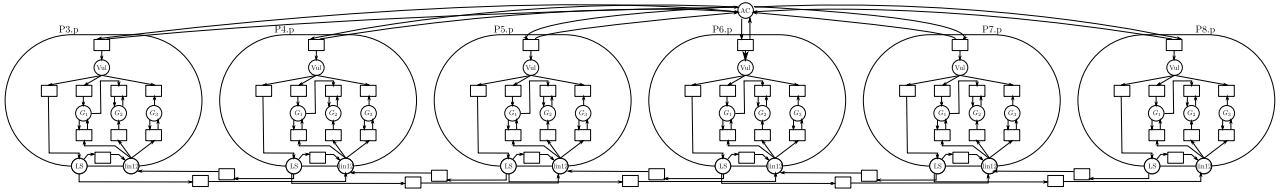


Figure 4.7: Model of the whole studied system: the six VPC and the AC.

Chapter 5

Interval Valued Abstract Maximally Parallel Semantics for Multiset Rewriting

In this chapter, we define an abstract probabilistic semantics for maximally parallel Multiset Rewriting (MSR) able to describe with a reduced number of states and transitions the semantics of systems with huge, possibly infinite, associated state space.

Such a semantics is effectively computed as *Interval Markov Chain* (IMC), which is derived from an abstract *Labelled Transition System* (LTS). The abstract states are obtained by approximating the exact multiplicities of reactants using intervals of integers, by means of interval valued predicate evaluation.

With the proposed approach we are able to obtain lower and upper bounds on transition probabilities. Since the abstraction is parametric on a set of predicates, the abstract probabilistic model can be refined until a right compromise between dimension and precision is reached.

As case study, we propose an example of probabilistic reachability computation on a simple model of seasonal animals reproduction.

5.1 Introduction

As discussed in Section 4.5, a major drawback of the maximally parallel semantics of MSR is that the number of transitions exiting from a state grows with respect to the size of the state (i.e. the total number of individuals in the population represented by the state).

This may represent a serious computational problem, depending on the system under study, both to perform simulations or model checking, as a probability has to be assigned to each transition exiting from a state. Moreover, the application of probabilistic model checking is limited to systems with a small and finite state space.

For these reasons we propose an abstract maximally parallel probabilistic semantics that, using interval valued predicate abstraction [GS97], allows a finite abstract probabilistic model, with a reduced number of states and transitions, to be obtained. More in details, we introduce a technique based on the idea of approximating the multiplicity of the elements of multisets by means of intervals of integers. The technique is parametric on a set of predicates, which determine the intervals, partitioning the values, for each species. By tuning the granularity of intervals it is possible to refine the abstract probabilistic model until a right compromise between dimension and precision is reached.

The abstraction technique is sound for probabilistic reachability. Specifically probabilistic model checking of the abstract probabilistic semantics reports lower and upper bounds for probability of reachability properties.

More in details, the domain of each variable (i.e. the number of individuals of a species) is partitioned into intervals of integers. This corresponds to impose a sort of grid, consisting of predicates, over the concrete state space. Then, we introduce a systematic method for calculating an abstract, approximated, probabilistic semantics, corresponding to an IMC. The IMC is derived from an abstract LTS semantics, by computing the intervals of probability from the information recorded on abstract transition (e.g. the transitions rates).

We introduce the concepts formalizing the abstraction of the state space by means of the interval valued predicates (Sect. 5.2). Then, in Section 5.3, we introduce the abstract LTS semantics; first we present the computation of the abstract reachable states (Sect. 5.3.1), then the computation of the abstract maximally parallel multiset of rule application (Sect. 5.3.2), and finally the computation of the abstract transition rates (Sect. 5.3.3). The soundness of the proposed abstract LTS semantics, with respect to the LTS semantics defined in Section 4.3, is discussed in Section 5.3.4. The used abstract probabilistic

semantics is defined in Section 5.4, its derivation from an abstract LTS and its soundness is presented in Section 5.4.1. In order to prove the soundness of our framework we apply notions of abstract interpretation, similarly as in Section 3.3.4.

An example of application of the proposed framework to a simple model of seasonal animals reproduction model is given in Section 5.5.

Finally, in Section 5.6 we discuss the limitations and possible further development of our work. In Section 5.7 we review related works and we conclude in Section 5.8.

For simplifying the presentation, great part of the proofs are presented in Section 5.9.

5.2 Interval Valued Abstract Models

We introduce the concepts of abstract states and systems, and the related notions necessary to relate them to their concrete version.

To abstract precise numeric values we use *Intervals* of values.

Definition 25 (Intervals)**.** $\mathbb{I} = \{\, [m, n] \mid m \in \mathbb{R}_{\geq 0}, n \in \mathbb{R}_{\geq 0} \cup \{\infty\}\}$.

We say that an interval is *well formed* if its lower bound is less or equal its upper bound; formally $WellFormed([m, n]) = m \leq n$.

In the following, given an interval $i = (m, n) \in \mathbb{I}$ we use $Precise(i)$ to denote $m = n$.

Since intervals may contain ∞, mathematical operations may give indeterminate forms. For this reason we extend mathematical operators $+, \times, -, /$ in order to consider, in some cases, ∞. This avoid the need to deal with certain indeterminate forms in each definition that follows. In particular we consider :

$$a + b = \begin{cases} \infty & \text{if } a = \infty \text{ or } b = \infty\,; \\ a + b & \text{otherwise.} \end{cases} \qquad a \times b = \begin{cases} \infty & \text{if } a = \infty \text{ or } b = \infty\,; \\ a \times b & \text{otherwise.} \end{cases}$$

$$a - b = \begin{cases} \infty & \text{if } a = \infty \text{ and } b \neq \infty\,; \\ -\infty & \text{if } b = \infty \text{ and } a \neq \infty\,; \\ a - b & \text{otherwise.} \end{cases} \qquad a/b = \begin{cases} \infty & \text{if } a = \infty \text{ or } b = \infty\,; \\ a/b & \text{otherwise.} \end{cases}$$

To represent interval valued states, we use an abstract version of multisets.

Definition 26 (Abstract Multiset)**.** *Given a finite set X, an abstract multiset is a function* $m^\circ : X \mapsto \mathbb{I}$*. We denote the universe of abstract multiset by* $\mathcal{MS}^\circ$*, and the universe of abstract multisets over a set X as* $\mathcal{MS}^\circ(X)$*.*

We say that an abstract multiset is *well formed* if it is composed by well formed intervals. Formally $WellFormed(m^\circ) = \forall_{i=1,|m^\circ|}\, WellFormed(m^\circ[i])$.

On abstract multisets $\mathcal{MS}^\circ$ an approximation order $\sqsubseteq_{\mathcal{MS}^\circ}$ can be defined as follows.

Definition 27 (Order on Abstract Multisets)**.** *Given abstract multisets* $m^\circ{}_1, m^\circ{}_2 \in \mathcal{MS}^\circ(X)$ *we say that* $m^\circ{}_1 \sqsubseteq_{\mathcal{MS}^\circ} m^\circ{}_2$ *iff* $\forall\, a \in X : m^\circ{}_1(a) \sqsubseteq_{\mathbb{I}} m^\circ{}_2(a)$*.*

We use predicates of the form of $(a \geq x_{low}) \wedge (a \leq x_{high})$, where $a \in \Sigma$ indicates a species while $[x_{low}\,,\, x_{high}] \in \mathbb{I}$ $(x_{low} \leq x_{high} \in \mathbb{N})$. For the sake of simplicity we denote predicates as pairs, specifying the species and the interval of values.

Definition 28 (Predicate)**.** *A Predicate p is a pair* (a, i)

- $a \in X$ *is a* species*;*
- $i \in \mathbb{I}$ *is an* interval *of values.*

We denote the universe of predicates as $\mathbb{P}$ *and the universe of predicates over a set of species X as* $\mathbb{P}(X)$*.*

To evaluate the truth of a predicate w.r.t. concrete and abstract states we use an *entailment function* $\vDash_{\mathbb{P}}$: $(\mathcal{MS} \cup \mathcal{MS}^\circ) \times \mathbb{P} \mapsto \{true, false\}$. A predicate $p = (a, i)$ is *true for a state* $s \in \mathcal{MS}$, denoted as $s \vDash_{\mathbb{P}} p$, iff $s(a) \in i$.
Moreover, $p = (a, i)$ is *true for an abstract state* $s^\circ \in \mathcal{MS}^\circ$, denoted as $s^\circ \vDash_{\mathbb{P}} p$, iff $s^\circ(a) \sqsubseteq_{\mathbb{I}} i$.

To abstract concrete models we use *sets of predicates* $\mathfrak{p} \in Parts(\mathbb{P}(\Sigma))$. In the following, $\forall a \in \Sigma\,,\ \forall \mathfrak{p} \in Parts(\mathbb{P}(\Sigma))$, we use $\mathfrak{p}(a) = \{\, p \in \mathfrak{p} \mid p = (a, i) \,\}$, the subset of predicates regarding a.

Specifically, we consider sets of predicates which are a partition with respect to the set of species Σ, denoted by $\widehat{\mathbb{P}}(\Sigma) \subset Parts(\mathbb{P}(\Sigma))$, and sets of predicates which are a partition with respect to the set of species Σ and the set of rules $\mathcal{R}$ of a model, denoted by $\widehat{\mathbb{P}}_{\mathcal{R}}(\mathcal{R}) \subset \widehat{\mathbb{P}}(\Sigma)$.

A set of predicates is *a partition w.r.t. a set of species* Σ if it partitions the domains associated to each species of Σ.

Definition 29. *A set of predicates* $\mathfrak{p} \in \widehat{\mathbb{P}}(\Sigma)$ *is a partition w.r.t.* Σ *iff*

- *covers all species in* Σ*:* $\bigcup_{(a,i)\in\mathfrak{p}}\{a\} = \Sigma$*;*
- *they are a partition of the values in the domain of each species:*
  - $\forall p' = (a_1, i_1), p'' = (a_2, i_2) \in \mathfrak{p} \,:\, a_1 = a_2 \Rightarrow i_1 \cap i_2 = \emptyset$*;*
  - $\forall a \in \Sigma, n \in \mathbb{N} : \exists p = (a, i) \in \mathfrak{p}$ *s.t.* $n \in i$ *that is* $\forall a \in \Sigma \,:\, \bigcup^{\mathbb{I}}_{(a,i)\in\mathfrak{p}} i = [0, \infty]$.

A set of predicates $\mathfrak{p}$ is *a partition w.r.t. a set of rules* $\mathcal{R}$ *over* Σ if: (a) it is a partition w.r.t. Σ and (b) for all species $a \in \Sigma$, for all rules $R = (l, k, r) \in \mathcal{R}$, and for all predicates $p = (a, i = [x_{min}, x_{max}]) \in \mathfrak{p}$, the number of individuals requested by the rule for the species, $l(a)$, if is included in the interval i, it can be only its minimum, i.e. $l(a) \notin [x_{min} + 1, x_{max}]$. Notice that this condition guarantees that a rule can be applied in any or in all of the states corresponding to a given abstract state.

Definition 30.
A set of predicates $\mathfrak{p} \in \widehat{\mathbb{P}}_{\mathcal{R}}(\Sigma)$ *is a partition w.r.t.* $\mathcal{R}$ *over* Σ *iff*

- *is a partition w.r.t.* Σ
- $\forall R = (l, r, k) \in \mathcal{R}\,,\ \forall p = (a, i = [x_{min}, x_{max}]) \in \mathfrak{p} \,:\, l(a) \notin [x_{min} + 1, x_{max}]$

In order to relate concrete multisets to abstract multisets we introduce *abstraction and concretization of multisets* function, $\alpha_{\mathcal{MS}}$ and $\gamma_{\mathcal{MS}}$, which are parametric w.r.t sets of predicates. For $m \in \mathcal{MS}$, the abstraction function reports its best approximation w.r.t. a set of predicates $\mathfrak{p}$. Conversely, for $m^\circ \in \mathcal{MS}^\circ$ the concretization function reports the (possibly infinite) set of multisets represented by m°.

Definition 31 (Abstraction of Multiset w.r.t. Set of Predicates and Concretization of Abstract Multiset)**.**

- $\alpha_{\mathcal{MS}} : \widehat{\mathbb{P}}(X) \mapsto \mathcal{MS}(X) \mapsto \mathcal{MS}^\circ(X)$ *is defined as*

$$\alpha_{\mathcal{MS}}(\mathfrak{p})(m) : m^\circ \ \text{ s.t. } \forall\, a \in X \,:\, m^\circ(a) = i \text{ s.t. } \exists p = (a, i) \in \mathfrak{p} \,\wedge\, m \vDash_{\mathbb{P}} p\,;$$

- $\gamma_{\mathcal{MS}(X)} : \mathcal{MS}^\circ \mapsto Parts(\mathcal{MS}(X))$ *is defined as*

$$\gamma_{\mathcal{MS}}(m^\circ) : \{m \mid \forall\, a \in X \,:\, [m(a)]^\circ \sqsubseteq_{\mathbb{I}} m^\circ(a)\}\,.$$

We introduce the abstract systems $\mathcal{M}^\circ$.

Definition 32 (Abstract System)**.** *An abstract* system M° *is a tuple* $(\Sigma, \mathcal{R}, s_0, \mathfrak{p})$*:*

- Σ *is a finite set of* species names *of size n;*
- $\mathcal{R} = \{R_1, \ldots, R_m\}$*,* $R_i \in \mathcal{MS}(\Sigma) \times \mathcal{MS}(\Sigma) \times \mathbb{R}_{\geqslant 0}$*, is a set of not-null* [1] rewriting rules*;*
- $s_0 \in \mathcal{MS}(\Sigma)$ *is the* starting state*;*
- $\mathfrak{p} \in \widehat{\mathbb{P}}_{\mathcal{R}}(\mathcal{R})$ *is a set of predicates which is a partition w.r.t. the set of rules* $\mathcal{R}$ *over* Σ*.*

We denote the universe of abstract models as $\mathcal{M}^\circ$.

Note that, using a set of predicates that is a partition w.r.t. a set of rules guarantees that all the concrete states abstracted by a an abstract multiset shares the same set of applicable rules. That is, as the following theorem states, if a rule is applicable in $m \in \gamma_{\mathcal{MS}}(m^\circ)$, then, $\forall m' \in \gamma_{\mathcal{MS}}(m^\circ)$, the rule is applicable to m'.

Lemma 5.2.1. *Let* $M^\circ = (\Sigma, \mathcal{R}, s_0, \mathfrak{p}) \in \mathcal{M}^\circ$*. For each* $s \in \mathcal{MS}^\circ(\Sigma)\,,\ s', s'' \in \gamma_{\mathcal{MS}}(\alpha_{\mathcal{MS}}(\mathfrak{p})(s))$ *and* $R = (r, l, k) \in \mathcal{R}$*,*

$$IsApplicable(R, s') \Leftrightarrow IsApplicable(R, s'')$$

where $IsApplicable(R = (l, r, k), s') \equiv l \subseteq s'$*.*

Proof. As $IsApplicable(R, s')$, $\forall a \in \Sigma\,,\ l(a) \leq s'(a)$. Let $\alpha_{\mathcal{MS}}(\mathfrak{p})(s_0) = [x_{min}, x_{max}]$, reasoning for a generic $a \in \Sigma$, given that $s' \in \gamma_{\mathcal{MS}}(\alpha_{\mathcal{MS}}(\mathfrak{p})(s_0))$, we have that $x_{min} \geq l(a)$ (by Definitions 32 and 30).

On the other side we have that, as $s'' \in \gamma_{\mathcal{MS}}(s_0{}^\circ)$, we have that $\forall a \in \Sigma\,,\ s''(a) \geq x_{min}$, that is $l \subseteq s''$, and thus $IsApplicable(R, s'')$. As the reasoning can be done also in the other sense, $\Leftrightarrow$ holds. □

[1] That is, not $\forall a \in \Sigma \,:\, l(a) = r(a) = 0$.

We now introduce an order over abstract models $\sqsubseteq_{\mathcal{M}^\circ}$ based on an order $\sqsubseteq_{\widehat{\mathbb{P}}}$ over the associated set of predicates.

An *approximation order over set of predicates* is defined as follows. The $\top$ of such an order is the infinite set $\mathfrak{p}^\bullet$ of predicates consisting of a precise interval for each possible value of each species in a system. Formally $\mathfrak{p}^\bullet(\Sigma) = \bigcup_{a\in\Sigma,\, x\in\mathbb{N}}\{(a, x^\bullet)\}$[2]. Note that $\forall \mathfrak{p} \in \widehat{\mathbb{P}}(\Sigma) \,:\, \mathfrak{p}^\bullet(\Sigma) \sqsubseteq_{\widehat{\mathbb{P}}} \mathfrak{p}$, and that $\forall s \in \mathcal{MS} \,:\, \gamma_{\mathcal{MS}^\circ}(\alpha_{\mathcal{MS}^\circ}(\mathfrak{p}^\bullet)(s)) = \{s\}$.

Definition 33 (Order on Set of Predicates)**.** *Given* sets of predicates $\mathfrak{p}_1, \mathfrak{p}_2 \in \widehat{\mathbb{P}}(X)$ *we say that* $\mathfrak{p}_1 \sqsubseteq_{\widehat{\mathbb{P}}} \mathfrak{p}_2$ *iff*

$$\forall\, p_1 = (a_1, i_1) \in \mathfrak{p}_1 \,:\, \exists!\, p_2 = (a_2, i_2) \in \mathfrak{p}_2 \text{ s.t. } a_1 = a_2 \wedge i_1 \sqsubseteq_{\mathbb{I}} i_2\,.$$

Definition 34 (Order on Abstract Systems)**.** *Let* $M_i^\circ = (\Sigma_i, \mathcal{R}_i, s_{0,i}, \mathfrak{p}_i)$ *for* $i \in \{1, 2\}$. *We say that*

$$M_1^\circ \sqsubseteq_{\mathcal{M}^\circ} M_2^\circ \text{ iff } (\alpha_{\mathcal{MS}}(\mathfrak{p}_1)(s_{0,1}) \sqsubseteq_{\mathcal{MS}} \alpha_{\mathcal{MS}}(\mathfrak{p}_2)(s_{0,2})) \wedge (\mathfrak{p}_1 \sqsubseteq_{\widehat{\mathbb{P}}} \mathfrak{p}_2)\,.$$

Intuitively, an abstract system $M^\circ{}_1$ is more precise than another $M^\circ{}_2$ if: (*a*) $M^\circ{}_1$ and $M^\circ{}_2$ have the same rules over the same set of species; (*b*) if the best abstraction of the initial state of $M^\circ{}_1$ is finer than that of the initial state of $M^\circ{}_1$; (*c*) if $M^\circ{}_1$ has a finer set of predicates than $M^\circ{}_2$.

To relate a concrete system to its best approximation, and vice versa, we introduce the following *abstraction and concretization functions*.

Definition 35 (Abstraction and Concretization Functions)**.**
We define $\alpha : \widehat{\mathbb{P}}_{\mathcal{R}} \mapsto \mathcal{M} \mapsto \mathcal{M}^\circ$ *and* $\gamma : \mathcal{M}^\circ \mapsto \mathcal{M}(\mathcal{M})$ *such that* $\forall M \in \mathcal{M}, \forall M^\circ \in \mathcal{M}^\circ$:

- $\alpha(\mathfrak{p})((\Sigma, \mathcal{R}, s_0)) = (\Sigma, \mathcal{R}, s_0, \mathfrak{p})$*;*
- $\gamma(M^\circ = (\Sigma, \mathcal{R}, s_0{}^\circ, \mathfrak{p})) = \{M \,|\, \alpha(\mathfrak{p})(M) \sqsubseteq_{\mathcal{M}^\circ} M^\circ\}\,.$

5.3 Abstract Labelled Transition System Semantics

We present an abstract, LTS semantics that approximates both the states and the transitions of the concrete LTS semantics, using intervals.

[2] In the following we omit Σ when it is clear from the context.

In the following we use the notation $s' \xrightarrow{\mu, r} s''$ to refer to a transition, labeled by μ, r, in the concrete probabilistic maximally parallel semantics as defined in Section 4.3. Formally, $s' \xrightarrow{\mu, r} s''$ stands for $IsMaximal(\mu, s', \mathcal{R}) \wedge r = Rate(\mu, s', \mathcal{R}) \wedge s'' = Apply(\mu, s', \mathcal{R})$.

We introduce the LTS semantics associated with abstract systems adopting an *abstract transition* relation $s'^{\circ} \xrightarrow{\mu^{\circ}, r^{\circ}} s''^{\circ}$ where $s^{\circ\prime}, s^{\circ\prime\prime} \in \mathcal{MS}^{\circ}$ are abstract states, $\mu^{\circ} \in \mathcal{MS}^{\circ}$ is an *abstract multiset of rule applications* and $r^{\circ} \in \mathbb{I}$ an *abstract transition rate*.

Formally, the abstract LTS we consider are tuples $(S^{\circ}(\mathfrak{p}), s_0{}^{\circ}, \rightarrow_{\circ})$ such that: $S^{\circ}(\mathfrak{p}) \subset \mathcal{MS}^{\circ}(\Sigma)$ is an abstract state space, with respect to a set of predicates $\mathfrak{p} \in \widehat{\mathbb{P}}(\Sigma)$; $s_0{}^{\circ} \in S^{\circ}(\mathfrak{p})$ is an abstract starting state; and $\rightarrow_{\circ} \subseteq \mathcal{MS}^{\circ} \times \mathcal{MS}^{\circ} \times \mathbb{I} \times \mathcal{MS}^{\circ}(\mathcal{R})$ is an abstract transition relation s.t. $\forall\, s^{\circ}, s^{\circ\prime} \in S^{\circ}(\mathfrak{p})\,, \exists!\, s^{\circ} \xrightarrow{\mu^{\circ}, r^{\circ}} s'^{\circ}$ for some μ° and r°. In the following we use $\mathcal{LTS}^{\circ}$ to denote the universe of abstract LTSs.

We define the function $LTS^{\circ} : \mathcal{M}^{\circ} \mapsto \mathcal{LTS}^{\circ}$ such that $LTS^{\circ}((\Sigma, \mathcal{R}, s_0{}^{\circ}, \mathfrak{p})) = (S^{\circ}(\mathfrak{p}), s_0{}^{\circ}, \rightarrow_{\circ})$ where $s_0{}^{\circ} = \alpha_{\mathcal{MS}}(\mathfrak{p})(s_0)$, $S^{\circ}(\mathfrak{p}) = \{s^{\circ} \in \mathcal{MS}^{\circ}(\Sigma) \,|\, \forall a \in \Sigma : \exists!\, p \in \mathfrak{p}(a) \text{ s.t. } s^{\circ} \vDash_{\mathbb{P}} p\}$, and $\rightarrow_{\circ}$ is obtained by the following inference rule (5.1) starting from $s_0{}^{\circ}$.

$$\frac{s''^{\circ} \in \widehat{Next}^{\circ}(\mathcal{R})(s^{\circ\prime}, \mathfrak{p}) \qquad \mu^{\circ} = \widehat{f^{\circ}}(\mathcal{R})(s'^{\circ}, s''^{\circ}) \qquad r^{\circ} = Rate^{\circ}(\mathcal{R})(\mu^{\circ}\,,\, s'^{\circ}\,,\, s''^{\circ})}{s'^{\circ} \xrightarrow{\mu^{\circ}, r^{\circ}}_{\circ} s''^{\circ}} \tag{5.1}$$

Rule (5.1) gives the abstract transitions, exiting from an abstract state $s^{\circ\prime}$. This is based on the calculation of a reachable abstract state $s^{\circ\prime}$, of an abstract multiset of rules μ° and of the associated abstract rate r°. The computation reachable abstract states (i.e. the $\widehat{Next}^{\circ}$ function) is described in Section 5.3.1, the computation of abstract maximally parallel application of rules (i.e. $\widehat{f^{\circ}}$ function) in Section 5.3.2 and their rates (i.e. the $Rate^{\circ}$ function) in Section 5.3.3. Finally we discuss the soundness of such an abstract LTS semantics with respect to the concrete one in Section 5.3.4.

5.3.1 Computation of Reachable Abstract States

The $\widehat{Next}^{\circ}(\mathcal{R}) : \mathcal{MS}^{\circ} \times \mathbb{P} \mapsto \mathcal{MS}^{\circ}$ function computes an over-approximation of the set of states reachable from an abstract state by the execution of a single maximal step. Formally, $\widehat{Next}^{\circ}(\mathcal{R})(s^{\circ}, \mathfrak{p})$ approximates the set of abstract

states corresponding to the concrete moves. Thus, its most precise value is $Next^{\circ}(\mathcal{R})(s^{\circ}, \mathfrak{p}) = \{s'^{\circ} \mid \exists\, s' \in Next(s, \mathcal{R}) \mid s \in \gamma_{\mathcal{MS}}(s^{\circ}), s^{\circ\prime} = \alpha_{\mathcal{MS}}(\mathfrak{p})(s')\}$ where $Next(s, \mathcal{R}) = \{s' | s \xrightarrow{\mu, r} s'\}$.

In order to approximate $Next^{\circ}$, for each species, we calculate a lower and an upper bound on the concentrations reachable by a single step of the semantics, and then we decompose such bounds by means of a predicate.

To this aim, we define $Decompose(s^{\circ}, \mathfrak{p}) : \mathcal{MS}^{\circ} \times \mathbb{P} \mapsto Parts(\mathcal{MS}^{\circ})$ as

$$Decompose(s^{\circ}, \mathfrak{p}) = \{s^{\circ\prime} \mid s^{\circ\prime} = \alpha_{\mathcal{MS}}(\mathfrak{p})(s) \ \wedge \ s \in \gamma_{\mathcal{MS}}(s^{\circ})\}\,.$$

Intuitively, given an abstract multiset s° and a set of predicates $\mathfrak{p}$, *Decompose* computes the minimum set of abstract multiset, w.r.t. to $\mathfrak{p}$, that covers all the concrete states represented by s°.

Then, we define $\widehat{Next}^{\circ}(\mathcal{R})(s^{\circ}, \mathfrak{p}) = Decompose(MR(s^{\circ}, \mathcal{R}), \mathfrak{p})$ where $MR(s^{\circ}, \mathcal{R})$ (for Max Reachable) is defined as follows: $\forall a \in \Sigma$

$$MR(s^{\circ}, \mathcal{R})^{\circ}(a)^{-} = \begin{cases} 0 & \text{if } \exists R = (l, r, k) \in \mathcal{R} : \\ & l(a) > 0 \ \wedge [s^{\circ}(a)]^{-} \geq l(a) \\ [s^{\circ}(a)]^{-} & \text{otherwise} \end{cases}$$

$$MR(s^{\circ}, \mathcal{R})^{\circ}(a)^{+} = \begin{cases} (\sum_{b \in \Sigma,\, r \in [1,m]} PR(b, a, r) * [s^{\circ}(b)]^{+}) + X & \text{if } \exists R = (l, r, k) \in \mathcal{R} : \\ & r(a) > 0 \wedge \\ & [s^{\circ}(a)]^{+} \geq l(a) \\ [s^{\circ}(a)]^{+} & \text{otherwise} \end{cases}$$

$$\text{where } X = \begin{cases} 0 & \text{if } \exists R = (l, r, k) \in \mathcal{R} \ : \ ContextFree(R, a) \\ [s^{\circ}(a)]^{+} & \text{otherwise} \end{cases}$$

and *PR*(standing for Production Ratio)

$$\forall i, j \in [1, n], \forall r \in [1, m] \ : \ PR(b, a, r) = \lceil R_r(a)/L_r(b) \rceil\,.$$

The following lemma states the monotonicity of *Decompose* and of *MR*.

Lemma 5.3.1. *Given* $s^{\circ\prime}, s^{\circ\prime\prime} \in \mathcal{MS}^{\circ}$, $s^{\circ\prime} \sqsubseteq_{\mathcal{MS}^{\circ}} s^{\circ\prime\prime}$ *and* $\mathfrak{p} \in \mathbb{P}$ *:*

i) $Decompose(s^{\circ\prime}, \mathfrak{p}) \subseteq Decompose(s^{\circ\prime\prime}, \mathfrak{p})$

ii) $MR(s^{\circ\prime}, \mathcal{R}) \sqsubseteq_{\mathcal{MS}^\circ} MR(s^{\circ\prime\prime}, \mathcal{R})$

Proof.

i) As $\gamma_{\mathcal{MS}}(s^{\circ\prime}) \subseteq \gamma_{\mathcal{MS}}(s^{\circ\prime\prime})$ it follows that $\bigcup_{s' \in \gamma_{\mathcal{MS}}(s^{\circ\prime})} \alpha_{\mathcal{MS}}(\mathfrak{p})(s') \subseteq \bigcup_{s'' \in \gamma_{\mathcal{MS}}(s^{\circ\prime\prime})} \alpha_{\mathcal{MS}}(\mathfrak{p})(s'')$ and so $Decompose(s^{\circ\prime}, \mathfrak{p}) \subseteq Decompose(s^{\circ\prime\prime}, \mathfrak{p})$.

ii) About $[MR(s^{\circ\prime}, \mathcal{R})]^-$, we have two cases :

- $\exists a \in \sigma, R \in \mathcal{R} : L(a) > 0$: $[MR(s^{\circ\prime}, \mathcal{R})]^- = 0 = [MR(s^{\circ\prime\prime}, \mathcal{R})]^-$
- otherwise : $[MR(s^{\circ\prime}, \mathcal{R})]^- = [s^{\circ\prime}]^- \leq [s^{\circ\prime\prime}]^- = [MR(s^{\circ\prime\prime}, \mathcal{R})]^-$.

On the other hand, about $[MR(s^{\circ\prime}, \mathcal{R})]^+$, we have two cases :

- $\exists\, a \in \sigma, R \in \mathcal{R} : R(a) > 0$:
  $MR(s^{\circ\prime}, \mathcal{R})^\circ(a)^+ = \sum_{b \in \Sigma,\, r \in [1,m]} PR(b, a, r) * [s^{\circ\prime}(b)]^+ + X'$
  $MR(s^{\circ\prime\prime}, \mathcal{R})^\circ(a)^+ = \sum_{b \in \Sigma,\, r \in [1,m]} PR(b, a, r) * [s^{\circ\prime\prime}(b)]^+ + X''$, where

$$X', X'' = \begin{cases} 0\,,\ 0 & \text{if } \exists R = (l, r, k) \in \mathcal{R} : \\ & ContextFree(R, a) \\ [s^{\circ\prime}(a)]^+, [s^{\circ\prime\prime}(a)]^+ & \text{otherwise} \end{cases}$$

  and the statement is true given that $\forall a \in \Sigma : s^{\circ\prime}(a) \sqsubseteq_{\mathbb{I}} s^{\circ\prime\prime}(a)$.
- otherwise : $[MR(s^{\circ\prime}, \mathcal{R})]^+ = [s^{\circ\prime}]^+ \leq [s^{\circ\prime\prime}]^+ = [MR(s^{\circ\prime\prime}, \mathcal{R})]^+$.

□

The following theorem states the soundness of $\widehat{Next}^\circ$ and its monotonicity.

Theorem 5.3.2. *$\widehat{Next}^\circ$ is*

i) is a sound approximation of $Next^\circ$; formally

$$\forall s \in \mathcal{MS}^\circ\,,\ \mathfrak{p} \in \mathbb{P} :\ Next^\circ(\mathcal{R})(s^\circ, \mathfrak{p}) \subseteq \widehat{Next}^\circ(\mathcal{R})(s^\circ, \mathfrak{p})$$

ii) is monotone; formally $\forall s^{\circ\prime}, s^{\circ\prime\prime} \in \mathcal{MS}^\circ$:

$$s^{\circ\prime} \sqsubseteq_{\mathcal{MS}^\circ} s^{\circ\prime\prime} \Rightarrow \widehat{Next}^\circ(\mathcal{R})(s^{\circ\prime}, \mathfrak{p}) \subseteq \widehat{Next}^\circ(\mathcal{R})(s^{\circ\prime\prime}, \mathfrak{p})$$

Proof. *i*) As $\widehat{Next}^{\circ}(\mathcal{R})(s^{\circ}, \mathfrak{p})$ is obtained applying $\alpha_{\mathcal{MS}}(\mathfrak{p})$ to each state in $\bigcup_{MR(s^{\circ},\mathcal{R})} \gamma_{\mathcal{MS}}(s)$, we prove that $\{s' \in Next(s, \mathcal{R}, \mathfrak{p}) | s \in \gamma_{\mathcal{MS}}(s^{\circ})\} \subseteq \bigcup_{MR(s^{\circ},\mathcal{R})} \gamma_{\mathcal{MS}}(s)$. Let's assume the previous statement to be false, that is $\exists\, s^{*} \in \{Next(s, \mathcal{R}) \mid s \in \gamma_{\mathcal{MS}}(s^{\circ})\}$ s.t. $s^{*} \notin \bigcup_{MR(s^{\circ},\mathcal{R})} \gamma_{\mathcal{MS}}(s)$. This means that $s^{*\circ} = \alpha_{\mathcal{MS}}(\mathfrak{p})(s^{*}) \not\sqsubseteq_{\mathcal{MS}^{\circ}} MR(s^{\circ}, \mathcal{R})$, that can happen only in one the following cases: $\exists a \in \Sigma$ s.t.

- $[s^{*\circ}(a)]^{-} \leq 0$ that is impossible;
- $[s^{*\circ}(a)]^{-} \leq [s^{\circ}(a)]^{-}$ and $\neg TC(a, \mathcal{R})$ that is impossible as the species a can not be consumed;
- $[s^{*\circ}(a)]^{+} \geq [s^{\circ}(a)]^{+}$ and $\neg TP(a, \mathcal{R})$ that is impossible as the species a can not be produced;
- $[s^{*\circ}(a)]^{+} \geq max_{a,b\in\Sigma,\, r\in[1,m]} PR(b, a, r) * [s^{\circ\prime}(b)]^{+}$ that means applying some rules more times that the available reactants. This is impossible as a rule application consumes a least an individual of a species.

ii) As $Decompose(MR(s^{\circ\prime}, \mathcal{R})) \subseteq Decompose(MR(s^{\circ\prime\prime}, \mathcal{R}))$ by the previous Theorem.

□

5.3.2 Computation of Abstract Maximally Parallel Rule Applications

Abstract maximally parallel rule applications, expressed as abstract multisets, reported on abstract LTS transitions, approximate the multisets of maximally parallel rule application reported be the corresponding concrete LTS.

Function $\widehat{f^{\circ}}(\mathcal{R}) : \mathcal{MS}^{\circ} \times \mathcal{MS}^{\circ} \mapsto \mathcal{MS}^{\circ}$ computes an approximation of the maximally parallel multisets of rules which produces a move from an abstract state to another one using the rules in $\mathcal{R}$.

Let $f^{\circ}(\mathcal{R})(s'^{\circ}, s''^{\circ})$ the abstract multiset abstracting the set of multisets associated with all transitions, from one of the concrete states abstracted by s'° to one of the concrete states abstracted by s''°.

Formally,

$$f^{\circ}(\mathcal{R})(s'^{\circ}, s''^{\circ}) = \bigcup^{\mathcal{MS}^{\circ}} \{\mu^{\bullet} \mid s' \xrightarrow{\mu, r} s'',\ s' \in \gamma_{\mathcal{MS}}(s'^{\circ}),\ s'' \in \gamma_{\mathcal{MS}}(s''^{\circ})\}.$$

Note that the computation of $f^{\circ}(\mathcal{R})(s'^{\circ}, s''^{\circ})$ requires to build all the transitions of the concrete semantics between each pair of concrete states

abstracted by s'° and s''°, respectively. We, therefore, introduce the function $\widehat{f^{\circ}}$, that computes in effective way and approximation of f°. In particular, $\widehat{f^{\circ}}(\mathcal{R})(s'^{\circ}, s''^{\circ})$ gives an approximation of the abstraction of concrete transitions between concrete multisets abstracted by s'° and s''°.

The abstract function $\widehat{f^{\circ}}$ uses a Δ function, that applied to two multisets returns their difference, while applied to abstract multisets returns bounds on the difference between all the corresponding concrete multisets.

Formally, let

$$\Delta : ((\mathcal{MS} \times \mathcal{MS}) \cup (\mathcal{MS}^{\circ} \times \mathcal{MS}^{\circ})) \mapsto (\mathcal{MS} \cup \mathcal{MS}^{\circ}) \text{ be s.t. } \forall a \in \Sigma$$

$$\forall m', m'' \in \mathcal{MS} \ : \ \Delta(m', m'') = m' - m'' \in \mathcal{MS} \text{ and}$$

$\forall m^{\circ\prime}, m^{\circ\prime\prime} \in \mathcal{MS}^{\circ}$:

$$\Delta(m^{\circ\prime}, m^{\circ\prime\prime})(a) = [[m''^{\circ}(a)]^{-} - [m'^{\circ}(a)]^{+}\ ,\ [m''^{\circ}(a)]^{+} - [m'^{\circ}(a)]^{-}] \in \mathcal{MS}^{\circ}\ .$$

The following lemma states that Δ applied to two abstract multisets $m^{\circ\prime}, m^{\circ\prime\prime}$ is a sound approximation of Δ applied to each pair of multisets $m' \in \gamma_{\mathcal{MS}}(m^{\circ\prime}), m'' \in \gamma_{\mathcal{MS}}(m^{\circ\prime\prime})$.

Lemma 5.3.3. $\forall a \in \Sigma,\ m^{\circ\prime}, m^{\circ\prime\prime} \in \mathcal{MS}^{\circ},\ m' \in \gamma_{\mathcal{MS}}(m^{\circ\prime}),\ m'' \in \gamma_{\mathcal{MS}}(m^{\circ\prime\prime})$: $[\Delta(m', m'')(a)]^{\bullet} \sqsubseteq_{\mathbb{I}} \Delta(m^{\circ\prime}, m^{\circ\prime\prime})(a)$

Proof. We have to prove $\forall a \in \Sigma \ : \ s''(a) - s'(a) \geq [s^{\circ\prime\prime}(a)]^{-} - [s^{\circ\prime\prime}(a)]^{+}$, that is true as $s''(a) \geq [s^{\circ\prime\prime}(a)]^{-}$ and $s'(a) \leq [s^{\circ\prime}(a)]^{+}$. The same reasoning applies to $s''(a) - s'(a) \leq [s^{\circ\prime\prime}(a)]^{+} - [s^{\circ\prime\prime}(a)]^{-}$ □

We now introduce function $\widehat{f^{\circ}}$, as the least fixpoint of a function $\widehat{f^{\circ(n)}}$, where at each refinement step not well formed abstract multisets are eliminated. Formally, it is defined as, $\forall_{i \in [1,m]}$:

$$\widehat{f^{\circ}}(\mathcal{R})(s'^{\circ}, s''^{\circ})(i) = \begin{cases} \mu(i) & \text{if } \mu = FixPoint(\widehat{f^{\circ(n)}}(\mathcal{R})(s'^{\circ}, s''^{\circ})) \wedge WellFormed(\mu) \\ [0,0] & \text{otherwise.} \end{cases}$$

where $\widehat{f^{\circ(n)}}$ is defined as

$$\widehat{f^{\circ(n)}}(\mathcal{R})(s'^{\circ}, s''^{\circ})(i) = \begin{cases} \widehat{f^{\circ(n-1)}}(\mathcal{R})(s'^{\circ}, s''^{\circ})(i) & \text{if } n > 0 \wedge \\ & Precise(\widehat{f^{\circ(n-1)}}(\mathcal{R})(s'^{\circ}, s''^{\circ})(i)) \\ X & \text{otherwise} \end{cases}$$

and

$$X = [\ \max_{a\in\Sigma}\{$$
$$\{\lceil[\Delta(sMod^{\circ\prime}, sMod^{\circ\prime\prime})(a)]^{-}/R_i(a)\rceil \text{ s.t. } [\Delta(sMod^{\circ\prime}, sMod^{\circ\prime\prime})(a)]^{-} > 0 \wedge R_i(a) > 0 \wedge OP(i,a,rMod))\} \quad \cup$$

$$\{\lceil-[\Delta(sMod^{\circ\prime}, sMod^{\circ\prime\prime})(a)]^{+}/L_i(a)\rceil \text{ s.t. } [\Delta(sMod^{\circ\prime}, sMod^{\circ\prime\prime})(a)]^{+} < 0 \wedge L_i(a) > 0 \wedge OC(i,a,rMod)\} \cup \{0\} \quad \},$$

$$\min_{a\in\Sigma}\{$$
$$\{\lfloor[\Delta(sMod^{\circ\prime}, sMod^{\circ\prime\prime})(a)]^{+}/R_i(a)\rfloor \text{ s.t. } [\Delta(sMod^{\circ\prime}, sMod^{\circ\prime\prime})(a)]^{+} \geq 0 \wedge R_i(a) > 0 \wedge \neg TOC(i,a,rMod)\} \quad \cup$$

$$\{\lfloor[sMod^{\circ\prime\prime}(a)]^{+}/R_i(a)\rfloor \text{ s.t. } R_i(a) > 0 \wedge TOC(i,a,rMod)\} \quad \cup$$

$$\{\lfloor-[\Delta(sMod^{\circ\prime}, sMod^{\circ\prime\prime})(a)]^{-}/L_i(a)\rfloor \text{ s.t. } [\Delta(sMod^{\circ\prime}, sMod^{\circ\prime\prime})(a)]^{-} \leq 0 \wedge L_i(a) > 0 \wedge \neg TOP(i,a,rMod\,)\} \quad \cup$$

$$\{\lfloor[sMod^{\circ\prime}(a)]^{+}/L_i(a)\rfloor \text{ s.t. } L_i(a) > 0 \wedge TOP(i,a,rMod)\} \quad \}\ ]$$

where (for R_i Only Producer of a, R_i Only Consumer of a)
$OP(i,a,\mathcal{R}) = \wedge_{ii\in[1,m]} R_{ii}(a) = 0$ and $UC(i,a,\mathcal{R}) = \wedge_{ii\in[1,m]} L_{ii}(a) = 0$,
and (for There is Other rule Consuming, There is Other rule Producing a)
$TOC(i,a,\mathcal{R}) = (\exists \mathcal{R}[j] = (l,r,k)\ j \neq i \text{ s.t. } l(a) \geq 0)$,
$TOP(i,a,\mathcal{R}) = (\exists \mathcal{R}[j] = (l,r,k)\ j \neq i \text{ s.t. } r(a) \geq 0)$ and

$$sMod^{\circ\prime} = \begin{cases} s^{\circ\prime} & \text{if } n = 0 \\ ReacMod(s^{\circ\prime}, \widehat{f^{\circ(n-1)}}(\mathcal{R})(s'^{\circ}, s''^{\circ})) & \text{otherwise} \end{cases},$$

$$sMod^{\circ\prime\prime} = \begin{cases} s^{\circ\prime\prime} & \text{if } n = 0 \\ ProdMod(s^{\circ\prime\prime}, \widehat{f^{\circ(n-1)}}(\mathcal{R})(s'^{\circ}, s''^{\circ})) & \text{otherwise} \end{cases},$$

$$rMod = \begin{cases} \mathcal{R} & \text{if } n = 0 \\ \mathcal{R}'(\mathcal{R}, \widehat{f^{\circ(n-1)}}(\mathcal{R})(s'^{\circ}, s''^{\circ})) & \text{otherwise}, \end{cases}$$

where

$$\mathcal{R}'(\mathcal{R}, \mu^{\circ}) = \mathcal{R}\,\{R_i | R_i \in \mathcal{R}\,,\, [\mu^{\circ}[i]]^{-} = [\mu^{\circ}[i]]^{+}\}\,,$$

and $\forall a \in \Sigma$:

$$ReacMod(s^{\circ}, \mu^{\circ}, \mathcal{R})(a) = [max(0, [s^{\circ}(a)]^{-} - Reac(\mu^{\circ}, \mathcal{R}, a)\,,\, [s^{\circ}(a)]^{+} - Reac(\mu^{\circ}, \mathcal{R}, a)]\,,$$

$$ProdMod(s^{\circ}, \mu^{\circ}, \mathcal{R})(a) = [[s^{\circ}(a)]^{-} + Prod(\mu^{\circ}, \mathcal{R}, a)\,,\, [s^{\circ}(a)]^{+} + Prod(\mu^{\circ}, \mathcal{R}, a)]$$

where

$$Reac(\mu^{\circ}, \mathcal{R}, a) = \begin{cases} \sum_{i=1}^{m} l_i(a)[i] & \text{if } Precise(\mu^{\circ}[i]) \\ 0 & \text{otherwise,} \end{cases}$$

$$Prod(\mu^{\circ}, \mathcal{R}, a) = \begin{cases} \sum_{i=1}^{m} r_i(a)[i] & \text{if } Precise(\mu^{\circ}[i]) \\ 0 & \text{otherwise.} \end{cases}$$

The computation of $\widehat{f^{\circ}}$ is based on the refinement $\widehat{f^{\circ(n)}}$, starting from $\widehat{f^{\circ(0)}}$, until a fixpoint is reached. Since each step of iteration excludes values contained in the previous abstract multiset (i.e. $\widehat{f^{\circ(i+1)}} \sqsubseteq_{\mathcal{MS}^{\circ}} \widehat{f^{\circ(i)}}$), the computation ends, at most with a precise abstract multiset, consisting of a precise number of rule applications. Note that, if $n = 0$, then $rMod = s^{\circ}$ and $rMod = \mathcal{R}$.

Intuitively, $\widehat{f^{\circ(0)}}(\mathcal{R})(s'^{\circ}, s''^{\circ})$ computes the minimum/maximum number of times each single rule, considered in isolation, may/has to be applied in order to produce the difference between $s^{\circ\prime}$ and $s^{\circ\prime\prime}$ (expressed by $\Delta(s'^{\circ}, s''^{\circ})$). The result depends on whether the considered rule is the only producer or the only consumer of a certain species.

More in details, the value $\widehat{f^{\circ(0)}}(\mathcal{R})(s'^{\circ}, s''^{\circ})[i]^{-}$ corresponds to the strongest constraint (i.e. the maximum) about the minimum number the rule has to be applied to produce a positive $[\Delta s^{\circ}(a)]^{-}$ (for each species a for which the rule is a producer), and the number of times the rule has to be applied to produce a negative $[\Delta s^{\circ}(a)]^{+}$ (for each species a for which the rule is a consumer). Finally, when the considered rule is neither the only producer nor the only consumer

of all the species, or when the $\Delta s^{\circ}(a)$ is equal to $0^{\bullet}$ for all the species in the reactants or the products of the rule, it may be applied a minimum of 0 times.

To compute the maximum $\widehat{f^{\circ(0)}}(\mathcal{R})(s'^{\circ}, s''^{\circ})[i]^{+}$ we consider the strongest constraint (i.e. the minimum) of the following values, $\forall a \in \Sigma$:

- if the rule R_i produces a
  - and there are not other rules consuming a, having that $[\Delta(s^{\circ\prime}, s^{\circ\prime\prime})(a)]^{+} > 0$, we consider $\lfloor [\Delta(s^{\circ\prime}, s^{\circ\prime\prime})(a)]^{+} / R_i(a) \rfloor$. Actually it may happen that the rule R_i produces all the a of $[\Delta(s^{\circ\prime}, s^{\circ\prime\prime})(a)]^{+}$;
  - and there are other rules consuming a, we consider $\lfloor [s^{\circ\prime}(a)]^{+} / L_i(a) \rfloor$. Actually it may happen that all the available a are consumed by the rule R_i (and possibly produced up to $[s^{\circ\prime\prime}(a)]^{+}$ by other rules).
- if the rule R_i consumes a
  - and there are not other rules producing a, having that $[\Delta(s^{\circ\prime}, s^{\circ\prime\prime})(a)]^{-} < 0$, we consider $\lfloor -[\Delta(s^{\circ\prime}, s^{\circ\prime\prime})(a)]^{-} / L_i(a) \rfloor$. Actually it may happen that the rule R_i consumes all the a of $[\Delta(s^{\circ\prime}, s^{\circ\prime\prime})(a)]^{-}$;
  - and there are other rules producing a, we consider $\lfloor [s^{\circ\prime\prime}(a)]^{+} / R_i(a) \rfloor$. Actually it may happen that all the a in the arrival state are produced by the rule R_i
    (e.g. all the occurrences of a are consumed by to other rules and then the number of a reaches $[s^{\circ\prime\prime}(a)]^{+}$ by applications of R_i).

The value of $\widehat{f^{\circ(n)}}$, for $n > 0$, is computed by refining $\widehat{f^{\circ(n-1)}}$. In particular, the approximation is refined by removing from $\widehat{f^{\circ(n-1)}}$ values corresponding to a not possible number of rule applications, by exploiting the exact values possibly contained in $\widehat{f^{\circ(n-1)}}$. In order to realize such computation, we consider: (a) a modified difference between starting and arrival state, taking into account the applications of rules with an exact multiplicity in the previous approximation (i.e. $\Delta(sMod^{\circ\prime}, sMod^{\circ\prime\prime})$); and (b) a set of rules $\mathcal{R}' \subset \mathcal{R}$, reproducing such a refined difference, in which rules with an exact multiplicity in the previous approximation are removed (i.e. $rMod$). In fact, if $\widehat{f^{\circ}}^{(n-1)}[i]^{-} = \widehat{f^{\circ}}^{(n-1)}[i]^{+}$, for some $i \in [1, m]$, we can construct $sMod^{\circ\prime}, sMod^{\circ\prime\prime}$ so that the starting state and the arrival state are modified by the application of such rules, and we can remove such rules from the set of rule applicable for realizing the remaining state change.

The following lemma states the soundness of the approximation given by $\widehat{f^\circ}$ w.r.t f°.

Lemma 5.3.4. $\forall s^{\circ\prime}, s^{\circ\prime\prime} \in \mathcal{MS}^\circ : f^\circ(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime}) \sqsubseteq_{\mathcal{MS}^\circ} \widehat{f^\circ}(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime})$.

Proof. See Section 5.9 □

5.3.3 Computation of Abstract Transition Rates

We introduce the abstract rate function, computing the rate of an abstract maximally parallel application of rules, $Rate^\circ(\mathcal{R}) : \mathcal{MS}^\circ(\mathcal{R}) \times \mathcal{MS}^\circ \times \mathcal{MS}^\circ \mapsto \mathbb{I}$. In particular, $Rate^\circ(\mathcal{R})(\mu^\circ, s'^\circ, s''^\circ)$ calculates the abstract rate for the move from s'° to s''°, corresponding to the abstract multiset μ°, w.r.t. the rules $\mathcal{R}$. The definition uses an abstract version of the concrete operators KIN, MUL and LIM (defined in Section 4.3): $\widehat{KIN}^\circ$, $\widehat{MUL}^\circ$ e $\widehat{LIM}^\circ$.

Formally, function $Rate^\circ$ is defined as

$$
\begin{aligned}
&Rate^\circ(^\circ)(\mu^\circ, s'^\circ, s''^\circ) = \\
&\quad [\quad [\widehat{MUL}^\circ(\mu^\circ, s^\circ, \mathcal{R})]^- * [\widehat{KIN}^\circ(\mu^\circ, s^\circ, \mathcal{R})]^- * [\widehat{LIM}^\circ(s'^\circ, s''^\circ, \mathcal{R})]^- , \\
&\qquad [\widehat{MUL}^\circ(\mu^\circ, s^\circ, \mathcal{R})]^+ * [\widehat{KIN}^\circ(\mu^\circ, s^\circ, \mathcal{R})]^+ * [\widehat{LIM}^\circ(s'^\circ, s''^\circ, \mathcal{R})]^+ \quad].
\end{aligned}
$$

In order to calculate the abstract multiplicity $\widehat{MUL}^\circ$ we use the interval calculated as follows.

$$
\begin{aligned}
\widehat{MUL}^\circ(\mu^\circ, s^\circ, \mathcal{R}) &= [1,\ \widehat{MUL}^*(s^\circ, \mathcal{R})\ ] \text{ where} \\
\widehat{MUL}^*(s^\circ, \mathcal{R}) &= \prod_{a \in \Sigma} \Upsilon'(a, \mathcal{R})
\end{aligned}
$$

where

$$
\Upsilon'(a, \mathcal{R}) \begin{cases} 1 & \text{if } ContextFree(R, a) \wedge (NAR(s^+(s^\circ), a, \mathcal{R}) = 1\,, \\ \Upsilon(s^+(s^\circ)(a), X) & \text{otherwise} \end{cases}
$$

in which

$$
X = \begin{cases} (NAR(s^+(s^\circ), a, \mathcal{R}) - 1 & \text{if } \exists R \in \mathcal{R} \text{ s.t. } ContextFree(R, a)\,, \\ (NAR(s^+(s^\circ), a, \mathcal{R}) & \text{otherwise }, \end{cases}
$$

and

$$\Upsilon(n,m) \quad = \quad \frac{n!}{\lfloor(\frac{n}{m+1})\rfloor!^{(m+1)}}\,,$$
$$s^+ : \mathcal{MS}^\circ \mapsto \mathcal{MS} \quad \text{s.t.} \quad \forall m^\circ \in \mathcal{MS}^\circ,\, a \in \Sigma \,:\, s^+(m)(a) = [m(a)]^+$$

and (for Number of Applicable Rules),

$$NAR(s,a,\mathcal{R}) = |\{R = (l,r,k) \in \mathcal{R} \,|\, l(a) > 0 \,\wedge\, l(a) \leq s(a)\}|\,.$$

In order to compute the minimum/maximum multiplicity for μ° we consider an approximation of the minimum/maximum multiplicity of the maximally parallel steps abstracted by μ°. The multiplicity of a maximally parallel step depends on the binomial function applied to the number of reactants required by each rule, on the number of applications of the rule, and on the availability of such reactants in the source state. To get an upper bound on such a value we consider an event μ such that $\mu^\bullet \sqsubseteq_{\mathbb{I}} \mu^\circ$ and such that it assigns to each applicable rule a number of reactants equal to $s(a)/X$, for each species $a \in \Sigma$, where X is equal to $NAR(s(a), a, \mathcal{R}) + 1$, if there are not context free rules on a. In this way we compute the multiplicity of a $\mu^\bullet \sqsubseteq_{\mathbb{I}} \mu^\circ$ where each rule takes $s(a)/X$ objects, and $s(a)/X$ are not assigned to any rule. Conversely, when there are context free rules on a, X is equal $NAR(s(a), a, \mathcal{R})$, since, by maximally parallelism, all the individuals of species a have to be assigned to some rule.

The step $\mu^\bullet \sqsubseteq_{\mathbb{I}} \mu^\circ$ constructed in this way, in practice, is not always possible, as it may be the case that: (a) the number of reactants given to each rule $R = (l,r,k)$ by μ may be not a multiple of $l(a)$; (b) the number of times each rule can be applied is limited by the availability of all the species in l (i.e. it is limited by the minimum, for $a \in \Sigma$, $\lfloor s(a)/l(a) \rfloor$). Both these cases are, instead, not considered in the computation of μ°. Hence, considering the not realistic situation where each rule takes, for each species, $s(a)/X$ elements, we get an upper bound on the values of MUL. On the other side, to get a lower bound for MUL we safely consider 1.

The following lemma states the soundness of the approximation given by the abstract operator $\widehat{MUL}^\circ$ w.r.t. its concrete version MUL.

Lemma 5.3.5. $\forall\, \mu \in \mu^\circ\,,\ s^\circ \in \mathcal{MS}^\circ(\Sigma)\,, s \in \gamma_{\mathcal{MS}}(s^\circ)\ :$

$$[MUL(\mu, s, \mathcal{R})]^\bullet \sqsubseteq_{\mathbb{I}} \widehat{MUL}^\circ(\mu^\circ, s^\circ, \mathcal{R})\,.$$

Proof. See Section 5.9 □

For the kinetic part of the rate function $\widehat{KIN}^\circ$ we use the interval calculated as follows.

$$\widehat{KIN}^\circ(\mu^\circ, s^\circ, \mathcal{R}) = \\ [\prod_{r\in[1,m]} LRR(r, s^-(s^\circ), \mathcal{R})^{[\mu^\circ[r]]^+}\,,\ \prod_{r\in[1,m]} LRR(r, s^+(s^\circ), \mathcal{R})^{[\mu^\circ[r]]^-}\ ]$$

where *LRR* is defined as in the concrete case (Section 4.3).
To compute the minimum/maximum kinetics for an abstract multiset μ° we consider the minimum/maximal kinetics over the maximally parallel steps abstracted by μ°. The kinetics of a maximally parallel step depends to the number of rules applicable in the source state (by the *LRR* term), and it is inversely proportional to the number of times each rule is applied. Note that all the concrete states abstracted by an abstract state share the same set of applicable rules (see Lemma 5.2.1). As a consequence, for each $R_r \in \mathcal{R}$, $LRR(r, s, \mathcal{R})$ is the same for all $s \in \gamma_{\mathcal{MS}}(s'^\circ)$. For this reason to get lower/upper bound for the value of *KIN* we take an approximation of the maximum/minimum number of times each rule $R_r \in \mathcal{R}$ can be applied, $[\mu^\circ[r]]^-/[\mu^\circ[r]]^+$, from any one of the concrete states abstracted by the source abstract state [3].

The following lemma states the soundness of the approximation given by $\widehat{KIN}^\circ$ w.r.t. *KIN*.

Lemma 5.3.6. $\forall\, \mu \in \mu^\circ\ \ s^\circ \in \mathcal{MS}^\circ(\Sigma)\,, s \in \gamma_{\mathcal{MS}}(s^\circ)\ :$

$$[KIN(\mu, s, \mathcal{R})]^\bullet \sqsubseteq_{\mathbb{I}} \widehat{KIN}^\circ(\mu^\circ, s^\circ, \mathcal{R})$$

Proof. See Section 5.9 □

Finally, function $\widehat{LIM}^\circ$ gives lower and upper bounds on the number of possible concrete transitions between all the concrete states, represented by two abstract states. Let $LIM^\circ(s^{\circ\prime}, s^{\circ\prime\prime}, \mathcal{R})$ be the interval corresponding to the

[3] For convenience we consider the maximum state abstracted by the abstract starting state $s^+(s^\circ)$.

minimum and maximum number of concrete transitions between a multiset abstracted by $s^{\circ\prime}$ ($s' \in \gamma_{\mathcal{MS}}(s^{\circ\prime})$) and one of the multisets abstracted by $s^{\circ\prime\prime}$ ($s'' \in \gamma_{\mathcal{MS}}(s''^{\circ})$). Formally we have:

$$LIM^{\circ}(s^{\circ\prime}, s^{\circ\prime\prime}, \mathcal{R}) = [\quad \min_{s' \in \gamma_{\mathcal{MS}}(s^{\circ\prime})} |\{s' \xrightarrow{\mu, r} s'' \in \rightarrow \wedge\, s'' \in \gamma_{\mathcal{MS}}(s^{\circ\prime\prime})\}|\,, \tag{5.2}$$

$$\max_{s' \in \gamma_{\mathcal{MS}}(s^{\circ\prime})} |\{s' \xrightarrow{\mu, r} s'' \in \rightarrow \wedge\, s'' \in \gamma_{\mathcal{MS}}(s^{\circ\prime\prime})\}| \quad]\,. \tag{5.3}$$

In order to compute an approximated upper bound for $LIM^{\circ}(s^{\circ\prime}, s^{\circ\prime\prime}, \mathcal{R})$ we consider $s^{\circ+}$ as it represents the concrete states, abstracted by s°, with the greatest number of exiting transitions (see Section 4.5). To get a lower bound on $LIM^{\circ}(s^{\circ\prime}, s^{\circ\prime\prime}, \mathcal{R})$ we consider two cases. In the case where there exist concrete states abstracted by the source state which have no transition into any of the concrete states abstracted by the target state (i.e. $\exists\, s' \in \gamma_{\mathcal{MS}}(s^{\circ\prime}) \;:\; \nexists\, s' \xrightarrow{\mu,r} s'' \mid s'' \in \gamma_{\mathcal{MS}}(s^{\circ\prime\prime})$), we use 0. Otherwise, if all the concrete states abstracted by the source state have at least a transition to a state abstracted by the target state, we safely consider 1.

Formally, we define

$$\widehat{LIM}^{\circ}(s^{\circ\prime}, s^{\circ\prime\prime}, \mathcal{R}) = [\psi(s^{\circ\prime}, s^{\circ\prime\prime}, \mathcal{R}), \prod_{a \in \Sigma\,,\, [s^{\circ}(a)]^{+} > 0} \phi(\|(\mathcal{R})_a\|, [s^{\circ}(a)]^{+})]$$

where ϕ is defined similarly[4] as in Section 4.5, that is

$$\phi(m, n) = \begin{cases} 1 & \text{if } m = 1\,, \\ \binom{m+n-1}{n} = \frac{(n+m-1)!}{(m-1)!n!} & \text{otherwise} \end{cases}$$

while $\psi \;:\; \mathcal{MS}^{\circ} \times \mathcal{MS}^{\circ} \times \mathcal{R}$ is defined as

$$\psi(s^{\circ\prime}, s^{\circ\prime\prime}, \mathcal{R}) = \begin{cases} 1 & \text{if } \forall s' \in \gamma_{\mathcal{MS}}(s^{\circ\prime})\, \exists\, s' \xrightarrow{\mu,r} s'' \mid s'' \in \gamma_{\mathcal{MS}}(s^{\circ\prime\prime})\,, \\ 0 & \text{otherwise}\,. \end{cases}$$

As the following lemma states, $\widehat{LIM}^{\circ}(s^{\circ\prime}, s^{\circ\prime\prime}, \mathcal{R})$ is a sound approximation of $LIM^{\circ}(s^{\circ\prime}, s^{\circ\prime\prime}, \mathcal{R})$.

[4] The only difference is that here n can be equal to ∞ and we have to deal with this particular case.

Lemma 5.3.7. $\forall s^{\circ\prime}, s^{\circ\prime\prime} \in \mathcal{MS}^\circ : LIM^\circ(s^{\circ\prime}, s^{\circ\prime\prime}, \mathcal{R}) \sqsubseteq_{\mathbb{I}} \widehat{LIM}^\circ(s^{\circ\prime}, s^{\circ\prime\prime}, \mathcal{R})$

Proof. See Section 5.9 □

The following theorem states the soundness of the abstract rates computed by $Rate^\circ$ w.r.t. the concrete rates computed by $Rate$.

Theorem 5.3.8. $\forall s'^\circ, s''^\circ \in \mathcal{MS}^\circ, s' \in \gamma_{\mathcal{MS}}(s'^\circ), \mu \in \mathcal{MS}(\mathcal{R})$, $[\mu, \mu] \sqsubseteq_{\mathcal{MS}^\circ} \mu^\circ$:

$$[Rate(\mu, s', \mathcal{R})]^\bullet \sqsubseteq_{\mathbb{I}} Rate^\circ(\mathcal{R})(\mu^\circ, s'^\circ, s''^\circ, \mathcal{R}) .$$

Proof. See Section 5.9 □

5.3.4 Soundness of abstract LTS semantics

We prove the soundness of the abstract LTS semantics with respect to the concrete one. The proof is based on a notion of approximation order on abstract LTS, using an approach similar to Section 3.3.4.

To relate an LTS to its abstract counterpart we introduce the concept of *best abstraction of an LTS*. The most precise abstract LTS has the same state space of the original LTS (formally, we use the best abstraction with respect to the most precise partitioning $\mathfrak{p}^\bullet$). For each move from s to s', the abstract multiset $r^\bullet$ and $\mu^\bullet$ are the union and the sum of the associated concrete moves, respectively.

Definition 36 (Best abstraction of LTS)**.** *We define the LTS best abstraction function* $\alpha_{\mathcal{LTS}} : \mathcal{LTS} \mapsto \mathcal{LTS}^\circ$ *such that*

$$\alpha_{\mathcal{LTS}}((S, s_0, \rightarrow)) = ((S^\circ(\mathfrak{p}^\bullet), \alpha_{\mathcal{MS}}(\mathfrak{p}^\bullet)(s_0), \rightarrow^\alpha_\circ))$$

with

$$\rightarrow^\alpha_\circ = \{ s^\circ \xrightarrow{\mu^*, r^*}_\alpha s'^\circ \mid s \xrightarrow{\mu, r} s' \in \rightarrow \ \wedge \ s \in \gamma_{\mathcal{MS}}(s^\circ) \ \wedge \ s' \in \gamma_{\mathcal{MS}}(s'^\circ) \}$$

where

$$(\mu^*, r^*) = (\bigcup^{\mathcal{MS}^\circ} \mu^\bullet, \sum^{\mathbb{I}} r^\bullet) \text{ and } s \xrightarrow{\mu, r} s' \in \rightarrow \ \wedge s \in \gamma_{\mathcal{MS}}(s^\circ) \wedge s' \in \gamma_{\mathcal{MS}}(s'^\circ) .$$

Note that $\alpha_{\mathcal{LTS}}$ introduces the least possible approximation, by means of abstract multisets $\mathcal{MS}^\circ$, to represent sets of multisets $\mathcal{MS}$. Conversely, $\alpha_{\mathcal{LTS}}$ does not introduce any approximation on transition rates, as the following Lemma states.

Lemma 5.3.9. *Given an $lts \in \mathcal{LTS}$ it holds that*

$$\alpha_{\mathcal{LTS}}(lts) = (S^\circ(\mathfrak{p}^\bullet), \alpha_{\mathcal{MS}}(\mathfrak{p}^\bullet)(s_0),\ \rightarrow^\alpha_\circ)\,,$$
$$\forall\, s^\circ, s^{\circ\prime} \in S^\circ(\mathfrak{p}^\bullet)\,,\ s^\circ \xrightarrow{r^\circ,\mu^\circ} s'^\circ \in \rightarrow^\alpha_\circ : [r^\circ]^+ = [r^\circ]^-\,.$$

Proof. By definition of $\alpha_{\mathcal{LTS}}$ ($r^\circ = \sum^{\mathbb{I}} r^\bullet$). □

Moreover, in the abstract LTS
$\alpha_{\mathcal{LTS}}((S, s_0, \rightarrow)) = (S^\circ(\mathfrak{p}^\bullet), \alpha_{\mathcal{MS}}(\mathfrak{p}^\bullet)(s_0), \rightarrow^\alpha_\circ)$ each concrete state is associated with a single abstract state and vice-versa. Formally $\forall s \in S\ !\exists\, s^\circ \in S^\circ(\mathfrak{p}^\bullet)$ s.t. $s \in \gamma_{\mathcal{MS}}(s^\circ)$. In the following we use $s = \gamma_{\mathcal{MS}}(s^\circ)$ to denote such a state. Hence it holds that

$$\{s^\circ \mid s^\circ \in S^\circ(\mathfrak{p}^\bullet)\} = \{\alpha_{\mathcal{MS}}(\mathfrak{p}^\bullet)(s) \mid s \in S\} = \{\gamma_{\mathcal{MS}}(s^\circ) \mid s^\circ \in S^\circ(\mathfrak{p}^\bullet)\} = S\,.$$

We introduce the approximation order on abstract LTSs, $\sqsubseteq_{\mathcal{LTS}^\circ}$. Using the order we can say that $lts^\circ \in \mathcal{LTS}^\circ$ is a *sound approximation* of $lts \in \mathcal{LTS}$ provided that $\alpha_{\mathcal{LTS}^\circ}(lts) \sqsubseteq_{\mathcal{LTS}^\circ} lts^\circ$.

Definition 37 (Order on Abstract LTSs)**.**
Let $lts_i^\circ = (S^\circ(\mathfrak{p}_i), s_{0,i}{}^\circ, \rightarrow^i_\circ), \in \mathcal{LTS}^\circ$, for $i \in \{1, 2\}$. We say that $lts_1^\circ \sqsubseteq_{\mathcal{LTS}^\circ} lts_2^\circ$ iff

i) $\mathfrak{p}_1 \sqsubseteq_{\widehat{\mathbb{P}}} \mathfrak{p}_2$*;*

ii) $\forall t_1^\circ = (s^\circ{}_1 \xrightarrow{\mu^\circ{}_1, r_1^\circ}_\circ s^\circ{}'_1) \in \rightarrow^1_\circ,\ \exists\, t_2^\circ = (s^\circ{}_2 \xrightarrow{\mu^\circ{}_2, r_2^\circ}_\circ s^\circ{}'_2) \in \rightarrow^2_\circ$ *such that*

a) $s^\circ{}_1 \sqsubseteq_{\mathcal{MS}^\circ} s^\circ{}_2\,,\ s^\circ{}'_1 \sqsubseteq_{\mathcal{MS}^\circ} s^\circ{}'_2$ *;*

b) $\widehat{\mu^\circ} \sqsubseteq_{\mathcal{MS}^\circ} \mu^\circ{}_2$ *and* $\widehat{r^\circ} \sqsubseteq_{\mathbb{I}} r_2{}^\circ$ *where*

$$\widehat{\mu^\circ} = \bigcup^{\mathcal{MS}^\circ}_{\substack{s^\circ{}_3 \xrightarrow{\mu^\circ{}_3, r^\circ_3}_\circ s^\circ{}'_3 \in \rightarrow^1_\circ s.t. \\ s^\circ{}_3 \sqsubseteq_{\mathcal{MS}^\circ} s^\circ{}_2, \\ s^\circ{}'_3 \sqsubseteq_{\mathcal{MS}^\circ} s^\circ{}'_2}} \mu^\circ{}_3\,,\quad \widehat{r^\circ} = \bigcup^{\mathbb{I}}_{\substack{s^\circ{}_3 \in S^\circ(S_1) \\ s^\circ{}_3 \sqsubseteq_{\mathcal{MS}^\circ} s^\circ{}_2}} \sum^{\mathbb{I}}_{s^\circ{}_3 \xrightarrow{\mu^\circ{}_3, r^\circ_3}_\circ s^\circ{}'_3 \in \rightarrow^1_\circ s.t.,\ s^\circ{}'_3 \sqsubseteq_{\mathcal{MS}^\circ} s^\circ{}'_2} r^\circ{}_3$$

iii) $\forall t_2^\circ = (s^\circ{}_2 \xrightarrow{\mu^\circ{}_2, r_2^\circ}_\circ s^\circ{}'_2) \in \rightarrow^2_\circ :\ ([r_2{}^\circ]^- = 0) \vee$
$(\exists\, t_1^\circ = (s^\circ{}_1 \xrightarrow{\mu^\circ{}_1, r_1^\circ}_\circ s^\circ{}'_1) \in \rightarrow^1_\circ,\ \ s.t.\ s_1{}^\circ \sqsubseteq_{\mathcal{MS}^\circ} s_2{}^\circ \wedge s_1{}^{\circ\prime} \sqsubseteq_{\mathcal{MS}^\circ} s_2{}^{\circ\prime})$

Intuitively, $lts_1{}^\circ \sqsubseteq_{\mathcal{LTS}^\circ} lts_2^\circ$ requires the following conditions.
i) The predicates used by $lts_1{}^\circ$ are more precise than the predicates used by $lts_2{}^\circ$. *ii*) Each transition of $lts_1{}^\circ$ has a corresponding transition in $lts_2{}^\circ$: if the transition of $lts_1{}^\circ$ goes from a state ${s^\circ}_1$ to a state ${s^\circ}'_1$, the corresponding transition in $lts_2{}^\circ$ goes from a state ${s^\circ}_2$ approximating ${s^\circ}_1$ to a state ${s^\circ}'_2$ approximating ${s^\circ}'_1$. Moreover, the transition of $lts_2{}^\circ$ has to approximate all the transitions of $lts_1{}^\circ$ from a state approximated by ${s^\circ}_2$ to a state approximated by ${s^\circ}'_2$. In particular, its abstract multiset ${\mu^\circ}_2$ has to approximate the union of multisets of the set corresponding to concrete moves, e.g. $\widehat{\mu^\circ}$. Similarly, its rate ${r^\circ}_2$ has to approximate the sum of rates of the set corresponding to concrete moves, e.g. $\widehat{\mathcal{R}^\circ}$. *iii*) Each transition of $lts_2{}^\circ$, either has a minimum rate equal to 0, or corresponds to at least a transition of $lts_1{}^\circ$.

The following theorem states that $LTS^\circ(M^\circ)$ is a sound approximation of each $LTS(M)$ such that $M \in \gamma(M^\circ)$.

Theorem 5.3.10 (Soundness of LTS°)**.**
$\forall M^\circ \in \mathcal{M}^\circ\,,\ \forall M \in \gamma(M^\circ) : \alpha_{\mathcal{LTS}}(LTS(M)) \sqsubseteq_{\mathcal{LTS}^\circ} LTS^\circ(M^\circ)\,.$

Proof. See Section 5.9 □

5.4 Abstract Probabilistic Semantics

We use *Interval Markov Chains* [JL91, KU02] (IMC), to define the probabilistic semantics of abstract systems. The definition of IMC and the approximation order over IMC we use are similar to the ones of Section 3.3.3. The difference consists in considering an abstract state space instead of a concrete one. We refer to Section 3.3.3 also for the definitions of scheduler and of abstract probabilistic reachability.

Definition 38 (Interval Markov Chain)**.** *An* IMC *is a tuple* $(S^\circ(\mathfrak{p}), {s_0}^\circ, P^-, P^+)$*, where:* $S^\circ(\mathfrak{p})$ *is the* set of abstract states *and* ${s_0}^\circ \in S^\circ(\mathfrak{p})$ *the* initial abstract state*;* $P^-, P^+ : S \to PDistr(S^\circ(\mathfrak{p}))$ *are the* lower and upper probability transition functions *such that* $\forall s^\circ, s^{\circ\prime} \in S^\circ(\mathfrak{p})$*,* $P^-(s^\circ, s^{\circ\prime}) \leq P^+(s^\circ, s^{\circ\prime})$ *and* $\sum_{s^{\circ\prime\prime} \in S^\circ(\mathfrak{p})} P^-(s^\circ, s^{\circ\prime\prime}) \leq 1 \leq \sum_{s^{\circ\prime\prime} \in S^\circ(\mathfrak{p})} P^+(s^\circ, s^{\circ\prime\prime})\,.$

We refer to Section 3.3.3 for the definitions of scheduler and of abstract probabilistic reachability.

To relate the DTMC semantics of a concrete system, to its abstract counterpart IMC, we use the *best DTMC abstraction function* $\alpha_{\mathcal{MC}}$.

Definition 39 (Best abstraction of DTMC)**.** *We define the DTMC best abstraction function* $\alpha_{\mathcal{MC}} : \mathcal{MC} \mapsto \mathcal{MC}^{\circ}$ *such that*

$$\alpha_{\mathcal{MC}}((S, s_0, \mathfrak{p})) = (S^{\circ}(\mathfrak{p}^{\bullet}), \alpha_{\mathcal{MS}}(\mathfrak{p})(s_0), \widehat{P}, \widehat{P}) \text{ where}$$

$$\forall s, s' \in S \ : \ \widehat{P}(\alpha_{\mathcal{MS}}(\mathfrak{p}^{\bullet})(s), \alpha_{\mathcal{MS}}(\mathfrak{p}^{\bullet})(s')) = P(s, s') \tag{5.4}$$

In the following, with an abuse of notation we use $\widehat{P} = P$ for (5.4).

The following Lemma states that the probabilities derived by $\alpha_{\mathcal{MC}}$ are exact.

Lemma 5.4.1.
$\forall A \in AP, mc \in \mathcal{MC} : [Reach_{A,mc}(s_0)]^{\bullet} = Reach^{\circ}_{A,\alpha_{\mathcal{MC}}(mc)}(\alpha_{\mathcal{MS}}(\mathfrak{p}^{\bullet})(s_0))$.

Proof. Let $mc = (S, s_0, P) \in \mathcal{MC}$ and hence $\alpha_{\mathcal{MC}}(mc) = (S^{\circ}(\mathfrak{p}^{\bullet}), \alpha_{\mathcal{MS}^{\circ}}(\mathfrak{p}^{\bullet})(s_0), \widehat{P}, \widehat{P})$. Note that mc and $\alpha_{\mathcal{MC}}(mc)$ are isomorphic as $\forall s \in S \ : \ \gamma_{\mathcal{MS}^{\circ}}(\alpha_{\mathcal{MS}^{\circ}}(\mathfrak{p}^{\bullet})(s)) = \{s\}$.

We have to prove that

$$\begin{aligned} &Reach_{A,mc}(s_0) = \\ &\qquad \inf_{\mathbb{S} \in Adm(mc^{\circ})} P^{\mathbb{S}}_{s^{\circ}}(\{\pi \in C(s^{\circ}) \mid \pi[i] \forall \vDash A \text{ for some } i \geq 0\}) = \\ &\qquad \sup_{\mathbb{S} \in Adm(mc^{\circ})} P^{\mathbb{S}}_{s^{\circ}}(\{\pi \in C(s^{\circ}) \mid \pi[i] \exists \vDash A \text{ for some } i \geq 0\}) \ = \\ &\qquad [Reach^{\circ}_{A,\alpha_{\mathcal{MC}}(mc)}(\alpha_{\mathcal{MS}}(\mathfrak{p}^{\bullet})(s_0))]^{-} = [Reach^{\circ}_{A,\alpha_{\mathcal{MC}}(mc)}(\alpha_{\mathcal{MS}}(\mathfrak{p}^{\bullet})(s_0))]^{+} \end{aligned}$$

As the abstract state space is $S^{\circ}(\mathfrak{p}^{\bullet})$, we have that $\forall s^{\circ} \in S^{\circ}(\mathfrak{p}^{\bullet}), A \in AP \ : \ s^{\circ} \forall \vDash A \Leftrightarrow s^{\circ} \exists \vDash A \Leftrightarrow s = \gamma_{\mathcal{MS}^{\circ}}(s^{\circ}) \exists \vDash A$. Moreover, as $\widehat{P} = P$ by definition of $\alpha_{\mathcal{MC}}$, it holds that $\inf_{\mathbb{S} \in Adm(mc^{\circ})} P^{\mathbb{S}}_{s^{\circ}}(\{\pi \in C(s^{\circ}) \mid \pi[i] \forall \vDash A \text{ for some } i \geq 0\}) = \sup_{\mathbb{S} \in Adm(mc^{\circ})} P^{\mathbb{S}}_{s^{\circ}}(\{\pi \in C(s^{\circ}) \mid \pi[i] \forall \vDash A \text{ for some } i \geq 0\})$. Finally, as the structure are isomorphic, to each abstract path corresponds a concrete path, with the same probabilities. □

Similarly as in Section 3.3.4, we introduce an approximation order over IMC $\sqsubseteq_{\mathcal{MC}^{\circ}}$.

Definition 40 (Order on IMCs)**.** *Let* $mc_i^\circ = (S^\circ(\mathfrak{p}_i), s_{0,i}, \mathcal{P}_i^-, \mathcal{P}_i^+), i \in \{1,2\}$*, two IMCs. We say that* $mc_1^\circ \sqsubseteq_{\mathcal{MC}^\circ} mc_2^\circ$ *iff* $\forall s^\circ{}_1 \in S^\circ(\mathfrak{p}_1)\, \exists!\, s^\circ{}_2 \in S^\circ(\mathfrak{p}_2)$:

- $s^\circ{}_1 \sqsubseteq_{\mathcal{MS}^\circ} s^\circ{}_2$*;*
- $\forall \rho_1 \in ADistr(s^\circ{}_1)\, \exists!\, \rho_2 \in ADistr(s^\circ{}_2)$ *s.t.*

$$\forall s^\circ{}'_2 \in S^\circ{}_2 \,:\, \rho_2(s_2{}^{\circ\prime}) = \sum_{s_1{}^{\circ\prime} \in S^\circ{}_1,\, s_1{}^{\circ\prime} \sqsubseteq_{\mathcal{MS}^\circ} s^\circ{}'_2} \rho_1(s_1{}^{\circ\prime})\,.$$

Intuitively, we say that $mc_1{}^\circ \sqsubseteq_{\mathcal{MC}^\circ} mc_2{}^\circ$ if each state $s^\circ{}_1$ in the state space of $mc_1{}^\circ$ corresponds to a state $s^\circ{}_2$ in the state space of $mc_2{}^\circ$, which is a sound approximation of $s^\circ{}_1$ and which over-approximates the probability distributions. More in details, each distribution of $s^\circ{}_1$ has a corresponding distribution of $s^\circ{}_2$ where the probabilities of the target states are summed up.

The following theorem states the soundness of the order on IMCs w.r.t. reachability properties.

Theorem 5.4.2. *Let* $mc_i^\circ = (S^\circ(\mathfrak{p}_i), s_{0,i}{}^\circ, P_i^-, P_i^+), i \in \{1,2\}$*, two IMCs. If* $mc_1^\circ \sqsubseteq_{\mathcal{MC}^\circ} mc_2^\circ$ *then* $\forall A \in AP,\ s^\circ{}_1 \in S^\circ(\mathfrak{p}_1),\ s^\circ{}_2 \in S^\circ(\mathfrak{p}_2),\ s^\circ{}_1 \sqsubseteq_{\mathcal{MS}^\circ} s^\circ{}_2$ *we have that*

$$Reach^\circ_{A,mc_1^\circ}(s^\circ{}_1) \sqsubseteq_{\mathbb{I}} Reach^\circ_{A,mc_2^\circ}(s^\circ{}_2)\,.$$

Proof. See Section 5.9 □

5.4.1 Abstract Probabilistic Semantics

We define the abstract probabilistic translation function $\mathcal{H}^\circ : \mathcal{LTS}^\circ \to \mathcal{MC}^\circ$. The most difficult part of the translation consists of the calculation of intervals of probabilities from intervals of rates.

We define $R^\circ : \mathcal{MS}^\circ \times \mathcal{MS}^\circ \mapsto \mathbb{I}$, and $E^\circ : \mathcal{MS}^\circ \mapsto \mathbb{I}$ as follows. Given an abstract LTS $lts^\circ = (S^\circ(\mathfrak{p}), s^\circ{}_0, \to_\circ)$, $\forall s^\circ, s^{\circ\prime} \in S^\circ(\mathfrak{p})$

$$R^\circ(s^\circ, s'^\circ) = r^\circ \text{ s.t. } s^\circ \xrightarrow{r^\circ, \mu^\circ} s'^\circ \in \to_\circ \text{ and } E^\circ(s^\circ) = \sum_{s^{\circ\prime} \in S^\circ(\mathfrak{p})}^{\mathbb{I}} R^\circ(s^\circ, s^{\circ\prime})\,.$$

Intuitively, $R^\circ(s^\circ, s^{\circ\prime})$ reports the interval of rates corresponding to the move from s° to $s^{\circ\prime}$, while $E^\circ(s^\circ)$ is the abstract exit rate.

For all the pairs of states $s^\circ, s^{\circ\prime} \in S^\circ(\mathfrak{p})$, both lower and upper bounds of the probability of moving from s° to $s^{\circ\prime}$ can be determined by $R^\circ(s^\circ, s^{\circ\prime})$ and

by $E^\circ(s^\circ)$. For these purposes we need to consider the *worst case* and *best case* scenario, respectively. That is, the transition to be maximized (minimized) takes as rate value its upper (lower) bound and all the others take their lower (upper) bound. This reasoning has to be properly combined with the special cases when $[E^\circ(s^\circ)]^+ = 0$ (the state s° is stable) or $[E^\circ(s^\circ)]^- = 0$ (the state s° is stable for some values of kinetic constant of some rules).

Definition 41 (Abstract Probabilistic Translation Function)**.** *We define* $\mathcal{H}^\circ : \mathcal{LTS}^\circ \to \mathcal{MC}^\circ$ *such that* $\mathcal{H}^\circ((S^\circ(\mathfrak{p}), s^\circ_0, \to^\circ)) = (S^\circ(\mathfrak{p}), s^\circ_0, P^-, P^+)$*, where* $P^-, P^+ : S^\circ(\mathfrak{p}) \to PDistr(S^\circ(\mathfrak{p}))$ *are obtained, for each* $s^\circ, s^{\circ\prime} \in S^\circ(\mathfrak{p})$, $s^\circ \neq s^{\circ\prime}$*, as follows:*

- *if* $[E^\circ(s^\circ)]^+ = 0$*, then* $P^+(s^\circ, s^{\circ\prime}) = P^-(s^\circ, s^{\circ\prime}) = 0$*,* $P^+(s^\circ, s^\circ) = P^-(s^\circ, s^\circ) = 1$*;*
- *if* $[E^\circ(s^\circ)]^+ > 0$*, then*
  - *(a) if* $[E^\circ(s^\circ)]^- = 0$*, then* $P^+(s^\circ, s^\circ) = 1$*,* $P^-(s^\circ, s^\circ) = 0$
  - *(b) if* $[R^\circ(s^\circ, s^{\circ\prime})]^- = 0$*, then* $P^-(s^\circ, s^{\circ\prime}) = 0$ *else* $P^-(s^\circ, s^{\circ\prime}) = [R^\circ(s^\circ, s^{\circ\prime})]^- / ([R^\circ(s^\circ, s^{\circ\prime})]^- + \sum_{\substack{s^{\circ\prime\prime} \in S^\circ(\mathfrak{p}) \\ s^{\circ\prime\prime} \neq s^\prime}} [R^\circ(s^\circ, s^{\circ\prime\prime})]^+)$
  - *(c) if* $[R^\circ(s^\circ, s^{\circ\prime})]^+ = 0$*, then* $P^+(s^\circ, s^{\circ\prime}) = 0$ *else* $P^+(s^\circ, s^{\circ\prime}) = [R^\circ(s^\circ, s^{\circ\prime})]^+ / ([R^\circ(s^\circ, s^{\circ\prime})]^+ + \sum_{\substack{s^{\circ\prime\prime} \in S^\circ(\mathfrak{p}), \\ s^{\circ\prime\prime} \neq s^{\circ\prime}}} [R^\circ(s^\circ, s^{\circ\prime\prime})]^-)$.

5.4.2 Soundness with respect to Probabilistic Reachability

The following lemma states that the approximation order over abstract LTSs obtained by the best LTS abstraction is preserved by the translation to IMCs.

Lemma 5.4.3. *Let* $lts = (S, s_0, \to)$ *and* $\alpha_{\mathcal{LTS}}(lts) = (S^\circ(\mathfrak{p}_1), s^\circ_{0,1}, \to^\circ_1)$*, for* $\mathfrak{p}_1 = \mathfrak{p}^\bullet$ *and* $s^\circ_{0,1} = \alpha_{\mathcal{MS}}(\mathfrak{p}^\bullet)(s_0)$*. Moreover, let* $lts^\circ = ((S^\circ(\mathfrak{p}_2), s^\circ_{0,2}, \to^\circ_2))$ *be an abstract LTS.*
If $\alpha_{\mathcal{LTS}}(lts) \sqsubseteq_{\mathcal{LTS}^\circ} lts^\circ$ *then* $\mathcal{H}^\circ(\alpha_{\mathcal{LTS}}(lts)) \sqsubseteq_{\mathcal{MC}^\circ} \mathcal{H}^\circ(lts^\circ)$*.*

Proof. See Section 5.9 □

Lemma 5.4.4 states that $\alpha_{\mathcal{MC}} \circ \mathcal{H} = \mathcal{H}^\circ \circ \alpha_{\mathcal{LTS}}$.

Lemma 5.4.4. $\forall M \in \mathcal{M},\ \alpha_{\mathcal{MC}}(\mathcal{H}(LTS(M))) = \mathcal{H}^{\circ}(\alpha_{\mathcal{LTS}}(LTS(M)))$.

Proof. See Section 5.9 □

The following theorem states the soundness of the abstract probabilistic semantics for an abstract system with respect to the best abstraction of the probabilistic semantics, for each approximated concrete system.

Theorem 5.4.5 (Soundness of the abstract probabilistic semantics)**.** $\forall M^{\circ} \in \mathcal{M}^{\circ},\ M \in \gamma(M^{\circ}) :\ \alpha_{\mathcal{MC}}(\mathcal{H}(LTS(M))) \sqsubseteq_{\mathcal{MC}^{\circ}} \mathcal{H}^{\circ}(LTS^{\circ}(M^{\circ}))$.

Proof. By Lemma 5.4.4, we have that

$$\alpha_{\mathcal{MC}}(\mathcal{H}(LTS(M))) = \mathcal{H}^{\circ}(\alpha_{\mathcal{LTS}}(LTS(M)))\,,$$

and given the monotonicity of $\mathcal{H}^{\circ}$ (see Lemma 5.4.3), it remains to prove that

$$\alpha_{\mathcal{LTS}}(LTS(M)) \sqsubseteq_{\mathcal{LTS}^{\circ}} LTS^{\circ}(M^{\circ})\,,$$

that is true by Theorem 5.3.10. □

Finally, we conclude that the IMC, derived from the abstract LTS of an abstract system M°, gives *conservative bounds* for probability of reachability properties for each concrete system $M \in \gamma(M^{\circ})$.

Theorem 5.4.6.
$\forall M^{\circ} = (\Sigma, \mathcal{R}, s_0, \mathfrak{p}) \in \mathcal{M}^{\circ},\ \forall M = (\Sigma, s_0, \mathcal{R}) \in \gamma(M^{\circ}), A \in AP, s \in S, s^{\circ} \in S^{\circ}(\mathfrak{p}), s \in \gamma_{\mathcal{MS}}(s^{\circ})$,

$$[Reach_{A,\mathcal{H}(\mathcal{LTS}(M))}(s)]^{\bullet} \sqsubseteq_{\mathbb{I}} Reach^{\circ}_{A,\mathcal{H}^{\circ}(\mathcal{LTS}^{\circ}(M^{\circ}))}(s)\,.$$

Proof. By Lemma 5.4.1 we have that $\forall \mathfrak{p} \in \mathbb{P}$

$$[Reach_{A,\mathcal{H}(\mathcal{LTS}(M))}(s)]^{\bullet} = Reach^{\circ}{}_{A,\alpha_{\mathcal{MC}}(\mathcal{H}(LTS(M)))}(\alpha_{\mathcal{MS}^{\circ}}(\mathfrak{p})(s))\,.$$

Since $s \in \gamma_{\mathcal{MS}}(s^{\circ})$ we have that $\alpha^{\circ}_{\mathcal{MS}}(\mathfrak{p})(s) \sqsubseteq_{\mathcal{MS}^{\circ}} s^{\circ}$, and hence, given Theorem 5.4.2, it remains to prove that

$$\alpha_{\mathcal{MC}}(\mathcal{H}(LTS(M))) \sqsubseteq_{\mathcal{MC}^{\circ}} \mathcal{H}^{\circ}(LTS^{\circ}(M^{\circ}))\,,$$

that is guaranteed by Theorem 5.4.5. □

5.5 Case study: Seasonal Reproduction Model

We show the efficacy of the proposed approach on a model of seasonal animals. Namely we model the reproduction of seasonal animals, we construct the corresponding abstract probabilistic semantics and we study the probabilistic reachability of an extinction state (i.e. a state with no more individuals).

Model. Seasonal animals have a cyclic behavior in which they alternatively couple and hatch. In nature the alternation of coupling and hatching periods is governed by the alternation of seasons. The main assumption is that all the animals reproduce in a certain season (e.g. spring), while they hatch and grow offspring in an other season (e.g. winter); no animals can couple during the hatching season.

The species involved are

$$\Sigma = \{F\,,\ F_o\,,\ F_i\}\,;$$

F represents female individuals ready to couple, F_o represents female individuals during hatching season, while F_i represents young animals. For the sake of simplicity, we don't model explicitly the presence of males and we assumes males to be always present.

In particular we can model such a behavior with the following set of rules $\mathcal{R}$:

$$\begin{array}{llllll}
\{ & F & \xrightarrow{1} & & (R_1), & F \xrightarrow{1} F_i\,F_o \quad (R_2), \\
 & F_o & \xrightarrow{1} & F & (R_3), & F_i \xrightarrow{1} \quad (R_4), \\
 & F_i & \xrightarrow{1} & F & (R_5) & \}.
\end{array}$$

Each female F can die (R_1) or couple (R_2), giving birth to a young female F_i, and becoming an hatching female F_o; in this period they can only rest and, eventually, become again a female ready to couple (R_3). Young females F_i may become an adult female (R_5) or may die (R_4).

For the sake of simplicity, we assume all the rule rates to be equal (i.e. equal to 1), that it that all events are equiprobable.

This kind of synchronous behavior is badly modelled with an interleaving semantics, showing system executions in which the system population consists for a part in females ready to couple and females hatching. This actually cannot happen as the behavior of females is timed by seasons. Moreover while a single female reproduces many times, the other females may stall.

Conversely, with a maximally parallel semantics we can represent the system dynamics as synchronous.

Note that the state space associated to the concrete semantics of the system is infinite as each species can grows indefinitely, while, using interval based predicate abstraction, we can obtain a finite abstract model.

Specifically, we construct an abstract system

$$M^{\circ}{}_{ex} = (\Sigma, \mathcal{R}, s_0, \mathfrak{p}),$$

where $s_0 = \{3, 0, 0\}$, using the following set of predicates

$$\mathfrak{p} = \bigcup_{a \in \Sigma} \{(a\,,\,[0,0]), (a\,,\,[1,2]), (a\,,\,[3,4]), \\ (a\,,\,[4,5]), (a\,,\,[6,7]), (a\,,\,[7,8]), (a\,,\,[9,\infty])\}.$$

Note that $\mathfrak{p}$ is a partition with respect to $\mathcal{R}$ over Σ, that is $\mathfrak{p} \in \widehat{\mathbb{P}}_{\mathcal{R}}(\Sigma)$.

Abstract Probabilistic Semantics. The IMC probabilistic semantics of $M^{\circ}{}_{ex}$ is shown in Figure 5.1, whose bounds on transition probabilities are the reported in Table 5.1, and abstract states are the following:

$$\begin{aligned}
s_0{}^{\circ} &= \{\ [3,4], & [0,0], & & [0,0] & \ \} \\
s_1{}^{\circ} &= \{\ [0,0], & [0,0], & & [0,0] & \ \} \\
s_2{}^{\circ} &= \{\ [0,0], & [1,2], & & [1,2] & \ \} \\
s_3{}^{\circ} &= \{\ [0,0], & [3,4], & & [3,4] & \ \} \\
s_4{}^{\circ} &= \{\ [0,0], & [5,6], & & [5,6] & \ \} \\
s_5{}^{\circ} &= \{\ [0,0], & [7,8], & & [7,8] & \ \} \\
s_6{}^{\circ} &= \{\ [0,0], & [9,\infty], & & [9,\infty] & \ \} \\
s_7{}^{\circ} &= \{\ [1,2], & [0,0], & & [0,0] & \ \} \\
s_8{}^{\circ} &= \{\ [5,6], & [0,0], & & [0,0] & \ \} \\
s_9{}^{\circ} &= \{\ [7,8], & [0,0], & & [0,0] & \ \} \\
s_{10}{}^{\circ} &= \{\ [9,\infty], & [0,0], & & [0,0] & \ \}.
\end{aligned}$$

We comment here the computation of abstract rates of transitions exiting from s_0 and the related probabilities, as an example.

From the abstract starting state s°_0 the reachable abstract states correspond to $\widehat{Next^\circ}(\mathcal{R})(s^\circ_0, \mathfrak{p}) = Decompose(\{[0,0],[0,4],[0,4]\}, \mathfrak{p})$. From such a set of reachable abstract states, many states are excluded, as arrival states, by the function $\widehat{f^\circ}$. Indeed, the only abstract states $s^{\circ\prime}$ for which $\widehat{f^\circ}(s^\circ_0, s^{\circ\prime}, \mathcal{R})$ return a value different from the null abstract multiset of rule application are $\{s^\circ_1,\ s^\circ_6,\ s^\circ_9\}$.

For such states we have that

$$\widehat{f^\circ}(\mathcal{R})(s^\circ_0, s^\circ_1) = \{[3,4],\ [0,0],\ [0,0],\ [0,0],\ [0,0]\} = \mu^\circ_1,$$
$$\widehat{f^\circ}(\mathcal{R})(s^\circ_0, s^\circ_2) = \{[0,4],\ [1,2],\ [0,0],\ [0,0],\ [0,0]\} = \mu^\circ_2,$$
$$\widehat{f^\circ}(\mathcal{R})(s^\circ_0, s^\circ_3) = \{[0,4],\ [3,4],\ [0,0],\ [0,0],\ [0,0]\} = \mu^\circ_3\ .$$

Instead, transitions from $s_0{}^\circ$ to state resulting from $Decompose(\{[0,0],[0,4],[0,4]\}, \mathfrak{p})$ are excluded by $\widehat{f^\circ}$ as the least fix-point of $\widehat{f^{\circ(n)}}$ consists in a not *WellFormed* abstract multisets.
For instance, $\widehat{f^\circ}(\mathcal{R})(s^\circ_0, \{[0,0],[0,0],[1,2]\})$ is equal the null abstract multiset as

$$FixPoint(\widehat{f^{\circ(n)}}(\mathcal{R})(s_0{}^\circ, \{[0,0],[0,0],[1,2]\}))[2] = [1,0]\,.$$

The computation of rates for such transitions is

$$\begin{aligned}
Rate^\circ(\mathcal{R})(s^\circ_0, s^\circ_1) &= [\,1\,,\,6\,] \times [\,\tfrac{1}{16}\ ,\ \tfrac{1}{8}\,] \times [\,1\,,\,5\,] = [\,\tfrac{1}{16}\ ,\ \tfrac{15}{4}\ ],\\
Rate^\circ(\mathcal{R})(s^\circ_0, s^\circ_2) &= [\,1\,,\,6\,] \times [\,\tfrac{1}{64}\ ,\ \tfrac{1}{2}\,] \times [\,1\,,\,5\,] = [\,\tfrac{1}{64}\ ,\ 15\ ],\\
Rate^\circ(\mathcal{R})(s^\circ_0, s^\circ_3) &= [\,1\,,\,6\,] \times [\,\tfrac{1}{256}\ ,\ \tfrac{1}{8}\,] \times [\,1\,,\,5\,] = [\,\tfrac{1}{256}\ ,\ \tfrac{15}{4}\ ],
\end{aligned}$$

and, hence, their probabilities are

$$\begin{aligned}
P^\circ(s^\circ_0, s^\circ_1) &= [\ \tfrac{1}{301}\ ,\ \tfrac{192}{193}\ ],\\
P^\circ(s^\circ_0, s^\circ_2) &= [\ \tfrac{1}{481}\ ,\ \tfrac{3840}{3857}\ ],\\
P^\circ(s^\circ_0, s^\circ_3) &= [\ \tfrac{1}{4801}\ ,\ \tfrac{48}{49}\ ].
\end{aligned}$$

Examples of computation of rate for transitions involving abstract states having ∞ as upper bound of at least a species are, for instance :

- a transition *to a an infinite abstract state*, as the one from s°_5 to s°_{10}: we have that
  $\widehat{f^\circ}(\mathcal{R})(s^\circ_5, s^\circ_{10}) = \{[0,0],\ [0,0],\ [7,8],\ [0,8],\ [0,8]\}$,
  and hence $Rate^\circ(\mathcal{R})(s^\circ_5, s^\circ_{10}) = [1,70] \times [\tfrac{1}{16777216}, \tfrac{1}{128}] \times [1,36]$
  $= [1/16777216, 315/16]$ and $P^\circ(s^\circ_5, s^\circ_{10})$ can be obtained in standard way;

- a transition *from a an infinite abstract state*, as the one from $s^\circ{}_{10}$ to $s^\circ{}_1$: we have that
  $\widehat{f^\circ}(\mathcal{R})(s^\circ{}_{10}, s^\circ{}_1) = \{[0,\infty],\ [0,0],\ [0,0],\ [0,0],\ [0,0],\ [0,0]\}$,
  and hence $Rate^\circ(\mathcal{R})(s^\circ{}_{10}, s^\circ{}_1) = [1,\infty] \times [0,1] \times [1,\infty]$
  $= [0,\infty]$ and $P^\circ(s^\circ{}_{10}, s^\circ{}_1) = [0,1]$.

Probabilistic Reachability. Looking for extinction probability (i.e. probabilistic reachability of s_1) through model checking we obtain that:

- starting from $s^\circ{}_0$ it is included in $[0.018378449702171482\,,\ 1]$;
- starting from $s^\circ{}_8$ it is included in $[1.7291907142970184 * 10^{-4}\,,\ 1]$;
- starting from $s^\circ{}_9$ it is included in $[9.519793254996947 * 10^{-6}\,,\ 1]$.

We can also obtain, for instance, bounds for the probability of reaching an extinction state within the first year (i.e. within two steps). The results are the following:

- starting from $s^\circ{}_0$ we have a probability included in $[0.00332225913621262\,,\ 0.994818652849741]$;
- starting from $s^\circ{}_8$ we have a probability included in $[1.70039108995069 * 10^{-4}\,,\ 0.998861973662819]$;
- starting from $s^\circ{}_9$ we have a probability included in $[9.33698098056974 * 10^{-6}\,,\ 0.999736552557765]$.

Bounds for the probability of reaching an extinction state within the second year (i.e. within four steps) are the following:

- starting from $s^\circ{}_0$, $[0.007385312320100682\,,\ 0.9999880841548489]$;
- starting from $s^\circ{}_8$, $[1.7068427116859715 * 10^{-4}\,,\ 0.999999204924427]$;
- starting from $s^\circ{}_9$, $[9.383470899327278 * 10^{-6}\,,\ 0.9999999516622782]$.

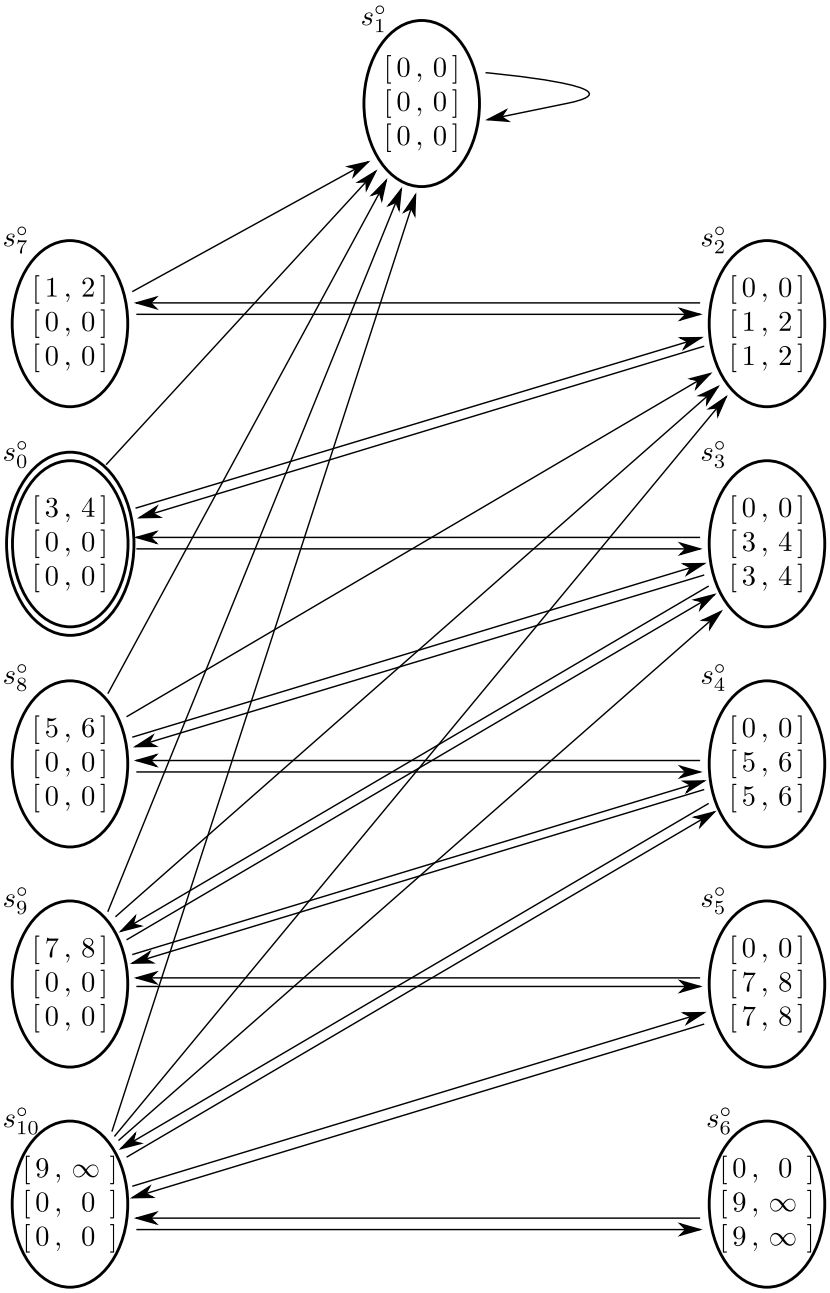


Figure 5.1: Transition system corresponding to the IMC probabilistic semantics for the model of seasonal animals reproduction $M^\circ{}_{ex}$ (see Table 5.1 for transition probabilities).

$P^\circ(s^\circ_7, s^\circ_1) =$	$[\frac{1}{13}$	$,\frac{48}{49}$	$],$
$P^\circ(s^\circ_7, s^\circ_1) =$	$[\frac{1}{49}$	$,\frac{12}{13}$	$],$
$P^\circ(s^\circ_0, s^\circ_1) =$	$[\frac{1}{301}$	$,\frac{192}{193}$	$],$
$P^\circ(s^\circ_0, s^\circ_2) =$	$[\frac{1}{481}$	$,\frac{3840}{3857}$	$],$
$P^\circ(s^\circ_0, s^\circ_3) =$	$[\frac{1}{4801}$	$,\frac{48}{49}$	$],$
$P^\circ(s^\circ_8, s^\circ_1) =$	$[\frac{1}{5881}$	$,\frac{6144}{6151}$	$],$
$P^\circ(s^\circ_8, s^\circ_2) =$	$[\frac{1}{6753}$	$,\frac{286720}{286789}$	$],$
$P^\circ(s^\circ_8, s^\circ_3) =$	$[\frac{1}{80769}$	$,\frac{71680}{71761}$	$],$
$P^\circ(s^\circ_8, s^\circ_4) =$	$[\frac{1}{376833}$	$,\frac{640}{643}$	$],$
$P^\circ(s^\circ_9, s^\circ_1) =$	$[\frac{1}{107101}$	$,\frac{64512}{64529}$	$],$
$P^\circ(s^\circ_9, s^\circ_2) =$	$[\frac{1}{110881}$	$,\frac{20643840}{20644117}$	$],$
$P^\circ(s^\circ_9, s^\circ_3) =$	$[\frac{1}{1411201}$	$,\frac{1032192}{1032257}$	$],$
$P^\circ(s^\circ_9, s^\circ_4) =$	$[\frac{1}{6612481}$	$,\frac{1290240}{1290577}$	$],$
$P^\circ(s^\circ_9, s^\circ_5) =$	$[\frac{1}{27417601}$	$,\frac{16128}{16145}$	$],$
$P^\circ(s^\circ_{10}, s^\circ_1) =$	$[0$	$,1$	$],$
$P^\circ(s^\circ_{10}, s^\circ_2) =$	$[0$	$,1$	$],$
$P^\circ(s^\circ_{10}, s^\circ_3) =$	$[0$	$,1$	$],$
$P^\circ(s^\circ_{10}, s^\circ_4) =$	$[0$	$,1$	$],$
$P^\circ(s^\circ_{10}, s^\circ_5) =$	$[0$	$,1$	$],$
$P^\circ(s^\circ_{10}, s^\circ_6) =$	$[0$	$,1$	$],$
$P^\circ(s^\circ_6, s^\circ_{10}) =$	$[0$	$,1$	$],$
$P^\circ(s^\circ_5, s^\circ_{10}) =$	$[\frac{1}{41287681}$	$,\frac{41287680}{41287681}$	$],$
$P^\circ(s^\circ_5, s^\circ_9) =$	$[\frac{1}{41287681}$	$,\frac{41287680}{41287681}$	$],$
$P^\circ(s^\circ_4, s^\circ_{10}) =$	$[\frac{1}{1474561}$	$,\frac{368640}{368641}$	$],$
$P^\circ(s^\circ_4, s^\circ_9) =$	$[\frac{1}{1474561}$	$,\frac{368640}{368641}$	$],$
$P^\circ(s^\circ_4, s^\circ_8) =$	$[\frac{1}{1474561}$	$,\frac{368640}{368641}$	$],$
$P^\circ(s^\circ_3, s^\circ_9) =$	$[\frac{1}{153661}$	$,\frac{38415}{38416}$	$],$
$P^\circ(s^\circ_3, s^\circ_8) =$	$[\frac{1}{153661}$	$,\frac{38415}{38416}$	$],$
$P^\circ(s^\circ_3, s^\circ_0) =$	$[\frac{1}{153661}$	$,\frac{38415}{38416}$	$],$
$P^\circ(s^\circ_2, s^\circ_0) =$	$[\frac{1}{97}$	$,\frac{96}{97}$	$],$
$P^\circ(s^\circ_2, s^\circ_7) =$	$[\frac{1}{97}$	$,\frac{96}{97}$	$],$
$P^\circ(s^\circ_2, s^\circ_2) =$	$[1$	$,1$	$],$

Table 5.1: Transition probabilities of IMC probabilistic semantics for the model of seasonal animals reproduction M°_{ex}.

5.6 Discussion

The proposed approach allows systems evolving with a maximally parallel probabilistic semantics, even with an infinite associated state space, to be studied. It allows a number of transitions smaller than the one of the concrete probabilistic semantics to be obtained. Conversely, a standard predicate abstraction approach (as the one of [KH09]) it is able to reduce the number of states but not of the number of transitions.

We have shown by the previous case study that our approach is correct and does not suffer from liveness related problems (i.e. lower bounds on transition probabilities are different from 0) typical of abstract semantics based on predicate abstraction. Nevertheless, it presents many points where precision can be improved.

Summarizing the main causes of imprecision, and some suggestions to their solution, are the following:

a) The function $\widehat{LIM}^{\circ}$, computing bounds on the number of concrete transitions between the states abstracted by two abstract states, considers the arrival state only for the computation of the lower bound. In other words, for some $s^{\circ\prime}, s^{\circ\prime\prime}, \mathcal{R}$ the value of $[\widehat{LIM}^{\circ}(s^{\circ\prime}, s^{\circ\prime\prime}, \mathcal{R})]^{+}$ depends only on $s^{\circ\prime}$. This is evident in the seasonal animals reproduction model of the previous section: we have that

$$\widehat{LIM}^{\circ}(s^{\circ}{}_0, s^{\circ}{}_1, \mathcal{R}) = \widehat{LIM}^{\circ}(s^{\circ}{}_0, s^{\circ}{}_6, \mathcal{R}) = \widehat{LIM}^{\circ}(s^{\circ}{}_0, s^{\circ}{}_9, \mathcal{R}) = [1, 6]$$

while

$$LIM^{\circ}(s^{\circ}{}_0, s^{\circ}{}_1, \mathcal{R}) = [1, 1]\,,\ LIM^{\circ}(s^{\circ}{}_0, s^{\circ}{}_6, \mathcal{R}) = [2, 2]$$

$$\text{and } LIM^{\circ}(s^{\circ}{}_0, s^{\circ}{}_9, \mathcal{R}) = [1, 2]\,.$$

A more precise version of this function should, instead, consider the information given by $s^{\circ\prime\prime}$.

b) The function $\widehat{MUL}^{\circ}$, computing the bounds on the multiplicity of maximally parallel rules application events between two abstract states, in the current definition ignores information about the abstract multiset of rule application in input and considers only the starting state.

This is evident in the oviparous reproduction model of the previous section: we have that

$$\widehat{MUL}^{\circ}(\mu^{\circ}{}_1, s^{\circ}{}_0, \mathcal{R}) = \widehat{MUL}^{\circ}(\mu^{\circ}{}_2, s^{\circ}{}_0, \mathcal{R}) = \widehat{MUL}^{\circ}(\mu^{\circ}{}_3, s^{\circ}{}_0, \mathcal{R}) = [1, 5]$$

while

$$\max_{s \in \gamma_{\mathcal{MS}}(s_0),\, \mu \in \gamma_{\mathcal{MS}}(\mu^{\circ}{}_1)} MUL(\mu, s, \mathcal{R}) = 1\,,$$
$$\max_{s \in \gamma_{\mathcal{MS}}(s_0),\, \mu \in \gamma_{\mathcal{MS}}(\mu^{\circ}{}_2)} MUL(\mu, s, \mathcal{R}) = 2 \text{ and}$$
$$\max_{s \in \gamma_{\mathcal{MS}}(s_0),\, \mu \in \gamma_{\mathcal{MS}}(\mu^{\circ}{}_3)} MUL(\mu, s, \mathcal{R}) = 2\,.$$

A more precise version should consider the information given by the abstract multiset of rule application.

c) The function $\widehat{f^{\circ(n)}}$ should refine the abstract multiset of rule applications not only considering the precise intervals in the previous approximation, but exploiting also information about the minimum/maximum number of times a rule each rule is applied in the previous approximation.

These points are not investigated here to keep the discussion as simple as possible in order to show the soundness of the approach.

The approach we propose is able to effectively compute a finite, compact, abstract probabilistic semantics for models of systems evolving with a synchronous, maximally parallel, behavior.

Actually, the result we have presented are not limited to this particular application and can be generalized. Indeed, the proposed approach could be adapted to any language and abstract semantics able to give concrete and abstract LTSs in a relation similar to the one presented here, $\sqsubseteq_{\mathcal{LTS}^{\circ}}$. More in details, Theorem 5.4.6 can be applied to any lts and lts°, independently from the language and the semantics used to compute them, such that $\alpha_{\mathcal{LTS}}(lts) \sqsubseteq_{\mathcal{LTS}^{\circ}} lts^{\circ}$[5].

5.7 Comparison with Related Works

With regard to related works, while the abstraction of probabilistic semantics has been widely studied over the last few years, to our knowledge there are not other works dealing with abstraction of a maximally parallel probabilistic semantics.

[5] In particular, only the condition over transition rates of $\sqsubseteq_{\mathcal{LTS}^{\circ}}$ in Definition 37 should be respected.

In literature many abstractions of probabilistic semantics have been recently proposed: infinite state abstraction [HHWZ10], predicate abstraction [WZH07, KKNP08, KH09], symmetry reduction [DMP07, KNP06], counter example driven abstraction refinement [HWZ08].

The approaches of [FLW06, DJJL01, SVA, Hut05, Šku06, Šku09] present similar abstractions of probabilistic systems, using MDP or IMC. The abstractions are designed for dealing with the traditional state explosion problem. In particular, the abstract model is derived from the concrete one (a DTMC), by partitioning the concrete state space and by calculating the abstract probability distributions directly from the concrete ones.

Our approach is different from other works as it aimed to effectively compute an abstract probabilistic semantics for maximally parallel rewriting systems, through the computation of an LTS, while other approaches discuss the problem of abstraction starting from the concrete DTMC. Moreover our approach allows systems with associated an infinite concrete state space to be studied, computing on the flight bounds on probabilities of transitions involving infinite states.

In the context of biological systems modelling similar approaches, are presented in [CGL09, GL09, BLMS09] to validate probabilistic temporal properties of biological systems. Namely these abstractions are designed for approximating the multiplicity of individuals, present in a state, using intervals of integers, and for supporting probabilistic model checking of MSR systems with uncertain kinetic rates, using intervals of reals.

The proposal of [DFF$^+$08, DFFK08] applies abstract interpretation techniques, in the context of formal studies of biological systems, to compute efficiently a superset of reachable complexes, and to generates smaller systems of differential equations from the concrete one.

The approach of [KRHK10] is aimed to perform abstraction of a particular kind of Markov chain, namely the ones structured as *Quasi-Birth/Dead processes*.

Finally, [Mon05, DPW00] investigate the application of abstract interpretation into the context of standard concurrent probabilistic programming languages.

The idea of partitioning the state space of biochemical system model is also used in [GH09], where states are assigned to classes of equivalence on the base of the set of applicable rules.

While the abstraction of probabilistic semantics has been widely studied over the last few years, to our knowledge there are not other works dealing with abstraction of a maximally parallel probabilistic semantics.

5.8 Conclusions

In this Chapter we defined an approach to construct effectively a sound approximation of the maximally parallel probabilistic semantics defined in Chapter 4.

It allows conservative bounds on probability of reachability properties to be obtained. Moreover it allows the number of states and transitions in the state space of the studied system to be drastically reduced and systems with an infinite associated states space to be analyzed. Since the abstraction is parametric on a set of predicates, it is possible to refine the abstract probabilistic model until a right compromise between dimension and precision is reached.

The approach is proved to be sound with respect to probabilistic reachability and its efficacy is shown on a simple model of seasonal animal reproduction behavior. The method can be further refined, defining more precise and complex functions for transition rates computation, preserving its soundness.

5.9 Proofs

Proof of Lemma 5.3.4. As $\widehat{f^{\circ}}$ is defined as the fix-point of $\widehat{f^{\circ(n)}}$, our proof proceeds by induction

1) $f^{\circ}(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime}) \sqsubseteq_{\mathcal{MS}^{\circ}} \widehat{f^{\circ(0)}}(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime})$

2) if $f^{\circ}(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime}) \sqsubseteq_{\mathcal{MS}^{\circ}} \widehat{f^{\circ(n)}}(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime})$ then
$f^{\circ}(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime}) \sqsubseteq_{\mathcal{MS}^{\circ}} \widehat{f^{\circ(n+1)}}(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime})$

1) We have to prove that $\forall i \in [1, m]$

a) $[f^{\circ}(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime})(i)]^{+} \leq [\widehat{f^{\circ(0)}}(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime})(i)]^{+}$

b) $[f^{\circ}(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime})(i)]^{-} \geq [\widehat{f^{\circ(0)}}(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime})(i)]^{-}$

To prove *a*):We have that $f^{\circ}(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime})(i)^{+}$
$= [\bigcup^{\mathcal{MS}^{\circ}} \mu^{\bullet}(i) \mid s' \xrightarrow{\mu, r} s'',\ s' \in \gamma_{\mathcal{MS}}(s'^{\circ}),\ s'' \in \gamma_{\mathcal{MS}}(s''^{\circ})]^{+}$
$= \max_{s' \xrightarrow{\mu, r} s'', s' \in \gamma_{\mathcal{MS}}(s'^{\circ}), s'' \in \gamma_{\mathcal{MS}}(s''^{\circ})} \mu(i)$
$= max_i$, and let s'_{max_i}, s''_{max_i} be states s.t. $s'_{max_i} \xrightarrow{\mu_{max_i}, r_{max_i}} s''_{max_i} \wedge \mu_{max_i}(i) = max_i$.
On the other side, we have that $[\widehat{f^{\circ(0)}}(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime})(i)]^{+}$ is less or equal, $\forall a \in \Sigma$, of each of the following values:

i) $\lfloor [\Delta(s^{\circ\prime}, s^{\circ\prime\prime})(a)]^{+}/R_i(a) \rfloor$ if
$[\Delta(s^{\circ\prime}, s^{\circ\prime\prime})(a)]^{+} \geq 0 \ \wedge\ R_i(a) > 0 \ \wedge\ \neg TC(a, \mathcal{R})$;

ii) $\{\lfloor [s^{\circ\prime\prime}(a)]^{+}/R_i(a) \rfloor$ if $R_i(a) > 0 \ \wedge\ TC(a, \mathcal{R})$;

iii) $\{\lfloor -[\Delta(s^{\circ\prime}, s^{\circ\prime\prime})(a)]^{-}/L_i(a) \rfloor$ if
$[\Delta(s^{\circ\prime}, s^{\circ\prime\prime})(a)]^{-} \leq 0 \ \wedge\ L_i(a) > 0 \ \wedge\ \neg TP(a, \mathcal{R})$;

iv) $\lfloor [s^{\circ\prime}(a)]^{+}/L_i(a) \rfloor$ if $L_i(a) > 0 \ \wedge\ TP(a, \mathcal{R})$.

Let us consider a generic $a \in \Sigma$. Lets us consider the *i*) case.
The condition $[\Delta(s^{\circ\prime}, s^{\circ\prime\prime})(a)]^{+} \geq 0 \ \wedge\ R_i(a) > 0 \ \wedge\ \neg TC(a, \mathcal{R})$ holds.
By Lemma 5.3.3 we have that $[\Delta(s^{\circ\prime}, s^{\circ\prime\prime})(a)]^{+}/R_i(a) \geq \Delta(s'_{max_i}, s''_{max_i})(a)/R_i(a)$.
As there are not rules consuming a, and R_i is producing a, no more than $\Delta(s', s'')(a)$ may be created by R_i, that consequently is applied no more than $\Delta(s'_{max_i}, s''_{max_i})(a)/R_i(a)$ times. Summarizing,

$f^\circ(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime})(i)^+ =$

$$max_i \leq min_{a\in\Sigma}\Delta(s'_{max_i}, s''_{max_i})(a)/R_i(a) \leq [\widehat{f^{\circ(0)}}(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime})(i)]^+ .$$

Lets us consider the *ii*) case. The condition $R_i(a) > 0 \wedge TC(a, \mathcal{R})$ holds.
As there are rules consuming a, and R_i is producing a, it may happen that all the a in the arrival state are produced by applications of R_i. Namely R_i cannot be applied more than $\lfloor s''_{max_i}(a)/R_i \rfloor$, times.
As $s''_{max_i} \in \gamma_{\mathcal{MS}}(s''^\circ)$ we have that $\lfloor s''_{max_i}(a)/R_i \rfloor \leq \lfloor [s^{\circ\prime\prime}(a)]^+/R_i(a) \rfloor$. Summarizing,

$f^\circ(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime})(i)^+ =$

$$max_i \leq min_{a\in\Sigma} s''_{max_i}(a)/R_i \leq [\widehat{f^{\circ(0)}}(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime})(i)]^+ .$$

Lets us consider the *iii*) case. The condition $[\Delta(s^{\circ\prime}, s^{\circ\prime\prime})(a)]^- \leq 0 \wedge L_i(a) > 0 \wedge \neg TP(a, \mathcal{R})$ holds.
By Lemma 5.3.3 we have that $-[\Delta(s^{\circ\prime}, s^{\circ\prime\prime})(a)]^-/L_i(a) \geq -\Delta(s'_{max_i}, s''_{max_i})(a)/L_i(a)$.
As there are not rules producing a, and R_i is consuming a, no more than $-\Delta(s', s'')(a)$ may be consumed by R_i, that consequently is applied no more than $-\Delta(s'_{max_i}, s''_{max_i})(a)/L_i(a)$ times. Summarizing,

$$f^\circ(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime})(i)^+ = max_i \leq min_{a\in\Sigma}\Delta(s'_{max_i}, s''_{max_i})(a)/R_i(a) \leq [\widehat{f^{\circ(0)}}(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime})(i)]^+ .$$

Lets us consider the *iv*) case. The condition $L_i(a) > 0 \wedge TP(a, \mathcal{R})$ holds.
As there are rules producing a, and R_i is consuming a, it may happen that all the a in the starting state are consumed by applications of R_i. Namely R_i can be applied no more than $\lfloor s'_{max_i}(a)/L_i \rfloor$, times.
As $s'_{max_i} \in \gamma_{\mathcal{MS}}(s'^\circ)$ we have that $\lfloor s'_{max_i}(a)/L_i \rfloor \leq \lfloor [s^{\circ\prime\prime}(a)]^+/R_i(a) \rfloor$. Summarizing,

$$f^\circ(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime})(i)^+ = max_i \leq min_{a\in\Sigma} s'_{max_i}(a)/L_i \leq [\widehat{f^{\circ(0)}}(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime})(i)]^+ .$$

To prove *b*): We have that $f^\circ(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime})(i)^-$
$= [\bigcup_{\mathcal{MS}^\circ} \mu^\bullet(i) \mid s' \xrightarrow{\mu, r} s'' ,\ s' \in \gamma_{\mathcal{MS}}(s'^\circ) ,\ s'' \in \gamma_{\mathcal{MS}}(s''^\circ)]^-$
$= \min_{s' \xrightarrow{\mu, r} s'' ,\ s' \in \gamma_{\mathcal{MS}}(s'^\circ) ,\ s'' \in \gamma_{\mathcal{MS}}(s''^\circ)} \mu(i)$
$= \min_i$, and let s'_{min_i}, s''_{min_i} be states s.t. $s'_{min_i} \xrightarrow{\mu_{min_i}, r_{min_i}} s''_{min_i} \wedge \mu_{min_i}(i) = min_i$.

On the other side, we have that $[\widehat{f^{\circ(0)}}(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime})(i)]^-$ is greater or equal, $\forall a \in \Sigma$, of each of the following values:

i) $\lceil [\Delta(s^{\circ\prime}, s^{\circ\prime\prime})(a)]^- / R_i(a) \rceil$ if $[\Delta(s^{\circ\prime}, s^{\circ\prime\prime})(a)]^- > 0 \wedge R_i(a) > 0 \wedge OP(i, a, \mathcal{R})$;

ii) $\lceil -[\Delta(s^{\circ\prime}, s^{\circ\prime\prime})(a)]^+ / L_i(a) \rceil$ if $[\Delta(s^{\circ\prime}, s^{\circ\prime\prime})(a)]^+ < 0 \wedge L_i(a) > 0 \wedge OC(i, a, \mathcal{R})$;

iii) 0.

Lets us consider a generic $a \in \Sigma$. Lets us consider the *i*) case.
The condition $[\Delta(s^{\circ\prime}, s^{\circ\prime\prime})(a)]^- > 0 \wedge R_i(a) > 0 \wedge OP(i, a, \mathcal{R})$ holds.
By Lemma 5.3.3 we have that $[\Delta(s^{\circ\prime}, s^{\circ\prime\prime})(a)]^- / R_i(a) \leq \Delta(s'_{min_i}, s''_{min_i})(a)/R_i(a)$.
As R_i is the only rule producing a, $\Delta(s'_{min_i}, s''_{min_i})(a)$ are created by R_i, that, consequently, is applied at least $\Delta(s'_{min_i}, s''_{min_i})(a)/R_i(a)$ times. Summarizing,

$$f^\circ(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime})(i)^- = min_i \geq max_{a\in\Sigma}\Delta(s'_{min_i}, s''_{min_i})(a)/R_i(a) \geq [\widehat{f^{\circ(0)}}(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime})(i)]^- .$$

Considering the *ii*) case, the condition $[\Delta(s^{\circ\prime}, s^{\circ\prime\prime})(a)]^+ < 0 \wedge L_i(a) > 0 \wedge OC(i, a, \mathcal{R})$ holds.
By Lemma 5.3.3 we have that $-[\Delta(s^{\circ\prime}, s^{\circ\prime\prime})(a)]^+ / L_i(a) \leq /, -\Delta(s'_{min_i}, s''_{min_i})(a)/L_i(a)$.
As R_i is the only rule consuming a, $-\Delta(s'_{min_i}, s''_{min_i})(a)$ are consumed by R_i, that, consequently, is applied at least $-\Delta(s'_{min_i}, s''_{min_i})(a)/L_i(a)$ times. Summarizing,

$$f^\circ(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime})(i)^- = min_i \geq max_{a\in\Sigma} -\Delta(s'_{min_i}, s''_{min_i})(a)/L_i(a) \geq [\widehat{f^{\circ(0)}}(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime})(i)]^- .$$

The *iii*) case is trivial as each rule cannot be applied less than 0 times.

2) It is immediate to show that $f^\circ(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime}) \sqsubseteq_{\mathcal{MS}^\circ} \widehat{f^{\circ(n)}}(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime})$, implies $f^\circ(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime}) \sqsubseteq_{\mathcal{MS}^\circ} \widehat{f^{\circ(n+1)}}(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime})$. In fact the refinement function uses a more precise Δ (based on *sMod*) and set of rules *rMod*, excluding only values of $\widehat{f^{\circ(n)}}(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime})$ not included in $f^\circ(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime})$. Formally, $f^\circ(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime}) \sqsubseteq_{\mathcal{MS}^\circ} \widehat{f^{\circ(n+1)}}(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime}) \sqsubseteq_{\mathcal{MS}^\circ} \widehat{f^{\circ(n)}}(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime})$. Moreover, for the same reasoning, $FixPoint(\widehat{f^{\circ(n)}}(\mathcal{R})(s^{\circ\prime}, s^{\circ\prime\prime}))$ always exists and the computation eventually halts, at most with a precise abstract multiset (i.e. μ° s.t. $\forall_{i\in[1,|\mu|]} : \mu[i]^+ = \mu[i]^-$). □

Proof of Lemma 5.3.5. We have to prove that :

i) $MUL(\mu, s, \mathcal{R}) \geq 1$;

ii) $MUL(\mu, s, \mathcal{R}) \leq [\widehat{MUL}^\circ(\mu^\circ, s^\circ, \mathcal{R})]^+$.

The case *i*) is obvious as a maximally parallel event μ has at least a multiplicity of 1.

Considering the case *ii*), we have to prove that $MUL(\mu, s, \mathcal{R}) \leq \widehat{MUL}^*(s^\circ, \mathcal{R})$ that is

$$\prod_{a\in\Sigma} \prod_{\substack{i\in[1,m] \\ s.t.\, Applied(i,\mu)}} \binom{s(a) - \sum_{r=1}^{i} l_r(a) * \mu[r]}{l_i(a) * \mu[i]} \leq \prod_{a\in\Sigma} \prod_{i\in[1,m]} \Upsilon(s^+(s^\circ)(a), X))$$

where

$$X = \begin{cases} (NAR(s^+(s^\circ), a, \mathcal{R}) - 1 & \text{if } \exists R \in \mathcal{R} \text{ s.t. } ContextFree(R, a) \\ (NAR(s^+(s^\circ), a, \mathcal{R}) & \text{otherwise ,} \end{cases}.$$

As $(i \in [1, m] \text{ s.t. } Applied(i, \mu)) \subseteq (i \in [1, m])$, $\forall a \in \Sigma$, this is equal to prove

$$\frac{s(a)!}{\prod_{\substack{i\in[1,m] \\ s.t.\, \mu[i]>0}} (l_i(a) * \mu[i])! * [s(a) - \sum_{\substack{i\in[1,m] \\ s.t.\, \mu[i]>0}} l_i(a) * \mu[i]]!} \leq \frac{s^+(s^\circ)(a)!}{\lfloor(\frac{s^+(s^\circ)(a)}{X})\rfloor!^X}.$$

We have that, $\forall a \in \Sigma$, $s(a)! \leq s^+(s^\circ)(a)!$.

It remains to prove that

$$\prod_{\substack{i\in[1,m] \\ s.t.\, \mu[i]>0}} (l_i(a) * \mu[i])! * [s(a) - \sum_{\substack{i\in[1,m] \\ s.t.\, \mu[i]>0}} l_i(a) * \mu[i]]! \leq \lfloor(\frac{s^+(s^\circ)(a)}{X+1})\rfloor!^{X+1}.$$

We have two cases:

- if $\exists R \in \mathcal{R}$ s.t. $ContextFree(R, a)$ then $\sum_{\substack{i\in[1,m] \\ s.t.\, \mu[i]>0}} l_i(a) * \mu[i] = s(a)$. We have that $\lfloor(\frac{s^+(s^\circ)(a)}{(NAR(s^+(s^\circ),a,\mathcal{R})})\rfloor!^{(NAR(s^+(s^\circ),a,\mathcal{R})}$ is a lower bound for $\prod_{\substack{i\in[1,m] \\ s.t.\, \mu[i]>0}} (l_i(a) * \mu[i])!$;

- otherwise, we have that $\lfloor(\frac{s^+(s^\circ)(a)}{(NAR(s^+(s^\circ),a,\mathcal{R})+1})\rfloor!^{(NAR(s^+(s^\circ),a,\mathcal{R})+1}$ is a lower bound for all the expressions of the form $k_1!k_2!\ldots k_m!(n-\sum_{i=1}^m k_i)!$ when $m = NA(s^+(s^\circ),a,\mathcal{R})$, $n = s^+(s^\circ)(a)$ and $\sum_{i=1}^m k_i \leq n$. Hence it is a lower bound for $\prod_{\substack{i\in[1,m]\\ s.t.\,\mu[i]>0}} (l_i(a) * \mu[i])!$.

□

Proof of Lemma 5.3.6. We have to prove that :

i) $KIN(\mu, s, \mathcal{R}) \geq [\widehat{KIN}^\circ(\mu^\circ, s^\circ, \mathcal{R})]^-$;

ii) $KIN(\mu, s, \mathcal{R}) \leq [\widehat{KIN}^\circ(\mu^\circ, s^\circ, \mathcal{R})]^+$.

Considering the case *i*), we have that $KIN(\mu, s, \mathcal{R}) = \prod_{r\in[1,m]} LRR(r, s, \mathcal{R})^{\mu[r]}$ is $\geq$ of $[\widehat{KIN}^\circ(\mu^\circ, s^\circ, \mathcal{R})]^- = \prod_{r\in[1,m]} LRR(r, s^+(s^\circ), \mathcal{R})^{[\mu^\circ[r]]^+}$ as LRR has $[0, 1]$ as co-domain, and $[\mu^\circ(r)]^+ \geq \mu(r)$.

Considering the case *ii*), a similar reasoning holds as $[\mu^\circ(r)]^- \leq \mu(r)$. □

Proof of Lemma 5.3.7. As we already seen in Section 4.5, the number of exiting transition from a concrete state s using rules in $\mathcal{R}$ is top bound by $\prod_{a\in\Sigma,\, s(a)>0} \phi(\|(\mathcal{R})_a\|, s(a))$.

$\widehat{LIM}^\circ(s^{\circ\prime}, s^{\circ\prime\prime}, \mathcal{R})^+$ consist of the result of same computation using $\forall a \in \Sigma[s^\circ(a)]^+$; As $\forall a \in \Sigma, \forall s \in \gamma_{\mathcal{MS}}(s^\circ) : s(a) \leq [s^\circ(a)]^+$, we have that $\widehat{LIM}^\circ(s^{\circ\prime}, s^{\circ\prime\prime}, \mathcal{R})^+ \leq LIM^\circ(s^{\circ\prime}, s^{\circ\prime\prime}, \mathcal{R})^+$.

$\widehat{LIM}^\circ(s^{\circ\prime}, s^{\circ\prime\prime}, \mathcal{R})^-$ is a sound lower approximation of $LIM^\circ(s^{\circ\prime}, s^{\circ\prime\prime}, \mathcal{R})^-$ as it is equal to 0 if there exists a state $s \in \gamma_{\mathcal{MS}}(s^{\circ\prime})$ for which there are no transitions to any state $s'' \in \gamma_{\mathcal{MS}}(s^{\circ\prime\prime})$; it is equal to 1 if there is at least a transitions exiting from each concrete state $s \in \gamma_{\mathcal{MS}}(s^{\circ\prime})$ to some state $s'' \in \gamma_{\mathcal{MS}}(s^{\circ\prime\prime})$.

□

Proof of Theorem 5.3.8. We have to prove that

a) $MUL(\mu, s, \mathcal{R}) * KIN(\mu, s, \mathcal{R}) \geq [\widehat{MUL}^\circ(\mu^\circ, s^\circ, \mathcal{R})]^- * [\widehat{KIN}^\circ(\mu^\circ, s^\circ, \mathcal{R})]^- * [\widehat{LIM}^\circ(s'^\circ, s''^\circ, \mathcal{R})]^-$

b) $MUL(\mu, s, \mathcal{R}) * KIN(\mu, s, \mathcal{R}) \leq [\widehat{MUL}^\circ(\mu^\circ, s^\circ, \mathcal{R})]^+ * [\widehat{KIN}^\circ(\mu^\circ, s^\circ, \mathcal{R})]^+ * [\widehat{LIM}^\circ(s'^\circ, s''^\circ, \mathcal{R})]^+$

To prove *a)* we have to prove that

i) $MUL(\mu, s, \mathcal{R}) \geq [\widehat{MUL}^\circ(\mu^\circ, s^\circ, \mathcal{R})]^-$

ii) $KIN(\mu, s, \mathcal{R}) \geq [\widehat{KIN}^{\circ}(\mu^{\circ}, s^{\circ}, \mathcal{R})]^{-}$

iii) $[\widehat{LIM}^{\circ}(s'^{\circ}, s''^{\circ}, \mathcal{R})]^{-} \geq [\widehat{LIM}^{\circ}(s'^{\circ}, s''^{\circ}, \mathcal{R})]^{-} = 1.$

But *i)* and *ii)* are guaranteed by Lemmata 5.3.5 and 5.3.6, respectively, while *iii)* is true by definition of $\widehat{LIM}^{\circ}$.

To prove *b)* we have to prove that

i) $MUL(\mu, s, \mathcal{R}) \leq [\widehat{MUL}^{\circ}(\mu^{\circ}, s^{\circ}, \mathcal{R})]^{+}$

ii) $KIN(\mu, s, \mathcal{R}) \leq [\widehat{KIN}^{\circ}(\mu^{\circ}, s^{\circ}, \mathcal{R})]^{+}$

iii) $[LIM^{\circ}(s'^{\circ}, s''^{\circ}, \mathcal{R})]^{+} \leq [\widehat{LIM}^{\circ}(s'^{\circ}, s''^{\circ}, \mathcal{R})]^{+}.$

But *i)* and *ii)* are guaranteed by Theorems 5.3.5 and 5.3.6, respectively, while *iii)* is true by definition of $\widehat{LIM}^{\circ}$. □

Proof of Theorem 3.3.3. Let $M^{\circ} = (\Sigma, \mathcal{R}, s_0, \mathfrak{p})$ and $M = (\Sigma, \mathcal{R}, s_0)$. $LTS(M)$ is $(S, s_0, \rightarrow)$ and $\alpha_{\mathcal{LTS}}(LTS(M)) = (S^{\circ}(\mathfrak{p}^{\bullet}), \alpha_{\mathcal{MS}}(\mathfrak{p}^{\bullet})(s_0), \rightarrow^{\alpha}_{\circ})$, while $LTS^{\circ}(M^{\circ}) = (S^{\circ}(\mathfrak{p}), s_0{}^{\circ}, \rightarrow_{\circ})$. We have to prove that

a) $\mathfrak{p}^{\bullet} \sqsubseteq_{\widehat{\mathbb{P}}} \mathfrak{p}$ that is true by definition of $\mathfrak{p}^{\bullet}$ and by the fact that $\mathfrak{p}$ is a partition with respect to Σ;

b) $\forall t_1^{\circ} = (s_1{}^{\circ} \xrightarrow{\mu^*, r^*}_{\circ} s_1{}^{\circ\prime}) \in \rightarrow^{\alpha}_{\circ}$, $\exists\, t_2^{\circ} = (s_2{}^{\circ} \xrightarrow{\mu^{\circ}, r^{\circ}}_{\circ} s_2{}^{\circ\prime}) \in \rightarrow_{\circ}$ such that

1) $s^{\circ}{}_1 \sqsubseteq_{\mathcal{MS}^{\circ}} s^{\circ}{}_2$, $s^{\circ\prime}{}_1 \sqsubseteq_{\mathcal{MS}^{\circ}} s^{\circ\prime}{}_2$;

2) Let

$$\widehat{\mu^{\circ}} = \bigcup_{\substack{s^{\circ}{}_3 \xrightarrow{\mu^{\circ}{}_3, r^{\circ}_3}_{\circ} s^{\circ\prime}{}_3 \in \rightarrow^{\alpha}_{\circ} s.t. \\ s^{\circ}{}_3 \sqsubseteq_{\mathcal{MS}^{\circ}} s^{\circ}{}_2 \\ s^{\circ\prime}{}_3 \sqsubseteq_{\mathcal{MS}^{\circ}} s^{\circ\prime}{}_2}}^{\mathcal{MS}^{\circ}} \mu^{\circ}{}_3 \,, \; \widehat{r^{\circ}} = \bigcup_{s^{\circ}{}_3 \sqsubseteq_{\mathcal{MS}^{\circ}} s^{\circ}{}_2}^{\mathbb{I}} \sum_{\substack{s^{\circ}{}_3 \xrightarrow{\mu^{\circ}{}_3, r^{\circ}_3}_{\circ} s^{\circ\prime}{}_3 \in \rightarrow^{\alpha}_{\circ} s.t. \\ s^{\circ\prime}{}_3 \sqsubseteq_{\mathcal{MS}^{\circ}} s^{\circ\prime}{}_2}}^{\mathbb{I}} r^{\circ}{}_3$$

i) $\widehat{\mu^{\circ}} \sqsubseteq_{\mathcal{MS}^{\circ}} \mu^{\circ}$ and *ii)* $\widehat{r^{\circ}} \sqsubseteq_{\mathbb{I}} r^{\circ}$

c) $\forall t_2^{\circ} = (s_2{}^{\circ} \xrightarrow{\mu^{\circ}, r^{\circ}}_{\circ} s_2{}^{\circ\prime}) \in \rightarrow_{\circ}$:
$([r^{\circ}]^{-} = 0) \vee$
$\exists\, t_1^{\circ} = (s_1{}^{\circ} \xrightarrow{\mu^*, r^*}_{\circ} s_1{}^{\circ\prime}) \in \rightarrow^{\alpha}_{\circ}$, s.t. $s_1{}^{\circ} \sqsubseteq_{\mathcal{MS}^{\circ}} s_2{}^{\circ} \wedge s_1{}^{\circ\prime} \sqsubseteq_{\mathcal{MS}^{\circ}} s_2{}^{\circ\prime})$

As $\mathfrak{p}^\bullet \sqsubseteq_{\widehat{\mathbb{P}}} \mathfrak{p}$ it holds that $\forall s^\circ{}_1 \in S(\mathfrak{p}^\bullet)\, \exists!\, s^\circ{}_2 \in S(\mathfrak{p})$ s.t. $s^\circ{}_1 \sqsubseteq_{\mathcal{MS}^\circ} s^\circ{}_2$. The same reasoning applies to $s^{\circ\prime}_1$ and $s^{\circ\prime}_2$. Moreover, given the fact that $\widehat{Next^\circ}$ is sound and monotone (see Theorem 5.3.2), and LTS° has a transition from a state s° to all states in $\widehat{Next^\circ}(\mathcal{R})(s^\circ, \mathfrak{p})$, the existence, for each transition in $\alpha_{\mathcal{LTS}}(LTS(M))$, of a transition in $LTS^\circ(M^\circ)$ respecting the conditions of 1) is guaranteed.

About 2), the condition *i*) is guaranteed by by Lemma 5.3.4, as μ° is computed by LTS° by $\widehat{f^\circ}$, that gives a sound approximation of all the maximally parallel multiset of rule applications between all the concrete states abstracted by $s_2{}^\circ$ and $s_2{}^{\circ\prime}$.

About the *ii*) condition we have to prove that

$$\widehat{r^\circ} = \bigcup^{\mathbb{I}}_{s^\circ{}_3 \sqsubseteq_{\mathcal{MS}^\circ} s^\circ{}_2} \sum^{\mathbb{I}}_{s^\circ{}_3 \xrightarrow[\circ]{\mu^\circ{}_3, r^\circ_3} s^{\circ\prime}_3 \in \rightarrow^\alpha_\circ s.t.,\ s^{\circ\prime}_3 \sqsubseteq_{\mathcal{MS}^\circ} s^{\circ\prime}_2} r^\circ{}_3 \sqsubseteq_{\mathbb{I}} Rate^\circ(\mathcal{R})(\mu^\circ,\, s^\circ{}_2,\, s^{\circ\prime}_2) = r^\circ$$

that is

$$\min_{s^\circ{}_3 \sqsubseteq_{\mathcal{MS}^\circ} s^\circ{}_2} \left[\sum^{\mathbb{I}}_{s^\circ{}_3 \xrightarrow[\circ]{\mu^\circ{}_3, r^\circ_3} s^{\circ\prime}_3 \in \rightarrow^\alpha_\circ s.t.,\ s^{\circ\prime}_3 \sqsubseteq_{\mathcal{MS}^\circ} s^{\circ\prime}_2} r^\circ{}_3 \right]^- \geq$$
$$[\widehat{MUL^\circ}(\mu^\circ, s^\circ{}_2, \mathcal{R})]^- * [\widehat{KIN^\circ}(\mu^\circ, s^\circ{}_2, \mathcal{R})]^- * [\widehat{LIM^\circ}(s^\circ{}_2, s'^\circ{}_2, \mathcal{R})]^-$$

and

$$\max_{s^\circ{}_3 \sqsubseteq_{\mathcal{MS}^\circ} s^\circ{}_2} \left[\sum^{\mathbb{I}}_{s^\circ{}_3 \xrightarrow[\circ]{\mu^\circ{}_3, r^\circ_3} s^{\circ\prime}_3 \in \rightarrow^\alpha_\circ s.t.,\ s^{\circ\prime}_3 \sqsubseteq_{\mathcal{MS}^\circ} s^{\circ\prime}_2} r^\circ{}_3 \right]^+ \leq$$
$$[\widehat{MUL^\circ}(\mu^\circ, s^\circ{}_2, \mathcal{R})]^+ * [\widehat{KIN^\circ}(\mu^\circ, s^\circ{}_2, \mathcal{R})]^+ * [\widehat{LIM^\circ}(s^\circ{}_2, s'^\circ{}_2, \mathcal{R})]^+$$

that is

$$\min_{s^\circ{}_3 \sqsubseteq_{\mathcal{MS}^\circ} s^\circ{}_2} \left[\sum_{\substack{s^\circ{}_3 \xrightarrow{\mu^\circ{}_3, r^\circ_3}_\circ s^{\circ\prime}{}_3 \in \rightarrow^a_\circ s.t. \\ s^{\circ\prime}{}_3 \sqsubseteq_{\mathcal{MS}^\circ} s^{\circ\prime}{}_2}}^{\mathbb{I}} \sum_{\substack{s \xrightarrow{\mu, r} s' \in \rightarrow \\ s \in \gamma_{\mathcal{MS}}(s^\circ{}_3) \\ s' \in \gamma_{\mathcal{MS}}(s'^\circ{}_3)}}^{\mathbb{I}} r^\bullet \right]^- \geq$$
$$[\widehat{MUL}^\circ(\mu^\circ, s^\circ{}_2, \mathcal{R})]^- * [\widehat{KIN}^\circ(\mu^\circ, s^\circ{}_2, \mathcal{R})]^- * [\widehat{LIM}^\circ(s^\circ{}_2, s'^\circ{}_2, \mathcal{R})]^-$$

and

$$\max_{s^\circ{}_3 \sqsubseteq_{\mathcal{MS}^\circ} s^\circ{}_2} \left[\sum_{\substack{s^\circ{}_3 \xrightarrow{\mu^\circ{}_3, r^\circ_3}_\circ s^{\circ\prime}{}_3 \in \rightarrow^a_\circ s.t. \\ s^{\circ\prime}{}_3 \sqsubseteq_{\mathcal{MS}^\circ} s^{\circ\prime}{}_2}}^{\mathbb{I}} \sum_{\substack{s \xrightarrow{\mu, r} s' \in \rightarrow \\ s \in \gamma_{\mathcal{MS}}(s^\circ{}_3) \\ s' \in \gamma_{\mathcal{MS}}(s'^\circ{}_3)}}^{\mathbb{I}} r^\bullet \right]^+ \leq$$
$$[\widehat{MUL}^\circ(\mu^\circ, s^\circ{}_2, \mathcal{R})]^+ * [\widehat{KIN}^\circ(\mu^\circ, s^\circ{}_2, \mathcal{R})]^+ * [\widehat{LIM}^\circ(s^\circ{}_2, s'^\circ{}_2, \mathcal{R})]^+$$

that is

$$\min_{s^\circ{}_3 \sqsubseteq_{\mathcal{MS}^\circ} s^\circ{}_2} \left[\sum_{\substack{s \xrightarrow{\mu, r} s' \in \rightarrow \\ s \in \gamma_{\mathcal{MS}}(s^\circ{}_3), s' \in \gamma_{\mathcal{MS}}(s'^\circ{}_3) \\ s^\circ{}_3 \xrightarrow{\mu^\circ{}_3, r^\circ_3}_\circ s^{\circ\prime}{}_3 \in \rightarrow^a_\circ s.t. \\ s^{\circ\prime}{}_3 \sqsubseteq_{\mathcal{MS}^\circ} s^{\circ\prime}{}_2}}^{\mathbb{I}} [MUL(\mu, s, \mathcal{R}) \times KIN(\mu, s, \mathcal{R})]\bullet \right]^- \geq$$
$$[\widehat{MUL}^\circ(\mu^\circ, s^\circ{}_2, \mathcal{R})]^- * [\widehat{KIN}^\circ(\mu^\circ, s^\circ{}_2, \mathcal{R})]^- * [\widehat{LIM}^\circ(s^\circ{}_2, s'^\circ{}_2, \mathcal{R})]^-$$

and

$$\max_{s^\circ_3 \sqsubseteq_{\mathcal{MS}^\circ} s^\circ_2} \left[\sum_{\substack{s \xrightarrow{\mu,r} s' \in \rightarrow \\ s \in \gamma_{\mathcal{MS}}(s^\circ_3),\, s' \in \gamma_{\mathcal{MS}}(s'^\circ_3) \\ s^\circ_3 \xrightarrow{\mu^\circ_3, r^\circ_3} {}_\circ s'^\circ_3 \in \rightarrow^\alpha_\circ s.t. \\ s'^\circ_3 \sqsubseteq_{\mathcal{MS}^\circ} s'^\circ_2}}^{\mathbb{I}} [MUL(\mu, s, \mathcal{R}) \times KIN(\mu, s, \mathcal{R})]\bullet \right]^+ \leq$$

$$[\widehat{MUL}^\circ(\mu^\circ, s^\circ_2, \mathcal{R})]^+ * [\widehat{KIN}^\circ(\mu^\circ, s^\circ_2, \mathcal{R})]^+ * [\widehat{LIM}^\circ(s^\circ_2, s'^\circ_2, \mathcal{R})]^+$$

We have that, by Lemmata 5.3.5 and 5.3.6 and by the fact that $s \in \gamma_{\mathcal{MS}}(s^\circ_3)$ and $s^\circ_3 \sqsubseteq_{\mathcal{MS}^\circ} s^\circ_2$ that

- $[\widehat{MUL}^\circ(\mu^\circ, s^\circ_2, \mathcal{R})]^- \leq MUL(\mu, s, \mathcal{R}) \leq [\widehat{MUL}^\circ(\mu^\circ, s^\circ_2, \mathcal{R})]^+$;
- $[\widehat{KIN}^\circ(\mu^\circ, s^\circ_2, \mathcal{R})]^- \leq KIN(\mu, s, \mathcal{R}) \leq [\widehat{KIN}^\circ(\mu^\circ, s^\circ_2, \mathcal{R})]^+$.

Thus $\forall s \in \gamma_{\mathcal{MS}}(s^\circ_3) \,|\, s^\circ_3 \sqsubseteq_{\mathcal{MS}^\circ} s^\circ_2$:

- $MUL(\mu, s, \mathcal{R}) \times KIN(\mu, s, \mathcal{R}) \geq [\widehat{MUL}^\circ(\mu^\circ, s_2)]^- \times [\widehat{KIN}^\circ(\mu^\circ, s_2)]^-$;
- $MUL(\mu, s, \mathcal{R}) \times KIN(\mu, s, \mathcal{R}) \leq [\widehat{MUL}^\circ(\mu^\circ, s_2)]^+ \times [\widehat{KIN}^\circ(\mu^\circ, s_2)]^+$.

Moreover the previous statements, being valid $\forall s \in \gamma_{\mathcal{MS}}(s^\circ_3)$ s.t. $s^\circ_3 \sqsubseteq_{\mathcal{MS}^\circ} s^\circ_2$, are valid for the $s \in \gamma_{\mathcal{MS}}(s^\circ_3)$ s.t. $s^\circ_3 \sqsubseteq_{\mathcal{MS}^\circ} s^\circ_2$ and for which $MUL(\mu, s, \mathcal{R}) \times KIN(\mu, s, \mathcal{R})$ are *min* or *max*.

Finally, let $X = \{s \xrightarrow{\mu,r} s' \in \rightarrow \,|s \in \gamma_{\mathcal{MS}}(s^\circ_3), s' \in \gamma_{\mathcal{MS}}(s'^\circ_3), s^\circ_3 \xrightarrow{\mu^\circ_3, r^\circ_3}_\circ s'^\circ_3 \in \rightarrow^\alpha_\circ s'^\circ_3 \sqsubseteq_{\mathcal{MS}^\circ} s'^\circ_2\}$; as $[\widehat{LIM}^\circ(s^\circ_2, s'^\circ_2, \mathcal{R})]^- \leq |\{X\}| \leq [\widehat{LIM}^\circ(s^\circ_2, s'^\circ_2, \mathcal{R})]^+$, we can conclude that $\widehat{r^\circ} \sqsubseteq_{\mathbb{I}} r^\circ$.

About c, $\forall t^\circ_2 = (s_2{}^\circ \xrightarrow{\mu^\circ, r^\circ}_\circ s_2{}^{\circ\prime}) \in \rightarrow_\circ$, the existence of corresponding $s_1{}^\circ, s_1{}^{\circ\prime}$ s.t. $\sqsubseteq_{\mathcal{MS}^\circ} s_2{}^\circ \wedge s_1{}^{\circ\prime} \sqsubseteq_{\mathcal{MS}^\circ} s_2{}^{\circ\prime}$ is given by the use of $S^\circ(\mathfrak{p}^\bullet)$. We have two cases: or exists $t^\circ_1 = (s_1{}^\circ \xrightarrow{\mu^*, r^*}_\circ s_1{}^{\circ\prime}) \in \rightarrow^\alpha_\circ$, and the order is satisfied, or, otherwise, we have that $\psi(s_2{}^\circ, s_2{}^{\circ\prime}, \mathcal{R}) = 0$ and hence $[r^\circ]^- = 0$. □

Proof of Theorem 5.4.2. In order to simplify the proof it is convenient to exploit the fact that $Reach_{A,mc^\circ}(s^\circ)$ can be specified as a linear equations system [CGL09, DJJL01, Kwi03, FLW06]. In particular, for $h \in \{1, 2\}$, $s \in$

$S^\circ{}_h$, $Reach_{A,mc_h^\circ}(s^\circ)^- = \bigcup_{i\in\{0,\infty\}} \rho^{-,i}_{A,mc_h^\circ}(s^\circ)$, $Reach_{A,mc_h^\circ}(s^\circ)^+ = \bigcup_{i\in\{0,\infty\}} \rho^{+,i}_{A,mc_h^\circ}(s^\circ)$ where

$$\rho^{-,i}_{A,mc_h^\circ}(s^\circ) = \begin{cases} 1 & \text{if } s^\circ \forall \vDash A, \\ 0 & \text{if } i = 0 \wedge \neg(s^\circ \forall \vDash A), \\ \inf\limits_{\rho_{j_h}\in ADistr_{mc_h^\circ}(s)} \sum\limits_{s^{\circ\prime}\in S} \rho_{j_h}(s^{\circ\prime}) \times \rho^{-,i-1}_{A,mc_h^\circ}(s^{\circ\prime}) & \text{otherwise;} \end{cases}$$

and

$$\rho^{+,i}_{A,mc_h^\circ}(s^\circ) = \begin{cases} 1 & \text{if } s^\circ \exists \vDash A, \\ 0 & \text{if } i = 0 \wedge \neg(s^\circ \exists \vDash A), \\ \sup\limits_{\rho_{j_h}\in ADistr_{mc_h^\circ}(s)} \sum\limits_{s^{\circ\prime}\in S} \rho_{j_h}(s^{\circ\prime}) \times \rho^{+,i-1}_{A,mc_h^\circ}(s^{\circ\prime}) & \text{otherwise.} \end{cases}$$

and where $\bigcup$ stands for the least upper bound with respect to the underlying order on pseudo-distributions, e.g. $\rho_1 \subseteq \rho_2$ iff for each $s^\circ \in \mathcal{MS}^\circ$, $\rho_1(s^\circ) \leq \rho_2(s^\circ)$. Intuitively, $\rho^{-,i}_{A,mc_h^\circ}(s^\circ)$ reports the minimum probability to reach a state satisfying A, starting from s°, after i-iterates.

We examine only the case $[Reach_{A,mc_2^\circ}(s^\circ{}_2)]^- \leq [Reach_{A,mc_1^\circ}(s^\circ{}_1)]^-$.

Therefore, it is enough to show that $\rho^{-,i}_{A,mc_2^\circ}(s^\circ{}_2) \leq \rho^{-,i}_{A,mc_1^\circ}(s^\circ{}_1)$, for every $i \geq 0$, $s^\circ{}_1 \in S^\circ(\mathfrak{p}_1)$, $s^\circ{}_2 \in S^\circ(\mathfrak{p}_2)$, $s^\circ{}_1 \sqsubseteq_{\mathcal{MS}^\circ} s^\circ{}_2$. The proof proceeds by induction.

($i = 0$) There are two possibilities:

($s_2{}^\circ \forall \vDash A$) then also $s_1{}^\circ \forall \vDash A$ and $\rho^{-,i}_{A,mc_2^\circ}(s^\circ{}_2) = \rho^{-,i}_{A,mc_1^\circ}(s^\circ{}_1) = 1$;

(otherwise) $\rho^{-,i}_{A,mc_2^\circ}(s_2{}^\circ) = 0$. In both the cases, of $\rho^{-,i}_{A,mc_1^\circ}(s^\circ{}_1) = 0$ and $\rho^{-,i}_{A,mc_1^\circ}(s^\circ{}_1) = 1$, it holds $\rho^{-,i}_{A,mc_2^\circ} \leq \rho^{-,i}_{A,mc_1^\circ}$.

($i > 0$) There are two possibilities:

($s_2{}^\circ \forall \vDash A$) then also $s_1{}^\circ \forall \vDash A$ and $\rho^{-,i}_{A,mc_2^\circ}(s^\circ{}_2) = \rho^{-,i}_{A,mc_1^\circ}(s^\circ{}_1) = 1$;

(otherwise) then

$$\rho^{-,i}_{A,mc^\circ{}_2}(s_2{}^\circ) = \inf_{\rho_{j2}\in ADistr_{mc_2{}^\circ}(s^\circ{}_2)} \sum_{s^{\circ\prime}{}_2\in S^\circ{}_2} \rho_{j2}(s^{\circ\prime}{}_2) \times \rho^{-,i-1}_{A,mc_2{}^\circ}(s^{\circ\prime}{}_2).$$

On the other hand we have two cases:

$(s_1{}^\circ \forall \vDash A)$ then $\rho^{-,i}_{A,mc^\circ{}_1}(s_1{}^\circ) = 1$ while $\rho^{-,i}_{A,mc^\circ{}_2}(s_2{}^\circ) \in [0,1]$.
(otherwise)

$$\rho^{-,i}_{A,mc^\circ{}_1}(s_1{}^\circ) = \inf_{\rho_{j1} \in ADistr_{mc_1{}^\circ}(s^\circ{}_1)} \sum_{s^{\circ\prime}_1 \in S^\circ{}_1} \rho_{j1}(s^{\circ\prime}_1) \times \rho^{-,i-1}_{A,mc_1{}^\circ}(s_1{}^{\circ\prime}).$$

Let $\rho^{min}_{j1} \in ADistr_{mc_1{}^\circ}(s^\circ{}_1)$ s.t. we can rewrite $\rho^{-,i}_{A,mc^\circ{}_1}(s^\circ{}_1)$ as

$$\rho^{-,i}_{A,mc^\circ{}_1}(s^\circ{}_1) = \sum_{s^{\circ\prime}_1 \in S^\circ{}_1} \rho^{min}_{j1}(s^{\circ\prime}_1) \times \rho^{-,i-1}_{A,mc_1{}^\circ}(s_1{}^{\circ\prime}).$$

Now, by inductive hypothesis $(s^{\circ\prime}_1 \sqsubseteq_{\mathcal{MS}^\circ} s^{\circ\prime}_2 \Rightarrow \rho^{-,i-1}_{A,mc^\circ{}_1}(s^{\circ\prime}_1) \geq \rho^{-,i-1}_{A,mc^\circ{}_2}(s^{\circ\prime}_2))$, we have that,

$$\rho^{-,i}_{A,mc^\circ{}_1}(s^\circ{}_1) \leq \sum_{s^{\circ\prime}_1 \in S^\circ{}_1} \rho^{min}_{j1}(s^{\circ\prime}_1) \times \rho^{-,i-1}_{A,mc_2{}^\circ}(s_2{}^{\circ\prime})$$

for s_2 s.t. $s_1{}^{\circ\prime\circ\prime} \sqsubseteq_{\mathcal{MS}^\circ} s_2{}^{\circ\prime}$[6]. As

$$S^\circ(\mathfrak{p}_1) = \bigcup_{s_2{}^\circ \in S^\circ(\mathfrak{p}_2)} \{s_1{}^\circ \in S^\circ(\mathfrak{p}_1) \mid s_1{}^\circ \sqsubseteq_{\mathcal{MS}^\circ} s_2{}^\circ\},$$

we can rewrite the last expression as

$$= \sum_{s^{\circ\prime}_2 \in S^\circ{}_2} \Big(\sum_{s_1{}^{\circ\prime} \in S_1{}^\circ,\, s^{\circ\prime}_1 \sqsubseteq_{\mathcal{MS}^\circ} s^{\circ\prime}_2} \rho^{min}_{j1}(s^{\circ\prime}_1) \Big) \times \rho^{-,i-1}_{A,mc_2{}^\circ}(s_2{}^{\circ\prime}).$$

Let $\rho^*_2 \in ADistr(s_2{}^\circ)$ be such that $\forall s_2{}^\circ \in S^\circ(\mathfrak{p}_2) : \rho^*_2(s_2{}^{\circ\prime}) = \sum_{s_1{}^{\circ\prime} \in S_1{}^\circ,\, s_1{}^{\circ\prime} \sqsubseteq_{\mathcal{MS}^\circ} s_2{}^{\circ\prime}} \rho^{min}_{j1}(s^{\circ\prime}_1)$, the last expression can be rewritten as

$$\sum_{s^{\circ\prime}_2 \in S^\circ{}_2} \rho^*_2(s_2{}^{\circ\prime}) \times \rho^{-,i-1}_{A,mc_2{}^\circ}(s_2{}^{\circ\prime}).$$

Finally, we have that the last expression is

$$\leq \inf_{\rho_{j2} \in ADistr_{mc_2{}^\circ}(s^\circ{}_2)} \sum_{s^{\circ\prime}_2 \in S^\circ{}_2} \rho_{j2}(s^{\circ\prime}_2) \times \rho^{-,i-1}_{A,mc_2{}^\circ}(s^{\circ\prime}_2) = \rho^{-,i}_{A,mc^\circ{}_2}(s_2{}^\circ).$$

□

[6] As $mc_1{}^\circ \sqsubseteq_{\mathcal{MC}^\circ} mc_2{}^\circ$ exists only one $s_2{}^\circ$ s.t. $s_1{}^{\circ\prime} \sqsubseteq_{\mathcal{MS}^\circ} s_2{}^{\circ\prime}$

Proof of Lemma 5.4.3. Let $\mathcal{H}^\circ(lts^\circ) = (S^\circ(\mathfrak{p}_2), {s_{0,2}}^\circ, P_2^-, P_2^+)$ and $\mathcal{H}^\circ(\alpha_{\mathcal{LTS}}(lts)) = (S^\circ(\mathfrak{p}_1), {s_{0,1}}^\circ, P_1^-, P_1^+)$.

By hypothesis $\alpha_{\mathcal{LTS}}(lts) \sqsubseteq_{\mathcal{LTS}^\circ} lts^\circ$ it holds that

- $\mathfrak{p}_1 \sqsubseteq_{\widehat{\mathbb{P}}} \mathfrak{p}_2$;
- $\forall t_1^\circ = ({s^\circ}_1 \xrightarrow{{\mu^\circ}_1, {r_1^\circ}}_\circ {s^\circ}'_1) \in \rightarrow_\circ^1,\ \exists\, t_2^\circ = ({s^\circ}_2 \xrightarrow{{\mu^\circ}_2, {r_2^\circ}}_\circ {s^\circ}'_2) \in \rightarrow_\circ^2$ such that
  1) ${s^\circ}_1 \sqsubseteq_{\mathcal{MS}^\circ} {s^\circ}_2\,,\ {s^\circ}'_1 \sqsubseteq_{\mathcal{MS}^\circ} {s^\circ}'_2$;
  2) $\widehat{\mu^\circ} \sqsubseteq_{\mathcal{MS}^\circ} {\mu^\circ}_2$ and $\widehat{r^\circ} \sqsubseteq_{\mathbb{I}} {r^\circ}_2$ where

$$\widehat{\mu^\circ} = \bigcup_{\substack{{s^\circ}_3 \xrightarrow{{\mu^\circ}_3, {r_3^\circ}}_\circ {s^\circ}'_3 \in \rightarrow_\circ^1 s.t. \\ {s^\circ}_3 \sqsubseteq_{\mathcal{MS}^\circ} {s^\circ}_2 \\ {s^\circ}'_3 \sqsubseteq_{\mathcal{MS}^\circ} {s^\circ}'_2}}^{\mathcal{MS}^\circ} \qquad {\mu^\circ}_3\,,\ \widehat{r^\circ} = \bigcup_{\substack{{s^\circ}_3 \in S^\circ(S_1) \\ {s^\circ}_3 \sqsubseteq_{\mathcal{MS}^\circ} {s^\circ}_2}}^{\mathbb{I}} \sum_{{s^\circ}_3 \xrightarrow{{\mu^\circ}_3, {r_3^\circ}}_\circ {s^\circ}'_3 \in \rightarrow_\circ^1 s.t. \atop {s^\circ}'_3 \sqsubseteq_{\mathcal{MS}^\circ} {s^\circ}'_2}^{\mathbb{I}} {r^\circ}_3$$

We have to prove that $\forall {s^\circ}_1 \in S^\circ(\mathfrak{p}_1)\, \exists!\, {s^\circ}_2 \in S^\circ(\mathfrak{p}_2)$:

a) ${s^\circ}_1 \sqsubseteq_{\mathcal{MS}^\circ} {s^\circ}_2$;

b) $\forall \rho_1 \in ADistr({s^\circ}_1)\, \exists\, !\, \rho_2 \in ADistr({s^\circ}_2)$ s.t.

$$\forall {s^\circ}'_2 \in {S^\circ}_2 \,:\, \rho_2({s_2}^{\circ\prime}) = \sum_{{s_1}^{\circ\prime} \in {S^\circ}_1\,,\, {s_1}^{\circ\prime} \sqsubseteq_{\mathcal{MS}^\circ} {s^\circ}'_2} \rho_1({s_1}^{\circ\prime})\,.$$

The condition *a)* is guaranteed by $\mathfrak{p}_1 \sqsubseteq_{\mathbb{I}} \mathfrak{p}_2$.

About *b)*, we have that $\forall {s^\circ}'_i, {s^\circ}''_i \in S^\circ(\mathfrak{p}_i) \,:\, ADistr({s^\circ}_i) = \{\rho \,|\, P^-({s^\circ}'_i, {s^\circ}''_i) \leq \rho_i({s_1}^{\circ\prime}) \leq P^+({s^\circ}'_i, {s^\circ}''_i)\}$.

To guarantee *b)* it is enough to prove that $\forall {s^\circ}_1 \in S^\circ(\mathfrak{p}_1)\,,\ {s^\circ}_2, {s^\circ}'_2 \in S^\circ(\mathfrak{p}_2)$ s.t. $\exists\, {s^\circ}'_1$ s.t. ${s_1}^\circ \xrightarrow{\mu^\circ, r^\circ} {s^\circ}'_1 \wedge {s^\circ}'_1 \sqsubseteq_{\mathcal{MS}^\circ} {s^\circ}'_2$

i) $\sum_{{s^\circ}'_1 \sqsubseteq_{\mathcal{MS}^\circ} {s^\circ}'_2} P_1^+({s^\circ}_1, {s^\circ}'_1) \leq P_2^+({s^\circ}_2, {s^\circ}'_2)$

ii) $\sum_{{s^\circ}'_1 \sqsubseteq_{\mathcal{MS}^\circ} {s^\circ}'_2} P_1^-({s^\circ}_1, {s^\circ}'_1) \geq P_2^-({s^\circ}_2, {s^\circ}'_2)$

Let us consider only *i)*; *ii)* can be proved with similar arguments.

We have to prove that, $\forall {s^\circ}_2, {s^\circ}'_2 \in S^\circ(\mathfrak{p}_2)$,

$$P_2^+({s^\circ}_2, {s^\circ}'_2) \stackrel{?}{\geq} \sum_{\substack{{s^\circ}' \in S^\circ(\mathfrak{p}_1) \\ {s^\circ}'_1 \sqsubseteq_{\mathcal{MS}^\circ} {s^\circ}'_2}} P^+({s^\circ}_1, {s^\circ}'_1)$$

that is

$$\frac{[R^\circ({s_2}^\circ, {s^\circ}'_2)]^+}{[R^\circ({s_2}^\circ, {s^\circ}'_2)]^+ + \sum_{\substack{{s^\circ}''_2 \in S^\circ(\mathfrak{p}_2) \\ {s^\circ}''_2 \neq {s^\circ}'_2}} [R^\circ({s^\circ}_2, {s^\circ}''_2)]^-} \overset{?}{\geq} \sum_{\substack{{s^\circ}' \in S^\circ(\mathfrak{p}_1) \\ {s^\circ}'_1 \sqsubseteq_{\mathcal{MS}^\circ} {s^\circ}'_2}} \frac{[R^\circ({s_1}^\circ, {s^\circ}'_1)]^+}{[R^\circ({s_1}^\circ, {s^\circ}'_1)]^+ + \sum_{\substack{{s^\circ}''_1 \in S^\circ(\mathfrak{p}_1) \\ {s^\circ}''_1 \neq {s^\circ}'_1}} [R^\circ({s^\circ}_1, {s^\circ}''_1)]^-}$$

By hypothesis of $\alpha_{\mathcal{LTS}}(lts) \sqsubseteq_{\mathcal{LTS}^\circ} lts^\circ$, namely 2), it holds that

- $[R({s^\circ}_2, {s^\circ}'_2)]^+ \geq \max_{\substack{{s^\circ}_3 \in S^\circ(\mathfrak{p}_1) \\ {s^\circ}_3 \sqsubseteq_{\mathcal{MS}^\circ} {s^\circ}_2}} \sum_{\substack{{s^\circ}'_3 \in S^\circ(\mathfrak{p}_1) \\ {s^\circ}'_3 \sqsubseteq_{\mathcal{MS}^\circ} {s^\circ}'_2}} [R({s^\circ}_3, {s^\circ}'_3)]^+$;
- $[R({s^\circ}_2, {s^\circ}''_2)]^- \leq \min_{\substack{{s^\circ}_3 \in S^\circ(\mathfrak{p}_1) \\ {s^\circ}_3 \sqsubseteq_{\mathcal{MS}^\circ} {s^\circ}_2}} \sum_{\substack{{s^\circ}'_3 \in S^\circ(\mathfrak{p}_1) \\ {s^\circ}'_3 \sqsubseteq_{\mathcal{MS}^\circ} {s^\circ}''_2}} [R({s^\circ}_3, {s^\circ}'_3)]^-$.

Hence we have to prove that

$$\frac{\sum_{\substack{{s^\circ}'_1 \in S^\circ(\mathfrak{p}_1) \\ {s^\circ}'_1 \sqsubseteq_{\mathcal{MS}^\circ} {s^\circ}'_2}} [R({s^\circ}_1, {s^\circ}'_1)]^+ + w}{\sum_{\substack{{s^\circ}'_1 \in S^\circ(\mathfrak{p}_1) \\ {s^\circ}'_1 \sqsubseteq_{\mathcal{MS}^\circ} {s^\circ}'_2}} [R({s^\circ}_1, {s^\circ}'_1)]^+ + w + \sum_{\substack{{s^\circ}''_2 \in S^\circ(\mathfrak{p}_2) \\ {s^\circ}''_2 \neq {s^\circ}'_2}} \sum_{\substack{{s^\circ}''_1 \in S^\circ(\mathfrak{p}_1) \\ {s^\circ}''_1 \sqsubseteq_{\mathcal{MS}^\circ} {s^\circ}''_2}} [R({s^\circ}_1, {s^\circ}''_1)]^- - w'} \overset{?}{\geq} \sum_{\substack{{s^\circ}' \in S^\circ(\mathfrak{p}_1) \\ {s^\circ}'_1 \sqsubseteq_{\mathcal{MS}^\circ} {s^\circ}'_2}} \frac{[R^\circ({s_1}^\circ, {s^\circ}'_1)]^+}{[R^\circ({s_1}^\circ, {s^\circ}'_1)]^+ + \sum_{\substack{{s^\circ}''_1 \in S^\circ(\mathfrak{p}_1) \\ {s^\circ}''_1 \neq {s^\circ}'_1}} [R^\circ({s^\circ}_1, {s^\circ}''_1)]^-}$$

where

$$w = [R({s^\circ}_2, {s^\circ}'_2)]^+ - \max_{\substack{{s^\circ}_3 \in S^\circ(\mathfrak{p}_1) \\ {s^\circ}_3 \sqsubseteq_{\mathcal{MS}^\circ} {s^\circ}_2}} \sum_{\substack{{s^\circ}'_3 \in S^\circ(\mathfrak{p}_1) \\ {s^\circ}'_3 \sqsubseteq_{\mathcal{MS}^\circ} {s^\circ}'_2}} [R({s^\circ}_3, {s^\circ}'_3)]^+ ,$$

$$w' = [R({s^\circ}_2, {s^\circ}''_2)]^- - \min_{\substack{{s^\circ}_3 \in S^\circ(\mathfrak{p}_1) \\ {s^\circ}_3 \sqsubseteq_{\mathcal{MS}^\circ} {s^\circ}_2}} \sum_{\substack{{s^\circ}'_3 \in S^\circ(\mathfrak{p}_1) \\ {s^\circ}'_3 \sqsubseteq_{\mathcal{MS}^\circ} {s^\circ}''_2}} [R({s^\circ}_3, {s^\circ}'_3)]^- .$$

As rates computed by $\alpha_{\mathcal{LTS}}$ are precise, it holds that $\forall s^\circ, {s^\circ}' \in S^\circ(\mathfrak{p}_1)$: $[R^\circ(s^\circ, {s^\circ}')]^+ = [R^\circ(s^\circ, {s^\circ}')]^- = R^\circ(s^\circ, {s^\circ}')$ and hence we can write

$$\frac{\sum_{\substack{s^{\circ\prime}_1 \in S^\circ(\mathfrak{p}_1) \\ s^{\circ\prime}_1 \sqsubseteq_{\mathcal{MS}^\circ} s^{\circ\prime}_2}} R(s^\circ{}_1, s^{\circ\prime}_1) + w}{\sum_{\substack{s^{\circ\prime}_1 \in S^\circ(\mathfrak{p}_1) \\ s^{\circ\prime}_1 \sqsubseteq_{\mathcal{MS}^\circ} s^{\circ\prime}_2}} R(s^\circ{}_1, s^{\circ\prime}_1) + w + \sum_{\substack{s^{\circ\prime\prime}_2 \in S^\circ(\mathfrak{p}_2) \\ s^{\circ\prime\prime}_2 \neq s^{\circ\prime}_2}} \sum_{\substack{s^{\circ\prime\prime}_1 \in S^\circ(\mathfrak{p}_1) \\ s^{\circ\prime\prime}_1 \sqsubseteq_{\mathcal{MS}^\circ} s^{\circ\prime\prime}_2}} R(s^\circ{}_1, s^{\circ\prime\prime}_1) - w'} \overset{?}{\geq} \sum_{\substack{s^{\circ\prime} \in S^\circ(\mathfrak{p}_1) \\ s^{\circ\prime}_1 \sqsubseteq_{\mathcal{MS}^\circ} s^{\circ\prime}_2}} \frac{R^\circ(s_1{}^\circ, s^{\circ\prime}_1)}{\sum_{s^{\circ\prime\prime}_1 \in S^\circ(\mathfrak{p}_1)} R^\circ(s^\circ{}_1, s^{\circ\prime\prime}_1)}$$

and as

$$\frac{\sum_{\substack{s^{\circ\prime}_1 \in S^\circ(\mathfrak{p}_1) \\ s^{\circ\prime}_1 \sqsubseteq_{\mathcal{MS}^\circ} s^{\circ\prime}_2}} R(s^\circ{}_1, s^{\circ\prime}_1) + w}{\sum_{\substack{s^{\circ\prime}_1 \in S^\circ(\mathfrak{p}_1) \\ s^{\circ\prime}_1 \sqsubseteq_{\mathcal{MS}^\circ} s^{\circ\prime}_2}} R(s^\circ{}_1, s^{\circ\prime}_1) + w + \sum_{\substack{s^{\circ\prime\prime}_2 \in S^\circ(\mathfrak{p}_2) \\ s^{\circ\prime\prime}_2 \neq s^{\circ\prime}_2}} \sum_{\substack{s^{\circ\prime\prime}_1 \in S^\circ(\mathfrak{p}_1) \\ s^{\circ\prime\prime}_1 \sqsubseteq_{\mathcal{MS}^\circ} s^{\circ\prime\prime}_2}} R(s^\circ{}_1, s^{\circ\prime\prime}_1) - w'} \geq \frac{\sum_{\substack{s^{\circ\prime}_1 \in S^\circ(\mathfrak{p}_1) \\ s^{\circ\prime}_1 \sqsubseteq_{\mathcal{MS}^\circ} s^{\circ\prime}_2}} R(s^\circ{}_1, s^{\circ\prime}_1)}{\sum_{\substack{s^{\circ\prime}_1 \in S^\circ(\mathfrak{p}_1) \\ s^{\circ\prime}_1 \sqsubseteq_{\mathcal{MS}^\circ} s^{\circ\prime}_2}} R(s^\circ{}_1, s^{\circ\prime}_1) + \sum_{\substack{s^{\circ\prime\prime}_2 \in S^\circ(\mathfrak{p}_2) \\ s^{\circ\prime\prime}_2 \neq s^{\circ\prime}_2}} \sum_{\substack{s^{\circ\prime\prime}_1 \in S^\circ(\mathfrak{p}_1) \\ s^{\circ\prime\prime}_1 \sqsubseteq_{\mathcal{MS}^\circ} s^{\circ\prime\prime}_2}} R(s^\circ{}_1, s^{\circ\prime\prime}_1) - w'} \geq \frac{\sum_{\substack{s^{\circ\prime}_1 \in S^\circ(\mathfrak{p}_1) \\ s^{\circ\prime}_1 \sqsubseteq_{\mathcal{MS}^\circ} s^{\circ\prime}_2}} R(s^\circ{}_1, s^{\circ\prime}_1)}{\sum_{\substack{s^{\circ\prime}_1 \in S^\circ(\mathfrak{p}_1) \\ s^{\circ\prime}_1 \sqsubseteq_{\mathcal{MS}^\circ} s^{\circ\prime}_2}} R(s^\circ{}_1, s^{\circ\prime}_1) + \sum_{\substack{s^{\circ\prime\prime}_2 \in S^\circ(\mathfrak{p}_2) \\ s^{\circ\prime\prime}_2 \neq s^{\circ\prime}_2}} \sum_{\substack{s^{\circ\prime\prime}_1 \in S^\circ(\mathfrak{p}_1) \\ s^{\circ\prime\prime}_1 \sqsubseteq_{\mathcal{MS}^\circ} s^{\circ\prime\prime}_2}} R(s^\circ{}_1, s^{\circ\prime\prime}_1)}$$

we can reduce our proof to

$$\frac{\sum_{\substack{s^{\circ\prime}_1 \in S^\circ(\mathfrak{p}_1) \\ s^{\circ\prime}_1 \sqsubseteq_{\mathcal{MS}^\circ} s^{\circ\prime}_2}} R(s^\circ{}_1, s^{\circ\prime}_1)}{\sum_{\substack{s^{\circ\prime}_1 \in S^\circ(\mathfrak{p}_1) \\ s^{\circ\prime}_1 \sqsubseteq_{\mathcal{MS}^\circ} s^{\circ\prime}_2}} R(s^\circ{}_1, s^{\circ\prime}_1) + \sum_{\substack{s^{\circ\prime\prime}_2 \in S^\circ(\mathfrak{p}_2) \\ s^{\circ\prime\prime}_2 \neq s^{\circ\prime}_2}} \sum_{\substack{s^{\circ\prime\prime}_1 \in S^\circ(\mathfrak{p}_1) \\ s^{\circ\prime\prime}_1 \sqsubseteq_{\mathcal{MS}^\circ} s^{\circ\prime\prime}_2}} R(s^\circ{}_1, s^{\circ\prime\prime}_1)} \overset{?}{\geq} \sum_{\substack{s^{\circ\prime} \in S^\circ(\mathfrak{p}_1) \\ s^{\circ\prime}_1 \sqsubseteq_{\mathcal{MS}^\circ} s^{\circ\prime}_2}} \frac{R^\circ(s_1{}^\circ, s^{\circ\prime}_1)}{\sum_{s^{\circ\prime\prime}_1 \in S^\circ(\mathfrak{p}_1)} R^\circ(s^\circ{}_1, s^{\circ\prime\prime}_1)}$$

that is

$$\sum_{\substack{s^{\circ\prime}_1 \in S^\circ(\mathfrak{p}_1)\\ s^{\circ\prime}_1 \sqsubseteq_{\mathcal{MS}^\circ} s^{\circ\prime}_2}} \frac{R(s^\circ{}_1, s^{\circ\prime}_1)}{\sum_{\substack{s^{\circ\prime}_1 \in S^\circ(\mathfrak{p}_1)\\ s^{\circ\prime}_1 \sqsubseteq_{\mathcal{MS}^\circ} s^{\circ\prime}_2}} R(s^\circ{}_1, s^{\circ\prime}_1) + \sum_{\substack{s^{\circ}_1 \in S^\circ(\mathfrak{p}_1)\\ s^{\circ\prime}_1 \not\sqsubseteq_{\mathcal{MS}^\circ} s^{\circ\prime}_2}} R(s^\circ{}_1, s^{\circ\prime\prime}_1)} \overset{?}{\geq}$$

$$\sum_{\substack{s^{\circ\prime} \in S^\circ(\mathfrak{p}_1)\\ s^{\circ\prime}_1 \sqsubseteq_{\mathcal{MS}^\circ} s^{\circ\prime}_2}} \frac{R^\circ(s_1{}^\circ, s^{\circ\prime}_1)}{\sum_{s^{\circ\prime\prime}_1 \in S^\circ(\mathfrak{p}_1)} R^\circ(s^\circ{}_1, s^{\circ\prime\prime}_1)}$$

that is true by =.

□

Proof of Lemma 5.4.4.

Let $M = (\Sigma, s_0, \mathcal{R})$ and hence $LTS(M) = (S, s_0, \rightarrow)$, $\mathcal{H}(LTS(M)) = (S, s_0, P)$ and $\alpha_{\mathcal{MC}}(\mathcal{H}(LTS(M))) = (S^\circ(\mathfrak{p}^\bullet), \alpha_{\mathcal{MS}}(\mathfrak{p}^\bullet)(s_0), \widehat{P}, \widehat{P})$ and $\widehat{P} = P$.

On the other side $\alpha_{\mathcal{LTS}}(LTS(M)) = (S^\circ(\mathfrak{p}^\bullet), \alpha_{\mathcal{MS}}(\mathfrak{p}^\bullet)(s_0), \rightarrow^\alpha_\circ)$ where $\rightarrow^\alpha_\circ = \{ s^\circ \xrightarrow{\mu^*, r^*} s'^\circ \mid s \xrightarrow{\mu, r} s' \in \rightarrow \ \wedge \ s \in \gamma_{\mathcal{MS}}(s^\circ) \ \wedge \ s' \in \gamma_{\mathcal{MS}}(s'^\circ) \}$ where

$$(\mu^*, r^*) = (\bigcup^{\mathcal{MS}^\circ} \mu^\bullet, \sum^{\mathbb{I}} r^\bullet) \text{ and } s \xrightarrow{\mu, r} s' \in \rightarrow \ \wedge s \in \gamma_{\mathcal{MS}}(s^\circ) \wedge s' \in \gamma_{\mathcal{MS}}(s'^\circ).$$

Hence,

$$\mathcal{H}^\circ(\alpha_{\mathcal{LTS}}(LTS(M))) = \mathcal{H}^\circ(S^\circ(\mathfrak{p}^\bullet), \alpha_{\mathcal{MS}}(\mathfrak{p}^\bullet)(s_0), \rightarrow^\alpha_\circ) = (S^\circ(\mathfrak{p}^\bullet), \alpha_{\mathcal{MS}}(\mathfrak{p}^\bullet)(s_0), P^-, P^+)$$

where $P^- = P^+$ as they are computed by $\mathcal{H}^\circ$ using precise transition rates.

$$P^-(s^\circ, s^{\circ\prime}) = P^+(s^\circ, s^{\circ\prime}) \text{ by def. of } \mathcal{H}^\circ \text{ and by Lemma 5.3.9}$$

$$= \frac{[R^\circ(s^\circ, s^{\circ\prime})]^+}{[R^\circ(s^\circ, s^{\circ\prime})]^+ + \sum_{\substack{s^{\circ\prime\prime} \in S^\circ(\mathfrak{p}^\bullet)\\ s^{\circ\prime\prime} \neq s^{\circ\prime}}} [R^\circ(s^\circ, s^{\circ\prime\prime})]^-}$$

$$= \frac{[r^*]^+ \mid s^\circ \xrightarrow{r^*, \mu^\circ} s^{\circ\prime} \in \rightarrow^\alpha_\circ}{[r^*]^+ \mid s^\circ \xrightarrow{r^*, \mu^\circ} s^{\circ\prime} \in \rightarrow^\alpha_\circ + \sum_{\substack{s^{\circ\prime\prime} \in S^\circ(\mathfrak{p}^\bullet)\\ s^{\circ\prime\prime} \neq s^{\circ\prime}}} [r^*]^- \mid s^\circ \xrightarrow{r^*, \mu^\circ} s^{\circ\prime\prime} \in \rightarrow^\alpha_\circ}$$

$$= \frac{\left[\sum^{\mathbb{I}}_{\substack{s \xrightarrow{r,\mu} s' \in \rightarrow \\ s \in \gamma_{\mathcal{MS}}(s^\circ),\, s' \in \gamma_{\mathcal{MS}}(s^{\circ\prime})}} r^\bullet\right]^+}{\left[\sum^{\mathbb{I}}_{\substack{s \xrightarrow{r,\mu} s' \in \rightarrow \\ s \in \gamma_{\mathcal{MS}}(s^\circ),\, s' \in \gamma_{\mathcal{MS}}(s^{\circ\prime})}} r^\bullet\right]^+ + \sum_{\substack{s^{\circ\prime\prime} \in S^\circ(\mathfrak{p}^\bullet) \\ s^{\circ\prime\prime} \neq s^{\circ\prime}}} \left[\sum^{\mathbb{I}}_{\substack{s \xrightarrow{r,\mu} s'' \in \rightarrow, \\ s \in \gamma_{\mathcal{MS}}(s^\circ),\, s'' \in \gamma_{\mathcal{MS}}(s^{\circ\prime\prime}) \\ s'' \in S,\, s'' \neq s'}} r^\bullet\right]^-}$$

$$= \frac{\sum_{\substack{s \xrightarrow{r,\mu} s' \in \rightarrow \\ s \in \gamma_{\mathcal{MS}}(s^\circ),\, s' \in \gamma_{\mathcal{MS}}(s^{\circ\prime})}} r}{\sum_{\substack{s \xrightarrow{r,\mu} s' \in \rightarrow \\ s \in \gamma_{\mathcal{MS}}(s^\circ),\, s' \in \gamma_{\mathcal{MS}}(s^{\circ\prime})}} r + \sum_{\substack{s^{\circ\prime\prime} \in S^\circ(\mathfrak{p}^\bullet) \\ s^{\circ\prime\prime} \neq s^{\circ\prime}}} \sum_{\substack{s \xrightarrow{r,\mu} s'' \in \rightarrow, \\ s \in \gamma_{\mathcal{MS}}(s^\circ),\, s'' \in \gamma_{\mathcal{MS}}(s^{\circ\prime\prime}) \\ s'' \in S,\, s'' \neq s'}} r}$$

and, as $\forall s \in S^\circ(\mathfrak{p}^\bullet)\,,\ \exists!\, s \in S \mid s \in \gamma_{\mathcal{MS}}(s^\circ)$,

$$= \quad \frac{R(s,s')}{R(s,s') + \sum_{\substack{s'' \in S \\ s'' \neq s'}} R(s,s'')} \quad = \quad P(s,s') \quad = \quad \widehat{P}(s^\circ, s^{\circ\prime})$$

□

Chapter 6

Conclusions

In this thesis, we have faced problems related to the use of MSR in the context of biological systems formal modelling and analysis. Namely, we have investigated the use of abstract interpretation techniques over the probabilistic semantics of MSR, both to deal with uncertainty of kinetic parameters, in the case of interleaving semantics, and to reduce the number of states and transitions, in the case of a maximally parallel probabilistic semantics.

In particular, we have presented an abstract probabilistic semantics able to represent the dynamics of systems of biochemical reactions, when kinetic rates of reactions are uncertain (i.e. expressed by intervals of values). This approach allows the semantics of an infinite set of systems to be safely and effectively managed in a finite way. We proved that probabilistic reachability results are, not only conservative but, exactly the most precise values which are correct. Indeed, they corresponds to the minimum and the maximum of values of probabilistic reachability corresponding to each concrete system represented by on abstract one. In particular, while a DTMC semantics is associated to models where reaction rates are expressed by precise values, an IMC semantics is associated to models where reaction rates are expressed by intervals. Such a semantics is computed via the construction of an LTS semantics and reports lower and upper bounds on transition probabilities. Over such abstract probabilistic semantics it is possible to perform probabilistic model checking obtaining conservative bounds on probability of reachability properties.

Moreover we have defined a probabilistic semantics for maximally parallel MSR. On such a semantics as many interactions as possible are executed on a single evolution step, resulting in a synchronous behavior, typical of certain types of biological systems (e.g. seasonal animals or cells populations). Indeed, for such kind of systems, a maximally parallel semantics is more

suitable than the interleaving one, that allows part of the system to evolve indefinitely while other system components stall and thus considering not realizable configurations. For these reasons we defined a probabilistic semantics tailored to describe the behavior of systems evolving in a maximally parallel way, where transitions have an associated probability depending on the system state and on the propensity of maximally parallel rewriting events.

As the maximally parallel semantics presents the drawback of having a number of transitions exiting from a state growing with respect to the number of individuals in the state, over this kind of semantics we developed an interval based predicate abstraction. Such an abstraction is able to drastically reduce the number of states and transitions in the semantics associated to a system, and to finitely represents the behavior of possibly infinite maximally parallel rewriting systems. Since the abstraction is parametric on a set of predicates, the abstract probabilistic model can be refined until a right compromise between dimension and precision is reached. We proved that probabilities bounds are conservative with respect to the concrete ones, and that soundness results are lifted to probabilistic reachability.

Also the proposed maximally parallel semantics are computed by the construction of appropriate LTSs. Subsequently, from such structures are derived the corresponding probabilistic structures, given in terms of DTMC or IMC in the concrete or abstract case respectively. Abstract semantics are proved to be sound approximations by means of abstract interpretation techniques, via the definition of suitable approximation orders.

The application of the different proposed approaches is shown by different case studies. The abstraction for uncertain kinetic rates has been tested on model of tumor cells growth. On such model interaction rates are described by intervals, has been studied, and different outcomes have been obtained by using different intervals of rates. The maximally parallel semantics has been tested on a model of *C. Elegans* vulval development, from evolutionary biology. Such a model have been simulated with maximally parallel semantics, and *in vivo* experiments results have been reproduced. Finally, the efficacy of the abstract maximally parallel probabilistic semantics, in terms of reduction of number of states and transitions has been shown by an example of probabilistic reachability analysis on a simple model of seasonal animal reproduction.

Outlook. This work could be continued in many directions.

The analysis of biochemical systems of reactions with uncertainty rates can be extended to include continuous-time information. In particular, the approach

proposed by Katoen et al. [KKLW07a] can be used: from transition rates of abstract LTS defined in Chapter 3 a uniform CTMC [BKHW05] can be derived. The verification of CSL properties, allowing to verify time-bounded reachability properties, is then straightforward.

The abstraction of the maximally parallel semantics for MSR can be improved in terms of precision. As we briefly discussed in Chapter 5, some transition rate computation functions could be refined, exploiting more information, in order to introduce less approximation while remaining sound with respect to concrete semantics. Moreover soundness results with respect to probabilistic reachability could be generalized for any language and abstract semantics able to give concrete and abstract LTSs in a relation similar to the one presented here.

Finally both the abstract semantics for reactions with uncertain kinetics, and the maximally parallel probabilistic semantics, here proposed for MSR, can be exploited to define corresponding semantics for more complex and expressive formalisms with a rewriting semantics (e.g. P Systems, the Calculus of Looping Sequences).

Bibliography

[AC03] I. I. Ardelean and M. Cavaliere, *Modelling biological processes by using a probabilistic p system software*, Natural Computing, vol. 2, no. 2, pp. 173–197, Kluwer Academic Publishers, 2003.

[AMS] *The AMSR2PRISM web page,* `http://www.di.unipi.it/msvbio/wiki/amsr2prism`.

[APP+04] M. Antoniotti, C. Piazza, A. Policriti, M. Simeoni and B. Mishra, *Taming the complexity of biochemical models through bisimulation and collapsing: theory and practice*, Theoretical Compututer Science, vol. 325, no. 1, pp. 45–67, Elsevier Science Publishers Ltd., 2004.

[ASB95] A. Aziz, V. Singhal and F. Balarin, *It usually works: The temporal logic of stochastic systems*, In: CAV-95, Lecture Notes in Computer Science, vol. 939, pp. 155–165, Springer-Verlag, 1995.

[ASSB96] A. Aziz, K. Sanwal, V. Singhal and R. Brayton, *Verifying continuous time markov chains*, In: CAV'96, Lecture Notes in Computer Science, vol. 1102, pp. 269–276, Springer-Verlag, 1996.

[AV08] A. Alhazoc and S. Verlan, *Minimization strategies for maximal parallel multiset rewriting systems*, Tech. report, Turku Centre for Computer Science (TUCS), 2008.

[BC89] G. Balbo and G. Chiola, *Stochastic petri net simulation*, In: WSC'89, pp. 266–276, ACM Press, 1989.

[BCPM08] D. Besozzi, P. Cazzaniga, D. Pescini and G. Mauri, *Modelling metapopulations with stochastic membrane systems*, Biosystems, vol. 91, no 3, pp. 499–514, Elsevier Science Publishers Ltd., 2008.

[BCHG+97] C. Baier, E. Clarke, V. Hartonas-Garmhausen, M. Kwiatkowska and M. Ryan, *Symbolic model checking for probabilistic processes*, In: ICALP'97, Lecture Notes in Computer Science, vol. 1256, pp. 430–440, Springer-Verlag, 1997.

[BCL+03] S. Bistarelli, I. Cervesato, G. Lenzini, R. Marangoni and F. Martinelli, *On representing biological systems through multiset rewriting*, In: EUROCAST'03, Lecture Notes in Computer Science, vol. 2809, pp. 415–426, 2003.

[BCMS+08] R. Barbuti, G. Caravagna, A. Maggiolo-Schettini, P. Milazzo and G. Pardini, *The calculus of looping sequences*, In: FMCSB'08, Lecture Notes in Computer Science, vol. 5016, pp. 387–423, Springer-Verlag, 2008.

[BMMG10] R. Barbuti, A. Maggiolo-Schettini, P. Milazzo, and D. P. Gruska, *A Notion of Biological Diagnosability Inspired by the Notion of Opacity in Systems Security*, Fundamenta Informaticae, vol. 102, no. 1, pp. 19–34, 2010.

[BdA95] A. Bianco and L. de Alfaro, *Model checking of probabilistic and nondeterministic systems*, In: FSTTCS'95, Lencture Notes in Computer Science, vol. 1026, pp. 499–513, Springer Berlin / Heidelberg, 1995.

[BGC09] C. Baier, M. Groesser and F. Ciesinski, *Quantitative analysis under fairness constraints*, In: ATVA '09, Lecture Notes in Computer Science, vol. 5799 pp. 135–150, Springer Berlin / Heidelberg, 2009.

[BHHK03] C. Baier, B. R. Haverkort, H. Hermanns and J. P. Katoen, *Model-checking algorithms for continuous-time markov chains*, IEEE Transactions on Software Engineering, vol. 29, pp. 524–541, IEEE Computer Society Press, 2003.

[BK98] C. Baier and M. Kwiatkowska, *Model checking for a probabilistic branching time logic with fairness*, Distributed Computing, vol. 11, no. 3, pp. 125–155, 1998.

[BK08] C. Baier and J. Katoen, *Principles of model checking*, The MIT Press, 2008.

[BKF+09] N. Bonzanni, E. Krepska, K. A. Feenstra, W. Fokkink, T. Kielmann, H.E. Bal and J. Heringa, *Executing multicellular differentiation: quantitative predictive modelling of* C.elegans vulval development, Bioinformatics, vol. 25 (16), pp. 2049-2056, Oxford University Press, 2009.

[BKHW05] C. Baier, J. P. Katoen, H. Hermanns and V. Wolf, *Comparative branching-time semantics for markov chains*, Information and Computation, vol. 200, no.2, pp. 149–214, Academic Press Inc., 2005.

[BLMS09] R. Barbuti, F. Levi, P. Milazzo and G. Scatena, *Probabilistic model checking of biological systems with uncertain kinetic rates*, In: RP'09, Lecture Notes in Computer Science, vol. 5797, pp. 64–78, Springer-Verlag, 2009.

[BLMS10] ———, *Maximally parallel probabilistic semantics for multiset rewriting.*, In: CS&P'10, Informatik-Bericht, vol. 237, pp. 25–36, Humboldt-Universitat zu Berlin Informatik-Berichte, 2010.

[BLO98] S. Bensalem, Y. Lakhnech and S. Owre, *Computing Abstractions of Infinite State Systems Compositionally and Automatically*, In: CAV'98, Lecture Notes in Computer Science, vol. 1427, pp. 319–331, Springer-Verlag, 1998.

[BMM08] P. Ballarini, I. Mura and R. Mardare, *Query-based verification of biochemical oscillations through probabilistic model checking*, Tech. report, COSBI: Center for Computational and Systems Biology - The Microsoft Research - University of Trento, Italy, 2008.

[BMSMT08] R. Barbuti, A. Maggiolo-Schettini, P. Milazzo and A. Troina, *Bisimulations in calculi modelling membranes*, Formal Aspects of Computing, vol. 20, no.4–5 pp. 351–377, Springer-Verlag, 2008.

[BRCG+05] F. Bernardini, F.J. Romero-Campero, M. Gheorghe, M.J. Perez-Jimenez, M. Margenstern, S. Verlan and N. Krasnogor, *On p systems with bounded parallelism*, In: SYNASC '05, p. 399, IEEE Computer Society Press, 2005.

[Bur80] H.D. Burkhard, *On priorities of parallelism*, In: LPTA'80, pp. 86–97, Springer-Verlag, 1980.

[Car05] L. Cardelli, *Brane calculi*, In: CMSB'04, Lecture Notes in Computer Science, vol. 3082, pp. 257–280, Springer-Verlag, 2005.

[CA06] M. Cavaliere and I. I. Ardelean, *Modeling Respiration in Bacteria and Respiration/Photosynthesis Interaction in Cyanobacteria Using a P System Simulator*, Applications of Membrane Computing, part 2, pp. 129–159, Springer, 2006.

[CC77] P. Cousot and R. Cousot, *Abstract interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints*, In: SIGPLAN'77, pp. 238–252, ACM Press, 1977.

[CC79] _____, *Systematic design of program analysis frameworks*, In: SIGPLAN'79, pp. 269–282, ACM Press, New York, NY, 1979.

[CC07] G. Ciobanu and L. Cornacel, *Probabilistic transitions for P systems*, Progress in Natural Science, vol. 17, pp. 431–441, Elsevier, 2007.

[CDL+99] I. Cervesato, N.A. Durgin, P .D. Lincoln, J.C. Mitchell and A. Scedrov, *A meta-notation for protocol analysis*, In: CSFW '99, pp. 55–69, IEEE Computer Society Press, 1999.

[CE81] E.M. Clarke and E. A. Emerson, *Design and synthesis of synchronization skeletons using branching time temporal logic*, In: LP'81, Lecture Notes In Computer Science, vol. 131, pp. 52–71, Springer-Verlag, 1981.

[CGL94] E.M. Clarke, O. Grumberg and D. E. Long, *Model checking and abstraction*, ACM Transactions on Programramming Langanguges and Systems, vol. 16, pp. 1512–1542, ACM Press, 1994.

[CGL09] A. Coletta, R. Gori and F. Levi, *Approximating probabilistic behaviors of biological systems using abstract interpretation*, Electronic Notes in Theoretical Computer Science, vol. 229, pp. 165–182, Elsevier Science Publishers Ltd., 2009.

[CLP04] Y. Cao, H. Li, and L. Petzold, *Efficient formulation of the stochastic simulation algorithm for chemically reacting systems*, Journal of Chemical Physics, vol. 121, pp. 4059–4067, 2004.

[CLS] *The CLSm web page:* `http://www.di.unipi.it/msvbio/wiki/sclsm`.

[CPPJ06] G. Ciobanu, G. Păun, and M. J. Pérez-Jiménez, *On the branching complexity of p systems*, Fundamenta Informaticae, vol. 73, no. 1-2, pp. 27–36, 2006.

[CS06] M. Cavaliere and S. Sedwards, *Modeling and simulating biological processes with stochastic multiset rewriting*, Dagstuhl Seminar Proceedings, Internationales Begegnungs- und Forschungszentrum für Informatik (IBFI), Schloss Dagstuhl, Germany, 2006.

[CY95] C. Courcoubetis and M. Yannakakis, *The complexity of probabilistic verification*, Journal of the ACM, vol. 42, pp. 857–907, ACM Press, 1995.

[CZ08] L. Cardelli and G. Zavattaro, *On the computational power of biochemistry*, In: AB'08, Lecture Notes in Computer Science, vol. 5147, pp. 65–80, Springer-Verlag, 2008.

[CK01] A. Chutinan and B. H. Krogh, *Verification of infinite-state dynamic systems using approximate quotient transition systems*, IEEE Trans. on Automatic Control, vol. 26, no. 9, pp. 1401–1410, IEEE Computer Society, 2001.

[dA99a] L. de Alfaro, *Computing minimum and maximum reachability times in probabilistic systems*, CONCUR '99, pp. 66–81, Springer-Verlag, 1999.

[dA99b] L. de Alfaro, *From fairness to chance*, In: PROBMIV'98, Electronic Notes in Theoretical Computer Science, vol. 22, pp. 55–87, Elsevier Science Publishers Ltd., 1999.

[dAKN+00] L. de Alfaro, M. Kwiatkowska, G. Norman, D. Parker and R. Segala, *Symbolic model checking of probabilistic processes using MTBDDs and the Kronecker representation*, In: TACAS'00, Lecture Notes in Computer Science, vol. 1785, pp. 395–410, Springer-Verlag, 2000.

[Das03] S. Das, *Predicate abstraction*, Ph.D. Thesis, Stanford University, USA, 2003.

[DFF+08] V. Danos, J. Feret, W. Fontana, R. Harmer and J. Krivine, *Rule-based modelling, symmetries, refinements.*, In: FMSB'08, Lecture Notes in Computer Science, vol. 5054, pp. 103–122, Springer-Verlag, 2008.

[DFFK08] V. Danos, J. Feret, W. Fontana and J. Krivine, *Abstract interpretation of cellular signalling networks*, In: VMCAI'08, Lecture Notes in Computer Science, vol. 4905, pp. 83–97, Springer-Verlag, 2008.

[DGG97] D. Dams, R. Gerth and O. Grumberg, *Abstract interpretation of reactive systems*, In: TOPLAS'97, ACM Transactions on Programogramming Languages and Systems, vol. 19, no. 2, pp. 253–291, ACM Press, 1997.

[DJJL01] P. D'Argenio, B. Jeannet, H. Jensen and K. Larsen, *Reachability analysis of probabilistic systems by successive refinements*, In: PAPM-PROBMIV '01, pp. 39–56, Springer-Verlag, 2001.

[DL04] V. Danos and C. Laneve, *Formal molecular biology*, Theoretical Computer Science, vol. 325, no. 1, pp. 69–110, 2004.

[DMP07] A. Donaldson, A. Miller and D. Parker, *GRIP: Generic representatives in PRISM*, In: QEST'07, pp. 115–116, IEEE Computer Society, 2007.

[DPW00] A. Di Pierro and H. Wiklicky, *Concurrent constraint programming: towards probabilistic abstract interpretation.*, In: PPDP'00. pp. 127-138. ACM, 2000.

[Eme90] E.A. Emerson, *Temporal and modal logic*, Handbook of Theoretical Computer Science, pp. 995–1072, Elsevier and MIT Press, 1990.

[FHMP07] J. Fisher, T. A. Henzinger, M. Mateescu and N. Piterman, *Bounded Asynchrony: A Biologically Inspired Notion of Concurrency*, Tech. report, EPFL, 2007.

[FHMP08] _____, *Bounded Asynchrony: Concurrency for Modeling Cell-Cell Interactions*, In: FMSB'08, Lecture Notes Computer Science, vol. 5054, pp. 17–32, Springer-Verlag, 2008.

[FLW06] H. Fecher, M. Leucker and V. Wolf, Don't Know *in probabilistic systems.*, Lecture Notes in Computer Science, vol. 3925, pp. 71–88, Springer-Verlag / Heidelberg, 2006.

[FPH+05] J. Fisher, N. Piterman, E. J. A. Hubbard, M. J. Stern and D. Harel, *Computational insights into* Caenorhabditis elegans vulval development, Proceedings of the National Academy of Sciences, vol. 102, no. 6, pp. 1951–1956, 2005.

[FPHH07] J. Fisher, N. Piterman, A. Hajnal and T. A. Henzinger, *Predictive modeling of signaling crosstalk during* C. elegans vulval development., PLoS Computational Biology vol. 3(5): e92, 2007.

[FS08] F. Fages and S. Soliman, *Abstract interpretation and types for systems biology*, Theoretical Compututer Science, vol. 403, pp. 52–70 Elsevier Science Publishers Ltd., 2008.

[FS08a] F. Fages and S. Soliman, *Formal Cell Biology in Biocham*, In: FMCSB'08, Lecture Notes in Computer Science, vol. 5016, pp. 54–80, Springer-Verlag, 2008.

[GB00] M. A. Gibson and J. Bruck, *Efficient Exact Stochastic Simulation of Chemical Systems with Many Species and Many Channels*, The Journal of Physical Chemistry A, vol. 104, pp. 1876–1889, ACS Publications, 2000.

[GH09] V. Galpin and J. Hillston, *Equivalence and discretisation in bio-pepa*, In: CMSB'09, Lecture Notes in Computer Science, vol. 5688, pp. 189–204, Springer-Verlag, 2009.

[GHL07] D. Gilbert, M. Heiner and S. Lehrack, *A unifying framework for modelling and analysing biochemical pathways using petri nets*,

In: CMSB'07, Lecture Notes in Computer Science, vol. 4695, pp. 200–216, Springer-Verlag, 2007.

[Gil77] D. Gillespie, *Exact stochastic simulation of coupled chemical reactions*, Journal of Physical Chemistry, vol. 81 (25), pp. 2340–2361, ACS Publications, 1977.

[Gil07] ———, *Stochastic simulation of chemical kinetics*, Annual Review of Physical Chemistry, vol. 58, Annual Review, 2007.

[GL09] R. Gori and F. Levi, *Abstract interpretation for probabilistic termination of biological systems*, In: MeCBIC'09, Electronic Proceedings in Theoretical Computer Science, vol. 11, pp. 137–153, 2009.

[GNPJRN07] M. A. Gutiérrez-Naranjo, M. J. Pérez-Jiménez and A. Riscos-Núñez, *On the degree of parallelism in membrane systems*, Theoretical Computer Science, vol. 372, pp. 183–195, Elsevier Science Publishers Ltd., 2007.

[GS97] S. Graf and H. Saidi, *Construction of abstract state graphs with pvs*, In: CAV'97, Lecture Notes in Computer Science, vol. 1254, pp. 72–83, Springer-Verlag, 1997.

[GW] *Gillespie's work on SSA:* `http://www.citeulike.org/tag/gillespie`.

[HGD08] H. Heiner, D. Gilbert and R. Donaldson, *Petri nets for systems and synthetic biology*, In: FMCSB'08, Lecture Notes in Computer Science, vol. 5016, pp. 215–264, Springer-Verlag, 2008.

[HHWZ09] E. M. Hahn, H. Hermanns, B. Wachter and L. Zhang, *Time-Bounded Model Checking of Infinite-State Continuous-Time Markov Chains*, Fundamenta Informaticae, vol. 95, no. 1, pp. 129–155, 2009.

[HHWZ10] E. M. Hahn, H. Hermanns, B. Wachter and L. Zhang, *PASS: Abstraction refinement for infinite probabilistic models*, Lecture Notes in Computer Science, vol. 6015, pp. 353–357, Springer-Verlag, 2010.

[Hil10] A. V. Hill, *The possible effects of the aggregation of the molecules of hemoglobin on its dissociation curves*, Journal of Physiology, vol. 40, pp. iv–vii, The Physiological Society, 1910.

[HJ94] H. Hansson and B. Jonsson, *A logic for reasoning about time and reliability*, Formal Aspects of Computing, vol. 6, pp. 102–111, Springer-Verlag, 1994.

[HP09] S. Haddad and N. Pekergin, *Using stochastic comparison for efficient model checking of uncertain markov chains*, In: QEST'09, pp. 177–186, IEEE Computer Society, 2009.

[Hut05] M. Huth, *On finite-state approximants for probabilistic computation tree logic*, Theoretical Computer Science, vol. 346, pp. 113–134, Elsevier Science Publishers Ltd., 2005.

[HWZ08] H. Hermanns, B. Wachter and L. Zhang, *Probabilistic CEGAR*, In: CAV'08, Lecture Notes in Computer Science, vol. 5123, pp. 162–175, Springer-Verlag, 2008.

[IM07] M. S. Iyengar and M. F. MCGuire, *Imprecise and Qualitative Probability in Systems Biology* , In: Proceedings of ICSB, 2007.

[JL91] B. Jonsson and K.G. Larsen, *Specification and refinement of probabilistic processes*, In: IEEE Symposium on Logic in Computer Science, pp. 266–277, IEEE Computer Society, 1991.

[Kea96] R.B. Kearfott, *Interval computations: Introduction, uses, and resources*, Euromath Bulletin, vol. 1, no. 2, pp. 95–112, 1996.

[KH09] M. Kattenbelt and M. Huth, *Abstraction Framework for Markov Decision Processes and PCTL via games*, Tech. Report RR-09-01, Oxford University Computing Laboratory, 2009.

[Kin94] E. Kindler, *Safety and liveness properties: A survey.*, EATCS Bulletin, vol. 53, pp. 268–272, European Association for Theoretical Computer Science, 1994.

[Kit02] H. Kitano, *Computational systems biology*, Nature, vol. 420, pp. 206–210, Nature Publishing Group, 2002.

[KKLW07a] J. Katoen, D. Klink, M. Leucker and V. Wolf, *Three-valued abstraction for continuous-time markov chains*, In: CAV'07, Lecture Notes in Computer Science, vol. 4590, pp. 311–324, Springer-Verlag, 2007.

[KKLW07b] ———, *Three-valued abstraction for probabilistic systems*, Tech. Report AIB-2007-20, RWTH Aachen, 2007.

[KKNP08] M. Kattenbelt, M. Kwiatkowska, G. Norman and D. Parker, *Game-based probabilistic predicate abstraction in PRISM*, In: QAPL'08, Electronic Notes in Theoretical Computer Science, vol. 220, no. 3, pp. 5–21, Elsevier Science Publishers Ltd., 2008.

[Kli10] D. Klink, *Three-valued abstraction for stochastic systems*, Ph.D. thesis, RWTH Aachen University, Germany, 2010.

[KNP02] M.Z. Kwiatkowska, G. Norman, and D. Parker, *PRISM: Probabilistic symbolic model checker.*, In: TOOLS'02, Lecture Notes in Computer Science, vol. 2324, pp. 200–204, Springer-Verlag, 2002.

[KNP06] M. Kwiatkowska, G. Norman, and D. Parker, *Symmetry reduction for probabilistic model checking*, In: CAV'06, Lecture Notes in Computer Science, vol. 4114, pp. 234–248, Springer-Verlag, 2006.

[KRHK10] D. Klink, A. K. I. Remke, B. R. Haverkort and J. P. Katoen, *Time-bounded reachability in tree-structured qbds by abstraction*, Performance Evaluation, vol. 68, pp. 105–125, Elsevier Science Publishers Ltd., 2010.

[KU02] I.O. Kozine and L.V. Utkin, *Interval-valued finite markov chains*, Reliable Computing, vol. 8, pp. 97–113(17), Springer-Verlag, 2002.

[Kwi03] M. Kwiatkowska, *Model checking for probability and time: from theory to practice*, In: LICS'03, p. 351–360, IEEE Computer Society, 2003.

[Lam77] L. Lamport, *Proving the correctness of multiprocess programs*, IEEE Transactions on Software Engineering, vol. 3, pp. 125–143, IEEE Computer Society Press, 1977.

[LNUM09] C. Li, M. Nagasaki, K. Ueno and S. Miyano, *Simulation-based model checking approach to cell fate specification during* Caenorhabditis elegans vulval development by hybrid functional petri net with extension, BMC Systems Biology, vol. 3, pp. 42–77, Springer-Verlag, 2009.

[MA99] H.H. McAdams and A. Arkin, *It's a noisy business! genetic regulation at the nanomolar scale*, Trends in Genetics, vol. 15, pp. 65–69, Elsevier Science Publishers Ltd., 1999.

[Mad03] M. Madhu, *Probabilistic rewriting P Systems*, International Journal of Foundations of Computer Science, vol. 14, pp. 157–166, World Scientific Publishing Company, 2003.

[MHS90] M. G. Morgan, M. Henrion and M. Small, *Uncertainty: A guide to dealing with uncertainty in quantitative risk and policy analysis*, Cambridge University Press, 1990.

[Mil99] R. Milner, *Communicating and mobile systems: the pi-calculus*, Cambridge University Press, 1999.

[Mil07] P. Milazzo, *Qualitative and quantitative formal modeling of biological systems*, Ph.D. thesis, University of Pisa, Italy, 2007.

[MM13] L. Michaelis and M. Menten, *Kinetik der invertinwirkung*, Biochem. Z, vol. 49, pp. 333–369., 1913.

[Mon05] D. Monniaux, *Abstract interpretation of programs as Markov decision processes*, In: SAS'03, vol. 58, pp. 179–205, Springer-Verlag, 2005.

[MP08] M. B. Mamoun and N. Pekergin, *Model Checking of Infinite State Space Markov Chains by Stochastic Bounds*, In: ASMTA'08, Lecture Notes in Computer Science, vol. 5055, pp. 264–278, Springer-Verlag, 2008.

[MPPRS11] M. A. Martínez-del-Amor, I. Pérez-Hurtado, M. J. Pérez-Jiménez, A. Riscos-Núñez and F. Sancho-Caparrini, *A Simulation Algorithm for Multienvironment Probabilistic P Systems: a Formal Verification*, International Journal of Foundations of Computer Science, vol. 22(1), pp. 107–118, World Scientific Publishing, 2011.

[MPV] V. A. Muganthan, A. Phillips, and M. G. Vigliotti, *Bam: Bioambient machine.*, In: ACDS'08, IEEE Computer Society, 2008.

[Obt02] A. Obtulowicz, *Probabilistic P Systems*, In: WMC-CdeA'02, Lecture Notes in Computer Science, vol. 2597, pp. 377/387, Springer-Verlag, 2003.

[OP03] A. Obtulowicz and G. Păun, *(In search of) Probabilistic P systems*, Biosystems, vol. 70, pp. 107–121, Elsevier Science Publishers Ltd., 2003.

[Pău02] G. Păun, *Membrane computing. An introduction*, Natural Computing Series, Springer-Verlag, 2002.

[Pau04] J. Paulsson, *Summing up the noise in gene networks*, Nature, vol. 427, Nature Publishing Group, 2004.

[PBMZ06] D. Pescini, D. Besozzi, G. Mauri and C. Zandron, *Dynamical probabilistic P systems*, International Journal of Foundations of Computer Science, vol. 17, pp. 183–204, World Scientific Publishing Company 2006.

[Pet62] C.A. Petri, *Kommunikation mit automaten*, Ph.D. thesis, University of Bonn, Germany, 1962.

[Phi07] *Efficient, Correct Simulation of Biological Processes in the Stochastic Pi-calculus.*, In: CMSB'07, Lecture Notes in Computer Science, vol. 4695, pp. 184–199, Springer-Verlag, 2007.

[PRI] *PRISM model checker web site:* `http://www.prismmodelchecker.org`.

[PRSS01] C. Priami, A. Regev, E. Shapiro and W. Silverman, *Application of a stochastic name-passing calculus to representation and simulation of molecular processes*, Information Processing Letters, vol. 80, pp. 25–31, Elsevier North-Holland, Inc., 2001.

[PSY] *The P System web page:* `http://ppage.psystems.eu/`.

[RKNP04] J. J. M. M. Rutten, M. Kwiatkowska, G. Norman and D. Parker, *Mathematical techniques for analyzing concurrent and probabilistic systems*, American Mathematical Society, 2004.

[QS82] J. P. Queille and J. Sifakis, *Specification and verification of concurrent systems in CESAR*, In: Symposium on Programming, Lecture Notes in Computer Science, vol. 137, pp. 337–351, Springer-Verlag, 1982.

[RCGB+06] F.J. Romero-Campero, M. Gheorghe, L. Bianco, D. Pescini, Pérez-Jiménez M. J. and R Ceterchi, *Towards Probabilistic Model Checking on P Systems Using PRISM*, In:Membrane Computing, Lecture Notes in Computer Science, vol. 4361, pp. 477–495, Springer-Verlag, 2006.

[RCPJ08] F. J. Romero-Campero and M. J. Pérez-Jiménez, *A model of the quorum sensing system in vibrio fischeri using P Systems*, Artificial Life, vol. 14, pp. 95–109, MIT Press, 2008.

[RC08a] F. J. Romero-Campero, *P systems, a computational modelling framework for systems biology*, Ph.D. Thesis, Universidad de Sevilla, Spain, 2008.

[Rei85] W. Reisig, *Petri Nets: an introduction*, Springer-Verlag, 1985.

[Ros83] S. Ross, *Stochastic processes*, John Wiley, 1983.

[RPS+04] A. Regev, E.M. Panina, W. Silverman, L. Cardelli and E. Shapiro, *Bioambients: an abstraction for biological compartments*, Theoretical Computer Science, vol. 325, pp. 141–167, Elsevier Science Publishers Ltd., 2004.

[RS02] A. Regev and E. Shapiro, *Cellular abstractions: Cells as computation*, Nature, vol. 419, p. 343, Nature Publishing Group, 2002.

[Sca07] G. Scatena, *Development of a stochastic simulator for biological systems based on Calculus of Looping Sequences*, Master's thesis, University of Pisa, Italy, 2007.

[Seg84] L.A. Segel, *Modeling dynamic phenomena in molecular and cellular biology*, Cambrige University Press, 1984.

[SES02] P.S. Swain, M.B. Elowitz and E.D. Siggia, *Intrinsic and extrinsic contributions to stochasticity in gene expression*, Proceedings of the National Academy of Sciences, vol. 99, pp. 12795–12800, 2002.

[SFB+08] A. Sadot, J. Fisher, D. Barak, Y. Admanit, M.J. Stern, E.J.A. Hubbard and D. Harel, *Toward verified biological models*, Transactions. Comput. Biol. Bioinformatics, vol. 5, pp. 223–234, IEEE Computer Society, 2008.

[SH86] P.W. Sternberg and H.R. Horvitz, *Pattern formation during vulval development in* C. elegans, Cell, vol. 44, pp. 761–772, Cell Press, 1986.

[SH89] ———, *The combined action of two intercellular signaling pathways specifies three cell fates during vulval induction in* C. elegans, Cell, vol. 58, pp. 679–693, Cell Pres, 1989.

[SKSW04] O. Shaw, A. Koelmans, J. Steggles and A. Wipat, *Applying petri nets to systems biology using xml technologies*, Tech. report, University of Newcastle upon Tyne, March 2004.

[Šku06] D. Škulj, *Finite discrete time markov chains with interval probabilities.*, Advances in Intelligent and Soft Computing, pp. 299–306, Springer-Verlag, 2006.

[Šku09] D. Škulj, *Discrete time markov chains with interval probabilities*, International Journal of Approximate Reasoning, vol. 50, pp. 1314–1329, Elsevier Science Inc., 2009.

[SMC+08] A. Spicher, O. Michel, M. Cieslak, J. L. Giavitto and P. Prusinkiewicz, *Stochastic p systems and the simulation of biochemical processes with dynamic compartments*, Biosystems, vol. 91, pp. 458–472, Elsevier Science Inc., 2008.

[SPI] *The SPiM web page:* `http://research.microsoft.com/~aphillip/spim/`.

[ST05] O. Schulz-Trieglaff, *Stochastic petri nets in systems biology*, BMC Bioinformatics, vol. 6(suppl.3), p. 25, Springer-Verlag, 2005.

[Ste05] P. W. Sternberg, *Vulval development*, Chapter on vulval development in Wormbook (`http://www.wormbook.org/chapters`), 2005.

[SVA] K. Sen, M. Viswanathan and G. Agha, *Model-checking markov chains in the presence of uncertainties*, In: TACAS'06, Lecture Notes in Computer Science, vol. 3920, pp. 394–410, Springer-Verlag, 2006.

[TSB04] T. E. Turner, S. Schnell, and K. Burrage, *Stochastic approaches for modelling in vivo reactions*, Computational Biology and Chemistry, vol. 28, pp. 165–178, Elsevier Science Inc. 2004.

[Var85] M.Y. Vardi, *Automatic verification of probabilistic concurrent finite state programs*, In:FOCS'85, pp. 327–338, IEEE Computer Society, 1985.

[VR03] M. Villasana and A. Radunskaya, *A delay differential equation model for tumor growth.*,Journal of Mathematical Biology, vol. 47, pp. 270–294, Springer-Verlag, 2003.

[Wei99] K. Weichselberger, *The theory of interval-probability as a unifying concept for uncertainty*, International Journal Approximated Reasoning, vol. 24, pp. 149–170, Elsevier Science Inc., 1999.

[Wil06] D.J. Wilkinson, *Stochastic modelling for systems biology (mathematical and computational biology)*, Chapman & Hall, 2006.

[WZH07] B. Wachter, L. Zhang, and H. Hermanns, *Probabilistic model checking modulo theories*, In:QUEST'07, pp. 129–140, IEEE Computer Society, 2007.