Probabilistic Models and Process Calculi for Mobile Ad Hoc Networks

Lei Song

Programming, Logic, and Semantics

IT University of Copenhagen

A thesis submitted for the degree of

Doctor of Philosophy in Computer Science

2012 03

Abstract

Due to the wide use of communicating mobile devices, mobile ad hoc networks (MANETs) have gained in popularity in recent years. In order that the devices communicate properly, many protocols have been proposed working at different levels. Devices in an MANET are not stationary but may keep moving, thus the network topology may undergo constant changes. Moreover the devices in an MANET are loosely connected not depending on pre-installed infrastructure or central control components, they exchange messages via wireless connections which are less reliable compared to wired connections. Therefore the protocols for MANETs are usually more complicated and error-prone. In this thesis we discuss different models and their underlying theories which will facilitate the verification of protocols for MANETs.

Process calculi have been used successfully as a formal method to verify and analyze functional behaviors of concurrent systems e.g. free of deadlock, and they also have been extended with probability to verify quantitative properties e.g. "the sent message will arrive at the destination in 5 seconds with probability no less than 0.99". In this thesis we extend the framework to deal with special issues in MANETs e.g. mobility and unreliable connections. Specially speaking,

1. We first propose a discrete probabilistic process calculus with which we can model in an MANET that the wireless connection is not reliable, and the network topology may undergo changes. We equip each wireless connection with a probability, and moreover we allow these probabilities to be changed according to some mobility rule to model the changes of the network topology. The semantics gives rise to *Probabilistic Automata* (1) (PA), thus allowing us to use PCTL (2) or PCTL*

(3) to express properties of protocols. We also propose several variants of bisimulations and simulations letting us abstract some details of protocols as well as the mobility of the network topology. The theory is then applied to a protocol for distribution of IP addresses (Zeroconf (4)).

2. Secondly we extend the discrete probabilistic process calculus in several directions: i) Generalize the notions of mobility rules which allow to change part of a network topology depending on an exponentially distributed random delay and a *network topology constraint*. ii) Introduce stochastic time behavior for processes running at network nodes. iii) A novel abstraction is proposed where several broadcasts may be simulated by one. The semantics is a combination of discrete and continuous probability, nondeterminism, and concurrency, thus giving rise to an Markov Automaton (5) (MA). Several variants of bisimulations and simulations are also defined some of which are defined over distributions. We show how to use the theory by applying it to a leader election protocol.

3. Various behavioral equivalences and their logical characterizations have been proposed to combat the infamous states space explosion problem of PAs, but unfortunately it is well known that the behavioral equivalences are strictly stronger than the logical equivalences induced by PCTL or PCTL*. We address this problem in this thesis by introducing a sequence of strong bisimulations, which will converge to the PCTL or PCTL* equivalence eventually. This work is then extended to weak bisimulations and simulations. Since CTMDPs can be seen as continuous-time extension of PAs, we also extend the work to the continuous setting in a natural way.

4. Recently, MAs have been proposed as a compositional behavior model supporting both probabilistic transitions and exponentially distributed random delays. Moreover two variants of weak bisimulation are also defined in (5) and (6). In this thesis, we introduce both early and late semantics for MAs based on which we define the early and late

weak bisimulation respectively. We also show that the early weak bisimulation coincides with the previous variants while the late weak bisimulation is strictly coarser than them, thus the late weak bisimulation enables us to reduce the state spaces of MAs even further. This work is also extended to simulations. For future work we will discuss logic characterization for both early and late weak (bi)simulations.

Acknowledgements

I would first thank my supervisor Jens Chr. Godskesen for his endless support of this work. He is always reading my drafts carefully, gives valuable suggestions and inspiring comments for improvement. He gives me lots of freedom to do the research, and it is very pleasant to work with him. This thesis would be impossible without his helps.

Lijun Zhang deserves a special thanks for this work. He is a great collaborator, and it is always inspiring and fruitful to discuss with him. His enthusiasm in research and the ability to solve problems is quite impressive.

Many thanks go to Flemming Nielson, and Bo Friis Nielsen, it was a great experience to work with them. Their attitudes and the way of doing research will influent me in the future.

I am also very grateful to Yuxi Fu and Yuxin Deng, my Master's thesis supervisor and instructor, for having introduced me to the field of process algebra and probabilistic model checking.

Thanks to Scott A. Smolka for hosting my staying abroad at Stony Brook University. The time spent there was very enjoyable.

Both MT-Lab and PLS group have creative and pleasant working atmosphere, which is a great stimulus for the research. Many thanks to my colleagues for interesting discussions, in particular, to Fabrizio Biondi, Louis-Marie Traonouez, and Andrzej Wąsowski.

The research presented in this thesis has been supported by MT-LAB, a VKR Center of Excellence for the Modeling of Information Technology.

Last, but not least, a special thank to my parents, Mingjian Song and Xuhong Cao, and to my fiancee Li Xu, this thesis is dedicated to them.

Declaration

I herewith declare that I have produced this thesis without the prohibited assistance of third parties and without making use of aids other than those specified; notions taken over directly or indirectly from other sources have been identified as such. This thesis has not previously been presented in identical or similar form to any other examination board.

The thesis work was conducted from 01/04/2009 to 31/03/2012 under the supervision of Jens Chr. Godskesen at IT University of Copenhagen, Denmark.

Copenhagen,

Contents

List of Figures

List of Tables

LIST OF TABLES

Chapter 1

Introduction

In this chapter we first introduce the mobile ad hoc networks and their characteristics, then we briefly present the classic process calculi and their applications in protocol verification, and we also show how the theory of process calculi can be extended with quantitative information to deal with randomized behaviors. Bisimulation and its logical characterization is discussed in Section 1.3 together with simulation and its logical characterization. We summarize our achievements of this thesis in Section 1.4 as well as the organization of the following chapters.

1.1 Mobile Ad Hoc Networks

Mobile ad hoc networks (MANETs) are composed by a lot of mobile devices which can communicate with each other via wireless connections. The mobile devices in an MANET are self organizing without the need of any pre-installed infrastructure or central control components, thus an MANET is supposed to be more fault tolerant compared to wired local area networks (Ethernet), since devices may crash or even leave the network. Due to the wide use of communicating mobile devices, MANETs have gained in popularity in recent years, and the application area is broad, spanning from ambient intelligence, wireless local area networks, sensor networks, and cellular networks for mobile telephony.

Due to the lack of pre-installed infrastructure and central control components, the protocols of MANETs are usually more complicated and error-prone than those for Ethernets, which makes the rigorous verification of these protocols difficult and necessary.

1. INTRODUCTION

Compared to Ethernets, MANETs have the following characteristics:

1. Local broadcast.

   The key communication primitive in an MANET is message broadcast but, different from Ethernets, broadcast in wireless networks is *local*, hence only devices within the communication range of the emitting device can receive a message, while all the other devices out of the transmission range cannot.

2. Mobility.

   The devices in an MANET are not stationary but keep moving, moreover they may also crash, therefore the connectivity topology undergos constant changes.

3. Unreliable connection.

   A wireless connection is not as reliable as a wired connection i.e. we cannot guarantee that a broadcast message will reach all the devices even if they are in the transmission range of the emitting device. Since the messages exchanged through wireless connections may get lost during transmission.

4. Unidirectional.

   The wireless connection is usually unidirectional instead of bidirectional, since the devices in an MANET may have different transmission ranges. If a device A can deliver messages to a device B, we cannot say that B is also able to deliver messages to A, because B may have a smaller transmission range than A.

5. Separated Connectivity.

   Connectivity should not be part of a protocol i.e. when designing a protocol we cannot make any assumption on the network connectivity, the protocol should work properly for any possible situation. But the specification of a protocol may refer to certain conditions about the connectivity. For instance, we may specify properties like "the messages broadcasted from a device A will eventually reach a device B as long as B is connected to A either directly or via some intermediate devices".

1.2 Process Calculi and Probability

Process calculi have been a popular framework and much used in the specification and verification of parallel and distributed software systems. During the last three decades several variants of process calculi have been proposed, the most important of which are CCS (Calculus of Communicating systems (7, 8)), CSP (Communication Sequential Processes (9)), and ACP (Algebra of Communicating Processes (10, 11, 12)). As the extension of CCS, the π-calculus is developed in (13, 14, 15) by Milner, Parrow and Walker which allows channel names to be transferred via channel names, it is able to model concurrent systems where the interconnection between processes may change during the computation. All these process calculi have very simple syntax and few operators by which we can describe both specification and implementation of concurrent systems. To describe the behaviors of processes, each process calculus is equipped with an operational semantics, usually in the form of a *labeled transition system* introduced in (16). One advantage of process calculi is that they have an algebraic basis enabling us to model and analyze concurrent systems in a formal and rigorous way.

Process calculi have been applied successfully to verify functional properties of concurrent systems, for example we may check whether a system is free of deadlock or not, and whether a certain message will reach all the devices eventually or not. But in many systems we are also interested in the quantitative properties of them, not just their functional properties, for instance we want to know what is the maximal probability of a system reaching deadlock states, and what is the minimal probability of a certain message reaching all the devices in 5 seconds. In order to do so, a variety of extensions of classical process calculi have been proposed (17, 18, 19, 20, 21, 22), whose semantics gives rise to different models. Depending on i) whether the time is discrete or continuous, and ii) whether nondeterministic choices are allowed or not, we can divide probabilistic models into several categories as follows:

1. Discrete-time Markov Chain (DTMC) or fully probabilistic systems.
   The DTMC is a probabilistic extension of the labeled transition system where all the transitions are associated with probabilities. As indicated by its name, the time is discretized as steps in DTMCs. The model has been studied in (19, 23, 24). Fig. 1.1 (a) is an example of DTMC such that s can evolve into s_1, s_2, and s_3 with probability 0.5, 0.2, and 0.3 respectively. Note that we omit the labels of

the transitions and all the transitions of $s_i (1 \leq i \leq 5)$ in Fig. 1.1. For models with transition labels, refer to (25) for a good overview.

2. Probabilistic Automata (PA) or Markov Decision Processes (MDP).
   Probabilistic automata can be seen as extensions of DTMCs with nondeterministic choices, and have been studied in (1, 26, 27). In a PA, each state may have several nondeterministic choices, after choosing a transition it will reach certain states with specified probabilities. Fig. 1.1 (b) gives an example of PA where s has two nondeterministic choices, either choosing the left transition or the right one. Suppose s chooses the right transition, then it will evolve into s_4 and s_5 with probability 0.6 and 0.4 respectively.

3. Continuous-time Markov Chain (CTMC).
   Similar with DTMC, the CTMC is an extension of the labeled transition system where each transition is associated with an exponentially distributed random variable. Such transitions are called *Markovian transitions*, and the variable associated with each transition is called the rate of it specifying the duration of the Markovian transition. CTMC has been widely used as the underlying model to analyze performance-oriented systems, such examples include TIPP (28), PEPA (29), EMPA (30), stochastic π-calculus (31), IMC (32), StoKlaim (33), and Stochastic Ambient Calculus (34). Fig. 1.1 (c) shows an example of CTMC where s has three Markovian transitions with rates 5, 2, and 3 respectively.

4. Continuous-time Markov Decision Processes (CTMDP).
   The CTMDP can be seen either as an extension of CTMC with nondeterministic choices, or as a continuous-time variant of MDP where all probabilities are replaced by exponentially distributed random variables. In a CTMDP, each state will first choose a transition nondeterministically from all available transitions, then it will delay for some time and evolve into certain states with specified probabilities. This model has been studied in (35, 36, 37), and applied in many fields such as stochastic scheduling (38, 39) and dynamic power management (40). Fig. 1.1 (d) gives an example of CTMDP where s has two nondeterministic choices: either s chooses the left transition first and then evolve into s_1, s_2, and s_3 with rates 5, 2, and 3 respectively, or it chooses the right transition first and evolve into s_4 and s_5 with rates 6 and 4 respectively.

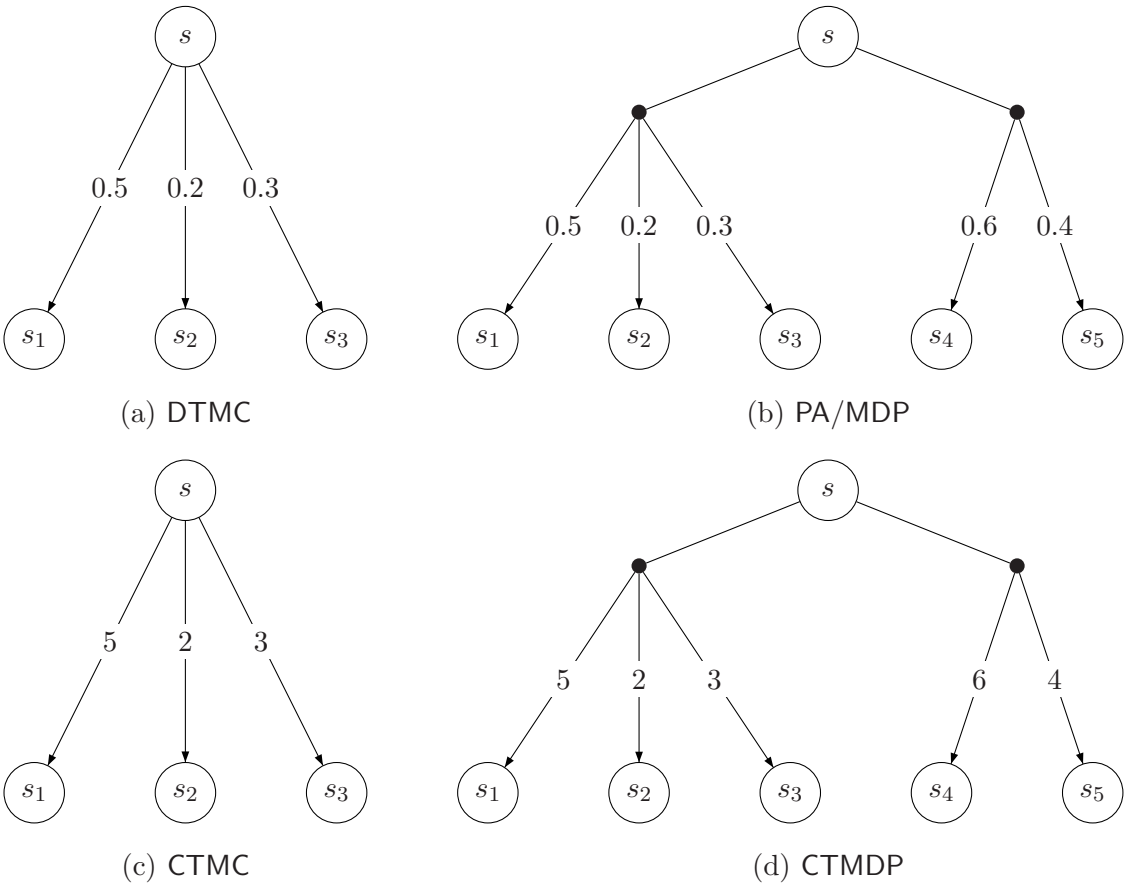

Figure 1.1: Different probabilistic models.

Besides the models mentioned above, a new stochastic model, called Markov automata (MA), has been proposed by Eisentraut, Hermanns, and Zhang in (5) recently. MA can be considered as a combination of PA and IMC, we will discuss MAs in Chapter 6. The probabilistic models can be further divided into alternating models and non-alternating models, we defer the detail discussion to Chapter 4.

1.3 (Bi)Simulation and Logical Characterization

As mentioned before both implementation and specification of a concurrent system can be described using process calculi. Usually the specification *Spec* of a concurrent system is more abstract than the implementation without considering many details, while the implementation *Impl* is more complicated describing the system at a lower

level. In order to establish the relation between the specification and implementation, a number of behavioral equivalences, called *bisimulation equivalences*, have been proposed (7, 8, 41). Refer to (42, 43) for a good overview of variants behavioral equivalences. There are two main kinds of bisimulation equivalences: strong bisimulation and weak bisimulation. Intuitively, two systems are strongly bisimilar iff they can mimic the behavior of each other stepwise, while in weak bisimulation this condition is relaxed such that two systems are weakly bisimilar iff they can mimic the "observable" behavior of each other stepwise. With these notions we can check whether *Impl* is a correct implementation of the given *Spec*.

Bisimulation equivalence is very important for verification purpose, especially to deal with the infamous state space explosion problem. Usually the properties of a system can be expressed by a kind of logic e.g. the Computation Tree Logic (CTL) or Extended Computation Tree Logic (CTL*) (44). Two bisimilar systems are guaranteed to satisfy the same properties, thus can be grouped together. In other words, bisimulation can be characterized using the logic equivalence, see e.g. (45). Therefore if *Spec* and *Impl* are bisimilar, then whenever *Spec* satisfies some property, we can be sure that *Impl* also satisfies the same property and vice versa. Since *Spec* is more abstract than *Impl*, it contains less states and is preferable for verification purpose.

Usually a complicated system is built upon several smaller components via parallel operator, thus one desirable property of bisimulation equivalences is congruence w.r.t. the parallel operator, it enables us to split a complicated system into several components, and then analyze these components one by one. Suppose that we have a system specification *Spec* which contains two components: $Spec_1$ and $Spec_2$. There is also an implementation *Impl* built upon $Impl_1$ and $Impl_2$, which are implementations of $Spec_1$ and $Spec_2$ respectively. We want to know whether *Impl* is a correct implementation of *Spec* or not, i.e. whether *Spec* and *Impl* are bisimilar. Instead of checking *Spec* and *Impl* directly, we can split the problem into two smaller ones and verify whether $Impl_i$ and $Spec_i$ are bisimilar ($i = 1, 2$). If the answer is yes, and the bisimulation is a congruence, then we can guarantee that *Spec* and *Impl* are also bisimilar.

For two systems *Spec* and *Impl* to be bisimilar, *Spec* need to mimic the behavior of *Impl* stepwise and vice versa. If we relax this condition and only require one direction mimicking, we will obtain the concept of simulation, that is, *Spec* simulates *Impl* iff *Spec* can perform whatever behavior *Impl* can perform, but the reverse is not required

to hold, therefore simulations are preorders instead of equivalences. Depending on whether we consider all the behaviors or just the observable behaviors, we will obtain strong simulation and weak simulation respectively as in the bisimulation scenario. The simulation can also be characterized by some proper fragment of logic, for instance in (46) $\forall$CTL*, the safe fragment of CTL*, is used to characterize strong simulation. In other words, if *Spec* simulates *Impl*, then for any formula φ of $\forall$CTL*, *Spec* satisfies φ implies that *Impl* satisfies φ.

Since bisimulations and simulations have been used successfully for verifying concurrent systems, there have been lots of efforts to extend them and their logical characterizations to probabilistic systems during the last two decades, for both discrete models (1, 2, 24, 25, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57) and continuous models (29, 32, 54, 58, 59, 60, 61). The extension is not trivial for probabilistic systems, especially when both nondeterministic choices and probabilistic choices occur simultaneously, for instance in PAs and CTMDPs. For PAs, bisimulations and simulations are characterized by variants of Hennessy-Milner logic in (62) and (57) respectively, but as pointed out in (1) the bisimulations cannot be characterized by a probabilistic extension of CTL i.e. PCTL (2, 3). For CTMDPs, the first logical characterization result is presented in (37). Unfortunately the strong bisimulation is only sound, but not complete w.r.t. continuous-time stochastic logic (CSL) equivalence where CSL is a continuous extension of CTL, in other words, two strongly bisimilar systems are guaranteed to satisfy the same CSL formulas, but two systems satisfying the same CSL formulas are not necessarily strongly bisimilar. We will address these problems in Chapter 4 and Chapter 5.

1.4 Contributions and Overview of the Thesis

In this dissertation we aim at developing probabilistic broadcast calculi for modeling and analyzing protocols for MANETs and establishing the necessary probabilistic semantic models for doing so. We summarize our contributions in each chapter and give an overview of the thesis as follows:

- In Chapter 2 we present a probabilistic broadcast calculus for MANETs whose connections are unreliable. In the calculus broadcasted messages can be lost

with a certain probability, and due to mobility the connection probabilities between two nodes may change. If a node at a location broadcasts a message, the network will evolve into a network distribution depending on whether nodes at other locations receive the message or not. Mobility of nodes is not arbitrary but guarded by a *probabilistic mobility function*. We define two notions of bisimulation equivalence, they are called *weak bisimulation* and *weak probabilistic bisimulation* respectively. In both cases, it is possible to have equivalent networks which have different connectivity information. Then we examine bisimulation relations between different probabilistic mobility functions, which enables us to abstract the mobility functions as well. We also extend these work to simulations. In this calculus the time is discrete and each model may have nondeterministic choices of probabilistic transitions, thus corresponds to a PA according to the semantics. Finally we apply our calculus on a small example called the Zeroconf protocol.

- Based on the calculus presented in Chapter 2, we introduce a continuous time stochastic broadcast calculus for MANETs in Chapter 3. The mobility of nodes in a network is modeled by a *stochastic mobility function* which allows to change part of a network topology depending on an exponentially distributed delay and a *network topology constraint*. We allow continuous time stochastic behavior of processes running at network nodes, e.g. in order to be able to model randomized protocols. The introduction of group broadcast and an operator to help avoid *flooding* enable us to define a novel broadcast abstraction. By the introduction of the continuous time stochastic behavior it turns out that the semantics of our calculus is a combination of discrete and continuous time probability, nondeterminism, and concurrency and thus gives rise to an MA. We also define two notions of weak bisimulation congruences one of which is over networks while the other one is over network distributions. Finally, we apply our theory on an example of a leader election protocol.

- Since each model in Chapter 2 is a PA, in Chapter 4 we will address the problem of verifying PAs. Specifically, we will discuss the logical characterizations of bisimulations and simulations w.r.t. PCTL* and its sublogics, which is the most often used logic for expressing properties of PAs. Even though various behavioral equivalences have been proposed before, as a powerful tool for abstraction and

compositional minimization for PAs, unfortunately these behavioral equivalences are well-known to be strictly stronger than the logical equivalences induced by PCTL or PCTL*. In Chapter 4 we will introduce novel notions of strong bisimulation relations, which characterizes PCTL and PCTL* exactly. We then extend to weak bisimulations characterizing PCTL and PCTL* without next operator, respectively. Further, we also extend the framework to simulations. Thus, we will bridge the gap between logical and behavioral equivalences (preorders) in the setting of PAs.

- In Chapter 5 we extend the work in Chapter 4 to continuous-time PAs i.e. CTMDPs. We study the branching time equivalences and preorders for CTMDPs, and the logical characterization problem of these relations w.r.t. CSL. For strong bisimulation, it is known that bisimulation is strictly finer than CSL equivalence. In Chapter 5, we first propose the notion of weak bisimulations for CTMDPs and show that for a subclass of CTMDPs, weak bisimulation is both sound and complete w.r.t. the equivalence induced by the sublogic of CSL without next operator. We then propose a sequence of i-depth bisimulation relations characterizing a sequence of sublogics with bounded until similar as in Chapter 4. The i-depth bisimulation equivalences converge to the CSL equivalence for arbitrary CTMDPs. Further, we extend the framework to simulations and their characterizations as well. Another notable contribution in Chapter 5 is the notion of a parallel composition operator for CTMDPs, moreover, we show that both strong and weak bisimulations are congruence relations with respect to it.

- Since the semantics introduced in Chapter 3 gives rise to MAs, in Chapter 6 we will talk about related problems for MAs. MA and its weak bisimulation was first proposed by Eisentraut, Hermanns and Zhang in (5), and later on Deng and Hennesy proposed another notion of weak bisimulation in (6), enjoying the nice property of being a *reduction barbed congruence*, i.e., it is compositional, barb-preserving and reduction-closed. In Chapter 6 we propose two different semantics for MAs called early semantics and late semantics respectively, and then we introduce early and late weak bisimulation based on the semantics. We show that the early weak bisimulation coincides with the weak bisimulations in

(5) and (6), and the late weak bisimulation is strictly coarser than them, thus using late weak bisimulation we can reduce the state space even further.

- We conclude the thesis in Chapter 7.

1.5 My Publications

During my PhD I have written the following 8 articles together with my supervisor Jens Chr. Godskesen and some other people from MT-Lab:

1. Lei Song and Jens Chr. Godskesen. Probabilistic Mobility Models for Mobile and Wireless Networks. IFIP TCS 2010: 86-100.
2. Lei Song and Jens Chr. Godskesen. Broadcast Abstraction in a Stochastic Calculus for Mobile Networks. Submitted for publication.
3. Lei Song, Lijun Zhang, and Jens Chr. Godskesen. Bisimulations Meet PCTL Equivalences for Probabilistic Automata. CONCUR 2011: 108-123.
4. Lei Song, Lijun Zhang, and Jens Chr. Godskesen. The Branching Time Spectrum for Continuous-Time MDPs. Submitted for publication.
5. Lei Song, Lijun Zhang, and Jens Chr. Godskesen. Late Weak Bisimulation for Markov Automata. Submitted for publication.
6. Lei Song, Lijun Zhang, and Jens Chr. Godskesen. Bisimulations Meet PCTL Equivalences for Probabilistic Automata. Submitted to CONCUR 2011 special issue of LMCS.
7. Lei Song, Flemming Nielson, and Bo Friis Nielsen. A Stochastic Broadcast Pi-Calculus. QAPL 2011: 74-88.
8. Lei Song and Jens Chr. Godskesen. A Probabilistic Calculus for Mobile and Ad Hoc Networks (Abstract). NWPT 2009.

where Article 8 is an abstract version of Article 1, and Article 6 is a journal version of Article 3. Chapter 2 to 6 of this dissertation are based on Article 1-5 respectively. Article 7 does not appear explicitly in this dissertation, but it can be seen as an initial

attempt to investigate the stochastic broadcast calculus, which later on leads us to develop the theory in Article 2.

Chapter 2

Discrete Model

In this chapter we introduce a discrete mobility model for wireless networks where one location may be connected to another with a certain probability. Moreover these probabilities are not fixed but can be changed dynamically to reflect the fact that the connection topology of a wireless network may change due to node's movement, node's crash and so on. We first motivate the work in Section 2.1. The syntax and semantics of the calculus is introduced in Section 2.2 and 2.3 respectively. In Section 2.4 we introduce weak (probabilistic) bisimulations, while weak (probabilistic) simulations are discussed in Section 2.5. The notions of bisimulations and simulations are extended to probabilistic mobility functions in Section 2.6. We show the application of our theory by applying it on the Zeroconf protocol in Section 2.7. This chapter is concluded with related work in Section 2.8.

2.1 Motivation

Mobility and local wireless broadcast has been studied in e.g. the calculi: CBS$^\sharp$ (63), the ω-calculus (64), CMN (65), RBPT (66), and CMAN (67, 68). All these calculi only deal with node connectivity in two modes: either two nodes are connected or disconnected. It is often assumed that when a node at location l is within the transmission range of another node at location k, then the node at l can receive messages broadcasted from k with probability 1, otherwise with probability 0. Here we refine this assumption and equip a connection with a probability, since in an unreliable medium we cannot guarantee that the broadcasted messages will always be received even within

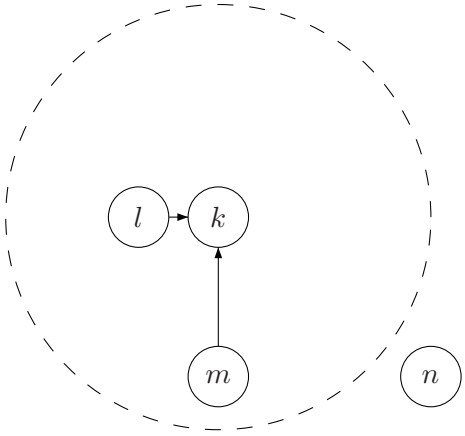

Figure 2.1: Connectivity example.

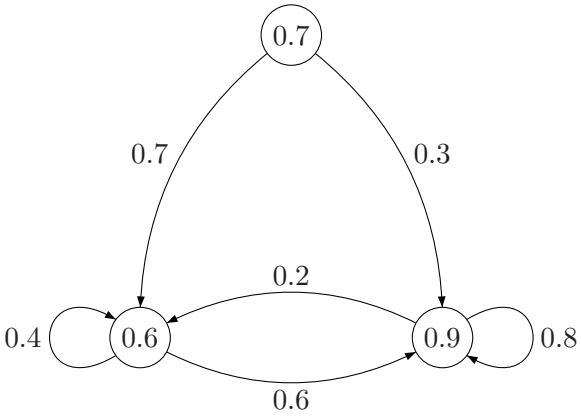

Figure 2.2: An example of mobility.

the transmission range. For example, in Fig. 2.1 the dashed circle denotes the transmission range of k, every node at a location within the circle, such as l and m, may receive the messages broadcasted from k, but the node at location n outside the circle cannot. Intuitively, although both l and m are in the transmission range of the node at location k, it is more reasonable to let the nodes receive messages from k with different probabilities since m is further away from k than l. In our calculus, the connectivity of this network can be denoted as $\{\{(0.9, l), (0.5, m), (0, n)\} \longmapsto k\}$ if nodes at l, m, n can receive messages from k with probability 0.9, 0.5, and 0 respectively.

In order to model mobility we let connection probabilities between the nodes at locations change, and the changes are also probabilistic. For instance, the node at

location m in Fig. 2.1 may move closer to location k with a certain probability in which case the node at m will be able to receive messages from k with a higher probability.

In practice, when verifying properties of a mobile network it will be reasonable to assume that mobility within a network is not arbitrary but respects certain rules or distributions. Therefore we introduce a *probabilistic mobility function* (PMF) which defines the mobility rules of all possible connections within a network. A PMF returns the probability for a connection evolving from one value into another. For example, if in a PMF the connection probability from l to k is given by Fig. 2.2, then we know that it can change from 0.9 to 0.6 with probability 0.2 or stay at 0.9 with probability 0.8, that is:

$$\{\{(0.9,l),(0.5,m),(0,n)\} \longmapsto k\} \longrightarrow \begin{cases} 0.2 : \{\{(0.6,l),(0.5,m),(0,n)\} \longmapsto k\} \\ 0.8 : \{\{(0.9,l),(0.5,m),(0,n)\} \longmapsto k\} \end{cases} \tag{2.1}$$

Hence we equip mobility with probabilities, and after each mobility action the network will evolve into a distribution with the probabilities specified by the given PMF. We expect that usually a PMF can be obtained based on measurement of case studies.

Our network calculus consists of concurrent processes (nodes) communicating internally over channels at (logical) locations and broadcasting messages to processes at neighboring locations over probabilistic connections that may change probabilistically over time as outlined above. The semantics is a combination of probability, concurrency, and non-determinism. Formally the labeled transition system semantics gives rise to a *probabilistic automata* as outlined in (1).

We also define two (weak) bisimulations along the lines of (56) and (1) respectively, as a novelty the bisimulations are parameterized by a PMF. The first weak bisimulation makes sure that two bisimilar networks have the same probability for every property (specified by pCTL* in (56) for instance) while the second bisimulation, called weak probabilistic bisimulation, only guarantees that they have the same maximum and minimum probabilities for each property. This work is also extended to simulations and (bi)simulations between PMFs.

Another important contribution is the introduction of *unknown probabilities*. Since we are dealing with open systems where contexts may contain new nodes and information about connection probabilities, we cannot in a network specification expect to know the probability of all possible connections. We integrate unknown probabilities in

our theory in order to deal with these cases. Intuitively a connection with an unknown probability means that the probability for the connection can be any value allowed by the given PMF.

2.2 The Calculus

We presuppose a countable set $\mathcal{N}$ of names, ranged over by x, y, z and a countable set $\mathcal{L}$ of location names, ranged over by k, l, m, and n. In addition, we also suppose a finite set of probabilities $\wp$ including 0 and 1 ranged over by $\rho, \rho', \rho_1 \ldots$. We define a *location connectivity set*, ranged over by $\mathbb{L}, \mathbb{K} \ldots$, as an element of

$$\{\{(\rho, l) \mid l \in L\} \mid \rho \in \wp\}$$

where $L \subset \mathcal{L}$ is finite. We use

$$l(\mathbb{L}) = \{l \mid (\rho, l) \in \mathbb{L}\}$$

to denote all the locations in $\mathbb{L}$. The convex combination of location connectivity sets $\sum_{i \in I} w_i \mathbb{L}_i$ is defined by

$$\{(\rho, l) \mid \sum_{i \in I, (\rho_i, l) \in \mathbb{L}_i} w_i \rho_i = \rho\}$$

where $l(\mathbb{L}_i) = l(\mathbb{L}_j)$ for any $i, j \in I$.

The syntax of processes $\mathcal{P}$, ranged over by $p, q, r \ldots$, is defined by the following grammar:

$$p, q ::= 0 \mid Act \cdot p \mid [x = y]p, q \mid \nu x p \mid p \parallel q \mid A$$

$$Act ::= \langle x \rangle \mid y\langle x \rangle \mid (x) \mid y(x)$$

where action $\langle x \rangle$ represents broadcasting a message x, while the reception of a broadcasted message is denoted by (x); $y\langle x \rangle$ denotes sending a message x via the channel y and $y(x)$ represents receiving a message x on channel y. Process 0 is the deadlocked process; $Act \cdot p$ is the process that can perform action Act and then behave as p; $[x = y]p, q$ behaves as p if names x and y match and as q otherwise; $\nu x p$ means that name x is bounded in the process p; in composition $p \parallel q$, the processes p and q can proceed in parallel and can also interact via shared names; we assume that there is a countable set of constants which are used to denote processes. By giving an equation such that $A \stackrel{def}{=} p$ we say that constant $A \in \mathscr{A}$ will behave as p, where $\mathscr{A}$ is a set of

Table 2.1: Structural congruence of processes (discrete).

$p \parallel 0 \equiv p$	$p \parallel q \equiv q \parallel p$	$(p \parallel q) \parallel r \equiv p \parallel (q \parallel r)$
$\nu x \nu y p \equiv \nu y \nu x p$	$\nu x p \parallel q \equiv \nu x(p \parallel q), x \notin fn(q)$	

process constants, and A is required to be guarded in p. As usual we often leave out a trailing 0. Structural congruence of processes, $\equiv$, is the least equivalence relation and congruence closed by the rules in Table 2.1 and α-conversion.

The set of networks $\mathscr{N}$ is defined by the grammar:

$$E, F ::= 0 \mid \lfloor p \rfloor_l \mid \{\mathbb{L} \longmapsto l\} \mid \nu x E \mid E \parallel F$$

Here $\lfloor p \rfloor_l$ is a process p at location l; $\nu x E$ and $E \parallel F$ are restriction and parallel composition respectively which have the standard meaning; $\{\mathbb{L} \longmapsto l\}$ denotes connection information, i.e. if $(\rho, k) \in \mathbb{L}$, the node at location k are connected to l and can receive messages from nodes at l with probability ρ. We use $E, F, G \ldots$ to range over $\mathscr{N}$. Let $\mathscr{C} \subseteq \mathscr{N}$ denote the set of networks which only contain connectivity information, called connectivity networks and ranged over by $C, C_1, \ldots$, it is defined by the following syntax:

$$C ::= \{\mathbb{L} \longmapsto l\} \mid C \parallel C.$$

Moreover let $\mathscr{B} \subseteq \mathscr{N}$ denote the set of networks which does not contain connectivity information i.e. $\mathscr{B}$ is defined by the following syntax and ranged over by $B, B_1, \ldots$:

$$B ::= 0 \mid \lfloor p \rfloor_l \mid \nu x B \mid B \parallel B.$$

A network distribution is a function

$$\mu : \mathscr{N} \to [0, 1]$$

satisfying

$$|\mu| \ = \sum_{E \in \mathscr{N}} \mu(E) \leq 1.$$

Let $\mathcal{ND}$ denote the set of distributions over $\mathscr{N}$, ranged over by $\mu, \mu_1 \ldots$. The support of μ,

$$Supp(\mu) = \{E \mid \mu(E) > 0\}$$

Table 2.2: Structural congruence of networks (discrete).

$E \parallel 0 \equiv E$	$\nu x \nu y E \equiv \nu y \nu x E$	$\{\emptyset \longmapsto l\} \equiv 0$
$\lfloor \nu x p \rfloor_l \equiv \nu x \lfloor p \rfloor_l$	$E \parallel F \equiv F \parallel E$	$\lfloor p \rfloor_l \equiv \lfloor q \rfloor_l, p \equiv q$
$(E \parallel F) \parallel G \equiv E \parallel (F \parallel G)$	$\nu x E \parallel F \equiv \nu x (E \parallel F), x \notin fn(F)$	
$\{\mathbb{L}_1 \longmapsto k\} \parallel \{\mathbb{L}_2 \longmapsto k\} \equiv \{\mathbb{L}_1 \cup \mathbb{L}_2 \longmapsto k\}, l(\mathbb{L}_1) \cap l(\mathbb{L}_2) = \emptyset$		

Table 2.3: Definition of function l

$loc(0) = \emptyset$	$loc(\lfloor p \rfloor_l) = \{l\}$	$loc(\{\mathbb{L} \longmapsto l\}) = \emptyset$
$loc(\nu x E) = loc(E)$	$loc(E \parallel F) = loc(E) \cup loc(F)$	

is the set of networks in μ with positive probability. Sometimes we also write $\{(\rho_i : E_i) \mid \mu(E_i) = \rho_i\}$ to denote μ. If $\mu(E) = 1$, then μ is the *Dirac* distribution δ_E. Given a real number x such that $a \cdot |\mu| \leq 1$, $a \cdot \mu$ is the distribution such that $(a \cdot \mu)(E) = a \cdot \mu(E)$ for each $E \in Supp(\mu)$. Moreover $\mu = \mu_1 + \mu_2$ whenever for each $E \in Supp(\mu)$, $\mu(E) = \mu_1(E) + \mu_2(E)$. Parallel composition of network distributions $\mu \parallel \mu'$ is defined as a distribution such that

$$(\mu \parallel \mu')(E \parallel F) = \mu(E) \cdot \mu'(F)$$

for any $E \parallel F$. Given an equivalence relation $\mathcal{R}$ on networks, $\mu \; \mathcal{R} \; \mu'$ iff $\mu(S) = \mu'(S)$ for each $S \in \mathcal{N}/\mathcal{R}$ where $\mu(S) = \sum_{E \in S} \mu(E)$.

A substitution $\{y/x\}$ can be applied to a node, network, or network distribution. When applied to a network distribution, it means applying this substitution to each network within the distribution. The set of free names and bound names in E, denoted by $fn(E)$ and $bn(E)$ respectively, are defined as expected. Structural congruence of networks, $\equiv$, is the least equivalence relation and congruence closed by the rules in Table 2.2 and α-conversion. $\equiv$ is extended to network distributions as expected. Let $loc(E)$ denote the set of locations located in a network which is defined inductively by Table 2.3. Differently, $l(E)$ is used to denote all the location names appearing in E including those in connectivity information, its definition is the same as $loc(E)$ except that $l(\{\mathbb{L} \longmapsto l\}) = l(\mathbb{L}) \cup \{l\}$.

In the following, we use $Pro(k \longmapsto l)$ as an abbreviation of the probability with which the node at location k can receive messages from l. As mentioned, we assume

that mobility is not arbitrary but respects certain rules. These rules are given by a function

$$\mathcal{M} : \mathcal{L} \times \mathcal{L} \times \wp \times \wp \to \mathbb{R}_{\leq 1}$$

called a *probabilistic mobility function* (PMF)[1], the probability for $Pro(k \longmapsto l)$ changing from ρ to ρ' is given by $\mathcal{M}(k, l, \rho, \rho')$. We assume there is a given $\mathcal{M}$ throughout this chapter.

Let $G_{k \longmapsto l}$ be the underlying directed graph for $Pro(k \longmapsto l)$, where vertices are possible values of $Pro(k \longmapsto l)$ and where there is an edge from state ρ to ρ' iff $\mathcal{M}(k, l, \rho, \rho') \in (0, 1]$, and we ignore nodes with 0 in-degree and 0 out-degree. For example, if $G_{k \longmapsto l}$ is defined by Fig. 2.3, then we know that if the current value of $Pro(k \longmapsto l)$ is 0.5, it could change to 0.6 with probability 0.3 or to 0.7 with probability 0.2. Without causing any confusion, sometimes we also use $G_{k \longmapsto l}$ to denote the set of nodes in the graph $G_{k \longmapsto l}$, this set is called the *support* of $Pro(k \longmapsto l)$. A PMF $\mathcal{M}$ is valid if for all $G_{k \longmapsto l}$, $G_{k \longmapsto l} \neq \emptyset$ and for each $\rho \in G_{k \longmapsto l}$,

$$\sum_{\rho' \in G_{k \longmapsto l}} \mathcal{M}(k, l, \rho, \rho') = 1.$$

This is not a restriction to the expressions of PMFs, since if

$$\sum_{\rho' \in G_{k \longmapsto l} \wedge \rho' \neq \rho} \mathcal{M}(k, l, \rho, \rho') < 1,$$

then the probability of $Pro(k \longmapsto l)$ will not change with probability

$$1 - \sum_{\rho' \in G_{k \longmapsto l} \wedge \rho' \neq \rho} \mathcal{M}(k, l, \rho, \rho')$$

intuitively, therefore we can always add extra rule such that

$$\mathcal{M}(k, l, \rho, \rho) = 1 - \sum_{\rho' \in G_{k \longmapsto l} \wedge \rho' \neq \rho} \mathcal{M}(k, l, \rho, \rho')$$

which makes the $\mathcal{M}$ valid.

Since the location set $\mathcal{L}$ is infinite, it is not reasonable to let users define the mobility rules of all the connections. Instead we allow users to only define the mobility rules of connections which they are interested in. We call those finitely many rules defined

[1] $\mathbb{R}_{\leq 1}$ is the set of real numbers in [0,1]

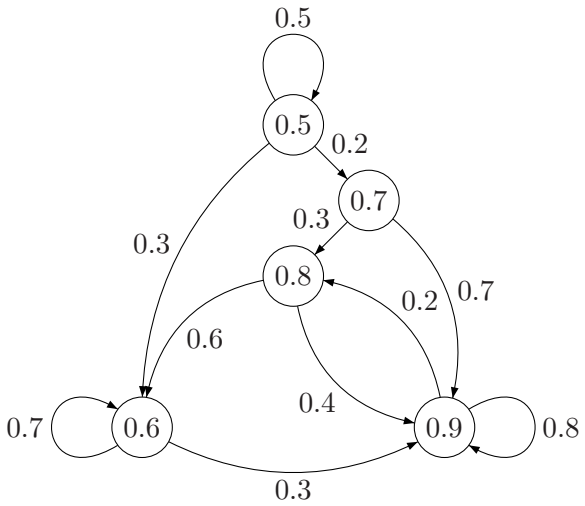

Figure 2.3: An example of a PMF.

by users *explicit* mobility rules, and those connections for which no rules are defined we let have *implicit* mobility. For all the connections with implicit mobility, we say that they can connect or disconnect with probability 1. Formally, if the mobility rule of $Pro(k \longmapsto l)$ is implicit, we assume that

$$G_{k\longmapsto l} = \{0, 1\} \text{ and } \mathcal{M}(k, l, 1, 0) = \mathcal{M}(k, l, 0, 1) = 1$$

by default. In the following, we only consider valid PMFs and let

$$G_l = \{k \in L \mid \text{ mobility rule of } Pro(k \longmapsto l) \text{ is explicit}\}$$

which is finite for each l.

We use $E(k, l)$ to denote the connection probability from k to l in the network E. When the requested probability is known in E, $E(k, l)$ returns this value, otherwise it returns $\theta_{k\longmapsto l}$ denoting an *unknown probability*, i.e.

$$E(k,l) = \begin{cases} \rho & \exists E'.(E \equiv \{\{(\rho, k)\} \longmapsto l\} \parallel E') \\ \theta_{k\longmapsto l} & \text{otherwise} \end{cases}$$

We use $\mathcal{D}_l(E)$ to denote the set of connectivity information from some locations to l in E, that is $\mathcal{D}_l(E)$ is the smallest set such that $E(k, l) \neq \theta_{k\longmapsto l}$ and $(E(k, l), k) \in \mathcal{D}_l(E)$ for each $k \in \mathcal{L}$.

We introduce the *well-formed networks* w.r.t. a given PMF as follows:

Definition 1 (Well-formed network)**.** *Given a* PMF $\mathcal{M}$*, the set of well-formed networks* $\mathscr{N}$ *is defined inductively by:*

1. $0, \lfloor p \rfloor_l \in \mathscr{N}$,
2. $\nu x E \in \mathscr{N}$ *if* $E \in \mathscr{N}$,
3. $\{\mathbb{L} \longmapsto l\} \in \mathscr{N}$ *if for each* $(\rho, k) \in \mathbb{L}$, $\rho \in G_{k \mapsto l}$,
4. $E \parallel F \in \mathscr{N}$ *if* $E, F \in \mathscr{N}$ *with* $loc(E) \cap loc(F) = \emptyset$ *and there does not exist* $l, k \in \mathcal{L}$ *such that* $E(l,k) \neq \theta_{l \mapsto k}$ *and* $F(l,k) \neq \theta_{l \mapsto k}$.

Clauses 1 and 2 are trivial. Clause 3 says that we can only have connectivity information which is allowed by the given $\mathcal{M}$. Since the given PMF $\mathcal{M}$ defines not only the mobility rules, but also all the possible probabilities of each connection, this allows us to omit some impossible states. Clause 4 has two restrictions: i) $loc(E) \cap loc(F) = \emptyset$ guarantees that each location name is unique, we disallow networks like $\lfloor p \rfloor_l \parallel \lfloor q \rfloor_l$. In this case we will write $\lfloor p \parallel q \rfloor_l$ instead, since otherwise processes p and q may not receive the coming messages at the same time even they are at the same location, which is against our intuition. This will be explained in more details in Section 2.3. ii) The other condition says that we cannot have duplicate connectivity information in a network, which is used to guarantee that we will never have inconsistent connectivity information for a connection. For instance networks like $\{\{(\rho, k), (\rho', k)\} \longmapsto l\}$ with $\rho \neq \rho'$ are not well-formed. In the sequel we only consider the set of well-formed networks.

We generalize network distributions to contain unknown probabilities. In the following let

$$\varrho_1, \varrho_2 ::= \rho \mid \theta_{k \mapsto l} \mid (1 - \theta_{k \mapsto l}) \mid \varrho_1 \cdot \varrho_2$$

define the set of *generalized probabilities* which may contain unknown values. The *generalized network distribution*, $\mathcal{GND}$, is defined inductively as follows:

1. $\mu \in \mathcal{GND}$ if $\mu \in \mathcal{ND}$;
2. $\mu \in \mathcal{GND}$ if there exists ϱ and $\mu_1, \mu_2 \in \mathcal{GND}$ such that

$$\mu = \varrho \cdot \mu_1 + (1 - \varrho) \cdot \mu_2.$$

Without causing any confusion, we also use μ, μ', $\mu_1, \cdot$ to range over $\mathcal{GND}$. For a generalized network distribution μ, we may substitute unknown probabilities in μ with known probabilities. In order to do so, we introduce the operator $\bullet$ such that $\mu \bullet \mathcal{D}_l(E)$ is a distribution equal to μ except that any unknown probability $\theta_{k \longmapsto l}$ in μ has been replaced with the probability ρ if $(\rho, k) \in \mathcal{D}_l(E)$. Formally,

$$(\mu \bullet \mathcal{D}_l(E))(F) = (\mu(F)) \bullet \mathcal{D}_l(E)$$

for each $F \in \mathit{Supp}(\mu)$ where $\bullet$ is overloaded to deal with generalized probabilities such that

1. $\varrho \bullet \mathcal{D}_l(E) = \rho$ if $\varrho = \rho$;
2. $\theta_{k \longmapsto l} \bullet \mathcal{D}_l(E) = \rho$ and $(1 - \theta_{k \longmapsto l}) \bullet \mathcal{D}_l(E) = 1 - \rho$ if $(\rho, k) \in \mathcal{D}_l(E)$;
3. $(\varrho_1 \cdot \varrho_2) \bullet \mathcal{D}_l(E) = (\varrho_1 \bullet \mathcal{D}_l(E)) \cdot (\varrho_2 \bullet \mathcal{D}_l(E))$.

To show how $\bullet$ works, we give an example as follows:

Example 1. *Let*

$$\mu = \{\theta_{k \longmapsto l} : E_1, (1 - \theta_{k \longmapsto l}) : E_2\},$$
$$E = \{\{(0.9, k)\} \longmapsto l\},$$

apparently $\mathcal{D}_l(E) = \{(0.9, k)\}$. *After applying* $\bullet$ *with parameter* $\mathcal{D}_l(E)$ *to* μ, *we will be able to substitute the unknown probability* $\theta_{k \longmapsto l}$ *in* μ *as follows:*

$$\begin{aligned} \mu \bullet \{(0.9, k)\} &= \{\theta_{k \longmapsto l} \bullet \{(0.9, k)\} : E_1, (1 - \theta_{k \longmapsto l}) \bullet \{(0.9, k)\} : E_2\} \\ &= \{0.9 : E_1, 0.1 : E_2\}. \end{aligned}$$

2.3 Labeled Transition System

In this section we introduce the labeled transition system semantics for our calculus; the semantics is parameterized by the given PMF $\mathcal{M}$. The semantics of networks is defined based on the semantics of processes. We begin with the semantics of processes.

Define a set of actions for processes, $\mathcal{A}_p$, ranged over by α_p, by:

$$\alpha_p ::= \nu\tilde{x}\langle x \rangle \mid (x) \mid \nu\tilde{x}y\langle x \rangle \mid y(x) \mid \tau$$

where $\nu\tilde{x}\langle x \rangle$ denotes that a process broadcasts a message x; (x) means that the process receives a message; $\nu\tilde{x}y\langle x \rangle$ and $y(x)$ are used to denote point-to-point communication,

that is, $\nu\tilde{x}y\langle x\rangle$ means sending a message x on channel y while $y(x)$ denotes receiving a message on channel y. The $\tilde{x}$ can be either $\{x\}$ or an empty set $\emptyset$, when $\tilde{x} = \{x\}$, x is bound, otherwise it is free. As usual τ is the internal action.

Table 2.4 gives the labeled transition system of processes. Note that we adopt a late semantics, i.e. the bound name of an input becomes instantiated only when inferring a communication. Rule (pPAR) says that in process $p \parallel q$, p can be executed independently with q if the performed action is not broadcast and reception. Rule (pBRD) means that q can receive broadcasted messages from p which is in parallel with q. Rule (pPRE) is straightforward illustrating that $Act \cdot p$ can execute Act, and then evolve into p. Rule (pLOS) means that any non deadlock process $Act \cdot p$ can perform a reception action (x) as long as $x \in fn(Act \cdot p)$, but if Act is not a reception prefix i.e. $Act \cdot p$ is not intended to receive a broadcasted message, it will simply discard the coming messages and stay unchanged. Similarly, in (pZERO) we allow the deadlock process 0 to be able to receive messages but without any impact. The intuition to introduce (pLOS) and (pZERO) is that broadcast actions in our calculus are non-blocking. Together with other rules we can guarantee that a process can broadcast a message no matter if there are recipients or not. This is different from the point-to-point communication where an output and input must synchronize with each other. Rule (pCON) indicates that the behavior of a process constant defined by $A \stackrel{def}{=} p$ is decided by the behavior of p. Rule (pCOM) is the standard point-to-point communication where two processes can communicate via the same channel. Rules (pIF) and (pELSE) are the conditional rules, that is, $[x = y]p, q$ will behave as p if $x = y$, otherwise it will behave as q. Intuitively, Rule (pREC) means that two processes in parallel can receive broadcasted messages simultaneously. Rule (pOPEN2) is the standard scope opening rule of the π-calculus in (69), while (pOPEN1) is its counterpart in a broadcast scenario. Rule (pRES) says that an action α_p will not be affected by the restriction operator whenever its free names are not bound. Rule (pSTR) illustrates the fact that two structural congruent processes have the same behaviors, with rules defined in Table 2.1, we can deduce the symmetric rules of (pPAR), (pBRD), and (pCOM).

Based on the semantics of processes, we define the semantics of networks. First we define a set of actions $\mathcal{A}$, ranged over by α, by:

$$\alpha ::= \nu\tilde{x}\langle x, \mathbb{K}\rangle@l \mid (x, \mathbb{K}) \lhd l \mid \tau$$

Table 2.4: Labeled transition system of processes (discrete).

$$\frac{p \xrightarrow{\alpha_p} p' \quad \alpha_p \notin \{(x), \nu\tilde{x}\langle x\rangle\}}{p \parallel q \xrightarrow{\alpha_p} p' \parallel q} \text{ (pPAR)}$$

$$\frac{p \xrightarrow{\nu\tilde{y}\langle y\rangle} p' \quad q \xrightarrow{(x)} q' \quad \tilde{y} \cap \{\{x\} \cup fn(q)\} = \emptyset}{p \parallel q \xrightarrow{\nu\tilde{y}\langle y\rangle} p' \parallel q'\{y/x\}} \text{ (pBRD)}$$

$$\frac{}{Act \cdot p \xrightarrow{Act} p} \text{ (pPRE)} \qquad \frac{x \notin fn(Act \cdot p) \quad Act \neq (y)}{Act \cdot p \xrightarrow{(x)} Act \cdot p} \text{ (pLOS)}$$

$$\frac{p \xrightarrow{\alpha_p} p' \quad A \stackrel{def}{=} p}{A \xrightarrow{\alpha_p} p'} \text{ (pCON)} \qquad \frac{p \xrightarrow{\nu\tilde{z}y\langle z\rangle} p' \quad q \xrightarrow{y(x)} q'}{p \parallel q \xrightarrow{\tau} \nu\tilde{z}(p' \parallel q'\{z/x\})} \text{ (pCOM)}$$

$$\frac{p \xrightarrow{\alpha_p} p'}{[x = x]p, q \xrightarrow{\alpha_p} p'} \text{ (pIF)} \qquad \frac{[x = y]p, q \xrightarrow{\alpha_p} q' \quad x \neq y}{q \xrightarrow{\alpha_p} q'} \text{ (pELSE)}$$

$$\frac{}{0 \xrightarrow{(x)} 0} \text{ (pZERO)} \qquad \frac{p \xrightarrow{(x)} p' \quad q \xrightarrow{(x)} q'}{p \parallel q \xrightarrow{(x)} p' \parallel q'} \text{ (pREC)}$$

$$\frac{p \xrightarrow{\langle x\rangle} p'}{\nu xp \xrightarrow{\nu x\langle x\rangle} p'} \text{ (pOPEN1)} \qquad \frac{p \xrightarrow{\alpha_p} p' \quad x \notin fn(\alpha_p)}{\nu xp \xrightarrow{\alpha_p} \nu xp'} \text{ (pRES)}$$

$$\frac{p \equiv q \xrightarrow{\alpha_p} q' \equiv p'}{p \xrightarrow{\alpha_p} p'} \text{ (pSTR)} \qquad \frac{p \xrightarrow{y\langle x\rangle} p' \quad x \neq y}{\nu xp \xrightarrow{\nu xy\langle x\rangle} p'} \text{ (pOPEN2)}$$

The actions of networks include only broadcasts, receptions and internal actions. In addition, connectivity information is attached to each broadcast and reception action. $\nu\tilde{x}\langle x, \mathbb{K}\rangle@l$ denotes that a node at location k receives a message broadcasted from l with probability ρ if $(\rho, k) \in \mathbb{K}$; $(x, \mathbb{K}) \lhd l$ means that the node at location k receives a message from location l with probability ρ if $(\rho, k) \in \mathbb{K}$.

Table 2.5 gives the labeled transition system of networks. Rules (nREC1), (nTAU), and (nBRD) illustrate that the behavior of a node is determined by the behavior of the process located inside the node. Specifically, Rule (nREC1) deals with receptions.

Whenever p can perform a reception, $\lfloor p \rfloor_l$ can receive broadcasted messages from any location k. Since the value of $Pro(l \longmapsto k)$ is currently not known in $\lfloor p \rfloor_l$, thus after receiving a message from k, it will evolve into a generalized distribution where $\theta_{l \longmapsto k}$ is used as a placehold. Note that (nREC1) is the only rule where unknown probability is introduced. Later we will show that these unknown probabilities can be resolved completely. Rule (nTAU) is straightforward saying that if p can perform an internal action τ, then $\lfloor p \rfloor_l$ is also able to perform τ, and evolve accordingly. Rule (nBRD) is the counterpart of Rule (nREC1) which deals with broadcasts. Since the process p is located at l, when it broadcasts a message x to the outside of the network, it should notify others where the message x is from. Also in network $\lfloor p \rfloor_l$, nothing is known about the connectivity information, thus an empty set is attached which gives us the network action $\nu \tilde{x} \langle x, \emptyset \rangle @ l$.

Rule (nREC2) has the same intuition as Rule (pREC) in Table 2.4, but needs more explanation. First, two networks E and F in parallel can receive a broadcasted message together, moreover E may contain connectivity information which is not unknown in F and vice versa, hence when put them in parallel, they should learn additional connectivity information from each other. At the moment when E performs a reception, and evolve into μ_1, it has no way to know the connectivity information in F, therefore the resulting distribution μ_1 may contain unknown probabilities which are known in F, similarly for F. This justifies why we need to update μ_1 with $\mathcal{D}_l(F)$ and μ_2 with $\mathcal{D}_l(E)$. It is worthwhile to note that the only unknown probability occurring in μ_1 and μ_2 are of the form $\theta_{k \longmapsto l}$ for some k, thus it is enough to consider $\mathcal{D}_l(F)$ and $\mathcal{D}_l(E)$. As we said before, the connectivity information in $E \parallel F$ is the union of the connectivity information in E and F, thus in the resulting reception of $E \parallel F$, the attached connectivity information is updated to $\mathbb{L} \cup \mathbb{K}$. Note here that the well-formed condition guarantees that $l(\mathbb{L}) \cap l(\mathbb{K}) = \emptyset$, so we can simply merge $\mathbb{L}$ and $\mathbb{K}$ together without causing inconsistency. To show how (nREC2) works, we give an example as follows:

Example 2. *Let $E = \lfloor (x) \cdot p \rfloor_l$ and $F = \{\{(0.5, l)\} \longmapsto k\}$, then according to (nREC1) and (nPRO1), we have the following transitions:*

$$\frac{p \xrightarrow{(x)} p'}{E \xrightarrow{(x,\emptyset) \lhd k} \{\theta_{k \longmapsto l} : \lfloor p' \rfloor_l, (1 - \theta_{k \longmapsto l}) : E\} \equiv \mu} \ ,$$

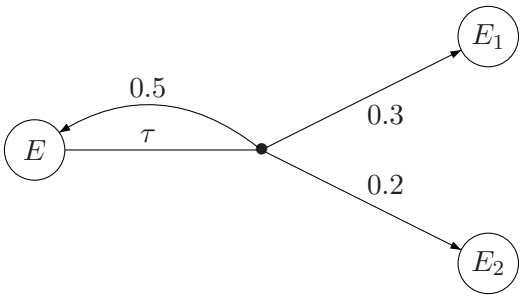

Figure 2.4: A mobility transition.

$$F \xrightarrow{(x,\{(0.5,l)\})\triangleleft k} F.$$

Combining these two transitions according to (nREC2), we have the following transition of $E \parallel F$*:*

$$E \parallel F \xrightarrow{(x,\{(0.5,l)\})\triangleleft k} \{0.5 : \lfloor p' \rfloor_l \parallel F, 0.5 : E \parallel F\}.$$

Obviously, although that the value of $Pro(l \longmapsto k)$ *is unknown in* E*, it is known in* F*, hence it is also known in* $E \parallel F$*. When putting* E *and* F *in parallel, the resulting distribution* μ *will be updated by substituting* $\theta_{l \longmapsto k}$ *with probability 0.5.*

Rule (nMOB) indicates that the connectivity information in a network can be changed according to the PMF $\mathcal{M}$ parameterizing the semantics. This rule is novel which makes our mobility model different from the previous mobility models, for instance the mobility model adopted in (65, 67, 68). The usage of rule (nMOB) is shown in the following example.

Example 3. *Suppose we have a network* E *with* $E(l,k) = 0.8$ *and we also know from the given* PMF $\mathcal{M}$ *that*

$$\mathcal{M}(l,k,0.8,0.9) = 0.3,$$

$$\mathcal{M}(l,k,0.8,0.7) = 0.2,$$

$$\mathcal{M}(l,k,0.8,0.8) = 0.5,$$

then we have the derivation in Fig. 2.4 with $E_1(l,k) = 0.9$*,* $E_2(l,k) = 0.7$*.*

Rule (nSYN) deals with synchronization and broadcast, in that a network can broadcast a message to any neighbor network where each node may receive with a certain probability. For the same reason as in (nREC2), the location connectivity set

in the resulting action is the union of the two location connectivity sets in the synchronizing actions. Rule (nOPEN) is similar as Rules (pOPEN1) and (pOPEN2) in Table 2.4 dealing with name restriction. Rule (nPAR) means that two networks in parallel can execute independently, in our calculus only the internal action τ need not to be synchronized with others. Rule (nPRO1) explains how a connectivity network adds its information of how nodes at destinations will receive messages with a certain probability to the semantics. Since according to (nREC2) and (nSYN), these information will be propagated until all the other networks in parallel get notified. On the other hand, (nPRO2) shows that a network only containing connectivity information of a certain location cannot offer connectivity information of other locations. In this case it is still able to perform a reception but with empty connectivity information, otherwise we may block the execution of a network, refer to the following example.

Example 4. *Let*

$$E = \lfloor \langle x \rangle \cdot p \rfloor_l,$$

$$F = \{\{(0.5, m)\} \longmapsto n\}$$

such that $l \neq n$. *According to (nBRD), we have* $E \xrightarrow{\langle x,\emptyset\rangle@l} \lfloor p \rfloor_l$. *If we do not have Rule (nPRO2),* F *can only perform a reception emitting from* n *i.e.*

$$F \xrightarrow{(x,\{(0.5,m)\})\lhd n} F,$$

thus (nSYN) cannot be applied, and the $E \parallel F$ *will not be able to perform a broadcast from* l *which is for sure not what we expect. By introducing (nPRO2), we have* $F \xrightarrow{(x,\emptyset)\lhd l} F$, *and then Rule (nSYN) can be applied.*

As we mentioned before, we treat networks like $\lfloor (x) \cdot p \rfloor_l \parallel \lfloor (x) \cdot q \rfloor_l$ as a non well-formed network, since otherwise according to Table 2.2 and 2.4, the processes at l may not receive messages simultaneously. Refer to the following example.

Example 5. *Let*

$$E = \lfloor (x) \cdot p \rfloor_l \parallel \lfloor (x) \cdot q \rfloor_l,$$

then according to (pPRE) and (nREC1), we have the following two transitions:

$$\lfloor (x) \cdot p \rfloor_l \xrightarrow{(x,\emptyset)\lhd k} \{\theta_{l \longmapsto k} : \lfloor p \rfloor_l, (1 - \theta_{l \longmapsto k}) : \lfloor (x) \cdot p \rfloor_l\},$$

$$\lfloor (x) \cdot q \rfloor_l \xrightarrow{(x,\emptyset)\lhd k} \{\theta_{l \longmapsto k} : \lfloor q \rfloor_l, (1 - \theta_{l \longmapsto k}) : \lfloor (x) \cdot q \rfloor_l\}.$$

Table 2.5: Labeled transition system of networks (discrete).

$$\frac{p \xrightarrow{(x)} p'}{\lfloor p \rfloor_l \xrightarrow{(x,\emptyset)\lhd k} \{\theta_{l \longmapsto k} : \lfloor p' \rfloor_l, 1 - \theta_{l \longmapsto k} : \lfloor p \rfloor_l\}} \text{ (nREC1)}$$

$$\frac{E \xrightarrow{(x,\mathbb{L})\lhd l} \mu_1 \quad F \xrightarrow{(x,\mathbb{K})\lhd l} \mu_2}{E \parallel F \xrightarrow{(x,\mathbb{L}\cup\mathbb{K})\lhd l} (\mu_1 \bullet \mathcal{D}_l(F)) \parallel (\mu_2 \bullet \mathcal{D}_l(E))} \text{ (nREC2)}$$

$$\frac{}{\{\{(\rho, l)\} \longmapsto k\} \xrightarrow{\tau} \{\mathcal{M}(l, k, \rho, \rho') : \{\{(\rho', l)\} \longmapsto k\}\}} \text{ (nMOB)}$$

$$\frac{E \xrightarrow{\nu\tilde{y}\langle y,\mathbb{L}\rangle@l} \mu_1 \quad F \xrightarrow{(x,\mathbb{K})\lhd l} \mu_2 \quad \tilde{y} \cap (\{x\} \cup fn(F)) = \emptyset}{E \parallel F \xrightarrow{\nu\tilde{y}\langle y,\mathbb{L}\cup\mathbb{K}\rangle@l} ((\mu_1 \bullet \mathcal{D}_l(F)) \parallel (\mu_2\{y/x\} \bullet \mathcal{D}_l(E)))} \text{ (nSYN)}$$

$$\frac{p \xrightarrow{\tau} p'}{\lfloor p \rfloor_l \xrightarrow{\tau} \lfloor p' \rfloor_l} \text{ (nTAU)} \qquad \frac{E \xrightarrow{\langle x,\mathbb{L}\rangle@l} \mu}{\nu x E \xrightarrow{\nu x\langle x,\mathbb{L}\rangle@l} \mu} \text{ (nOPEN)}$$

$$\frac{E \xrightarrow{\tau} \mu}{E \parallel F \xrightarrow{\tau} \mu \parallel F} \text{ (nPAR)} \qquad \frac{E \xrightarrow{\alpha} \mu \quad x \notin fn(\alpha)}{\nu x E \xrightarrow{\alpha} \nu x \mu} \text{ (nRES)}$$

$$\frac{p \xrightarrow{\nu\tilde{x}\langle x\rangle} p'}{\lfloor p \rfloor_l \xrightarrow{\nu\tilde{x}\langle x,\emptyset\rangle@l} \lfloor p' \rfloor_l} \text{ (nBRD)} \qquad \frac{}{\{\mathbb{K} \longmapsto k\} \xrightarrow{(x,\mathbb{K})\lhd k} \{\mathbb{K} \longmapsto k\}} \text{ (nPRO1)}$$

$$\frac{E \equiv F \xrightarrow{\alpha} \mu_2 \equiv \mu_1}{E \xrightarrow{\alpha} \mu_1} \text{ (nSTR)} \qquad \frac{l \neq k}{\{\mathbb{K} \longmapsto k\} \xrightarrow{(x,\emptyset)\lhd l} \{\mathbb{K} \longmapsto k\}} \text{ (nPRO2)}$$

By applying (nREC2) E has a transition as follows:

$$E \xrightarrow{(x,\emptyset)\lhd k} = \begin{cases} \theta_{l \longmapsto k} \cdot \theta_{l \longmapsto k} & : \lfloor p \rfloor_l \parallel \lfloor q \rfloor_l, \\ \theta_{l \longmapsto k} \cdot (1 - \theta_{l \longmapsto k}) & : \lfloor p \rfloor_l \parallel \lfloor (x) \cdot q \rfloor_l, \\ (1 - \theta_{l \longmapsto k}) \cdot \theta_{l \longmapsto k} & : \lfloor (x) \cdot p \rfloor_l \parallel \lfloor q \rfloor_l, \\ (1 - \theta_{l \longmapsto k}) \cdot (1 - \theta_{l \longmapsto k}) & : E \end{cases}$$

Obviously, in the networks $\lfloor p \rfloor_l \parallel \lfloor (x) \cdot q \rfloor_l$ and $\lfloor (x) \cdot p \rfloor_l \parallel \lfloor q \rfloor_l$, the processes $(x) \cdot p$ and $(x) \cdot q$ did not receive messages even that they are located at the same location l. This

is against our intuition, and should be avoided.

The following is a more complicated example to illustrate how the rules in Table 2.4 and 2.5 can be used.

Example 6. *Assume there is a network* $E = E_1 \parallel E_2 \parallel E_3$ *where*

$$\begin{aligned} E_1 &= \lfloor \langle y \rangle \cdot p \rfloor_l, \\ E_2 &= \lfloor (x) \cdot \langle x \rangle \rfloor_k \parallel \{\{(0.6, k)\} \longmapsto l\}, \\ E_3 &= \lfloor (x).\langle x \rangle \rfloor_m \parallel \{\{(0.8, m)\} \longmapsto l\}. \end{aligned}$$

Intuitively, we have that after the node at location l *has broadcasted the message* y*,* E *will evolve into a distribution* μ *where the probability for both nodes at locations* k *and* m *receiving* y *is* $0.6 \cdot 0.8 = 0.48$*, the probability of only the node at location* k *receiving* y *is* $0.6 \cdot (1 - 0.8) = 0.12$ *and so on. We show how to obtain* μ *based on the labeled transition system in Table 2.4 and 2.5.*

$$\frac{(x).\langle x \rangle \xrightarrow{(x)} \langle x \rangle \quad (pPRE)}{\lfloor (x).\langle x \rangle \rfloor_k \xrightarrow{(x,\emptyset) \lhd l} \{(\theta_{k \longmapsto l} : \lfloor \langle x \rangle \rfloor_k), (1 - \theta_{k \longmapsto l} : \lfloor (x).\langle x \rangle \rfloor_k)\}} \; (nREC1)$$

$$\frac{\{\{(0.6, k)\} \longmapsto l\} \xrightarrow{(x,\{(0.6,k)\}) \lhd l} \{\{(0.6, k)\} \longmapsto l\} \quad (nPRO1)}{E_2 \xrightarrow{(x,\{(0.6,k)\}) \lhd l} \{(0.6 : \lfloor \langle x \rangle \rfloor_k \parallel \{\{(0.6, k)\} \longmapsto l\}), (0.4 : E_2)\}} \; (nREC2)$$

Similarly, for E_3 *we have the following transition.*

$$\frac{(x).\langle x \rangle \xrightarrow{(x)} \langle x \rangle \quad (pPRE)}{\lfloor (x).\langle x \rangle \rfloor_m \xrightarrow{(x,\emptyset) \lhd l} \{(\theta_{m \longmapsto l} : \lfloor \langle x \rangle \rfloor_m), (1 - \theta_{m \longmapsto l} : \lfloor (x).\langle x \rangle \rfloor_m)\}} \; (nREC1)$$

$$\frac{\{\{(0.8, m)\} \longmapsto l\} \xrightarrow{(x,\{(0.8,m)\}) \lhd l} \{\{(0.8, m)\} \longmapsto l\} \; (nPRO1)}{E_3 \xrightarrow{(x,\{(0.8,m)\}) \lhd l} \{(0.8 : \lfloor \langle x \rangle \rfloor_m \parallel \{\{(0.8, m)\} \longmapsto l\}), (0.2 : E_3)\}} \; (nREC2)$$

By combing transitions of E_2 *and* E_3*, we get the following transition according to (nREC2):* $E_2 \parallel E_3 \xrightarrow{(x,\{(0.6,k),(0.8,m)\}) \lhd l}$

$$\left\{ \begin{array}{l} 0.6 \cdot 0.8 : \lfloor \langle x \rangle \rfloor_k \parallel \lfloor \langle x \rangle \rfloor_m \parallel \{\{(0.6, k), (0.8, m)\} \longmapsto l\} \\ 0.6 \cdot 0.2 : \lfloor \langle x \rangle \rfloor_k \parallel \{\{(0.6, k)\} \longmapsto l\} \parallel E_3 \\ 0.4 \cdot 0.8 : E_2 \parallel \lfloor \langle x \rangle \rfloor_m \parallel \{\{(0.8, m)\} \longmapsto l\} \\ 0.4 \cdot 0.2 : E_2 \parallel E_3 \end{array} \right\} \equiv \mu$$

Finally, we get the following transition of E.

$$\dfrac{\dfrac{\langle y\rangle.p \xrightarrow{\langle y\rangle} p \ (pPRE)}{E_1 \xrightarrow{\langle y,\emptyset\rangle@l} \lfloor p\rfloor_l}\ (nBRD) \qquad E_2 \parallel E_3 \xrightarrow{(x,\{(0.6,k),(0.8,m)\})\triangleleft l} \mu \ (nREC2)}{E \xrightarrow{\langle y,\{(0.6,k),(0.8,m)\}\rangle@l} \lfloor p\rfloor_l \parallel \mu\{y/x\}}\ (nSYN)$$

2.4 Weak (Probabilistic) Bisimulation

Similarly as in Section 2.3 where we define the semantics of processes and networks separately, in this section we will first define weak bisimulations for processes and then later for networks.

2.4.1 Weak Bisimulation

Bellow follows the definition of weak bisimulation for processes where we let $\stackrel{\tau}{\Longrightarrow}$ denote $(\stackrel{\tau}{\rightarrow})^*$ representing an arbitrary number (including 0) of τ actions in sequence. We define

$$\stackrel{\alpha}{\Longrightarrow} = \stackrel{\tau}{\Longrightarrow}\stackrel{\alpha}{\rightarrow}\stackrel{\tau}{\Longrightarrow}$$

provided that $\alpha \neq \tau$.

Definition 2 (Weak Process Bisimulation)**.** *An equivalence relation $\mathcal{R} \subseteq \mathcal{P} \times \mathcal{P}$ is a weak process bisimulation if $p\ \mathcal{R}\ q$ implies that whenever $p \xrightarrow{\alpha_p} p'$ then:*

1. *if $\alpha_p = (x)$ or $y(x)$ then there exists $q \stackrel{\alpha_p}{\Longrightarrow} q'$ such that $p'\{z/x\}\ \mathcal{R}\ q'\{z/x\}$ for each $z \in \mathcal{N}$;*
2. *otherwise there exists $q \stackrel{\alpha_p}{\Longrightarrow} q'$ such that $p'\ \mathcal{R}\ q'$.*

Two processes p and q are weakly bisimilar, written as $p \approx q$, if there exists a weak process bisimulation $\mathcal{R}$ such that $p\ \mathcal{R}\ q$.

Definition 2 is a conservative extension of the weak bisimulation defined in (69). Clause 1 says that whenever p can perform an input or reception, q should be able to mimic it by performing the same action via a weak transition. Since in principle the received message x can be any one in $\mathcal{N}$, p and q are weakly bisimilar if they behave the same no matter which message is received, thus the resulting processes p' and q' should be in $\mathcal{R}$ under each substitution. Clause 2 is similar except we do not need to consider all the possible substitution since no bound name appears in this case.

As usual we first prove the following lemma in order to prove the congruence of $\approx$.

Lemma 1. *1.* $p \xrightarrow{\nu x\langle x\rangle} p'$ *iff* $p \equiv \nu x q$ *and* $q \xrightarrow{\langle x\rangle} p'$*;*

2. $p \xrightarrow{\nu xy\langle x\rangle} p'$ *iff* $p \equiv \nu x q$ *and* $q \xrightarrow{y\langle x\rangle} p'$ *where* $y \neq x$*.*

Proof. The *only if* direction follows by induction in the latest inference of $p \xrightarrow{\alpha_p} p'$ and the *if* direction is due to (pSTR), (pOPEN1), and (pOPEN2) of the transition system. □

The following theorem shows that the weak process bisimulation is a congruence.

Theorem 1. $\approx$ *is a congruence.*

Proof. To prove Theorem 1, it is sufficient to prove that $p \approx q$ implies:

- $Act.p \approx Act.q$;
- $[x = y]p, r \approx [x = y]q, r$;
- $[x = y]r, p \approx [x = y]r, q$;
- $\nu x p \approx \nu x q$;
- $p \parallel r \approx q \parallel r$.

We take the last two cases as an example, and prove the following set

$$\mathcal{R} = \{(\nu\tilde{x}(p \parallel r), \nu\tilde{x}(q \parallel r)) \mid p \approx q\}$$

to be a weak bisimulation. Let

$$p_0 \equiv \nu\tilde{x}(p \parallel r) \text{ and } q_0 \equiv \nu\tilde{x}(q \parallel r),$$

obviously $(p_0, q_0) \in \mathcal{R}$. Suppose $p_0 \xrightarrow{\alpha_p} p_0'$, we analyze by cases as follows:

- $\alpha_p = \langle y\rangle$, $y \notin \tilde{x}$. By (pBRD) we have
  - $p \xrightarrow{\langle y\rangle} p'$ and $r \xrightarrow{(x)} r'$. Since $p \approx q$, we have $q \xrightarrow{\langle y\rangle} q'$ and $p' \approx q'$. By (pBRD)

    $$\nu\tilde{x}(q \parallel r) \xrightarrow{\langle y\rangle} \nu\tilde{x}(q' \parallel r'\{y/x\})$$

    and clearly

    $$\nu\tilde{x}(p' \parallel r'\{y/x\}) \ \mathcal{R} \ \nu\tilde{x}(q' \parallel r'\{y/x\});$$

– $p \xrightarrow{(x)} p'$ and $r \xrightarrow{\langle y \rangle} r'$. Since $p \approx q$, we have $q \xrightarrow{(x)} q'$ and

$$p'\{z/x\} \approx q'\{z/x\}$$

for any $z \in \mathcal{N}$. By (pBRD)

$$\nu\tilde{x}(q \parallel r) \xrightarrow{\langle y \rangle} \nu\tilde{x}(q'\{y/x\} \parallel r')$$

and clearly

$$\nu\tilde{x}(p'\{y/x\} \parallel r') \; \mathcal{R} \; \nu\tilde{x}(q'\{y/x\} \parallel r').$$

- $\alpha_p = \nu y\langle y \rangle$, $y \in \tilde{x}$. Then $p_0 \equiv \nu y \nu(\tilde{x} \setminus \{y\})(p' \parallel r')$, the following proof is similar to the one above.

- $\alpha_p = \nu y\langle y \rangle$, $y \notin \tilde{x}$. By (pBRD) we have

  – $p \xrightarrow{\nu y\langle y \rangle} p'$ and $r \xrightarrow{(x)} r'$. Since $p \approx q$, we have $q \xrightarrow{\nu y\langle y \rangle} q'$ and $p' \approx q'$. By (pBRD) and (pRES)

  $$\nu\tilde{x}(q \parallel r) \xrightarrow{\nu y\langle y \rangle} \nu\tilde{x}(q' \parallel r'\{y/x\})$$

  where $y \notin (\tilde{x} \cup fn(r))$, and clearly

  $$\nu\tilde{x}(p' \parallel r'\{y/x\}) \; \mathcal{R} \; \nu\tilde{x}(q' \parallel r'\{y/x\}).$$

  – $p \xrightarrow{(x)} p'$ and $r \xrightarrow{\nu y\langle y \rangle} r'$. Since $p \approx q$, we have $q \xrightarrow{(x)} q'$ and

  $$p'\{z/x\} \approx q'\{z/x\}$$

  for any $z \in \mathcal{N}$. By (pBRD) and (pRES)

  $$\nu\tilde{x}(q \parallel r) \xrightarrow{\nu y\langle y \rangle} \nu\tilde{x}(q'\{y/x\} \parallel r')$$

  where $y \notin (\tilde{x} \cup fn(p) \cup fn(q))$, and clearly

  $$\nu\tilde{x}(p'\{y/x\} \parallel r') \; \mathcal{R} \; \nu\tilde{x}(q'\{y/x\} \parallel r').$$

- the other cases are similar and are omitted here.

□

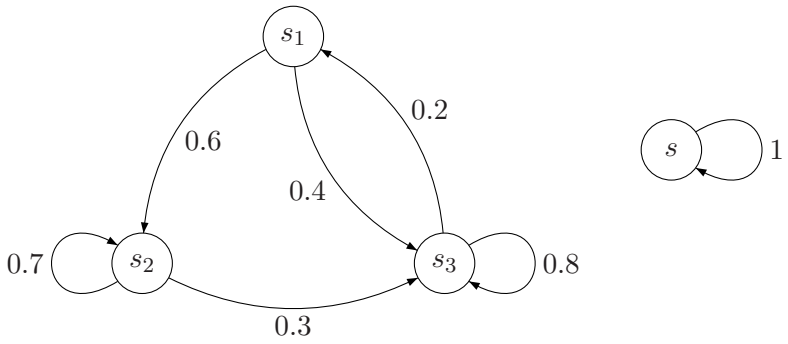

Figure 2.5: Two weakly bisimilar states in fully probabilistic processes.

Before we introduce the definitions of weak bisimulation of networks, we first give some definitions from graph theory which will be used in the following. A subgraph SG of $G_{l\longmapsto k}$ is called *strongly connected* if for each pair (ρ, ρ') of states in SG there exists a path fragment $\rho_0\rho_1 \ldots \rho_i$ of nodes in SG and $\mathcal{M}(l, k, \rho_j, \rho_{j+1}) > 0$ for $0 \leq j < i$ with $\rho = \rho_0$ and $\rho' = \rho_i$. A *strongly connected component* (SCC) denotes a strongly connected subgraph such that no proper superset of it is strongly connected. A *bottom* SCC (BSCC) is a SCC from which no state outside this SCC is reachable. If probabilities are in the same BSCC, like for instance the nodes 0.6, 0.8 and, 0.9 in Fig. 2.3, they can for sure evolve into each other, or in probabilistic terms, they can evolve into each other eventually with probability 1.

In our weak bisimulation equivalence, we as usual abstract from internal steps which in our case also involve the probabilistic mobility steps changing connection probabilities. In order to capture that a connection probability for sure (with probability 1) can evolve into another, we introduce the relation $\rightarrow$. Let $\rightarrow$ be the least relation closed by parallel composition, restriction and structural congruence such that

$$\{\{(\rho, l)\} \longmapsto k\} \rightarrow \{\{(\rho', l)\} \longmapsto k\}$$

if ρ and ρ' belong to a BSCC of $G_{l\longmapsto k}$. Intuitively, we abstract from immediate mobility steps (probably infinitely many), and thus make the mobility rule simpler. This is inspired by the weak bisimulation defined on fully probabilistic processes in (24), we illustrate this by an example as follows:

Example 7. *Consider the fours states s_1, s_2, s_3, and s in Fig. 2.5, suppose we assume that they satisfy the same properties, for instance they can satisfy the same set of*

atomic propositions. Then according to the weak bisimulation in (24), we can prove that s_1, s_2, s_3, *and* s *are all weakly bisimilar. Recalling that* s_1, s_2, s_3, *and* s *are equivalent, now consider the mobility rule of some connection* $Pro(l \longmapsto k)$ *in Fig. 2.3 which can be seen as a fully probabilistic process. If we consider the states 0.6, 0.8, and 0.9 satisfy the same property at which the node at* l *can receive messages from* k *with probability 0.6, 0.8, or 0.9, then we can simplify the mobility rule by replacing states 0.6, 0.8, and 0.9 and their correspondent transitions with a single state with self loop of probability 1. At the new state the property is held i.e. the node at* l *can receive messages from* k *with probability 0.6, 0.8, or 0.9. This is exactly the same as allowing* $\{\{(\rho, l)\} \longmapsto k\} \to \{\{(\rho', l)\} \longmapsto k\}$ *for any* $\rho, \rho' \in \{0.6, 0.8, 0.9\}$.

Following (1) we define the weak transition $\stackrel{\alpha}{\Longrightarrow}$ as follows:

Definition 3 (Weak Transition)**.** *We use* $E \stackrel{\alpha}{\Longrightarrow} \mu$ *to denote that a distribution* μ *is reached through a sequence of steps some of which are internal. Formally* $\stackrel{\alpha}{\Longrightarrow}$ *is the least relation such that,* $E \stackrel{\alpha}{\Longrightarrow} \mu$ *iff either*

1. $\alpha = \tau$ *and* $\mu = \delta_E$, *or*
2. $E \stackrel{\alpha}{\rightarrow} \mu$, *or*
3. *there exists a transition* $E \stackrel{\beta}{\rightarrow} \mu'$ *such that*

$$\mu = \sum_{E' \in Supp(\mu')} \mu'(E') \cdot \mu_{E'}$$

where $E' \stackrel{\tau}{\Longrightarrow} \mu_{E'}$ *if* $\beta = \alpha$, *otherwise* $E' \stackrel{\alpha}{\Longrightarrow} \mu_{E'}$ *and* $\beta = \tau$.

Clause 1 says that a weak τ transition can be an empty sequence, and the resulting distribution is δ_E. Clause 2 indicates that the set of strong transitions is a subset of the weak transitions, the distribution μ can be reached without going through any intermediate networks. Clause 3 means that E can first evolve into μ' via a transition labeled with β, and then each network E' in the support of μ' will continue evolving into $\mu_{E'}$ via weak transition labeled with τ if $\beta = \alpha$, otherwise via weak transition labeled with α if $\beta = \tau$.

According to Rule (nREC1) in Table 2.5, there might occur unknown probabilities during the evolution of networks, since a network may not always contain enough connectivity information to resolve them. Therefore before introducing the weak bisimulation we need to resolve all the possible unknown probabilities. In order to do so, we introduce the following definition:

Definition 4. *Let* $\propto: \mathscr{N} \times \mathscr{C} \to \mathscr{N}$ *be defined inductively as follows:*

1. $E \propto C = E$ *if* $C = 0$,
2. $E \propto C = (E \propto C_1) \propto C_2$ *if* $C = C_1 \parallel C_2$,
3. $E \propto C = E$ *if* $C = \{\{(\rho, k)\} \longmapsto l\}$ *and* $E(k,l) \neq \theta_{k \longmapsto l}$,
4. $E \propto C = E \parallel \{\{(\rho, k)\} \longmapsto l\}$ *if* $C = \{\{(\rho, k)\} \longmapsto l\}$ *and* $E(k,l) = \theta_{k \longmapsto l}$,

for any E *and* C *where we write* $E \propto C$ *instead of* $\propto (E, C)$.

Intuitively, $E \propto C$ denotes a network behaving like E but obtaining new information from C. Clause 1 is trivial, since if the second parameter is 0, E can obtain no connectivity information from it, thus will stay unchanged. Clause 2 means that if we supply E with connectivity network $C \parallel C'$, then it makes no difference if we supply E with C first, and then C'. Since according to the well-formed condition, the connectivity information in C and C' is disjoint. If the given connectivity information has already known in E, it will simply be ignored by E which is shown in Clause 3, otherwise in Clause 4 the connectivity information will be adopted by E. The following example illustrates how $\propto$ works.

Example 8. *Let*

$$E = \lfloor p \rfloor_l \parallel \{\{(0.6, l)\} \longmapsto k\},$$

$$C = \{\{(0.8, l)\} \longmapsto k\} \parallel \{\{(0.5, m)\} \longmapsto n\}.$$

Since C *contains connectivity information for both* $Pro(l \longmapsto k)$ *and* $Pro(m \longmapsto n)$, *after applying* $\propto$ *with parameter* C *to* E, E *should be able to obtain the connectivity information of* $Pro(m \longmapsto n)$ *from* C, *and ignore the connectivity information of* $Pro(l \longmapsto k)$ *since it has been known in* E. *We show how* $\propto$ *can do so step by step according to Definition 4:*

$$\begin{aligned} E \propto C &= (E \propto \{\{(0.8, l)\} \longmapsto k\}) \propto \{\{(0.5, m)\} \longmapsto n\} && \textit{Clause 2} \\ &= E \propto \{\{(0.5, m)\} \longmapsto n\} && \textit{Clause 3} \\ &= E \parallel \{\{(0.5, m)\} \longmapsto n\} && \textit{Clause 4} \end{aligned}$$

Let

$$\mathscr{C}_L = \{C \in \mathscr{C} \mid \forall k, l.(l, k \in L \text{ iff } C(k,l) \neq \theta_{k \longmapsto l})\}$$

be the subset of $\mathscr{C}$ which comprises all the connectivity networks C such that for all $l, k \in L$, $C(k,l) \neq \theta_{k \longmapsto l}$. Here C is constrained since it contains no extra connectivity information beyond that for pairs in L, this condition guarantees that $\mathscr{C}_L$ is finite whenever L is finite. Refer to the following example:

Example 9. *Suppose that the mobility rule of* $Pro(l \longmapsto k)$ *is given by Fig. 2.2, and* $Pro(k \longmapsto l)$ *is always equal to 1. Let* $L = \{l, k\}$*, then* $\mathscr{C}_L$ *should be comprised of the networks which only contain connectivity information of* $Pro(l \longmapsto k)$ *and* $Pro(k \longmapsto l)$*, i.e.*

$$\mathscr{C}_L = \left\{ \begin{array}{l} \{\{(0.6, l)\} \longmapsto k\} \parallel \{\{(1, k)\} \longmapsto l\}, \\ \{\{(0.7, l)\} \longmapsto k\} \parallel \{\{(1, k)\} \longmapsto l\}, \\ \{\{(0.9, l)\} \longmapsto k\} \parallel \{\{(1, k)\} \longmapsto l\} \end{array} \right\}$$

If we do not require that the networks in $\mathscr{C}_L$ *to be the smallest ones, then networks like*

$$\{\{(0.6, l)\} \longmapsto k\} \parallel \{\{(1, k), (\rho, m)\} \longmapsto l\}$$

for some ρ *and* m *will also be in* $\mathscr{C}_L$*, which makes* $\mathscr{C}_L$ *infinite even that* L *is finite.*

Let $C_{E,F,k}$ range over $\mathscr{C}_{(l(E) \cup l(F) \cup \{k\})}$. According to (nREC1) and (nREC2) in Table 2.5, when $E \xrightarrow{(x, \mathbb{K}) \lhd k} \mu$, there might be unknown probabilities in μ where all the unknown probabilities are of the form of $\theta_{l \longmapsto k}$ with $l \in loc(E)$. Note that $loc(E) \subseteq l(E)$, therefore we can make sure that no unknown probability will appear after $E \propto C_{E,F,k}$ performing receptions from k. Similarly, when $E \xrightarrow{\langle x, \mathbb{L} \rangle @ m} \mu$, the unknown probabilities which might appear in μ are of the form $\theta_{n \longmapsto m}$ such that $n \in loc(E)$. Additionally, it must be the case that $m \in loc(E)$ according to (nBRD) and (nSYN), thus no unknown probability shows up after $E \propto C_{E,F,k}$ performing broadcast actions. The same arguments apply to F too, thus we can guarantee that all the unknown probabilities will be eliminated after applying $\propto$ with parameter $C_{E,F,k}$ to E and F, provided that we only consider reception actions from k.

Below follows the definition of weak bisimulation of networks.

Definition 5 (Weak Bisimulation)**.** *An equivalence relation* $\mathcal{R} \subseteq \mathscr{N} \times \mathscr{N}$ *is a weak bisimulation if* $E \mathcal{R} F$ *implies that for each* $k \in L$ *and* $C_{E,F,k}$ *whenever* $E \propto C_{E,F,k} \xrightarrow{\alpha} \mu_1$ *then:*

1. *if* $\alpha = (x, \mathbb{L}) \lhd k$*, then there exists* $F \propto C_{E,F,k} \stackrel{\alpha}{\Longrightarrow} \mu_2$ *such that for each* $y \in \mathcal{N}$*,* $\mu_1\{y/x\} \mathcal{R} \mu_2\{y/x\}$*;*

2. *if* $\alpha = \nu\tilde{x}\langle x, \mathbb{L}\rangle@l$, *then there exists* $F \propto C_{E,F,k} \xrightarrow{\nu\tilde{x}\langle x,\mathbb{L}\rangle@m} \mu_2$ *such that* $\mu_1 \; \mathcal{R} \; \mu_2$;

3. *if* $\alpha = \tau$, *then there exists* $F \propto C_{E,F,k} \stackrel{\tau}{\Longrightarrow} \mu_2$ *such that* $\mu_1 \; \mathcal{R} \; \mu_2$.

Two networks E *and* F *are weakly bisimilar, written as* $E \approx^{\mathcal{M}} F$, *if* $E \; \mathcal{R} \; F$ *for some weak bisimulation* $\mathcal{R}$.

Clause 1 requires that if nodes at locations $l(\mathbb{L})$ in network E can receive a message from location k with specific probabilities, then nodes at locations $l(\mathbb{L})$ in F must be able to receive the same message from the location k with the same probability. Since k might be any location, and in particular one not appearing in either E or F, the resulting distributions μ_1 and μ_2 may risk containing unknown probabilities. These unknown probabilities can only be of the form $\theta_{l \longmapsto k}$ where $l \in l(E) \cup l(F)$ which justifies that $C_{E,F,k}$ is enough to substitute all the unknown probabilities. Clause 2 means that if E can broadcast a message from the node at location l with receivers at locations $l(\mathbb{L})$, then F can also broadcast the same message from the node at location m to $l(\mathbb{L})$ with the same probabilities, m is not required to be the same as l i.e. we abstract from the emitters of broadcast actions. Clause 3 deals with internal actions and is standard except for the use of $C_{E,F,k}$.

The following example illustrates how we can obtain connectivity information from the given PMF.

Example 10. *Suppose the mobility of* $Pro(k \longmapsto l)$ *is explicitly defined by Fig. 2.3, then* $\{\{(0.7, k)\} \mapsto l\} \not\approx^{\mathcal{M}} 0$ *since by Definition 5,*

$$\{\{(0.7, k)\} \mapsto l\} \approx^{\mathcal{M}} 0 \text{ iff } \{\{(0.7, k)\} \mapsto l\} \approx^{\mathcal{M}} \{\{(\rho, k)\} \mapsto l\}$$

for any $\rho \in G_{k \mapsto l} = \{0.5, 0.6, 0.7, 0.8, 0.9\}$, *which obviously does not hold. But if the mobility of* $Pro(k \mapsto l)$ *is implicitly defined, then we know* $\{\{(\rho, k)\} \mapsto l\} \approx^{\mathcal{M}} 0$ *where* ρ *is 0 or 1, since* $Pro(k \mapsto l)$ *will be either 1 or 0.*

According to Clause 2 in Definition 5, two broadcast actions are not distinguishable if the only difference is their emitters. Therefore if two locations have the same mobility, and the processes located at them are weakly bisimilar, then the two nodes are also weakly bisimilar.

Example 11. *Suppose that* $\mathcal{M}$ *is a* PMF *where all the connections have implicit mobility, then for all locations* l *and* k, $\lfloor p \rfloor_l \approx^{\mathcal{M}} \lfloor q \rfloor_k$ *provided that* $p \approx q$, *since* l

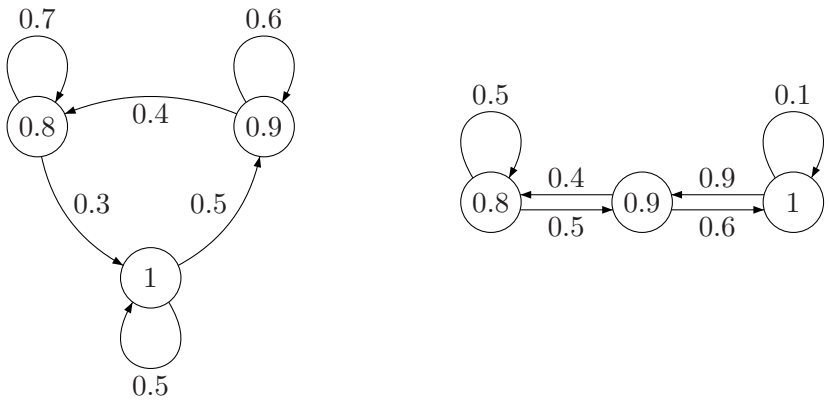

Figure 2.6: Two equivalent mobility.

and k have the same mobility rules. Furthermore if there is a location m such that the mobility of $Pro(m \longmapsto l)$ and $Pro(m \longmapsto k)$ is not implicitly defined, but is given by Fig. 2.6 (a) and (b) respectively, then still we have $\lfloor p \rfloor_l \approx^{\mathcal{M}} \lfloor q \rfloor_k$ provided that $p \approx q$. Since for any $C_1, C_2 \in \mathscr{C}$ such that $C_1(m,l) \neq \theta_{m \longmapsto l}$ and $C_2(m,k) \neq \theta_{m \longmapsto k}$, whenever $C_1(m,l) = \rho$ with $\rho \in \{0.8, 0.9, 1\}$, there exists C_2' such that $C_2 \to C_2'$ and $C_2'(m,k) = \rho$, i.e. we can always make sure that the node at m can receive messages from l and k with the same probability.

In general if the node at m can always receive messages from or broadcast messages to l and k with the same probability, then l and k have the same mobility, thus the following result holds:

$$p \approx q \text{ implies } \lfloor p \rfloor_l \approx^{\mathcal{M}} \lfloor q \rfloor_k.$$

Observe that in Definition 5, it is necessary to take the $C_{E,F,k}$ into account, otherwise we would obtain a more restrict weak bisimulation. After applying $\propto$ with parameter $C_{E,F,k}$ we can make sure that

$$E \propto C_{E,F,k}(m,n) = \theta_{m \mapsto n} \text{ iff } F \propto C_{E,F,k}(m,n) = \theta_{m \mapsto n},$$

i.e. if a connection probability is unknown in $E \propto C_{E,F,k}$, then it is also unknown in $F \propto C_{E,F,k}$ and vice versa. Refer to the following example.

Example 12. *Consider two networks:*

$$E = \lfloor \langle x \rangle \rfloor_l \parallel \{\{(1,k)\} \mapsto l\} \text{ and } F = \lfloor \langle x \rangle \rfloor_l$$

and assume all the mobility rules are implicitly defined. If we do not consider $C_{E,F,k}$*, then we will conclude that* $E \not\approx^{\mathcal{M}} F$ *since* $E \xrightarrow{\langle x,\{(1,k)\}\rangle@l}$ *which cannot be simulated by* F*. But intuitively, this is wrong, since from both* E *and* F *all other locations can receive the message* x *from* l *with probability 1 or 0. By taking* $C_{E,F,k}$ *into consideration, we can easily check that* E *and* F *are weakly bisimilar.*

The following lemma related to bound names is used to prove the congruence of $\approx^{\mathcal{M}}$.

Lemma 2. $E \xRightarrow{\nu x\langle x,\mathbb{L}\rangle@l} \mu$ *iff* $E \equiv \nu x E'$ *and* $E' \xRightarrow{\langle x,\mathbb{L}\rangle@l} \mu$.

Proof. The *only if* direction follows by induction in the latest inference of $E \xrightarrow{\alpha} \mu$ and the *if* direction is due to (nSTR) and (nOPEN) of the transition system. □

Let $\mu \propto C = \{(\rho : E \propto C) \mid \mu(E) = \rho\}$, the following lemma shows that we can always associate extra connectivity information to networks while preserving the bisimulation equivalence.

Lemma 3. $E \propto C \approx^{\mathcal{M}} F \propto C$ *for any* C *provided that* $E \approx^{\mathcal{M}} F$.

Proof. We prove by structural induction on E and F. The base case is trivial. Let $E' = E \propto C$ and $F' = F \propto C$. Now assume that

$$E' \propto C_{E',F',l} \xrightarrow{(x,\mathbb{L})\triangleleft l} \mu_1'$$

for some $C_{E',F',l}$, then we need to prove that there exists

$$F' \propto C_{E',F',l} \xRightarrow{(x,\mathbb{L})\triangleleft l} \mu_2'$$

such that

$$\mu_1'\{y/x\} \approx^{\mathcal{M}} \mu_2'\{y/x\}$$

for any $y \in \mathcal{N}$. It is not hard to see that for each $C_{E',F',l}$, there exists $C_{E,F,l}$ and C' such that

$$E' \propto C_{E',F',l} \equiv E \propto C_{E,F,l} \propto C'$$

and

$$F' \propto C_{E',F',l} \equiv F \propto C_{E,F,l} \propto C'.$$

Note that by definition of $C_{E,F,l}$, $E \propto C_{E,F,l}$ contains enough connectivity information to resolve the unknown probability which may appear after performing $(x,\mathbb{L}) \triangleleft l$, as result

$$E \propto C_{E,F,l} \xrightarrow{(x,\mathbb{L}')\triangleleft l} \mu_1$$

such that $\mathbb{L}' \subseteq \mathbb{L}$ and $\mu_1 \propto C' \equiv \mu_1'$. Since $E \approx^{\mathcal{M}} F$, then there exists $F \propto C_{E,F,l} \xrightarrow{(x,\mathbb{L}')\triangleleft l} \mu_2$ such that

$$\mu_1\{y/x\} \approx^{\mathcal{M}} \mu_2\{y/x\}$$

for any $y \in \mathcal{N}$. As for any k,

$$(E \propto C_{E,F,l})(k,l) = \theta_{k\mapsto l} \text{ iff } (F \propto C_{E,F,l})(k,l) = \theta_{k\mapsto l},$$

so

$$(E \propto C_{E,F,l} \propto C')(k,l) = \theta_{k\mapsto l} \text{ iff } (F \propto C_{E,F,l} \propto C')(k,l) = \theta_{k\mapsto l}$$

for any k, therefore there exists $F' \propto C_{E',F',l} \xrightarrow{(x,\mathbb{L})\triangleleft l} \mu_2'$ such that $\mu_2 \propto C' \equiv \mu_2'$. By induction

$$(\mu_1 \propto C')\{y/x\} \approx^{\mathcal{M}} (\mu_2 \propto C')\{y/x\},$$

that is, $\mu_1'\{y/x\} \approx^{\mathcal{M}} \mu_2'\{y/x\}$ for any $y \in \mathcal{N}$. Other cases are similar and omitted here. □

Let $\approx^{\mathcal{M}}$ be the largest weak bisimulation, we show that:

Theorem 2. $\approx^{\mathcal{M}}$ *is a congruence.*

Proof. Let

$$\mathcal{D}(E) = \parallel_{l\in l(E)} \{\mathcal{D}_l(E) \mapsto l\}$$

as a network which only contains all the connection information of E.

It is sufficient to prove that

$$\mathcal{R} = \{(\nu\tilde{x}(E \parallel G), \nu\tilde{x}(F \parallel G)) \mid E \approx^{\mathcal{M}} F\}$$

is a weak bisimulation. Let $E_0 \equiv \nu\tilde{x}(E \parallel G)$, $F_0 \equiv \nu\tilde{x}(F \parallel G)$ and suppose

$$E_0 \propto C \xrightarrow{\alpha} \mu_0 \qquad (*)$$

Obviously, $E_0 \mathcal{R} F_0$. The proof is by analysis of the derivation of $(*)$. We write C as the abbreviation of $C_{E_0,F_0,l}$ in the following.

1. $\alpha = (x,\mathbb{L}) \triangleleft l$, $x \notin \tilde{x}$.

- Suppose
$$E_0 \propto C \xrightarrow{(x,\mathbb{L})\lhd l} \mu_0 \;\equiv\; \nu\tilde{x}(\mu_1 \parallel \mu_3 \parallel \mathcal{D}(E_0 \propto C)),$$
where μ_1 and μ_3 do not contain any connection information, hence we infer:
$$(E \parallel \mathcal{D}(G)) \propto C \xrightarrow{(x,\mathbb{L})\lhd l} \mu_1 \parallel \mathcal{D}(E_0 \propto C),$$
$$(G \parallel \mathcal{D}(E)) \propto C \xrightarrow{(x,\mathbb{L})\lhd l} \mu_3 \parallel \mathcal{D}(E_0 \propto C).$$
Since $E \;\approx^{\mathcal{M}}\; F$, then
$$(E \propto \mathcal{D}(G)) \propto C \;\approx^{\mathcal{M}}\; (F \propto \mathcal{D}(G)) \propto C$$
by Lemma 3. Note here
$$E \propto \mathcal{D}(G) \;\equiv\; E \parallel \mathcal{D}(G)$$
and
$$F \propto \mathcal{D}(G) \;\equiv\; F \parallel \mathcal{D}(G)$$
because E_0 is well-formed. Then we have
$$(E \parallel \mathcal{D}(G)) \propto C \;\approx^{\mathcal{M}}\; (F \parallel \mathcal{D}(G)) \propto C.$$
So
$$(F \parallel \mathcal{D}(G)) \propto C \xrightarrow{(x,\mathbb{L})\lhd l} \mu_2 \tag{2.2}$$
and $\mu_1 \parallel \mathcal{D}(E_0 \propto C)\{y/x\} \;\approx^{\mathcal{M}}\; \mu_2\{y/x\}$ for all $y \in \mathcal{N}$. Since
$$(G \parallel \mathcal{D}(E)) \propto C \xrightarrow{(x,\mathbb{L})\lhd l} \mu_3 \parallel \mathcal{D}(E_0 \propto C),$$
by (nREC2) we have
$$G' \xrightarrow{(x,\emptyset)\lhd l} \mu_3' \tag{2.3}$$
where $G \;\equiv\; G' \parallel \mathcal{D}(G)$ and $\mu_3 \;\equiv\; \mu_3' \bullet \mathbb{L}$ with $\mathbb{L} = \mathcal{D}_l(E_0 \propto C)$. Also
$$F_0 \propto C \;\equiv\; \nu\tilde{x}(G' \parallel ((F \parallel \mathcal{D}(G)) \propto C)),$$
so we can now combine transitions 2.2 and 2.3 using (nREC2) and (nRES), and obtain the following transition:
$$F_0 \propto C = \nu\tilde{x}(F \parallel G) \propto C \xrightarrow{(x,\mathbb{L})\lhd l} \nu\tilde{x}(\mu_2 \parallel \mu_3)$$
and $\nu\tilde{x}(\mu_1 \parallel \mu_3 \parallel \mathcal{D}(E_0 \propto C))\{y/x\} \;\mathcal{R}\; \nu\tilde{x}(\mu_2 \parallel \mu_3)\{y/x\}$.

- The other cases are similar.

2. $\alpha = \langle y, \mathbb{L}\rangle @ l$, $y \notin \tilde{x}$.

- Suppose $E_0 \propto C \xrightarrow{\langle y,\mathbb{L}\rangle @ l} \mu_0 \equiv \nu\tilde{x}(\mu_1\{y/x\} \parallel \mu_3 \parallel \mathcal{D}(E_0 \propto C))$ where

$$(E \parallel \mathcal{D}(G)) \propto C \xrightarrow{(x,\mathbb{L})\lhd l} \mu_1 \parallel \mathcal{D}(E_0 \propto C),$$

$$(G \parallel \mathcal{D}(E)) \propto C \xrightarrow{\langle y,\mathbb{L}\rangle @ l} \mu_3 \parallel \mathcal{D}(E_0 \propto C).$$

Since $E \approx^{\mathcal{M}} F$, we have $(E \parallel \mathcal{D}(G)) \propto C \approx^{\mathcal{M}} (F \parallel \mathcal{D}(G)) \propto C$ and

$$(F \parallel \mathcal{D}(G)) \propto C \xRightarrow{(x,\mathbb{L})\lhd l} \mu_2 \tag{2.4}$$

such that $\mu_1 \parallel \mathcal{D}(E_0 \propto C)\{y/x\} \approx^{\mathcal{M}} \mu_2\{y/x\}$ for all $y \in \mathcal{N}$. Since

$$(G \parallel \mathcal{D}(E)) \propto C \xrightarrow{\langle y,\mathbb{L}\rangle @ l} \mu_3 \parallel \mathcal{D}(E_0 \propto C),$$

by (nSYN) we have

$$G' \xrightarrow{\langle y,\emptyset\rangle @ l} \mu_3' \tag{2.5}$$

where $G \equiv G' \parallel \mathcal{D}(G)$ and $\mu_3 \equiv \mu_3' \bullet \mathbb{L}$. Similarly, by knowing that $F_0 \propto C \equiv \nu\tilde{x}(G' \parallel ((F \parallel \mathcal{D}(G)) \propto C))$, we can combine transitions 2.4 and 2.5 using (nSYN), and get the following transition

$$F_0 \propto C \xRightarrow{\langle y,\mathbb{L}\rangle @ l} \nu\tilde{x}(\mu_2\{y/x\} \parallel \mu_3)$$

such that

$$\nu\tilde{x}(\mu_1\{y/x\} \parallel \mu_3 \parallel \mathcal{D}(E_0 \propto C)) \; \mathcal{R} \; \nu\tilde{x}(\mu_2\{y/x\} \parallel \mu_3)$$

for all $y \in \mathcal{N}$.

- Suppose $E_0 \propto C \xrightarrow{\langle y,\mathbb{L}\rangle @ l} \mu_0 \equiv \nu\tilde{x}(\mu_1\{y/x\} \parallel \mu_3 \parallel \mathcal{D}(E_0 \propto C))$ where

$$(E \parallel \mathcal{D}(G)) \propto C \xrightarrow{\langle y,\mathbb{L}\rangle @ l} \mu_1 \parallel \mathcal{D}(E_0 \propto C),$$

$$(G \parallel \mathcal{D}(E)) \propto C \xrightarrow{(x,\mathbb{L})\lhd l} \mu_3 \parallel \mathcal{D}(E_0 \propto C).$$

Since $E \approx^{\mathcal{M}} F$, we have $(E \parallel \mathcal{D}(G)) \propto C \approx^{\mathcal{M}} (F \parallel \mathcal{D}(G)) \propto C$ and

$$(F \parallel \mathcal{D}(G)) \propto C \xRightarrow{\langle y,\mathbb{L}\rangle @ m} \mu_2 \tag{2.6}$$

such that $\mu_1 \parallel \mathcal{D}(E_0 \propto C) \approx^{\mathcal{M}} \mu_2$. Since

$$(G \parallel \mathcal{D}(E)) \propto C \xrightarrow{(x,\mathbb{L})\triangleleft l} \mu_3 \parallel \mathcal{D}(E_0 \propto C),$$

by (nREC2) we have

$$G' \xrightarrow{(x,\emptyset)\triangleleft l} \mu_3' \tag{2.7}$$

where $G \equiv G' \parallel \mathcal{D}(G)$ and $\mu_3 \equiv \mu_3' \bullet \mathbb{L}$. Since

$$F_0 \propto C \equiv \nu\tilde{x}(G' \parallel ((F \parallel \mathcal{D}(G)) \propto C)),$$

so we can now combine transitions 2.6 and 2.7 using (nREC2) and (nRES), and get the following transition:

$$F_0 \propto C \xRightarrow{\langle y,\mathbb{L}\rangle@m} \nu\tilde{x}(\mu_2 \parallel \mu_3\{y/x\})$$

such that

$$\nu\tilde{x}(\mu_1 \parallel \mu_3\{y/x\} \parallel \mathcal{D}(E_0 \propto C)) \mathrel{\mathcal{R}} \nu\tilde{x}(\mu_2 \parallel \mu_3\{y/x\}).$$

3. $\alpha = \nu\tilde{y}(\langle y,\mathbb{L}\rangle@l)$ and $y \in \tilde{y}$.

   - Suppose $E_0 \propto C \xrightarrow{\nu y(\langle y,\mathbb{L}\rangle@l)} \mu_0 \equiv \nu\tilde{x}(\mu_1 \parallel \mu_3\{y/x\}) \parallel \mathcal{D}(E_0 \propto C)$ where

   $$(E \parallel \mathcal{D}(G)) \propto C \xrightarrow{\nu y(\langle y,\mathbb{L}\rangle@l)} \mu_1 \parallel \mathcal{D}(E_0 \propto C),$$

   $$(G \parallel \mathcal{D}(E)) \propto C \xrightarrow{(x,\mathbb{L})\triangleleft l} \mu_3 \parallel \mathcal{D}(E_0 \propto C)$$

   and $y \notin \tilde{x} \cup fn(G)$($\alpha$-conversion rule may be used if necessary). By Lemma 2, we know $E_0 \equiv (\nu\tilde{x} \cup \{y\})(E_1 \parallel G)$ such that $E \equiv (\nu y)E_1$,

   $$(E_1 \parallel \mathcal{D}(G)) \propto C \xrightarrow{\langle y,\mathbb{L}\rangle@l} \mu_1 \parallel \mathcal{D}(E_0 \propto C).$$

   Since $E \approx^{\mathcal{M}} F$, we know

   $$(F \parallel \mathcal{D}(G)) \propto C \xRightarrow{\nu y(\langle y,\mathbb{L}\rangle@m)} \mu_2,$$

   so there exists F_1 such that $F \equiv (\nu y)F_1$ and

   $$(F_1 \parallel \mathcal{D}(G)) \propto C \xRightarrow{\langle y,\mathbb{L}\rangle@m} \mu_2'$$

   by Lemma 2, so $F_0 \equiv (\nu\tilde{x} \cup \{y\})(F_1 \parallel G)$. The continuation of the proof is on E_1 and F_1 and is omitted here.

- The other cases are similar.

4. $\alpha = \tau$. This case is trivial, we omit the detail here.

□

The following theorem shows the relationship between $\approx$ and $\approx^{\mathcal{M}}$. Intuitively, if two processes are weakly bisimilar, after putting them at the same location the resulting networks are also weakly bisimilar.

Theorem 3. *$p \approx q$ implies $\lfloor p \rfloor_l \approx^{\mathcal{M}} \lfloor q \rfloor_l$ for any $\mathcal{M}$ and l.*

Proof. We only need to consider transitions where $\alpha = \nu\tilde{x}\langle x, \emptyset\rangle@l$, $(x, \emptyset) \triangleleft l$, and τ since neither $\lfloor p \rfloor_l$ nor $\lfloor q \rfloor_l$ contain connectivity information. Take $\alpha = \nu\tilde{x}\langle x, \emptyset\rangle@l$ as an example, the other cases can be proved in a similar way. Suppose that $\lfloor p \rfloor_l \xrightarrow{\nu\tilde{x}\langle x,\emptyset\rangle@l} \lfloor p' \rfloor_l$, then by (nBRD) in Table 2.5 we know $p \xrightarrow{\nu\tilde{x}\langle x\rangle} p'$, since $p \approx q$, then there exists $q \xRightarrow{\nu\tilde{x}\langle x\rangle} q'$ such that $p' \approx q'$, so by induction hypothesis $\lfloor q \rfloor_l \xRightarrow{\nu\tilde{x}\langle x,\emptyset\rangle@l} \lfloor q' \rfloor_l$ and $\lfloor p' \rfloor_l \approx \lfloor q' \rfloor_l$. □

With Theorem 3, when there is a network $E \equiv \nu\tilde{x}(\lfloor p \rfloor_l \parallel E')$, we can always replace p with another process q provided that $p \approx q$. Since according to Theorem 2, the resulting network $\nu\tilde{x}(\lfloor q \rfloor_l \parallel E')$ is weakly bisimilar with E. Furthermore, the congruence of $\approx^{\mathcal{M}}$ can be extended to process level in certain scenarios. For example, suppose now

$$E \equiv \nu\tilde{x}(\lfloor p \rfloor_l \parallel E') \text{ and } F \equiv \nu\tilde{x}(\lfloor q \rfloor_l \parallel F')$$

with $E' \approx^{\mathcal{M}} F'$ and $p \approx q$, then

$$\nu\tilde{x}(\lfloor p \parallel r \rfloor_l \parallel E') \approx^{\mathcal{M}} \nu\tilde{x}(\lfloor q \parallel r \rfloor_l \parallel F')$$

for any r. Since $E' \approx^{\mathcal{M}} F'$ and $\lfloor p \parallel r \rfloor_l \approx^{\mathcal{M}} \lfloor q \parallel r \rfloor_l$ by Theorem 1 and 3, and we can apply Theorem 2 twice as follows:

$$\nu\tilde{x}(\lfloor p \parallel r \rfloor_l \parallel E') \approx^{\mathcal{M}} \nu\tilde{x}(\lfloor p \parallel r \rfloor_l \parallel F') \approx^{\mathcal{M}} \nu\tilde{x}(\lfloor q \parallel r \rfloor_l \parallel F').$$

Scenarios for other operators of processes can be deduced in a similar way.

Now we are going to give two examples of the weak bisimulation which show how two networks with different connectivity information can be weakly bisimilar.

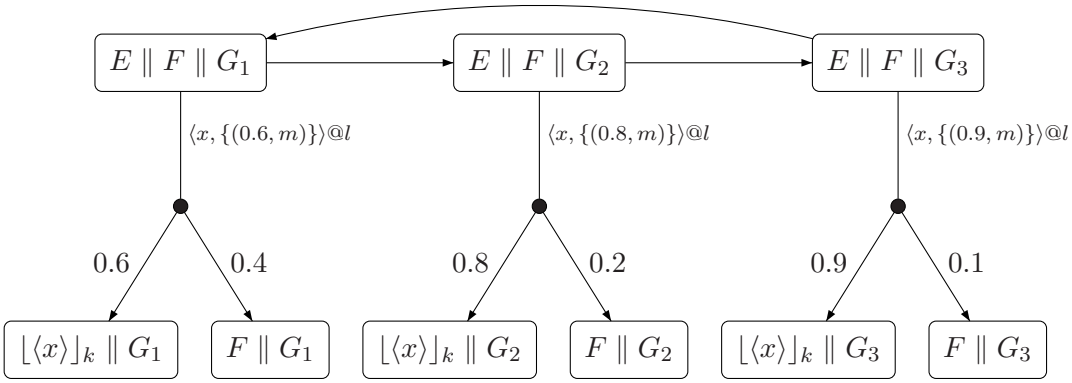

Figure 2.7: Network derivation

Example 13. *Suppose there are two networks*

$$E = \lfloor\langle x\rangle\rfloor_l, \quad F = \lfloor(y).\langle y\rangle\rfloor_k$$

and three connectivity networks:

$$G_1 = \{\{0.6, k\} \mapsto l\}, G_2 = \{\{0.8, k\} \mapsto l\}, G_3 = \{\{0.9, k\} \mapsto l\}.$$

Let the mobility of $Pro(k \mapsto l)$ be given by $\mathcal{M}$ in Fig. 2.3, and let all the other connections be implicitly defined. Since $\approx^{\mathcal{M}}$ is a congruence, to show that

$$E \parallel F \parallel G_1 \;\approx^{\mathcal{M}}\; E \parallel F \parallel G_2 \;\approx^{\mathcal{M}}\; E \parallel F \parallel G_3,$$

it is enough to prove that

$$G_1 \;\approx^{\mathcal{M}}\; G_2 \;\approx^{\mathcal{M}}\; G_3.$$

It is not hard to see that the following set $\mathcal{R}$ is a weak bisimulation.

$$\mathcal{R} = \{G_1, G_2, G_3\} \times \{G_1, G_2, G_3\}$$

Derivations for $E \parallel F \parallel G_i$ $(i = 1, 2, 3)$ are shown in Fig. 2.7 where we only show the essential transitions. Observe that in each of the three networks the node at location k can always receive the message from l with probability 0.6, 0.8, or 0.9.

Example 14. *Given two networks such that*

$$E = \lfloor A\rfloor_l \parallel \lfloor\langle x\rangle\rfloor_k \parallel \{\{(0.8, m)\} \mapsto l\} \parallel \{\{(0.6, m)\} \mapsto k\}$$

$$F = \lfloor A \rfloor_l \parallel \{\{(0.8, m)\} \mapsto l\} \parallel \{\{(0.6, m)\} \mapsto k\}$$

where $A \stackrel{def}{=} \langle x \rangle.A$. *The only difference between* E *and* F *is that* E *can broadcast the message* x *from location* k *once while* F *can only broadcast the message* x *from location* l, *so certainly* E *can simulate* F *under any* PMF, *but not the other way around. Suppose we are given a* PMF $\mathcal{M}$ *such that the mobility rule of* $Pro(m \mapsto l)$ *is given by Fig. 2.3 while the mobility rule of* $Pro(m \mapsto k)$ *is given by Fig. 2.2, and all the others are implicitly defined. It turns out that* $E \approx^{\mathcal{M}} F$. *The only non-trivial transition we should consider is when* E *broadcasts the message* x *from location* k. *Intuitively, because in* E *the node at location* m *can receive message* x *from* k *with probability 0.6 or 0.9, this can be simulated by* F *since in* F *the node at location* m *can receive message* x *from* l *with probability 0.6, 0.8, or, 0.9. Before we introduce the weak bisimulation* $\mathcal{R}$, *we give the following definitions:*

$$E_{\rho_1\rho_2} = \{\{(\rho_1, m)\} \mapsto l\} \parallel \{\{(\rho_2, m)\} \mapsto k\}$$
$$S_1 = \{\lfloor A \rfloor_l \parallel \lfloor \langle x \rangle \rfloor_k \parallel E_{\rho_1\rho_2} \mid \rho_1 \in \{0.6, 0.8, 0.9\}, \rho_2 \in \{0.6, 0.9\}\}$$
$$S_2 = \{\lfloor A \rfloor_l \parallel E_{\rho_1\rho_2} \mid \rho_1 \in \{0.6, 0.8, 0.9\}, \rho_2 \in \{0.6, 0.9\}\}$$

Then

$$\mathcal{R} = (S_1 \cup S_2) \times (S_1 \cup S_2).$$

2.4.2 Weak Probabilistic Bisimulation

In Section 2.4.1, two weakly bisimilar networks can broadcast messages to or receive messages from locations with the same probabilities. But sometimes, we may only be concerned about the extreme values, the maximum and minimum values of certain properties. For example, we may want to make sure that in a network the probability for a certain message being delivered to a node within 5 steps is at least 0.99 or the probability for a certain error not being reported successfully is at most 0.05.

Example 15. *Considering three simple networks:*

$$E_1 = \lfloor (x).\langle x \rangle \rfloor_l \parallel \{\{(0.6, l)\} \mapsto k\}$$
$$E_2 = \lfloor (x).\langle x \rangle \rfloor_l \parallel \{\{(0.9, l)\} \mapsto k\}$$
$$E_3 = \lfloor (x).\langle x \rangle \rfloor_l \parallel \{\{(0.7, l)\} \mapsto k\}$$

where the mobility of $Pro(l \mapsto k)$ *is given by Fig. 2.2. It is not hard to infer that* $E_1 \approx^{\mathcal{M}} E_2$ *but* $E_2 \not\approx^{\mathcal{M}} E_3$ *since in* E_1 *and* E_2 *the nodes at location* l *can receive*

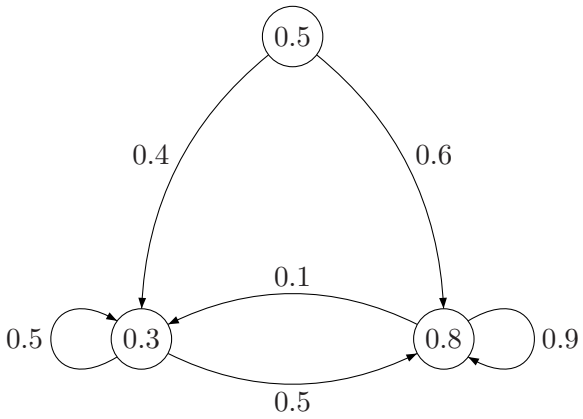

Figure 2.8: An example of mobility.

messages from k with probability 0.6 or 0.9 while in E_3 the probability can be 0.6, 0.7, or, 0.9. But, if we are only concerned with extreme probabilities of certain properties such as the maximum (minimum) probability of the node at location l receiving messages from k, then we would like that all these three networks are weakly bisimilar.

From the above example we know that $\approx^{\mathcal{M}}$ is too strict in this case. We need a coarser bisimulation which only captures the probability bounds and not the exact probabilities, so we define $\stackrel{\alpha}{\Longrightarrow}_c$ to denote a *combined step* as in (1), that is, $E \stackrel{(x,\mathbb{L})\triangleleft l}{\Longrightarrow}_c \mu$ iff there exists

$$\{E \stackrel{(x,\mathbb{L}_i)\triangleleft l}{\Longrightarrow} \mu_i \mid l(\mathbb{L}) = l(\mathbb{L}_i)\}_{i\in I}$$

such that $\sum_{i\in I} w_i \cdot \mathbb{L}_i = \mathbb{L}$ and $\sum_{i\in I} w_i \cdot \mu_i = \mu$, where $\sum_{i\in I} w_i = 1$. Similarly, $E \stackrel{\nu\tilde{x}\langle x,\mathbb{L}\rangle@l}{\Longrightarrow}_c \mu$ iff there exists

$$\{E \stackrel{\nu\tilde{x}\langle x,\mathbb{L}_i\rangle@l}{\Longrightarrow} \mu_i \mid l(\mathbb{L}) = l(\mathbb{L}_i)\}_{i\in I}$$

such that $\sum_{i\in I} w_i \cdot \mathbb{L}_i = \mathbb{L}$ and $\sum_{i\in I} w_i \cdot \mu_i = \mu$, where $\sum_{i\in I} w_i = 1$. Note here that the probabilistic combination of different transitions does not affect the probability bounds of each connection, in other words the probability bounds of transitions from a network to others are not changed. Confer the following example.

Example 16. *Suppose there are two networks as follows:*

$$E \equiv \lfloor (x).\langle x\rangle \rfloor_m \parallel \lfloor (x).\langle x\rangle \rfloor_n \parallel G_{0.5,0.8},$$

$$F \equiv \lfloor (x).\langle x\rangle \rfloor_m \parallel \lfloor (x).\langle x\rangle \rfloor_n \parallel G_{0.3,0.9}$$

where

$$G_{\rho_1,\rho_2} \equiv \{\{(\rho_1, m), (\rho_2, n)\} \mapsto l\}.$$

The mobility rules of $Pro(m \mapsto l)$ *and* $Pro(n \mapsto l)$ *are given by Fig. 2.8 and Fig. 2.2 respectively. By the semantics we can infer that*

$$E \xrightarrow{(x,\{(0.5,m),(0.8,n)\})\triangleleft l} \begin{cases} 0.5 \cdot 0.8 : & \lfloor\langle x\rangle\rfloor_m \parallel \lfloor\langle x\rangle\rfloor_n \parallel G_{0.5,0.8} \\ 0.5 \cdot 0.2 : & \lfloor\langle x\rangle\rfloor_m \parallel \lfloor(x).\langle x\rangle\rfloor_n \parallel G_{0.5,0.8} \\ 0.5 \cdot 0.8 : & \lfloor(x).\langle x\rangle\rfloor_m \parallel \lfloor\langle x\rangle\rfloor_n \parallel G_{0.5,0.8} \\ 0.5 \cdot 0.2 : & \lfloor(x).\langle x\rangle\rfloor_m \parallel \lfloor(x).\langle x\rangle\rfloor_n \parallel G_{0.5,0.8} \end{cases} \equiv \mu$$

It is not hard to see that F *cannot perform such a transition directly, but instead it has the following four transitions:*

$$F \xrightarrow{(x,\{(0.3,m),(0.9,n)\})\triangleleft l} \begin{cases} 0.3 \cdot 0.9 : & \lfloor\langle x\rangle\rfloor_m \parallel \lfloor\langle x\rangle\rfloor_n \parallel G_{0.3,0.9} \\ 0.3 \cdot 0.1 : & \lfloor\langle x\rangle\rfloor_m \parallel \lfloor(x).\langle x\rangle\rfloor_n \parallel G_{0.3,0.9} \\ 0.7 \cdot 0.9 : & \lfloor(x).\langle x\rangle\rfloor_m \parallel \lfloor\langle x\rangle\rfloor_n \parallel G_{0.3,0.9} \\ 0.7 \cdot 0.1 : & \lfloor(x).\langle x\rangle\rfloor_m \parallel \lfloor(x).\langle x\rangle\rfloor_n \parallel G_{0.3,0.9} \end{cases} \equiv \mu_1'$$

$$F \xrightarrow{(x,\{(0.3,m),(0.6,n)\})\triangleleft l} \begin{cases} 0.3 \cdot 0.6 : & \lfloor\langle x\rangle\rfloor_m \parallel \lfloor\langle x\rangle\rfloor_n \parallel G_{0.3,0.6} \\ 0.3 \cdot 0.4 : & \lfloor\langle x\rangle\rfloor_m \parallel \lfloor(x).\langle x\rangle\rfloor_n \parallel G_{0.3,0.6} \\ 0.7 \cdot 0.6 : & \lfloor(x).\langle x\rangle\rfloor_m \parallel \lfloor\langle x\rangle\rfloor_n \parallel G_{0.3,0.6} \\ 0.7 \cdot 0.4 : & \lfloor(x).\langle x\rangle\rfloor_m \parallel \lfloor(x).\langle x\rangle\rfloor_n \parallel G_{0.3,0.6} \end{cases} \equiv \mu_2'$$

$$F \xrightarrow{(x,\{(0.8,m),(0.9,n)\})\triangleleft l} \begin{cases} 0.8 \cdot 0.9 : & \lfloor\langle x\rangle\rfloor_m \parallel \lfloor\langle x\rangle\rfloor_n \parallel G_{0.8,0.9} \\ 0.8 \cdot 0.1 : & \lfloor\langle x\rangle\rfloor_m \parallel \lfloor(x).\langle x\rangle\rfloor_n \parallel G_{0.8,0.9} \\ 0.2 \cdot 0.9 : & \lfloor(x).\langle x\rangle\rfloor_m \parallel \lfloor\langle x\rangle\rfloor_n \parallel G_{0.8,0.9} \\ 0.2 \cdot 0.1 : & \lfloor(x).\langle x\rangle\rfloor_m \parallel \lfloor(x).\langle x\rangle\rfloor_n \parallel G_{0.8,0.9} \end{cases} \equiv \mu_3'$$

$$F \xrightarrow{(x,\{(0.8,m),(0.6,n)\})\triangleleft l} \begin{cases} 0.8 \cdot 0.6 : & \lfloor\langle x\rangle\rfloor_m \parallel \lfloor\langle x\rangle\rfloor_n \parallel G_{0.8,0.6} \\ 0.8 \cdot 0.4 : & \lfloor\langle x\rangle\rfloor_m \parallel \lfloor(x).\langle x\rangle\rfloor_n \parallel G_{0.8,0.6} \\ 0.2 \cdot 0.6 : & \lfloor(x).\langle x\rangle\rfloor_m \parallel \lfloor\langle x\rangle\rfloor_n \parallel G_{0.8,0.6} \\ 0.2 \cdot 0.4 : & \lfloor(x).\langle x\rangle\rfloor_m \parallel \lfloor(x).\langle x\rangle\rfloor_n \parallel G_{0.8,0.6} \end{cases} \equiv \mu_4'$$

Since $\frac{3}{5}\cdot 0.3+\frac{2}{5}\cdot 0.8=0.5$ *and* $\frac{1}{3}\cdot 0.6+\frac{2}{3}\cdot 0.9=0.8$*, we can have a transition* $F \xrightarrow{(x,\mathbb{L})\triangleleft l}_c \mu'$ *where*

$$\mathbb{L}=\{(0.5,m),(0.8,n)\}=\begin{cases}\frac{3}{5}\cdot\frac{2}{3}\cdot\{(0.3,m),(0.9,n)\}\\ +\frac{3}{5}\cdot\frac{1}{3}\cdot\{(0.3,m),(0.6,n)\}\\ +\frac{2}{5}\cdot\frac{2}{3}\cdot\{(0.8,m),(0.9,n)\}\\ +\frac{2}{5}\cdot\frac{1}{3}\cdot\{(0.8,m),(0.6,n)\}\end{cases}$$

and

$$\mu'=\frac{3}{5}\cdot\frac{2}{3}\cdot\mu'_1+\frac{3}{5}\cdot\frac{1}{3}\cdot\mu'_2+\frac{2}{5}\cdot\frac{2}{3}\cdot\mu'_3+\frac{2}{5}\cdot\frac{1}{3}\cdot\mu'_4.$$

It is not hard to see that in μ *and* μ' *the probability of the networks where both nodes at locations* m *and* n *have received the message from* l *is the same and it is similar for the other cases.*

In this example, even after the combined transition the probability bounds of each transition are still not changed. For instance, the probability from F *to the networks where both nodes at locations* m *and* n *have received the message from* l *is always between* $0.3\cdot 0.6$ *and* $0.8\cdot 0.9$*.*

Below follows our definition of a weak bisimulation, *weak probabilistic bisimulation*, that takes extreme probabilities into account.

Definition 6 (Weak Probabilistic Bisimulation)**.** *An equivalence relation* $\mathcal{R}\subseteq\mathcal{N}\times\mathcal{N}$ *is a weak probabilistic bisimulation if* $E\ \mathcal{R}\ F$ *implies that for each* $k\in L$ *and* $C_{E,F,k}$ *whenever* $E\propto C_{E,F,k}\xrightarrow{\alpha}\mu$ *then:*

1. *if* $\alpha=(x,\mathbb{L})\triangleleft k$ *then there exists* $F\propto C_{E,F,k}\stackrel{\alpha}{\Longrightarrow}_c\mu'$ *such that for each* $y\in\mathcal{N}$*,* $\mu\{y/x\}\ \mathcal{R}\ \mu'\{y/x\}$*;*
2. *if* $\alpha=\nu\tilde{x}\langle x,\mathbb{L}\rangle@l$ *then there exists* $F\propto C_{E,F,k}\xrightarrow{\nu\tilde{x}\langle x,\mathbb{L}\rangle@m}_c\mu'$ *such that* $\mu\ \mathcal{R}\ \mu'$*;*
3. *if* $\alpha=\tau$ *then there exists* $F\propto C_{E,F,k}\stackrel{\tau}{\Longrightarrow}_c\mu'$ *such that* $\mu\ \mathcal{R}\ \mu'$*.*

Two networks E *and* F *are weakly probabilistic bisimilar, written as* $E\approx_p^{\mathbb{M}}F$*, if* $E\ \mathcal{R}\ F$ *for some weak probabilistic bisimulation* $\mathcal{R}$*.*

The clauses here are very similar with those in Definition 5 except that the normal weak transitions are replaced by combined weak transitions. Clause 1 requires that if locations $l(\mathbb{L})$ in network E can receive a message from location l with specific

probabilities, then locations $l(\mathbb{L})$ in F must be able to receive the same message from the location l with the same probabilities via combined transition. Clause 2 means that if E can broadcast a message from l with receivers at locations $l(\mathbb{L})$, then F can also broadcast the same message from some location m to $l(\mathbb{L})$ with the same probabilities via a combined transition. Clause 3 deals with internal actions. The $C_{E,F,k}$ plays the same role as in Definition 5.

Let $\approx_p^{\mathcal{M}}$ be the largest weak probabilistic bisimulation, we show that:

Theorem 4. *$\approx_p^{\mathcal{M}}$ is a congruence.*

Proof. The proof is by structural induction as in Theorem 2, and is omitted here. □

The following theorem shows that $\approx^{\mathcal{M}}$ is strictly finer than $\approx_p^{\mathcal{M}}$.

Theorem 5. $\approx^{\mathcal{M}} \subset \approx_p^{\mathcal{M}}$.

Proof. The proof is straightforward from Definition 5 and 6, since the weak transition is a special case of the weak probability transition. □

The theorem for weak bisimulation in Section 2.4.1 is obviously still valid for weak probabilistic bisimulation, that is,

Theorem 6. *$p \approx q$ implies $\lfloor p \rfloor_l \approx_p^{\mathcal{M}} \lfloor q \rfloor_l$ for any $\mathcal{M}$ and l.*

Proof. The proof is similar to the one for Theorem 3, and is omitted here. □

The congruence of $\approx_p^{\mathcal{M}}$ can be extended to process level in certain scenarios in the same way as for $\approx^{\mathcal{M}}$.

Following Example 13, we compare the two definitions of weak bisimulation and illustrate their differences.

Example 17. *We take all the notations from Example 13 and define*

$$G_4 = \{\{0.7, k\} \mapsto l\} \text{ and } G_5 = \{\{0.5, k\} \mapsto l\}.$$

By Definition 5 we know $G_i \not\approx^{\mathcal{M}} G_4$ since in G_i there is no way for the node at location k receiving messages from l with probability 0.7 for $i \in \{1, 2, 3\}$. But since $0.7 \in [0.6, 0.9]$ and all the probabilities of $Pro(k \mapsto l)$ reachable from 0.7 by mobility are always in [0.6,0.9], we obtain that in G_4 the node at location k can always receive messages from l with probability in [0.6,0.9] and $G_i \approx_p^{\mathcal{M}} G_4$. If $G_4 \xrightarrow{(x,\{(0.7,k)\})\triangleleft l}$, G_i can always simulate

it by a combined transition, that is, $G_i \xRightarrow{(x,\{(0.7,k)\})\triangleleft l}_c$, *since we have* $G_i \xRightarrow{(x,\{(0.6,k)\})\triangleleft l}$ *and* $G_i \xRightarrow{(x,\{(0.9,k)\})\triangleleft l}$, *note we omit the parameter* $C_{G_i,G_4,l}$ *which is not important here.*

As a counterexample, we know $G_i \not\approx_p^{\mathcal{M}} G_5$, *since in* G_5 *the node at location* k *can receive messages from* l *with probability 0.5 which is not in [0.6,0.9] while in* G_i *the probability of the node at location* k *receiving messages from* l *is always in [0.6,0.9].*

2.5 Weak (Probabilistic) Simulation

In Section 2.4 we define weak (probabilistic) bisimulations which are equivalence relations among networks. Two networks E and F are bisimilar iff E can mimic stepwise all the observable transitions of F and vice versa. In this section we relax the symmetric conditions of weak (probabilistic) bisimulations, and only requires one direction mimicking, which introduces us the definitions of weak (probabilistic) simulation. Simulations are preorders on the networks, which has been used widely for verification purpose (1, 8, 54, 70, 71). Intuitively, if F simulates E, then F can be seen as a correct implementation of E. Since often E is more abstract and contains less details, it is much easier to be analyzed. More importantly, certain properties satisfied by E are guaranteed to be true for F too.

Before introducing weak (probabilistic) simulation, as usual we define the *weight function* in the same way as in (48).

Definition 7 (Weight Function)**.** *Let* $\mathcal{R} = \mathscr{N} \times \mathscr{N}$ *be a relation over* $\mathscr{N}$. *A weight function for* μ *and* μ' *w.r.t.* $\mathcal{R}$ *is a function* $\Delta : \mathscr{N} \times \mathscr{N} \mapsto [0,1]$ *such that:*

- $\Delta(E,F) > 0$ *implies that* $E\ \mathcal{R}\ F$,
- $\mu(E) = \sum_{F\in\mathscr{N}} \Delta(E,F)$ *for any* $E \in \mathscr{N}$,
- $\mu'(F) = \sum_{E\in\mathscr{N}} \Delta(E,F)$ *for any* $F \in \mathscr{N}$.

We write $\mu \sqsubseteq_{\mathcal{R}} \mu'$ *iff there exists a weight function for* μ *and* μ' *w.r.t.* $\mathcal{R}$.

When $\mu \sqsubseteq_{\mathcal{R}} \mu'$, it may happen that for a certain set of networks $S \subseteq Supp(\mu)$, there exists a set of networks $S' \subseteq Supp(\mu')$ such that $\mu(S) = \mu'(S')$ where $S \times S' \subseteq \mathcal{R}$, but this does not mean that for each $E \in S$, there exists $E' \in S'$ such that $\mu(E) = \mu'(E')$. For instance if there are two distributions: μ and μ' such that $\mu(E) = 1$, and $\mu'(E_1) = \mu'(E_2) = 0.5$. Apparently, it should hold that $\mu \sqsubseteq_{\mathcal{R}} \mu'$ provided $E\ \mathcal{R}\ E_1$ and $E\ \mathcal{R}\ E_2$,

but neither $\mu(E) = \mu'(E_1)$ nor $\mu(E) = \mu'(E_2)$ holds. Essentially, Δ corresponds in a way to divide the support of distributions μ and μ' such that μ and μ' will coincide with probability of sets of network. For the above example, we can let $\Delta(E, E_1) = 0.5$ and $\Delta(E, E_2) = 0.5$ i.e. dividing E into two parts one of which is for E_1, and the other part is for E_2. Clause 1 says that Δ can only associate two networks when they are in $\mathcal{R}$. Clause 2 guarantees that for each $E \in Supp(\mu)$ the total probability assigned to E by Δ i.e. $\sum_{F \in \mathscr{N}} \Delta(E, F)$ should coincide with the probability of E in μ. Clause 3 is the counterpart of Clause 2, which guarantees that for each $F \in Supp(\mu')$ the total probability assigned to F by Δ i.e. $\sum_{E \in \mathscr{N}} \Delta(E, F)$ should be the same as $\mu'(F)$.

2.5.1 Weak Simulation

In this section we first introduce the weak simulation without considering the combined transitions as before. The weak simulation can be seen as a one direction weak bisimulation in Definition 5. We will also give a few examples to show what the weak simulation can be used for, and also show that it is too fine in some cases which leads us to the definition of weak probabilistic simulation.

Bellow follows the definition of weak simulation.

Definition 8 (Weak Simulation)**.** *A relation $\mathcal{R} \subseteq \mathscr{N} \times \mathscr{N}$ is a weak simulation if $E \ \mathcal{R} \ F$ implies that for each $k \in L$ and $C_{E,F,k}$ whenever $E \propto C_{E,F,k} \xrightarrow{\alpha} \mu$ then:*

1. *if $\alpha = (x, \mathbb{L}) \triangleleft k$ then there exists $F \propto C_{E,F,k} \stackrel{\alpha}{\Longrightarrow} \mu'$ such that for each $y \in \mathcal{N}$, $\mu\{y/x\} \ \sqsubseteq_{\mathcal{R}} \ \mu'\{y/x\}$;*
2. *if $\alpha = \nu\tilde{x}\langle x, \mathbb{L}\rangle@l$ then there exists $F \propto C_{E,F,k} \stackrel{\nu\tilde{x}\langle x,\mathbb{L}\rangle@m}{\Longrightarrow} \mu'$ such that $\mu \ \sqsubseteq_{\mathcal{R}} \ \mu'$;*
3. *if $\alpha = \tau$ then there exists $F \propto C_{E,F,k} \stackrel{\tau}{\Longrightarrow} \mu'$ such that $\mu \ \sqsubseteq_{\mathcal{R}} \ \mu'$.*

The network E is weakly simulated by F, written as $E \ \precapprox^{\mathcal{M}} \ F$, if there exists a weak simulation $\mathcal{R}$ such that $E \ \mathcal{R} \ F$.

Lemma 4. *$E \propto C \ \precapprox^{\mathcal{M}} \ F \propto C$ for any C provided that $E \ \precapprox^{\mathcal{M}} \ F$.*

Proof. Similar with the proof of Lemma 3 and is omitted here. □

The following theorem shows that $\precapprox^{\mathcal{M}}$ is a congruence and preorder.

Theorem 7. *$\precapprox^{\mathcal{M}}$ is a congruence and a preorder.*

Proof. We first prove that $\precsim^{\mathcal{M}}$ is a preorder. The reflexivity is trivial, we only prove the transitivity here i.e. $E \precsim^{\mathcal{M}} F$ and $F \precsim^{\mathcal{M}} G$ implies that $E \precsim^{\mathcal{M}} G$. In order to do so, we need another definition of weak simulation, called $\precsim_1^{\mathcal{M}}$. The definition of $\precsim_1^{\mathcal{M}}$ is almost the same as $\precsim^{\mathcal{M}}$ except that $E \propto C_{E,F,k} \xrightarrow{\alpha} \mu$ is replaced by the weak transition $E \propto C_{E,F,k} \stackrel{\alpha}{\Longrightarrow} \mu$.

It can be proved that $\precsim^{\mathcal{M}} = \precsim_1^{\mathcal{M}}$. It is easy to see that $E \precsim_1^{\mathcal{M}} F$ implies that $E \precsim^{\mathcal{M}} F$ since $E \propto C_{E,F,k} \xrightarrow{\alpha} \mu$ is a special case of $E \propto C_{E,F,k} \stackrel{\alpha}{\Longrightarrow} \mu$. We prove that $E \precsim^{\mathcal{M}} F$ implies $E \precsim_1^{\mathcal{M}} F$, it is enough to show that

$$\mathcal{R} = \{(E, F) \in \mathscr{N} \times \mathscr{N} \mid E \precsim^{\mathcal{M}} F\}$$

is a weak simulation under the new definition. For simplicity we will omit the parameter $C_{E,F,k}$ in the sequel. Suppose that $E \mathcal{R} F$ and $E \stackrel{\alpha}{\Longrightarrow} \mu$. If $\alpha = (x, \mathbb{L}) \lhd k$, we need to prove that there exists $F \stackrel{\alpha}{\Longrightarrow} \mu'$ such that $\mu \sqsubseteq_{\mathcal{R}} \mu'$. We are going to prove by induction on $E \stackrel{\alpha}{\Longrightarrow} \mu$. According to Definition 3, there are two cases to be considered:

1. $E \xrightarrow{\tau} \mu_1 \stackrel{\alpha}{\Longrightarrow} \mu$. Since $E \mathcal{R} F$ i.e. $E \precsim^{\mathcal{M}} F$, there exists $F \stackrel{\tau}{\Longrightarrow} \mu_1'$ such that $\mu_1 \sqsubseteq_{\mathcal{R}} \mu_1'$. By induction there exists $F \stackrel{\tau}{\Longrightarrow} \stackrel{\alpha}{\Longrightarrow} \mu'$ such that $\mu \sqsubseteq_{\mathcal{R}} \mu'$.

2. $E \xrightarrow{\alpha} \mu_1 \stackrel{\tau}{\Longrightarrow} \mu$. Since $E \precsim^{\mathcal{M}} F$, there exists $F \stackrel{\tau}{\Longrightarrow} \mu_1'$ such that $\mu_1 \sqsubseteq_{\mathcal{R}} \mu_1'$. The following proof is similar with Clause 1, and is omitted here.

The cases when $\alpha = \tau$ or $\nu\tilde{x}\langle x, \mathbb{L}\rangle@l$ are similar.

Since we have proved that $\precsim^{\mathcal{M}} = \precsim_1^{\mathcal{M}}$, in order to show that $\precsim^{\mathcal{M}}$ is a preorder, it is equivalent to prove that $\precsim_1^{\mathcal{M}}$ is a preorder. Suppose that $E \precsim_1^{\mathcal{M}} F$ and $F \precsim_1^{\mathcal{M}} G$, we prove that $E \precsim_1^{\mathcal{M}} G$. According to the definition of $\precsim_1^{\mathcal{M}}$, there exists weak simulations $\mathcal{R}_1$ and $\mathcal{R}_2$ such that $E \mathcal{R}_1 F$ and $F \mathcal{R}_2 G$. Therefore whenever $E \xRightarrow{(x,\mathbb{L})\lhd k} \mu_1$, there exists $F \xRightarrow{(x,\mathbb{L})\lhd k} \mu_2$ and $G \xRightarrow{(x,\mathbb{L})\lhd k} \mu_3$ such that $\mu_1 \sqsubseteq_{\mathcal{R}_1} \mu_2$ and $\mu_2 \sqsubseteq_{\mathcal{R}_2} \mu_3$. In other words, there exists Δ_1 and Δ_2 satisfying the conditions in Definition 7. Let

$$\mathcal{R} = \mathcal{R}_1 \circ \mathcal{R}_2 = \{(E', G') \mid \exists F'.(E' \mathcal{R}_1 F' \wedge F' \mathcal{R}_2 G')\},$$

then we need to find a Δ between μ_1 and μ_3 over $\mathcal{R}$. Let

$$\Delta(E, G) = \sum_{F \in \mathscr{N}} \Delta_1(E, F) \cdot \frac{\Delta_2(F, G)}{\mu_2(F)},$$

we show that Δ defined in this way does satisfy the conditions in Definition 7. Condition one is easy since $\Delta(E, G) > 0$ implies that there exists F such that $\Delta_1(E, F) > 0$ and

$\Delta_2(F, G) > 0$, that is, $E \ \mathcal{R}_1 \ F$ and $F \ \mathcal{R}_2 \ G$, thus $E \ \mathcal{R} \ G$, and vice versa. Also

$$\begin{aligned}\sum_{G\in\mathcal{N}} \Delta(E, G) &= \sum_{G\in\mathcal{N}} \sum_{F\in\mathcal{N}} \Delta_1(E, F) \cdot \frac{\Delta_2(F, G)}{\mu_2(F)} \\ &= \sum_{F\in\mathcal{N}} \Delta_1(E, F) \cdot \frac{1}{\mu_2(F)} \cdot (\sum_{G\in\mathcal{N}} \Delta_2(F, G)) \\ &= \sum_{F\in\mathcal{N}} \Delta_1(E, F) = \mu_1(E)\end{aligned}$$

we prove that the second condition is satisfied too. The third condition is similar as the second one, and is omitted here. Therefore $\mu_1 \ \sqsubseteq_{\mathcal{R}} \ \mu_3$, this completes the proof.

Finally we prove that $\precsim^{\mathcal{M}}$ is a congruence which is similar with the proof of Theorem 2, it is enough to show that

$$\mathcal{R} = \{(\nu\tilde{x}(E \parallel G), \nu\tilde{x}(F \parallel G)) \mid E \ \precsim^{\mathcal{M}} \ F\}$$

is a weak simulation. Let

$$E_0 = \nu\tilde{x}(E \parallel G),$$

$$F_0 = \nu\tilde{x}(F \parallel G).$$

If $E_0 \xrightarrow{\alpha} \mu$, we need to distinguish among several cases. Again we simply write C as the abbreviation of $C_{E_0,F_0,l}$.

- Suppose

$$E_0 \propto C \xrightarrow{(x,\mathbb{L})\lhd l} \mu_0 \ \equiv \ \nu\tilde{x}(\mu_1 \parallel \mu_3 \parallel \mathcal{D}(E_0 \propto C)),$$

  where μ_1 and μ_3 do not contain any connection information, hence we infer:

$$(E \parallel \mathcal{D}(G)) \propto C \xrightarrow{(x,\mathbb{L})\lhd l} \mu_1 \parallel \mathcal{D}(E_0 \propto C),$$

$$(G \parallel \mathcal{D}(E)) \propto C \xrightarrow{(x,\mathbb{L})\lhd l} \mu_3 \parallel \mathcal{D}(E_0 \propto C).$$

  Since $E \ \precsim^{\mathcal{M}} \ F$, then

$$(E \propto \mathcal{D}(G)) \propto C \ \precsim^{\mathcal{M}} \ (F \propto \mathcal{D}(G)) \propto C$$

  by Lemma 4. Note here

$$E \propto \mathcal{D}(G) \ \equiv \ E \parallel \mathcal{D}(G)$$

$$F \propto \mathcal{D}(G) \ \equiv \ F \parallel \mathcal{D}(G)$$

because E_0 is well-formed. Then we have

$$(E \parallel \mathcal{D}(G)) \propto C \;\precapprox^{\mathcal{M}}\; (F \parallel \mathcal{D}(G)) \propto C, \text{thus}$$

$$(F \parallel \mathcal{D}(G)) \propto C \xrightarrow{(x,\mathbb{L})\lhd l} \mu_2 \tag{2.8}$$

and $(\mu_1 \parallel \mathcal{D}(E_0 \propto C))\{y/x\} \;\precapprox^{\mathcal{M}}\; \mu_2\{y/x\}$ for all $y \in \mathcal{N}$. Since

$$(G \parallel \mathcal{D}(E)) \propto C \xrightarrow{(x,\mathbb{L})\lhd l} \mu_3 \parallel \mathcal{D}(E_0 \propto C),$$

by (nREC2) we have

$$G' \xrightarrow{(x,\emptyset)\lhd l} \mu_3' \tag{2.9}$$

where $G \equiv G' \parallel \mathcal{D}(G)$ and $\mu_3 \equiv \mu_3' \bullet \mathbb{L}$ with $\mathbb{L} = \mathcal{D}_l(E_0 \propto C)$. Also

$$F_0 \propto C \equiv \nu\tilde{x}(G' \parallel ((F \parallel \mathcal{D}(G)) \propto C)),$$

so we can now combine transitions 2.8 and 2.9 using (nREC2) and (nRES), and obtain the following transition:

$$F_0 \propto C = \nu\tilde{x}(F \parallel G) \propto C \xrightarrow{(x,\mathbb{L})\lhd l} \nu\tilde{x}(\mu_2 \parallel \mu_3) \text{ and}$$

$$\mu_0 \equiv \nu\tilde{x}(\mu_1 \parallel \mu_3 \parallel \mathcal{D}(E_0 \propto C))\{y/x\} \;\sqsubseteq_{\mathcal{R}}\; \nu\tilde{x}(\mu_2 \parallel \mu_3)\{y/x\}.$$

- The other cases are similar.

□

To illustrate how weak simulation works, we give two examples. Since our weak simulation is a conservative extension of the standard weak simulation, we are more interested in the examples related to the mobility.

Example 18. *Suppose we are given a* PMF *such that the mobility of* $Pro(m \longmapsto l)$ *and* $Pro(n \longmapsto l)$ *is explicitly defined by Fig. 2.2 and 2.3 respectively, and all the others are implicitly defined. Let*

$$E \equiv \lfloor\langle x\rangle\rfloor_m \parallel C,$$

$$F \equiv \lfloor\langle x\rangle\rfloor_n \parallel C$$

where $C = \{\{(0.6, l)\} \longmapsto m\} \parallel \{\{(0.5, l)\} \longmapsto n\}$. *Apparently, neither* $E \;\approx^{\mathcal{M}}\; F$ *nor* $E \;\approx_p^{\mathcal{M}}\; F$ *holds, since in* F *the node at location* l *can receive the* x *with probability 0.5 which is impossible for* E. *But according to Definition 8, we have* $E \;\precapprox^{\mathcal{M}}\; F$. *Intuitively, because in* E *the probability of the node at* l *receiving* x *is either 0.6 or 0.9, and the probability can be also 0.6 or 0.9 in* F *even if it has more choices for instance with probability 0.5.*

Example 19. *Suppose we are given a* PMF *such that the mobility of* $Pro(m \longmapsto l)$ *is explicitly defined by Fig. 2.2, while all the others are implicitly defined, therefore the only possible values of* $Pro(n \longmapsto l)$ *are 0 and 1. Let*

$$E \equiv \lfloor \langle x \rangle \rfloor_m \parallel C,$$

$$F \equiv \lfloor \langle x \rangle \rfloor_n \parallel C \text{ where}$$

$$C = \{\{(0.6, l)\} \longmapsto m\} \parallel \{\{(0, l)\} \longmapsto n\}.$$

It turns out $E \not\approx^{\mathcal{M}} F$ *since in* E *the node at* l *can receive* x *with probability 0.6 while it is not possible in* F*. But since in* F *the node at* l *can receive* x *with probability either 0 or 1, it should be able to simulate* E*, which introduces us the weak probabilistic simulation in the next section.*

2.5.2 Weak Probabilistic Simulation

According to Example 19, $\precsim^{\mathcal{M}}_{\approx}$ seems to be too fine in some cases. In this section we will introduce the weak probabilistic simulation making use of the combined transition as in Definition 6. Bellow follows the definition of weak probabilistic simulation.

Definition 9 (Weak Probabilistic Simulation)**.** *A relation* $\mathcal{R} \subseteq \mathscr{N} \times \mathscr{N}$ *is a weak probabilistic simulation if* $E \ \mathcal{R} \ F$ *implies that for each* $k \in L$ *and* $C_{E,F,k}$ *whenever* $E \propto C_{E,F,k} \xrightarrow{\alpha} \mu$ *then:*

1. *if* $\alpha = (x, \mathbb{L}) \triangleleft k$ *then there exists* $F \propto C_{E,F,k} \stackrel{\alpha}{\Longrightarrow}_c \mu'$ *such that for each* $y \in \mathcal{N}$, $\mu\{y/x\} \ \sqsubseteq_{\mathcal{R}} \ \mu'\{y/x\}$;
2. *if* $\alpha = \nu\tilde{x}\langle x, \mathbb{L}\rangle @ l$ *then there exists* $F \propto C_{E,F,k} \stackrel{\nu\tilde{x}\langle x,\mathbb{L}\rangle @ m}{\Longrightarrow}_c \mu'$ *such that* $\mu \ \sqsubseteq_{\mathcal{R}} \ \mu'$;
3. *if* $\alpha = \tau$ *then there exists* $F \propto C_{E,F,k} \stackrel{\tau}{\Longrightarrow}_c \mu'$ *such that* $\mu \ \sqsubseteq_{\mathcal{R}} \ \mu'$.

The network E *is weakly probabilistic simulated by* F*, written as* $E \precsim^{\mathcal{M}}_{p} F$*, if there exists a weak probabilistic simulation* $\mathcal{R}$ *such that* $E \ \mathcal{R} \ F$*.*

We can also show that $\precsim^{\mathcal{M}}_{p}$ is a congruence and preorder.

Theorem 8. $\precsim^{\mathcal{M}}_{p}$ *is a congruence and preorder.*

Proof. Similar with the proof of Theorem 7 and is omitted here. □

Obviously, $\precsim^{\mathcal{M}}_{\approx}$ is strictly finer than $\precsim^{\mathcal{M}}_{p}$.

Theorem 9. $\precsim^{\mathcal{M}} \subset \precsim_p^{\mathcal{M}}$.

Proof. It is straightforward from Definition 8 and 9. □

In Example 19 we show that $E \not\precsim^{\mathcal{M}} F$, but according to Definition 9, $E \precsim_p^{\mathcal{M}} F$.

Example 20. *Consider the networks E and F in Example 19. As we said before in E the node at l can receive x with probability 0.6, i.e.*

$$E \xrightarrow{\langle x,\{(0.6,l)\}\rangle@m} \delta_{(\lfloor 0\rfloor_m \| C)},$$

since there does not exist $F \xrightarrow{\langle x,\{(0.6,l)\}\rangle@n}$, thus $E \not\precsim^{\mathcal{M}} F$. But we have

$$F \xrightarrow{\langle x,\{(0,l)\}\rangle@n} \delta_{(\lfloor 0\rfloor_n \| C)},$$

$$F \xrightarrow{\langle x,\{(1,l)\}\rangle@n} \delta_{(\lfloor 0\rfloor_n \| C)},$$

therefore there exists

$$F \xrightarrow{\langle x,\{(0.6,l)\}\rangle@n}_c \delta_{(\lfloor 0\rfloor_m \| C)}$$

such that

$$\delta_{(\lfloor 0\rfloor_m \| C)} \sqsubseteq_{\precsim_p^{\mathcal{M}}} \delta_{(\lfloor 0\rfloor_n \| C)},$$

as a result $E \precsim_p^{\mathcal{M}} F$.

2.6 Bisimulations and Simulations between PMFs

In Section 2.4 and 2.5 we discussed the weak bisimulations and simulations between networks, in this section we show how we can define these relations between mobility models. Intuitively, this allows us to abstract from not only the behaviors of a network, but also the mobility of the given PMF. Being able to do so is important for protocols for MANETs, since usually these protocols are designed irrespectively of the mobility of networks, in order to verify these protocols sufficiently we need to consider all the possible mobility which is not possible in practice. If we are given a PMF $\mathcal{M}_1$ and E_1 where $\mathcal{M}_1$ denotes the mobility of the network and E_1 denotes the behavior of the verified protocol, both $\mathcal{M}_1$ and E_1 may contain too many details, and make the state space huge. Using weak bisimulations or simulations introduced in Section 2.4 and 2.5, it is safe to consider a simpler network E_2 provided that E_1 and E_2 are weakly (probabilistic) (bi)similar. On the other hand, if we can also abstract from $\mathcal{M}_1$, and

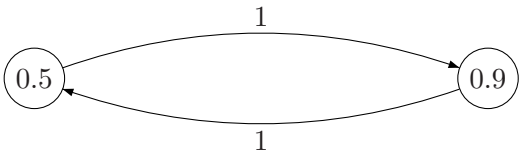

Figure 2.9: A simpler mobility.

give a simpler PMF $\mathcal{M}_2$ such that $\mathcal{M}_1$ and $\mathcal{M}_2$ are equivalent in some sense, then we only need to verify E_2 under $\mathcal{M}_2$. Since E_2 and $\mathcal{M}_2$ are simpler, and contain less details, the state space can be further reduced. Refer to the following example.

Example 21. *Suppose we are given two* PMF*s:* $\mathcal{M}_1$ *and* $\mathcal{M}_2$ *which coincide with each other except for the mobility of* $Pro(k \longmapsto l)$*. If the mobility of* $Pro(k \longmapsto l)$ *is given by Fig. 2.3 in* $\mathcal{M}_1$*, while the mobility of* $Pro(k \longmapsto l)$ *is given by Fig. 2.9 in* $\mathcal{M}_2$*, it is easy to see that* $\mathcal{M}_2$ *is simpler than* $\mathcal{M}_1$*. Moreover in the following we will define certain relations between* $\mathcal{M}_1$ *and* $\mathcal{M}_2$ *enabling us to use* $\mathcal{M}_2$ *instead of* $\mathcal{M}_1$ *in certain situations.*

2.6.1 Weak Bisimulations between PMFs

In the sequel suppose we are given two PMFs: $\mathcal{M}_1$ and $\mathcal{M}_2$, moreover let $\mathscr{N}_i$ denote the set of well-formed networks under $\mathcal{M}_i$ where $i = 1, 2$, and similarly for $\mathscr{C}_i$ which denotes the connectivity networks. The set of connectivity networks is dependent on the given PMF, and may be different under different PMFs i.e. we cannot guarantee that $\mathscr{C}_1 = \mathscr{C}_2$. Therefore when we want to check whether E and F are weak (probabilistic) bisimilar or not where $E \in \mathscr{N}_1$ and $F \in \mathscr{N}_2$, Definition 5 and 6 will not work, since the parameter $C_{E,F,k}$ may not always be in $\mathscr{C}_1 \cap \mathscr{C}_2$. Refer to the following example.

Example 22. *Suppose that* $\mathcal{M}_1$ *and* $\mathcal{M}_2$ *are the same except that the mobility of* $Pro(l \longmapsto k)$ *is given by Fig. 2.3 and 2.9 in* $\mathcal{M}_1$ *and* $\mathcal{M}_2$ *respectively. Let* $E = \lfloor p \rfloor_l$ *and* $F = \lfloor q \rfloor_l$*, we want to check whether* E *and* F*, executed under the guidance of* $\mathcal{M}_1$ *and* $\mathcal{M}_2$ *respectively, are weakly bisimilar or not. Following Definition 5, we need to check if* $E \propto C_{E,F,m}$ *and* $F \propto C_{E,F,m}$ *satisfy the conditions of Definition 5 for any* m *and* $C_{E,F,m} \in \mathscr{C}_{E,F,m}$*. Let* $m = k$*, we can select a* $C_{E,F,k}$ *such that* $C_{E,F,k}(l, k) = 0.8$*, apparently* $E \propto C_{E,F,k}$ *is a well-formed network w.r.t.* $\mathcal{M}_1$*, but* $F \propto C_{E,F,k}$ *is not well-formed w.r.t.* $\mathcal{M}_2$ *because of* $0.8 \notin G_{l \longmapsto k}$ *in* $\mathcal{M}_2$*. Therefore it makes no sense to talk about the execution* $F \propto C_{E,F,k}$ *under the guidance of* $\mathcal{M}_2$*.*

According to Example 22, we cannot apply Definition 5 and 6 directly when two different PMFs are involved, since different PMFs may correspond to different set of connectivity networks. We fix this problem by modifying Definition 5 and 6 as follows where we do not need to select the same parameter $C_{E,F,k}$ for both E and F, but allow them to choose different parameters.

Definition 10 (Weak Bisimulation)**.** *An equivalence relation $\mathcal{R} \subseteq (\mathscr{N}_1 \cup \mathscr{N}_2) \times (\mathscr{N}_1 \cup \mathscr{N}_2)$ is a weak bisimulation if $E \mathcal{R} F$ implies that for each $k \in L$ and $C_{E,F,k} \in \mathscr{C}_i$, there exists $C'_{E,F,k} \in \mathscr{C}_j$ whenever $E \propto C_{E,F,k} \xrightarrow{\alpha} \mu$,*

1. *if $\alpha = (x, \mathbb{L}) \triangleleft k$, there exists $F \propto C'_{E,F,k} \stackrel{\alpha}{\Longrightarrow} \mu'$ such that for each $y \in \mathcal{N}$, $\mu\{y/x\} \mathcal{R} \mu'\{y/x\}$;*
2. *if $\alpha = \nu\tilde{x}\langle x, \mathbb{L}\rangle@l$, there exists $F \propto C'_{E,F,k} \stackrel{\nu\tilde{x}\langle x,\mathbb{L}\rangle@m}{\Longrightarrow} \mu'$ such that $\mu \mathcal{R} \mu'$;*
3. *if $\alpha = \tau$ then there exists $F \propto C'_{E,F,k} \stackrel{\tau}{\Longrightarrow} \mu'$ such that $\mu \mathcal{R} \mu'$.*

where $E \in \mathscr{N}_i$ and $F \in \mathscr{N}_j$ with $i, j \in \{1, 2\}$.

Two networks E and F are weakly bisimilar, written as $E \approx F$, if there exists a weak bisimulation $\mathcal{R}$ such that $E \mathcal{R} F$.

Similarly, we can redefine the weak probabilistic bisimulation of networks when two PMFs are considered as follows.

Definition 11 (Weak Probabilistic Bisimulation)**.** *An equivalence relation $\mathcal{R} \subseteq (\mathscr{N}_1 \cup \mathscr{N}_2) \times (\mathscr{N}_1 \cup \mathscr{N}_2)$ is a weak probabilistic bisimulation if $E \mathcal{R} F$ implies that for each $k \in L$ and $C_{E,F,k} \in \mathscr{C}_i$, there exists $C'_{E,F,k} \in \mathscr{C}_j$ whenever $E \propto C_{E,F,k} \xrightarrow{\alpha} \mu$,*

1. *if $\alpha = (x, \mathbb{L}) \triangleleft k$, there exists $F \propto C'_{E,F,k} \stackrel{\alpha}{\Longrightarrow}_c \mu'$ such that for each $y \in \mathcal{N}$, $\mu\{y/x\} \mathcal{R} \mu'\{y/x\}$;*
2. *if $\alpha = \nu\tilde{x}\langle x, \mathbb{L}\rangle@l$, there exists $F \propto C'_{E,F,k} \stackrel{\nu\tilde{x}\langle x,\mathbb{L}\rangle@m}{\Longrightarrow}_c \mu'$ such that $\mu \mathcal{R} \mu'$;*
3. *if $\alpha = \tau$ then there exists $F \propto C'_{E,F,k} \stackrel{\tau}{\Longrightarrow}_c \mu'$ such that $\mu \mathcal{R} \mu'$.*

where $E \in \mathscr{N}_i$ and $F \in \mathscr{N}_j$ with $i, j \in \{1, 2\}$.

Two networks E and F are weakly probabilistic bisimilar, written as $E \approx_p F$, if there exists a weak probabilistic bisimulation $\mathcal{R}$ such that $E \mathcal{R} F$.

When $\mathcal{M}_1 = \mathcal{M}_2 = \mathcal{M}$ i.e. $\mathscr{N}_1 = \mathscr{N}_2 = \mathscr{N}$, it holds that $\approx^{\mathcal{M}} = \approx$ and $\approx_p^{\mathcal{M}} = \approx_p$, thus we can say that Definition 10 and 11 are conservative extensions of Definition 5 and 6 respectively.

Now we are ready to discuss the weak (probabilistic) bisimulation between PMFs. Intuitively, $\mathcal{M}_1$ and $\mathcal{M}_2$ are weak (probabilistic) bisimilar iff for each $C_1 \in \mathscr{C}_1$ and $l, k \in \mathcal{L}$, if the node at k can receive messages from l with probability ρ in C_1, then there exists $\mathscr{C}_2$ where the node at k can also receive messages from l with the same probability as in C_2 (probably after several mobility steps). In other words, for each $C_1 \in \mathscr{C}_1$ there exists $C_2 \in \mathscr{C}_2$ such that C_1 and C_2 are weak (probabilistic) bisimilar. Below follows the definition of weak (probabilistic) bisimulation between PMFs.

Definition 12. *Let $\mathcal{M}_1$ and $\mathcal{M}_2$ be weak (probabilistic) bisimilar, written as $\mathcal{M}_1 \approx \mathcal{M}_2$ ($\mathcal{M}_1 \approx_p \mathcal{M}_2$), iff for each $C_1 \in \mathscr{C}_1$, there exists $C_2 \in \mathscr{C}_2$ such that $C_1 \approx C_2$ ($C_1 \approx_p C_2$), and vice versa.*

When restricted to connectivity networks, Condition 2 in Definition 5 and 6 can be omitted, since connectivity networks cannot perform broadcast actions. Therefore if $C_1 \approx C_2$ ($C_1 \approx_p C_2$), then whenever $C_1 \xrightarrow{(x,\mathbb{L})\lhd l} \mu$, there exists μ' such that $C_2 \xRightarrow{(x,\mathbb{L})\lhd l} \mu'$ and $\mu \approx \mu'$ ($C_2 \xRightarrow{(x,\mathbb{L})\lhd l}_c \mu'$ and $\mu \approx_p \mu'$). Note that $(\rho, k) \in \mathbb{L}$ implies the node at k can receive messages from l with probability ρ, thus $C_1 \approx C_2$ implies that whenever the node at k can receive messages from l with probability ρ, it is also the case for C_2 probably after several (combined) mobility steps.

The following lemma shows the congruence property of $\approx$ and $\approx_p$ where we only concentrate on the connectivity networks. The congruence property is slightly different from the standard one like in Theorem 2 which we will discuss later, it enables us to consider the mobility of each connection individually.

Lemma 5. *Let $C_1, C_1' \in \mathscr{C}_1$ and $C_2, C_2' \in \mathscr{C}_2$, then*

1. *$C_1 \parallel C_1' \approx C_2 \parallel C_2'$ provided that $C_1 \approx C_2$ and $C_1' \approx C_2'$.*
2. *$C_1 \parallel C_1' \approx_p C_2 \parallel C_2'$ provided that $C_1 \approx_p C_2$ and $C_1' \approx_p C_2'$.*

Proof. We only prove the first clause since the other one is similar. It is enough to prove that

$$\mathcal{R} = \{(C_1 \parallel C_1', C_2 \parallel C_2') \mid C_1 \approx C_2 \wedge C_1' \approx C_2'\}$$

is a weak bisimulation according to Definition 10. Since we only consider connectivity networks in $\mathscr{C}$, no unknown probability can occur, thus we can omit the parameters $C_{E,F,k}$ and $C'_{E,F,k}$ in Definition 10 here. Suppose that $C_1 \parallel C_1' \xrightarrow{\alpha} \mu$, we prove by structural induction and there are only three cases we need to consider:

1. $\alpha = (x, \mathbb{L})\triangleleft l$. Then according to (nREC2) in Table 2.5, there exists $C_1 \xrightarrow{(x,\mathbb{M})\triangleleft l} \mu_1$ and $C_1' \xrightarrow{(x,\mathbb{N})\triangleleft l} \mu_1'$ such that $\mathbb{M} \cup \mathbb{N} = \mathbb{L}$, and $\mu_1 \parallel \mu_1' = \mu$. Since $C_1 \approx C_2$ and $C_1' \approx C_2'$, there exists $C_2 \xRightarrow{(x,\mathbb{M})\triangleleft l} \mu_2$ and $C_2' \xRightarrow{(x,\mathbb{N})\triangleleft l} \mu_2'$ such that $\mu_1 \approx \mu_1'$ and $\mu_2 \approx \mu_2'$, thus $C_2 \parallel C_2' \xRightarrow{(x,\mathbb{L})\triangleleft l} \mu' = (\mu_2 \parallel \mu_2')$, by induction $\mu \mathcal{R} \mu'$.

2. $\alpha = \tau$ and there exists $C_1 \xrightarrow{\tau} \mu_1$ such that $\mu = \mu_1 \parallel \delta_{C_1'}$. Since $C_1 \approx C_2$, there exists $C_2 \xRightarrow{\tau} \mu_2$ such that $\mu_1 \approx \mu_2$, thus $C_2 \parallel C_2' \xRightarrow{\tau} \mu' = (\mu_2 \parallel \delta_{C_2'})$. By induction $\mu \mathcal{R} \mu'$.

3. $\alpha = \tau$ and there exists $C_1' \xrightarrow{\tau} \mu_1'$ such that $\mu = \delta_{C_1} \parallel \mu_1'$. This case is similar with Clause 2, and is omitted here.

□

When restricted to networks in $\mathscr{C}_1 \cap \mathscr{C}_2$, Lemma 5 coincides with the standard congruence property i.e. $C_1 \parallel C \approx C_2 \parallel C$ provided that $C_1 \approx C_2$. Since apparently $C \approx C$, it is easy to see that Lemma 5 implies the standard congruence property. On the other hand, if $C_1 \approx C_2$ and $C_1' \approx C_2'$ where $C_1, C_2, C_1', C_2' \in \mathscr{C}_1 \cap \mathscr{C}_2$, we can imply $C_1 \parallel C_1' \approx C_2 \parallel C_2'$ using the standard congruence in two steps together with the transitivity of $\approx$ as follows: $C_1 \parallel C_1' \approx C_2 \parallel C_1'$ and $C_2 \parallel C_1' \approx C_2 \parallel C_2'$. It is similar for $\approx_p$. Note that in general Lemma 5 cannot be changed to the standard congruence definition, since we cannot always guarantee that $C \in \mathscr{C}_1$ and $C \in \mathscr{C}_2$ for arbitrary C, thus networks $C_1 \parallel C$ and $C_2 \parallel C$ may not be well-formed w.r.t. $\mathcal{M}_1$ and $\mathcal{M}_2$ respectively.

According to Definition 12 we need to consider every $C_1 \in \mathscr{C}_1$ and $C_2 \in \mathscr{C}_2$ in order to check whether $\mathcal{M}_1$ and $\mathcal{M}_2$ are weak (probabilistic) bisimilar or not. This is not possible in practice since $\mathscr{C}_1$ and $\mathscr{C}_2$ are essentially infinite. Due to Lemma 5, it is enough to check each connection individually i.e. networks in $\mathscr{C}_1 \cup \mathscr{C}_2$ of form $\{\{(\rho, k)\} \longmapsto l\}$ for some k, l. Furthermore we only check those connections whose mobility is explicitly defined, since all the others with implicit mobility are guaranteed to be equivalent. We have the following lemma.

Lemma 6. *$\mathcal{M}_1 \approx \mathcal{M}_2$ ($\mathcal{M}_1 \approx_p \mathcal{M}_2$) iff for each $C_1 = \{\{(\rho_1, k)\} \longmapsto l\} \in \mathscr{C}_1$ such that the mobility of $Pro(k \longmapsto l)$ is explicitly defined, there exists $C_2 = \{\{(\rho_2, k)\} \longmapsto l\} \in \mathscr{C}_2$ such that $C_1 \approx C_2$ ($C_1 \approx_p C_2$), and vice versa.*

Proof. The proof is straightforward from Definition 12 and Lemma 5. □

Definition 5 and 6 enable us to abstract the given network. By introducing Definition 12 we can also abstract the given PMF to reduce the state space furthermore without changing the properties we are interested in. We can do so due to the following theorem which states that for any two weak (probabilistic) bisimilar connectivity networks, the resulting networks after putting them in parallel with the same behavior network are still weak (probabilistic) bisimilar. This is the key step in order to abstract the given PMF which we will show in detail later on.

Theorem 10. *Let $B \in \mathscr{B}$, $C_1 \in \mathscr{C}_1$, and $C_2 \in \mathscr{C}_2$, then*

1. $B \parallel C_1 \approx B \parallel C_2$ *provided that* $C_1 \approx C_2$,
2. $B \parallel C_1 \approx_p B \parallel C_2$ *provided that* $C_1 \approx_p C_2$.

Proof. We only prove the first clause since the other one is similar. It is enough to prove that

$$\mathcal{R} = \{(B \parallel C_1, B \parallel C_2) \mid B \in \mathscr{B} \wedge C_1 \approx C_2\}$$

is a weak bisimulation. We first prove that for each $C_1' \in \mathscr{C}_1$ there exists $C_2' \in \mathscr{C}_2$ such that $C_1 \propto C_1' \approx C_2 \propto C_2'$ provided that $C_1 \approx C_2$. It is easy to see that $C_1 \propto C_1' \equiv C_1 \parallel C_1''$ and $C_2 \propto C_2' \equiv C_2 \parallel C_2''$ where C_1'' only contains connectivity information in C_1' which does not occur in C_1, and similar for C_2''. Due to Lemma 6, the following proof is trivial.

Let $E \equiv B \parallel C_1$ and $F \equiv B \parallel C_2$, apparently $E \mathrel{\mathcal{R}} F$. Since for each $C_{E,F,k} \in \mathscr{C}_1$, there exists $C'_{E,F,k} \in \mathscr{C}_2$ such that $C_1 \propto C_{E,F,k} \approx C_2 \propto C'_{E,F,k}$, thus in the following we are safe to assume that both C_1 and C_2 contain enough connectivity information, and the parameters $C_{E,F,k}$ and $C'_{E,F,k}$ can be simply omitted. Suppose $E \xrightarrow{\alpha} \mu$, there are several cases we need to consider:

1. $\alpha = (x, \mathbb{L}) \lhd k$. According to (nREC2) in Table 2.5, there exists $B \xrightarrow{(x,\emptyset)\lhd k} \mu_1$ and $C_1 \xrightarrow{(x,\mathbb{L})\lhd k} \mu_2$ such that $\mu_1 \parallel \mu_2 \equiv \mu$. Since $C_1 \approx C_2$, there exists $C_2 \xRightarrow{(x,\mathbb{L})\lhd k} \mu_2'$ such that $\mu_2 \approx \mu_2'$, thus there exists $F \xRightarrow{(x,\mathbb{L})\lhd k} \mu' = (\mu_1 \parallel \mu_2')$. By induction $\mu\{y/x\} \mathrel{\mathcal{R}} \mu'\{y/x\}$.

2. $\alpha = \langle x, \mathbb{L}\rangle @ k$. According to (nSYN) in Table 2.5, there exists $B \xrightarrow{\langle x,\emptyset\rangle @ k} \mu_1$ and $C_1 \xrightarrow{(x,\mathbb{L})\lhd k} \mu_2$ such that $\mu_1 \parallel \mu_2 \equiv \mu$. Since $C_1 \approx C_2$, there exists $C_2 \xRightarrow{(x,\mathbb{L})\lhd k} \mu_2'$ such that $\mu_2 \approx \mu_2'$, thus there exists $F \xRightarrow{\langle x,\mathbb{L}\rangle @ k} \mu' = (\mu_1 \parallel \mu_2')$. By induction $\mu \mathrel{\mathcal{R}} \mu'$.

3. $\alpha = \tau$. This case is similar and omitted here.

□

Now we show how we can abstract from both behaviors and mobility in two steps. Suppose we are given a network E and a PMF $\mathcal{M}_1$, there exists B_1 and C_1 such that $E \equiv B_1 \parallel C_1$ where B_1 denotes the behavior of the network while C_1 denotes the connectivity information in E. First if we find a simpler B_2 such that

$$B_1 \parallel C_1 \ \approx^{\mathcal{M}_1} \ B_2 \parallel C_1$$

according to Definition 5, then in the following we need only focus on $B_2 \parallel C_1$ which is simpler than $B_1 \parallel C_1$, note that

$$B_1 \parallel C_1 \ \approx^{\mathcal{M}_1} \ B_2 \parallel C_1 \text{ implies that } B_1 \parallel C_1 \ \approx \ B_2 \parallel C_1.$$

As the second step, we can abstract $\mathcal{M}_1$ too. Suppose there exists a simpler $\mathcal{M}_2$ such that $\mathcal{M}_1 \approx \mathcal{M}_2$ according to Definition 12, then for each $C_1 \in \mathscr{C}_1$ there exists $C_2 \in \mathscr{C}_2$ such that $C_1 \approx C_2$. By Theorem 10 we can replace C_1 in E by C_2, and guarantee that

$$E \equiv B_1 \parallel C_1 \ \approx \ B_2 \parallel C_1 \ \approx \ B_2 \parallel C_2.$$

For now on we can analyze $B_2 \parallel C_2$ under the $\mathcal{M}_2$, which shall be much simpler than analyzing E under the $\mathcal{M}_1$. Similarly, we can also do so for $\approx_p$. To illustrate how it works, we give a simple example as follows:

Example 23. *Suppose that there are two* PMF*s:* $\mathcal{M}_1$ *and* $\mathcal{M}_2$ *such that they are the same except for the connection from* l *to* k *i.e.* $Pro(l \longmapsto k)$*. The mobility of* $Pro(l \longmapsto k)$ *is given by Fig. 2.3 in* $\mathcal{M}_1$*, while the mobility of* $Pro(l \longmapsto k)$ *is given by Fig. 2.10 in* $\mathcal{M}_2$*. It is easy to check that* $\mathcal{M}_1 \approx_p \mathcal{M}_2$*, since for any connectivity network* $\{\{(\rho_1, l)\} \longmapsto k\}$ *in* $\mathscr{C}_1$ *where* $\rho_1 \in \{0.5, 0.6, 0.7, 0.8, 0.9\}$*, there exists* $\{\{(\rho_2, l)\} \longmapsto k\}$ *in* $\mathscr{C}_2$ *where* $\rho_2 \in \{0.5, 0.6, 0.7, 0.9\}$ *such that*

$$\{\{(\rho_1, l)\} \longmapsto k\} \ \approx_p \ \{\{(\rho_2, l)\} \longmapsto k\}.$$

Furthermore there is a network

$$E = \lfloor (x) \parallel p \rfloor_l \parallel \{\{(0.8, l)\} \longmapsto k\}$$

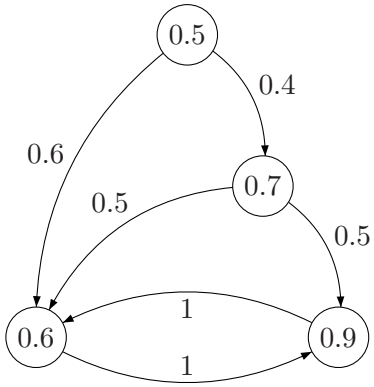

Figure 2.10: A simpler PMF weak probabilistic bisimilar with Fig. 2.3.

in $\mathscr{N}_1$*. First it is easy to see that* $(x) \parallel p \approx p$ *for any* p*, thus*

$$\lfloor (x) \parallel p \rfloor_l \approx_p^{\mathcal{M}_1} \lfloor p \rfloor_l.$$

By Theorem 4,

$$\lfloor (x) \parallel p \rfloor_l \parallel \{\{(0.8, l)\} \longmapsto k\} \approx_p^{\mathcal{M}_1} \lfloor p \rfloor_l \parallel \{\{(0.8, l)\} \longmapsto k\}.$$

Since $\mathcal{M}_2$ *is simpler than* $\mathcal{M}_1$*, it is more preferable for analysis purpose. But according to Definition 1* E *is not well-formed w.r.t.* $\mathcal{M}_2$*, thus we cannot apply* $\mathcal{M}_2$ *directly to* E*. Note that there exists* $\{\{(0.9, l)\} \longmapsto k\} \in \mathscr{C}_2$ *such that*

$$\{\{(0.8, l)\} \longmapsto k\} \approx_p \{\{(0.9, l)\} \longmapsto k\},$$

according to Theorem 10 we have

$$\lfloor p \rfloor_l \parallel \{\{(0.8, l)\} \longmapsto k\} \approx_p \lfloor p \rfloor_l \parallel \{\{(0.9, l)\} \longmapsto k\}$$

where $\lfloor p \rfloor_l \parallel \{\{(0.9, l)\} \longmapsto k\}$ *is a well-formed network w.r.t.* $\mathcal{M}_2$*. As a result* E *and* $\mathcal{M}_1$ *can be replaced by* $\lfloor p \rfloor_l \parallel \{\{(0.9, l)\} \longmapsto k\}$ *and* $\mathcal{M}_2$ *respectively.*

2.6.2 Weak Simulation between PMFs

In this section we extend the work in Section 2.6.1 to simulations. All the definitions and properties are straightforward, but for completeness we write down them here.

Definition 13 (Weak Simulation)**.** *A relation $\mathcal{R} \subseteq (\mathscr{N}_1 \cup \mathscr{N}_2) \times (\mathscr{N}_1 \cup \mathscr{N}_2)$ is a weak simulation if $E\ \mathcal{R}\ F$ implies that for each $k \in L$ and $C_{E,F,k} \in \mathscr{C}_1$, there exists $C'_{E,F,k} \in \mathscr{C}_2$ such that whenever $E \propto C_{E,F,k} \xrightarrow{\alpha} \mu$,*

1. *if $\alpha = (x, \mathbb{L}) \triangleleft k$, there exists $F \propto C'_{E,F,k} \stackrel{\alpha}{\Longrightarrow} \mu'$ such that for each $y \in \mathcal{N}$, $\mu\{y/x\} \sqsubseteq_{\mathcal{R}} \mu'\{y/x\}$;*
2. *if $\alpha = \nu\tilde{x}\langle x, \mathbb{L}\rangle @ l$, there exists $F \propto C'_{E,F,k} \stackrel{\nu\tilde{x}\langle x,\mathbb{L}\rangle @ m}{\Longrightarrow} \mu'$ such that $\mu \sqsubseteq_{\mathcal{R}} \mu'$;*
3. *if $\alpha = \tau$ then there exists $F \propto C'_{E,F,k} \stackrel{\tau}{\Longrightarrow} \mu'$ such that $\mu \sqsubseteq_{\mathcal{R}} \mu'$.*

Let F weakly simulate E, written as $E \lessapprox F$, if there exists a weak simulation $\mathcal{R}$ such that $E\ \mathcal{R}\ F$.

Definition 14 (Weak Probabilistic Simulation)**.** *A relation $\mathcal{R} \subseteq (\mathscr{N}_1 \cup \mathscr{N}_2) \times (\mathscr{N}_1 \cup \mathscr{N}_2)$ is a weak probabilistic simulation if $E\ \mathcal{R}\ F$ implies that for each $k \in L$ and $C_{E,F,k} \in \mathscr{C}_1$, there exists $C'_{E,F,k} \in \mathscr{C}_2$ such that whenever $E \propto C_{E,F,k} \xrightarrow{\alpha} \mu$,*

1. *if $\alpha = (x, \mathbb{L}) \triangleleft k$, there exists $F \propto C'_{E,F,k} \stackrel{\alpha}{\Longrightarrow}_c \mu'$ such that for each $y \in \mathcal{N}$, $\mu\{y/x\} \sqsubseteq_{\mathcal{R}} \mu'\{y/x\}$;*
2. *if $\alpha = \nu\tilde{x}\langle x, \mathbb{L}\rangle @ l$, there exists $F \propto C'_{E,F,k} \stackrel{\nu\tilde{x}\langle x,\mathbb{L}\rangle @ m}{\Longrightarrow}_c \mu'$ such that $\mu \sqsubseteq_{\mathcal{R}} \mu'$;*
3. *if $\alpha = \tau$ then there exists $F \propto C'_{E,F,k} \stackrel{\tau}{\Longrightarrow}_c \mu'$ such that $\mu \sqsubseteq_{\mathcal{R}} \mu'$.*

Let F weakly probabilistic simulate E, written as $E \lessapprox_p F$, if there exists a weak probabilistic simulation $\mathcal{R}$ such that $E\ \mathcal{R}\ F$.

As before we can prove that $\lessapprox$ and $\lessapprox_p$ are preorders.

Theorem 11. *$\lessapprox$ and $\lessapprox_p$ are preorders.*

Proof. Similar with the proof of Theorem 7 and 8. □

Intuitively, $\mathcal{M}_2$ can simulate $\mathcal{M}_1$ iff for each $C_1 \in \mathscr{C}_1$ there exists $C_2 \in \mathscr{C}_2$ such that C_2 can simulate C_1, formally

Definition 15. *Let $\mathcal{M}_2$ weak (probabilistic) simulate $\mathcal{M}_1$, written as $\mathcal{M}_2 \lessapprox \mathcal{M}_1$ ($\mathcal{M}_2 \lessapprox_p \mathcal{M}_1$), iff for each $C_1 \in \mathscr{C}_1$ there exists $C_2 \in \mathscr{C}_2$ such that $C_1 \lessapprox C_2$ ($C_1 \lessapprox_p C_2$).*

The $\lessapprox$ and $\lessapprox_p$ have similar properties as $\approx$ and $\approx_p$. We first show their congruence related to networks in $\mathscr{C}$.

Lemma 7. *Let $C_1, C_1' \in \mathscr{C}_1$ and $C_2, C_2' \in \mathscr{C}_2$, then*

1. *$C_1 \parallel C_1' \precsim C_2 \parallel C_2'$ provided that $C_1 \precsim C_2$ and $C_1' \precsim C_2'$.*
2. *$C_1 \parallel C_1' \precsim_p C_2 \parallel C_2'$ provided that $C_1 \precsim_p C_2$ and $C_1' \precsim_p C_2'$.*

Proof. We only prove the first clause since the other one is similar. It is enough to show that

$$\mathcal{R} = \{(C_1 \parallel C_1', C_2 \parallel C_2') \mid C_1 \precsim C_2 \wedge C_1' \precsim C_2'\}$$

is a weak simulation. For the same reason as in Lemma 7, we can omit the parameters $C_{E,F,k}$ and $C'_{E,F,k}$ in Definition 13. Suppose that $C_1 \parallel C_1' \xrightarrow{\alpha} \mu$, we prove by structural induction and there are only three cases we need to consider:

1. $\alpha = (x, \mathbb{L}) \triangleleft l$. Then according to (nREC2) in Table 2.5, there exists $C_1 \xrightarrow{(x,\mathbb{M})\triangleleft l} \mu_1$ and $C_1' \xrightarrow{(x,\mathbb{N})\triangleleft l} \mu_1'$ such that $\mathbb{M} \cup \mathbb{N} = \mathbb{L}$, and $\mu_1 \parallel \mu_1' = \mu$. Since $C_1 \precsim C_2$ and $C_1' \precsim C_2'$, there exists $C_2 \xRightarrow{(x,\mathbb{M})\triangleleft l} \mu_2$ and $C_2' \xRightarrow{(x,\mathbb{N})\triangleleft l} \mu_2'$ such that $\mu_1 \precsim \mu_1'$ and $\mu_2 \precsim \mu_2'$, thus $C_2 \parallel C_2' \xRightarrow{(x,\mathbb{L})\triangleleft l} \mu' = (\mu_2 \parallel \mu_2')$, by induction $\mu \sqsubseteq_{\mathcal{R}} \mu'$.
2. $\alpha = \tau$. Then according to (nPAR) in Table 2.5, there exists $C_1 \xrightarrow{\tau} \mu_1$ such that $\mu = \mu_1 \parallel \delta_{C_1'}$. Since $C_1 \precsim C_2$, there exists $C_2 \xRightarrow{\tau} \mu_2$ such that $\mu_1 \precsim \mu_2$, thus $C_2 \parallel C_2' \xRightarrow{\tau} \mu' = (\mu_2 \parallel \delta_{C_2'})$. By induction $\mu \sqsubseteq_{\mathcal{R}} \mu'$.
3. $\alpha = \tau$. There exists $C_1' \xrightarrow{\tau} \mu_1'$ such that $\mu = \delta_{C_1} \parallel \mu_1'$. This case is similar with Clause 2, and is omitted here.

□

With Lemma 7 it is enough to check each connection individually in order to determine whether two PMFs are weakly similar. Since we only have finitely many connections whose mobility is explicitly defined, thus we have the analogue lemma as follows:

Lemma 8. *$\mathcal{M}_1 \precsim \mathcal{M}_2$ ($\mathcal{M}_1 \precsim_p \mathcal{M}_2$) iff for each $C_1 = \{\{(\rho_1, k)\} \longmapsto l\} \in \mathscr{C}_1$ such that the mobility of $Pro(k \longmapsto l)$ is explicitly defined, there exists $C_2 = \{\{(\rho_2, k)\} \longmapsto l\} \in \mathscr{C}_2$ such that $C_1 \precsim C_2$ ($C_1 \precsim_p C_2$).*

Proof. The proof is straightforward from Definition 15 and Lemma 7. □

Finally, we have the following theorem.

Theorem 12. *Let $B \in \mathscr{B}$, $C_1 \in \mathscr{C}_1$, and $C_2 \in \mathscr{C}_2$, then*

1. *$B \parallel C_1 \precsim B \parallel C_2$ provided that $C_1 \precsim C_2$,*

2. $B \parallel C_1 \precsim_p B \parallel C_2$ *provided that* $C_1 \precsim_p C_2$.

Proof. We only prove the first clause since the other one is similar. It is enough to prove that

$$\mathcal{R} = \{(B \parallel C_1, B \parallel C_2) \mid B \in \mathscr{B} \wedge C_1 \precsim C_2\}$$

is a weak simulation. The proof is similar with the proof of Theorem 10. We first prove that for each $C_1' \in \mathscr{C}_1$ there exists $C_2' \in \mathscr{C}_2$ such that $C_1 \propto C_1' \precsim C_2 \propto C_2'$ provided that $C_1 \precsim C_2$. It is easy to see that $C_1 \propto C_1' \equiv C_1 \parallel C_1''$ and $C_2 \propto C_2' \equiv C_2 \parallel C_2''$ where C_1'' only contains connectivity information in C_1' which does not occur in C_1, and similar for C_2''. Due to Lemma 8, the following proof is trivial.

Let $E \equiv B \parallel C_1$ and $F \equiv B \parallel C_2$, apparently $E \mathrel{\mathcal{R}} F$. Since for each $C_{E,F,k} \in \mathscr{C}_1$, there exists $C'_{E,F,k} \in \mathscr{C}_2$ such that $C_1 \propto C_{E,F,k} \precsim C_2 \propto C'_{E,F,k}$, thus in the following we are safe to assume that both C_1 and C_2 contain enough connectivity information, and the parameters $C_{E,F,k}$ and $C'_{E,F,k}$ can be simply omitted. Suppose $E \xrightarrow{\alpha} \mu$, there are several cases we need to consider:

1. $\alpha = (x, \mathbb{L}) \lhd k$. According to (nREC2) in Table 2.5, there exists $B \xrightarrow{(x,\emptyset)\lhd k} \mu_1$ and $C_1 \xrightarrow{(x,\mathbb{L})\lhd k} \mu_2$ such that $\mu_1 \parallel \mu_2 \equiv \mu$. Since $C_1 \precsim C_2$, there exists $C_2 \xRightarrow{(x,\mathbb{L})\lhd k} \mu_2'$ such that $\mu_2 \precsim \mu_2'$, thus there exists $F \xRightarrow{(x,\mathbb{L})\lhd k} \mu' = (\mu_1 \parallel \mu_2')$. By induction $\mu\{y/x\} \mathrel{\mathcal{R}} \mu'\{y/x\}$.

2. $\alpha = \langle x, \mathbb{L}\rangle @ k$. According to (nSYN) in Table 2.5, there exists $B \xrightarrow{\langle x,\emptyset\rangle @ k} \mu_1$ and $C_1 \xrightarrow{(x,\mathbb{L})\lhd k} \mu_2$ such that $\mu_1 \parallel \mu_2 \equiv \mu$. Since $C_1 \precsim C_2$, there exists $C_2 \xRightarrow{(x,\mathbb{L})\lhd k} \mu_2'$ such that $\mu_2 \precsim \mu_2'$, thus there exists $F \xRightarrow{\langle x,\mathbb{L}\rangle @ k} \mu' = (\mu_1 \parallel \mu_2')$. By induction $\mu \mathrel{\mathcal{R}} \mu'$.

3. $\alpha = \tau$. This case is similar and omitted here.

□

As mentioned before, for any E there exists B_1 and C_1 such that $E \equiv B_1 \parallel C_1$ where B_1 only describes the behavior and C_1 contains all the known connectivity information. If there exists a simpler B_2 such that $B_1 \parallel C_1 \precsim B_2 \parallel C_1$, then we can use $B_2 \parallel C_1$ instead for analysis purpose. Secondly, if there exists $\mathcal{M}_2$ such that $\mathcal{M}_1 \precsim \mathcal{M}_2$, according to Definition 15, for each C_1 there exists $C_2 \in \mathscr{C}_2$ such that $C_1 \precsim C_2$. By Theorem 12, we have $B_2 \parallel C_1 \precsim B_2 \parallel C_2$. Since $\precsim$ is a preorder, thus $E \equiv B_1 \parallel C_1 \precsim B_2 \parallel C_2$. By doing so it is enough to analyze $B_2 \parallel C_2$ under $\mathcal{M}_2$. As an

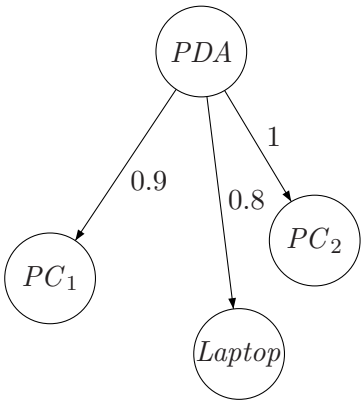

Figure 2.11: A home network.

extreme case the most abstract PMF where every connection has implicit mobility can be used to simulate any arbitrary PMF, thus in some cases we can use this PMF instead depending on what properties we are interested in, which would reduce the state space a lot.

2.7 The Zeroconf Protocol

The Zeroconf protocol is designed for self-configuring home local networks. For example, Fig. 2.11 gives a typical home local network which contains four nodes: PC_1, PC_2, *Laptop*, and *PDA*. The arrows indicate that PC_1, PC_2, and *Laptop* can receive messages from *PDA* with probability 0.9, 1, and 0.8 respectively. Here we assume that all other connections have probability 1.

In order to ensure correct mutual communication, each node must have a unique IP address, so when a new node joins a network it must be assigned an unused IP address. The Zeroconf protocol solves this in the following way:

1. The new node selects randomly an IP address out of all available IP addresses;
2. It broadcasts a message to other nodes to probe if the selected IP address is in use or not;
3. If the new node receives a message indicating the IP address is already taken, then it returns to step 1 and restarts the process;

Table 2.6: The Zeroconf protocol.

$$
\begin{array}{l}
oldnode_{ip} = (x).([x = ip]\langle err\rangle.oldnode_{ip}, oldnode_{ip}) \\
newnode_i^p = \langle p\rangle.waitawk_i^p \\
newnode_0^p = \langle suc\rangle \\
waitawk_i^p = (x).(([x = err]newnode, waitawk_i^p) + newnode_{i-1}^p) \\
newnode = \nu y(y(p).\langle p\rangle.waitawk_{pn}^p \parallel \prod_{ip\in IP} y\langle ip\rangle)
\end{array}
$$

4. Due to unreliable connections, messages can be lost with a certain probability. To increase the reliability of the protocol, the new node is required to send several probes for the same IP address;

5. If no error message has been received after these probes, the selected IP address will be used by the new node.

Note that after running the protocol it is indeed possible for a new node to use an IP address that is already used by another node. This is called address collision and is highly undesirable.

In the following, we model and analyze the Zeroconf protocol, the model of the protocol is given in Table 2.6. [1] We use $oldnode_{ip}$ to denote an existing network node, i.e. a process with IP address ip running at a location; $oldnode_{ip}$ repeatedly receives messages and compares these messages with its own IP address ip. If a message is identical to ip, it will broadcast an error message, err, informing the new node that the selected IP address is being used already. $newnode_i^p$ denotes a process which will probe i times before assuming that the selected IP address p is not used by other nodes. It will evolve into process $waitawk_i^p$ after broadcasting a probe. $newnode_0^p$ is a special process which denotes that the protocol succeeded in finding an unused IP address p (although this might not be true with a certain probability). The process $waitawk_i^p$ waits for the responses from other nodes. If it receives an err message because the selected IP address is not valid, it will restart the whole process, otherwise it will recurse and become $waitawk_i^p$ again. The summation here is used to denote timeout from waiting for responses and then start a new round of probing. $newnode$ starts the protocol by selecting an IP address from IP randomly, here IP is the finite set of all

[1] Summation is defined by: $p + q = \nu x(x\langle y\rangle \parallel x(y)\cdot p \parallel x(y)\cdot q)$.

available addresses and $\prod$ means parallel composition of processes. In the above, we use pn to denote the maximum number of probes for the same IP address.

The behavior of the network in Fig. 2.11 can be represented as follows:

$$E = \lfloor newnode \rfloor_k \parallel \lfloor oldnode_{ip_1} \rfloor_l \parallel \lfloor oldnode_{ip_2} \rfloor_m \parallel \lfloor oldnode_{ip_3} \rfloor_n$$

We assume Laptop, PC1, and PC2 are existing nodes which are located at l, m, and n respectively, and PDA at k is a node that wants to join the network; here ip_1, ip_2, and ip_3 are used to denote IP addresses in IP already in use. Concerning mobility we assume a PMF $\mathcal{M}$ such that the mobility rule of $Pro(k \mapsto l)$ is given by Fig. 2.2 and the mobility rules of $Pro(k \mapsto m)$ and $Pro(k \mapsto n)$ are given by Fig. 2.3, and the nodes at locations l, m, n can always receive messages from the node at location k with probability 1. In addition, the mobility of all the other connections is implicitly defined.

With the logic which we will introduce in Chapter 4, we can denote the obvious property that "if an unused IP address is selected by the new node then the probability of this IP address being allocated to the new node is equal to 1". We may also specify the property: "if an used IP address is selected by the new node then the probability of address collision is less than q". Assuming the maximum number of probes pn to be 3, it turns out that q here cannot be smaller than 0.064 for E satisfying this property. Intuitively, if the new node selects an used IP address such as ip_1, then among all cases to consider there exists a worst case under which $oldnode_{ip_1}$ may fail to receive the probe from the new node for three times with probability $(1 - 0.6)^3 = 0.064$. In the above we assume that $E(k, l) = E(k, m) = E(k, n) = 0.9$.

In order to illustrate analysis through the use of weak bisimulation we may define

$$F \equiv \lfloor newnode \rfloor_k \parallel \lfloor oldnode_{ip_1} \rfloor_l \parallel \lfloor oldnode_{ip_3} \rfloor_m \parallel \lfloor oldnode_{ip_2} \rfloor_n$$

i.e. compared to E in the network F the two old nodes PC1 and PC2 have swapped their locations m and n. Further let

$$E' \equiv \{\{(k, 0.8)\} \mapsto l\} \parallel \{\{(k, 0.6)\} \mapsto m\} \parallel \{\{(k, 0.9)\} \mapsto n\}$$

and let

$$F' \equiv \{\{(k, 0.6)\} \mapsto l\} \parallel \{\{(k, 0.9)\} \mapsto m\} \parallel \{\{(k, 0.8)\} \mapsto n\}$$

then we infer

$$E \parallel E' \approx^{\mathcal{M}} F \parallel F'$$

Intuitively, by the given $\mathcal{M}$ nodes at locations m and n can always receive messages from other locations with the same probability, in addition they can also broadcast messages to other locations with the same probabilities. If the new node selecting an used IP address such as ip_2 broadcasts a probe, then the node at location m in E can receive it with probability 1 and then broadcast an *err* message. The node at location n in F can simulate this by performing the same actions in addition with some mobility transitions. In both E and F, the *newnode* can receive the *err* message with the same probability. A similar argument holds for other transitions.

Suppose that

$$F'' \equiv \{\{(k, 0.7)\} \mapsto l\} \parallel \{\{(k, 0.9)\} \mapsto m\} \parallel \{\{(k, 0.7)\} \mapsto n\}$$

then we know that $E \parallel E' \not\approx^{\mathcal{M}} F \parallel F''$ because if *newnode* selects an used IP address such as ip_2, it will receive the *err* message from location n with probability 0.7 in $F \parallel F''$ which can not be simulated by $E \parallel E'$, but $E \parallel E' \approx_p^{\mathcal{M}} F \parallel F''$ since $E \parallel E'$ has a combined transition where *newnode* can receive *err* message from location m with probability 0.7. The theory introduced in Section 2.5 can be applied to perform one direction abstraction in a similar way, and we omit the detail here.

Now we will show how the theory in Section 2.6 can be used to abstract the given PMF. Suppose that we have a PMF $\mathcal{M}'$ which is the same as $\mathcal{M}$ except that the mobility rule of $Pro(k \mapsto l)$ is given by Fig. 2.12 (a) and the mobility rules of $Pro(k \mapsto m)$ and $Pro(k \mapsto n)$ are given by Fig. 2.12 (b). Then it is easy to check that $\mathcal{M} \approx_p \mathcal{M}'$. Since $\mathcal{M}'$ is simpler than $\mathcal{M}$, thus instead of analyzing E with $\mathcal{M}$ being the mobility function, we can analyze E under $\mathcal{M}'$ which has less states but preserves certain properties. The simulations between PMFs can be applied in a similar way, and are omitted here.

2.8 Related Work

We end this chapter with some related work. In (63) Nanz and Hankin introduced the calculus CBS$^\sharp$ for mobile ad hoc networks (MANETs) which is used as a framework for security analysis of protocols for MANETs. In CBS$^\sharp$ the process connectivity is separated from process actions, and is represented by connectivity graphs whose vertices are

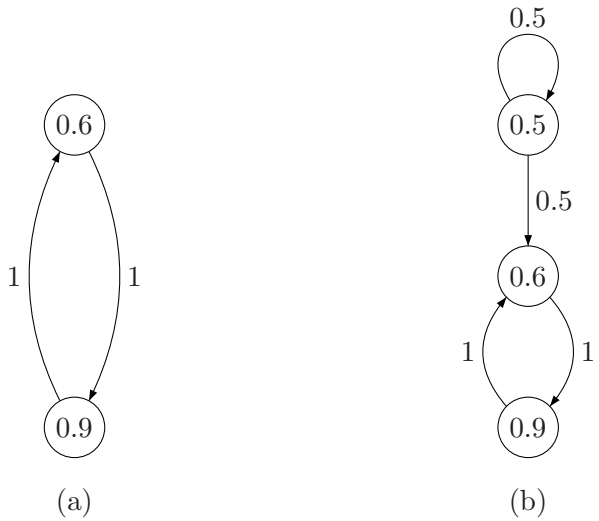

Figure 2.12: A more abstract PMF.

all the locations. Differently, the connections are bidirectional instead of unidirectional. An edge between two locations indicates that they are connected, otherwise they are disconnected. Merro (65) proposed a value-passing process calculus, called CMN, for MANETs. In CMN each node is located at a physical location with a transmission radius denoting its transmission radius. Moreover CMN distinguishes between mobile nodes and stationary nodes. Since the locations in CMN are physical, the connectivity graph is determined by the physical positions of all the locations. A location l is connected to another location k iff l is in the transmission range of k. CMAN was proposed by Godskesen (67) where the connectivity graph is an explicit part of the network syntax and each mobility step corresponds to a computational step, similar as in our calculus. Singh, Ramakrishnan, and Smolka (64) proposed the ω-calculus which is a conservative extension of π-calculus. One of the most important features of ω-calculus is that it separates a node's communication and computational behavior from the description of the physical transmission range. The maximal clique in the connectivity graph is called *group* in ω-calculus. Each location is associated with a set of groups which the location belongs to. Two locations are connected if they have common groups. The change of the interface of each location will also change the underlying connectivity graph. As in (63), ω-calculus deals with bidirectional connectivity. In (66) a restricted broadcast process theory (RBPT) for MANETs was proposed by Ghassemi et al., where connec-

tivity and mobility are modeled implicitly in the semantics instead of in the syntax. By eliminating connectivity information from the syntax, a more compact state space is often obtained. Furthermore, an equational theory for RBPT was proposed in (72) as well as an extended algebra to axiomatize restricted broadcast.

In this chapter we assume that each connection is independent, this might be an unrealistic assumption in practice, since the movement of a node may affect the connectivity probabilities of several connections. In the next chapter we will show how we can extend this calculus in order to deal with dependent mobility. Also we enrich the calculus with other features like continuous time behaviors and mobility, group broadcast and so on.

Chapter 3

Continuous Model

In this chapter we extend the work in Chapter 2 to the continuous scenario. We motivate the work in Section 3.1. The syntax and semantics of the calculus is introduced in Section 3.2 and 3.3 respectively. In Section 3.4 we introduce two notions of weak bisimulations, one of which is defined on networks, while the other one is defined on network distributions. We extend this work to simulations in Section 3.5. In Section 3.6 we show how to remove the limitation that a message can only be received by each node for at most once. We apply our theory to a leader election protocol in Section 3.7. This chapter is concluded with some related work in Section 3.8.

3.1 Motivation

In Chapter 2 we introduced a calculus for MANETs where one of the key features is letting a communication link between two nodes not just be in one of the two states 'connected' or 'disconnected', but also we allowed a decoration of connection links with a probability. The meaning being that messages broadcasted along a connection decorated with a probability ρ will be received by that probability. Intuitively this reflects that connection links in wireless networks may not always be reliable. We also enforced restricted mobility by means of a *probabilistic mobility function* saying that a given node with a certain probability may move and thereby change the probability of the connection to another node. The models we obtain are discrete and each network in our calculus in Chapter 2 gives rise to a probabilistic automata (1). A major contribution in this chapter is a generalization of the notion of a mobility function. In Chapter 2

a mobility function returns the change (the new probability) of just a single connection between two nodes, in this chapter we let a mobility function be able to change a number of connections at the same time, i.e. we recognize that mobility of a single node may not just influence the connection to a single neighbor, instead a mobility step may change a larger part of the network topology. Moreover, the new kind of mobility functions introduced in this chapter makes use of *network topology constraints*. For instance we may specify that the probability for the node l being connected to m must be the same as k being connected to m, i.e. $Pro(l \longmapsto m) = Pro(k \longmapsto m)$. Intuitively this may represent that k and l are always within the same distance from m. Another example could be to require that the likelihood one of k and l receiving a broadcasted message from m is sufficiently high, we may for instance specify $Pro(l \longmapsto m) + Pro(k \longmapsto m) \geq 0.9$, intuitively meaning that m is always sufficiently close to at least one of k and l. We demonstrate the usefulness of topology constraints in Section 3.7.

Another novel contribution of this chapter is the introduction of stochastically timed behavior for MANETs, our contribution follows the tradition of having rates for exponential probability distributions, known from say continuous time Markov processes, as part of our calculus. A major motivation for this contribution is that we would like to more realistically being able to model mobility of nodes as time dependent stochastic phenomenon, this is obtained by letting a stochastic mobility function return no longer a discrete probability as in Chapter 2 but a rate for an exponential probability distribution. Formally we will write $\mathcal{M}(C, C', \mathbb{c}) = \lambda$ where C is the current (partial) network configuration, C' is the new configuration reached by a mobility step, $\mathbb{c}$ is the network topology constraint the transition from C to C' depends on, and the transition occurs with a delay exponentially distributed by λ. Intuitively the rate signifies how fast the network topology will change, i.e. the higher rate the more likely it is that the topology will change fast. Another reason for introducing continuous time stochastic behavior is that many protocols for MANETs make use of time dependent randomized back-off techniques. In order to be able to model such protocols we introduce, in the style of Interactive Markov Chains (32), a prefix construct λ for processes such that we may write e.g. $p = q + \lambda.p$ meaning that p may behave as q or it may after some delay exponentially distributed by λ back off and iterate its behavior. This back-off

style encoding is utilized in our model of a leader election protocol for MANETs defined in Section 3.7. By the introduction of the continuous time stochastic behavior it turns out that the semantics of our calculus is a combination of discrete and continuous time probability, non-determinism, and concurrency and thus gives rise to a Markov Automaton (MA) (5).

A third contribution is that we allow for two novel operators as part of our calculus. To the best of our knowledge these two operators have not before been considered in calculi for mobile and wireless systems. In many broadcast protocols it is quite common for a node to broadcast messages just to a limited number of nodes and hence not to all nodes in the network; to accommodate this feature we introduce a *group broadcast* prefix in our calculus denoted by $\langle x \triangleright L \rangle$ where x is the message to be broadcasted and L is the set of intended receivers of x. The other new operator is a kind of a low level protocol that is often used in many wireless broadcast protocols, it is meant to deal with the problem of *flooding*. Flooding occurs when the same message is broadcasted over and over again in the execution of a protocol, but where it is sufficient to have received and dealt with the message just once. Flooding may e.g. occur in a protocol if a node is naively supposed to forward all requests for being part of a protocol, a node receiving similar requests for participating in the same execution of the protocol from multiple neighbors will then forward each of these requests to its neighbors although forwarding just one of these identical requests would ideally be sufficient. The operator is defined by introducing a memory M for each node, formally we write $\lfloor p \rfloor_l^M$ for a node with the processes p running a location l and with memory M. Intuitively the semantics is that whenever the node receives a broadcasted message x it is first checked whether x belongs to M, if it does x is discarded and p will remain unchanged, otherwise x is added to M and p is updated accordingly. We also show how to remove the flooding avoidance operator in Section 3.6.

In a nutshell we present a continuous time stochastic broadcast calculus for wireless networks with a stochastic mobility function depending on topology constraints where group broadcast and flooding avoidance are integrated operators.

3.2 The Calculus

We take all notations from Chapter 2, moreover we may write l directly for singleton set $\{l\}$. Define the syntax of *topology constraints* $\mathbb{C}$, ranged over by $\mathbb{c}$, as follows:

$$\mathbb{c} ::= Pro(k \longmapsto l) = \rho \mid \mathbb{c} \wedge \mathbb{c} \mid \mathbb{c} \vee \mathbb{c}$$

where $\mathbb{c}$ evaluates to true and false in an obvious way. The above syntax is simple but expressive. For example we can define constraints such as $Pro(k \longmapsto l) \geq 0.8$ and $Pro(l \longmapsto m) + Pro(l \longmapsto n) = 1$ as follows where $\bowtie \in \{<, >, \leq, \geq\}$:

- $Pro(k \longmapsto l) \bowtie \rho \equiv (\bigvee_{\rho' \in \wp \wedge \rho' \bowtie \rho} Pro(k \longmapsto l) = \rho')$;
- $Pro(l \longmapsto m) + Pro(l \longmapsto n) \bowtie \rho \equiv$
  $(\bigvee_{\rho_1, \rho_2 \in \wp \wedge \rho_1 + \rho_2 \bowtie \rho} (Pro(l \longmapsto m) = \rho_1 \wedge Pro(l \longmapsto n) = \rho_2))$.

Other operators can be defined in a similar way. In the sequel instead of writing the whole expressions, we will use these shorthand.

Let $\mathcal{P}$ denote the set of the processes which is ranged over by $p, q, r \ldots$, and defined by the following grammar:

$$p, q ::= 0 \mid Act \cdot p \mid p + q \mid [x = y]p, q \mid \nu x p \mid A$$

$$Act ::= \lambda \mid \langle x \rhd L^* \rangle \mid (x),$$

where $p + q$ denotes nondeterministic choices between p and q, and $Act \cdot p$ means that p is prefixed by Act and will behave as p after Act being preformed. Specially, $\lambda \cdot p$ means that p is guarded by a delay which is exponentially distributed with rate $\lambda \in R^+$.[1] Let $\langle x \rhd L^* \rangle$ and (x) denote (group) broadcast and reception respectively where L^* is either L or $\mathcal{L}$. We usually write $\langle x \rhd \mathcal{L} \rangle$ as $\langle x \rangle$ for simplicity in the following. If $L^* = L$, then $\langle x \rhd L \rangle$ denotes a group broadcast with L as its destination locations which can deliver the message x only to nodes at locations in L. All the other operators are the same as in Chapter 2.

The set of networks $\mathcal{N}$ is defined by:

$$E, F ::= 0 \mid \lfloor p \rfloor_l^M \mid \{\mathbb{L} \longmapsto l\} \mid \nu x E \mid E \parallel F$$

[1] R^+ is the set of all the positive rational numbers.

Table 3.1: Structural congruence of processes and networks (continuous).

$$\nu x E \parallel F \equiv \nu x(E \parallel F), x \notin fn(F)$$

$$(p+q)+r \equiv p+(q+r) \qquad (E \parallel F) \parallel G \equiv E \parallel (F \parallel G)$$

$$\{\mathbb{L}_1 \longmapsto k\} \parallel \{\mathbb{L}_2 \longmapsto k\} \equiv \{\mathbb{L}_1 \cup \mathbb{L}_2 \longmapsto k\}, l(\mathbb{L}_1) \cap l(\mathbb{L}_2) = \emptyset$$

$$p + 0 \equiv p \qquad p + q \equiv q + p \qquad \nu x \nu y p \equiv \nu y \nu x p$$

$$E \parallel 0 \equiv E \qquad \nu x \nu y E \equiv \nu y \nu x E \qquad \{\emptyset \longmapsto l\} \equiv 0$$

$$\lfloor \nu x p \rfloor_l \equiv \nu x \lfloor p \rfloor_l \qquad E \parallel F \equiv F \parallel E \qquad \lfloor p \rfloor_l \equiv \lfloor q \rfloor_l, p \equiv q$$

which is almost the same as in Chapter 2 except for the extra parameter M. The parameter M is a finite memory which is used to keep track of all the messages having been received, and is often omitted if it is not important for the discussion.

The set of free and bound names in E, denoted by $fn(E)$ and $bn(E)$ respectively, are defined as before except that $fn(\lfloor p \rfloor_l^M) = fn(p) \cup M$. Structural congruence of processes and networks, $\equiv$, is the least equivalence relation and congruence closed by α-conversion and the rules in Table 3.1, which can be extended to distributions as usual.

We adopt the same notation here, and let a *stochastic mobility function* (SMF)

$$\mathcal{M} : \mathscr{C} \times \mathscr{C} \times \mathbb{C} \to R^+$$

be a partial function where $\mathcal{M}(C, C', \mathbb{c})$ returns the mobility rate from C to C' given $\mathbb{c}$ evaluates to true. Different from Chapter 2 and (73) where the SMF is defined on a single connection, here we define a SMF on connectivity networks which can be seen as a collection of different connections. The reason to do so is that we can model dependent mobility as described in the introduction. We assume $\mathcal{M}(C, C, \mathit{true}) = 0$ if the connectivity network C is stable. For simplicity we let $\mathcal{M}(C, C', \mathbb{c}) = \perp$ denote that the mobility rule from C to C' under condition $\mathbb{c}$ is undefined.

A SMF is valid if for each C, C' such that $\mathcal{M}(C, C', \mathbb{c}) \neq \perp$ for some $\mathbb{c}$, then

$$C(k,l) = \theta_{k \longmapsto l} \text{ iff } C'(k,l) = \theta_{k \longmapsto l}$$

for all k and l. Intuitively, the condition guarantees that when a mobility step from C to C' happens, it only changes the probability of connectivities in C, and we can neither obtain information about connectivities not in C, nor lose connectivities in C. For instance let $C = \{\{(0.5, m), (0.9, n)\} \longmapsto l\}$ and $C' = \{\{(0.8, m)\} \longmapsto l\}$, a mobility rule from C to C' is not valid since the connectivity information of $\rho_{n \longmapsto l}$ is lost in C', similarly a mobility rule from C' to C is not valid either. In the following we will only consider valid SMFs, and we assume that there is a given $\mathcal{M}$ throughout this chapter.

Since we have infinitely many connectivity networks, it is not reasonable to always define mobility rules for all of them. Instead we allow $\mathcal{M}$ to be defined for just finitely many pairs C and C' and topology constraints $\mathbb{c}$. We call those rules *explicit* mobility rules. A connection $k \longmapsto l$ has an explicit mobility rule if there exists $\mathcal{M}(C, C', \mathbb{c}) \neq \perp$ with $C(k,l) \neq \theta_{k \longmapsto l}$. For any connection $k \longmapsto l$ with no explicit mobility rule we assume it has the implicit mobility rule

$$\mathcal{M}(\{\{(0,k)\} \longmapsto l\}, \{\{(0,k)\} \longmapsto l\}, \mathit{true}) = 0,$$

that is k is not and will never be connected to l. The default implicit mobility can be changed without affecting our theory.

The structural congruence closed set of *well-formed* networks $\mathcal{N}$ under a given SMF $\mathcal{M}$ is inductively defined as follows:

1. $0 \in \mathcal{N}$, and $\lfloor p \rfloor_l^M \in \mathcal{N}$,
2. $\nu x E \in \mathcal{N}$ if $E \in \mathcal{N}$,
3. $E \parallel F \in \mathcal{N}$ if $E, F \in \mathcal{N}$ with $loc(E) \cap loc(F) = \emptyset$ and there does not exist $l, k \in L$ such that $E(k,l) \neq \theta_{k \longmapsto l}$ and $F(k,l) \neq \theta_{k \longmapsto l}$,
4. $C \in \mathcal{N}$ if there exists C' and $\mathbb{c}$ such that $\mathcal{M}(C, C', \mathbb{c}) \neq \perp$.

Clause 1 and 2 is trivial. Clause 3 means that locations are unique and that connectivity information for a single connection can only appear once, while Clause 4 requires that the mobility of each connectivity network must be defined by the given $\mathcal{M}$. A

distribution μ is *well-formed* iff $Supp(\mu) \subseteq \mathcal{N}$, and for any $E, F \in Supp(\mu)$, we have $loc(E) = loc(F)$.

Given a topology constraint $\mathbb{c}$, define operator $E[\mathbb{c}]$ to evaluate $\mathbb{c}$ under a network E by:

- $E[\mathbb{c}_1 \bowtie \mathbb{c}_2] = E[\mathbb{c}_1] \bowtie E[\mathbb{c}_2]$ with $\bowtie \in \{\wedge, \vee\}$,
- $E[Pro(k \longmapsto l) = \rho] = \begin{cases} true & E(k,l) = \rho \\ false & \text{otherwise} \end{cases}$,

and boolean operators are evaluated as usual.

3.3 Labeled Transition System

We use $\mathcal{A}_p$ to denote the actions of processes which are ranged over by $\alpha_p, \beta_p, \ldots$, and defined as follows:

$$\alpha_p ::= \nu\tilde{x}\langle x \rhd L^* \rangle \mid (x) \mid \lambda,$$

where $\nu\tilde{x}\langle x \rhd L^* \rangle$ denotes broadcasting the message x to nodes at locations in L^*, and (x) means that the process can receive a (group) broadcasted message. λ denotes a Markovian action with specified rate. The semantics of processes is given in Table 3.2 where all the rules are standard, and $\rightsquigarrow = (\rightarrow \cup \twoheadrightarrow)$ with $\twoheadrightarrow$ denoting Markovian transitions.

We use $\mathcal{A}$ to denote the actions of networks ranged over by $\alpha, \beta, \ldots$ and defined as follows:

$$\alpha ::= \nu\tilde{x}\langle x \rhd L^*, \mathbb{L} \rangle @ l \mid (x @ L^*, \mathbb{L}) \lhd l \mid \lambda \mid \mathbb{c} : \lambda \mid \tau.$$

Different from processes, for the actions of networks connectivity information is attached to each broadcast and reception. $\nu\tilde{x}\langle x \rhd L^*, \mathbb{L} \rangle @ l$ denotes that the node at location l can broadcast the message x to the node at location $k \in L^*$ with probability ρ if $(\rho, k) \in \mathbb{L}$. Accordingly $(x @ L^*, \mathbb{L}) \lhd l$ means that the node at location $k \in L^*$ can receive the messages from location l with probability ρ if $(\rho, k) \in \mathbb{L}$. $\mathbb{c} : \lambda$ is a novel action named *condition guarded Markovian action*. This action is used to model topology constrained mobility where mobility is triggered only when certain conditions are satisfied. τ and λ are standard.

The semantics of network is given in Table 3.3 with $\rightsquigarrow$ being the union of $\twoheadrightarrow$ and $\rightarrow$ (deliberately overloading symbols for process transitions). When putting a process in a

Table 3.2: Labeled transition system of processes (continuous).

$$\frac{}{\lambda \cdot p \overset{\lambda}{\twoheadrightarrow} p} \text{ (MAR)} \qquad \frac{}{\langle x \rhd L^* \rangle \cdot p \xrightarrow{\langle x \rhd L^* \rangle} p} \text{ (PRE)}$$

$$\frac{p \overset{\alpha_p}{\rightsquigarrow} p'}{p + q \overset{\alpha_p}{\rightsquigarrow} p'} \text{ (SUM)} \qquad \frac{}{(x) \cdot p \xrightarrow{(y)} p\{y/x\}} \text{ (INP)}$$

$$\frac{p \overset{\alpha_p}{\rightsquigarrow} p' \quad x = y}{[x = y]p, q \overset{\alpha_p}{\rightsquigarrow} p'} \text{ (IF)} \qquad \frac{q \overset{\alpha_p}{\rightsquigarrow} q' \quad x \neq y}{[x = y]p, q \overset{\alpha_p}{\rightsquigarrow} q'} \text{ (ELSE)}$$

$$\frac{q \equiv p \overset{\alpha_p}{\rightsquigarrow} p' \equiv q'}{q \overset{\alpha_p}{\rightsquigarrow} q'} \text{ (STR)} \qquad \frac{p \overset{\alpha_p}{\rightsquigarrow} p' \quad A \overset{def}{=} p}{A \overset{\alpha_p}{\rightsquigarrow} p'} \text{ (CON)}$$

$$\frac{p \overset{\alpha_p}{\rightsquigarrow} p' \quad x \notin fn(\alpha_p)}{\nu x p \overset{\alpha_p}{\rightsquigarrow} \nu x p'} \text{ (RES)} \qquad \frac{p \xrightarrow{\langle x \rhd L^* \rangle} p' \quad y \notin fn(\nu x p)}{\nu x p \xrightarrow{\nu y \langle y \rhd L^* \rangle} p'\{y/x\}} \text{ (bOPEN)}$$

location, it will become a node. The behavior of a node is determined by the process in it, but the actions of each node will be enriched with connectivity information as well as the source and destination if they are broadcast and reception, otherwise they will stay unchanged. Note in (nBRD) and (nREC1) there is no connectivity information, so the correspondent connectivity sets in the labels are empty, and furthermore in (nREC1) the node at location l is able to receive a message from location k with unknown probability denoted by $\theta_{l \longmapsto k}$, this is the only rule where unknown probability is added.

Two parallel networks E and F can communicate by broadcast which is shown by (nSYN), the resulting transition will obtain connectivity information from both participants, so the resulting information is the union of the connectivity information from each side, $\mathbb{L} \cup \mathbb{K}$. Also E and F may obtain new connectivity information from each other and update the unknown probabilities that might appear in distributions μ and μ' via the operator $\bullet$. Similarly for (nREC2) two networks in parallel can receive messages concurrently, and obtain connectivity information from each other. In (nSYN) K is the union of the set of locations in F, $loc(F)$, and the set of locations in $\mathbb{K}$ which are not connected to l,

$$\mathcal{Z}(\mathbb{K}) = \{l \mid (0, l) \in \mathbb{K}\}.$$

We remove K from the resulting action where

$$\mathbb{L} \setminus K = \{(\rho, k) \in \mathbb{L} \mid k \notin K\}.$$

It makes sense to remove $\mathcal{Z}(\mathbb{K})$ since nodes at locations $\mathcal{Z}(\mathbb{K})$ will for sure not receive messages from l, thus it is safe to remove them from the destination set of the broadcast. Also we remove locations $loc(F)$ since all the nodes at locations $loc(F)$ in F have already received the broadcasted message. Rules (nBRD), (nREC1), (nREC2), and (nSYN) deal with group broadcast when $L^* = L$. Different from broadcast where the broadcasted messages can be received by any node in any location, group broadcast has specified destinations, nodes at locations which are not in the set of the destinations will simply ignore the messages and stay unchanged, this is taken care of by rule (nIGN). As explained in the introduction we introduce a low level protocol taking care of flooding assuming that a message can only be received by a node at most once. The parameter M at a node is used to keep track of the messages already been received, so only if the coming message is not already in M, it will be dealt with, otherwise it will be simply ignored as explained in rules (nREC1) and (nIGN). On the other hand, if process p at location l cannot perform a reception, it will simply ignore all the coming messages, and stay unchanged as illustrated by (nIGN).

If an action is not broadcast or reception networks can execute in parallel, but still one participant may obtain new connectivity information from the other, this gives the rule (nPAR). Network $\{\mathbb{K} \longmapsto l\}$ only contains connectivity information about l, it can reveal its connectivity information by performing a (group) reception which is shown by (nCONN); it can also, in order to synchronize on broadcast from locations not being l, perform a (group) reception whose source location is different from l with empty connectivity information as illustrated by the rule (nLOS). A broadcast with empty destination has no impact to the outside of the emitting network, therefore it should be seen as an internal action τ which is shown by (nLOC). Rule (nMOB) allows a connectivity network to evolve into another according to the mobility rule defined by the given $\mathcal{M}$ carrying out a condition guarded Markovian action $\mathbb{c} : \lambda$. By (nTRU) if $\mathbb{c}$ is evaluated to true, then $\mathbb{c} : \lambda$ will become a Markovian transition λ. Note in (nREC1) and (nIGN), we require that $l \neq k$ which means that a process at location l cannot receive messages broadcasted from the same location. The rules (nOPEN), (nRES), (nMAR), and (nSTR) are standard.

In our calculus we allow continuous delay, probabilistic choice, and non-deterministic choice, as result each network corresponds to a Markov Automata (5) which is the integration of probabilistic automata (1) with interactive Markov chains (32).

3.4 Weak Bisimulations

3.4.1 Weak Bisimulation on States

In this section we provide a weak bisimulation congruence for our calculus. As usual we do not consider systems (networks) where infinitely many internal actions happen with positive probability since this corresponds to an unrealistic situation where infinitely many actions can happen in finite time i.e. we assume networks to be free of divergence with probability 1, see e.g. (1). For instance network $E \stackrel{def}{=} \lfloor A \rfloor_l \parallel \lfloor \lambda \cdot 0 \rfloor_k$ with $A \stackrel{def}{=} \langle x \rangle \cdot A$ is not free of divergence, since E can perform broadcast from l for infinitely many times, thus blocks the Markovian transition at l for ever. Also we say that a network E is *stable*, written $E\downarrow$, if

$$E \stackrel{\tau}{\not\longrightarrow} \text{ and } E \stackrel{\langle x \triangleright L^*, \mathbb{L} \rangle @ l}{\not\longrightarrow}$$

Note that broadcasts are considered to be immediate and take no time, since they are non-blocking and will be triggered immediately. Accordingly, a network distribution μ is stable, written $\mu\downarrow$, iff $E\downarrow$ for each $E \in Supp(\mu)$.

In order to evaluate the exit rate of a network we, similar with (32), define the function

$$\gamma : \mathscr{N} \times 2^{\mathscr{N}} \mapsto R^+$$

which returns the exit rate from a given network to a set of networks via weak transitions. The formal definition is as follows where $\{\!|\}$ denotes multiset:

$$\gamma(E, S) = \sum \{\!| \lambda \cdot \mu(S) \mid E \stackrel{\lambda}{\twoheadrightarrow} \mu |\!\}.$$

Due to *race condition* (29, 32) among Markov transitions they will compete in order to be executed first, this gives us the following natural transitions. Let $E \stackrel{\lambda}{\rightarrow} \mu$ if $E\downarrow$ where

$$\lambda = \gamma(E, \mathscr{N}) \text{ and } \mu(F) = \frac{\gamma(E, F)}{\lambda}$$

for all F in the support of μ. Refer to the following example for an illustration of race condition.

Table 3.3: Labeled transition system of networks (continuous).

$$\frac{l \neq k}{\{\mathbb{K} \longmapsto k\} \xrightarrow{(x@L^*,\emptyset)\lhd l} \{\mathbb{K} \longmapsto k\}} \text{ (nLOS)}$$

$$\frac{}{\{\mathbb{K} \longmapsto l\} \xrightarrow{(x@L^*,\mathbb{K})\lhd l} \{\mathbb{K} \longmapsto l\}} \text{ (nCONN)}$$

$$\frac{E \xrightarrow{(x@L^*,\mathbb{L})\lhd l} \mu \quad F \xrightarrow{(x@L^*,\mathbb{K})\lhd l} \mu'}{E \parallel F \xrightarrow{(x@L^*,\mathbb{L}\cup\mathbb{K})\lhd l} (\mu \bullet \mathcal{D}(F)) \parallel (\mu' \bullet \mathcal{D}(E))} \text{ (nREC2)}$$

$$\frac{p \xrightarrow{(x)} p' \quad (l \in L^* \wedge x \notin M \wedge k \neq l)}{\lfloor p \rfloor_l^M \xrightarrow{(x@L^*,\emptyset)\lhd k} \{(\theta_{l\longmapsto k} : \lfloor p' \rfloor_l^{M\cup\{x\}}), (1-\theta_{l\longmapsto k} : \lfloor p \rfloor_l^M)\}} \text{ (nREC1)}$$

$$\frac{E \xrightarrow{\nu\tilde{y}\langle y\rhd L^*,\mathbb{L}\rangle@l} \mu \quad F \xrightarrow{(y@L^*,\mathbb{K})\lhd l} \mu' \quad \tilde{y} \cap fn(F) = \emptyset \quad K = loc(F) \cup \mathcal{Z}(\mathbb{K})}{E \parallel F \xrightarrow{\nu\tilde{y}\langle y\rhd(L^*\backslash K),(\mathbb{L}\cup\mathbb{K})\backslash K\rangle@l} (\mu \bullet \mathcal{D}(F)) \parallel (\mu' \bullet \mathcal{D}(E))} \text{ (nSYN)}$$

$$\frac{E \xrightarrow{\mathbb{c}:\lambda} \mu \quad E[\mathbb{c}] = true}{E \overset{\lambda}{\twoheadrightarrow} \mu} \text{ (nTRU)} \qquad \frac{E \xrightarrow{\langle x\rhd L^*,\mathbb{L}\rangle@l} \mu \quad y \notin fn(\nu x E)}{\nu x E \xrightarrow{\nu y\langle y\rhd L^*,\mathbb{L}\rangle@l} \mu\{y/x\}} \text{ (nOPEN)}$$

$$\frac{p \overset{\lambda}{\twoheadrightarrow} p'}{\lfloor p \rfloor_l \overset{\lambda}{\twoheadrightarrow} \lfloor p' \rfloor_l} \text{ (nMAR)} \qquad \frac{p \xrightarrow{\nu\tilde{x}\langle x\rhd L^*\rangle} p'}{\lfloor p \rfloor_l^M \xrightarrow{\nu\tilde{x}\langle x\rhd(L^*\backslash l),\emptyset\rangle@l} \lfloor p' \rfloor_l^M} \text{ (nBRD)}$$

$$\frac{F \equiv E \overset{\alpha}{\rightsquigarrow} \mu \equiv \mu'}{F \overset{\alpha}{\rightsquigarrow} \mu'} \text{ (nSTR)} \qquad \frac{E \xrightarrow{\alpha} \mu \quad \alpha \in \{\tau, \mathbb{c} : \lambda\}}{E \parallel F \xrightarrow{\alpha} (\mu \bullet \mathcal{D}(F)) \parallel F} \text{ (nPAR)}$$

$$\frac{E \overset{\alpha}{\rightsquigarrow} \mu \quad x \notin fn(\alpha)}{\nu x E \overset{\alpha}{\rightsquigarrow} \nu x \mu} \text{ (nRES)} \qquad \frac{\mathcal{M}(C, C', \mathbb{c}) = \lambda}{C \xrightarrow{\mathbb{c}:\lambda} C'} \text{ (nMOB)}$$

$$\frac{E \xrightarrow{\nu\tilde{y}\langle x\rhd\emptyset,\mathbb{L}\rangle@l} \mu}{E \xrightarrow{\tau} \mu} \text{ (nLOC)} \qquad \frac{k \neq l \wedge (l \notin L^* \vee x \in M \vee p \overset{(x)}{\not\longrightarrow})}{\lfloor p \rfloor_l^M \xrightarrow{(x@L^*,\emptyset)\lhd k} \lfloor p \rfloor_l^M} \text{ (nIGN)}$$

Example 24. *Let*

$$E = \lfloor \lambda_1 \cdot p + \lambda_2 \cdot q \rfloor_l,$$

It is easy to see that E has two Markovian transitions according to Table 3.2 and 3.3:

$$E \overset{\lambda_1}{\twoheadrightarrow} \lfloor p \rfloor_l \text{ and } E \overset{\lambda_2}{\twoheadrightarrow} \lfloor q \rfloor_l.$$

The exit rate of E is equal to $\lambda = \lambda_1 + \lambda_2$*, and moreover the two Markovian transitions will compete with each other to be executed first. According to the race condition, the first transition will be executed with probability* $\frac{\lambda_1}{\lambda}$*, while the second one will be executed with probability* $\frac{\lambda_2}{\lambda}$*, i.e.*

$$E \overset{\lambda}{\rightarrow} \{\frac{\lambda_1}{\lambda} : \lfloor p \rfloor_l, \frac{\lambda_2}{\lambda} : \lfloor q \rfloor_l\}.$$

As always in a weakly bisimilar setting we abstract from internal actions. We use $E \overset{\alpha}{\Longrightarrow} \mu$ to denote that a distribution μ is reached through a sequence of steps which are internal except one being equal to α. Formally $\overset{\alpha}{\Longrightarrow}$ is the least relation such that, $E \overset{\alpha}{\Longrightarrow} \mu$ iff either

1. $\alpha = \tau$ and $\mu = \delta_E$, or
2. $E \overset{\alpha}{\rightarrow} \mu$, or
3. there exists a transition $E \overset{\beta}{\rightarrow} \mu'$ such that

$$\mu = \sum_{E' \in Supp(\mu')} \mu'(E') \cdot \mu_{E'},$$

where $E' \overset{\tau}{\Longrightarrow} \mu_{E'}$ if $\beta = \alpha$, otherwise $E' \overset{\alpha}{\Longrightarrow} \mu_{E'}$ and $\beta = \tau$.

As in (1) we also define the combined transition $\overset{\alpha}{\Longrightarrow}_c$ such that: $E \overset{\alpha}{\Longrightarrow}_c \mu$ iff there exists

$$\{E \overset{\alpha}{\Longrightarrow} \mu_i\}_{1 \leq i \leq n} \text{ and } \{w_i\}_{1 \leq i \leq n}$$

such that

$$\sum_{1 \leq i \leq n} w_i = 1 \text{ and } \sum_{1 \leq i \leq n} w_i \cdot \mu_i = \mu.$$

Another abstraction is that we disregard the emitter of a broadcast message and allow to equate $\nu\tilde{x}\langle x \rhd L^*, \mathbb{L}\rangle@l$ and $\nu\tilde{x}\langle x \rhd L^*, \mathbb{L}\rangle@k$ indicating that in a wireless broadcast setting the sender of a message is not important, that is only the message (and the probability by which it is received), since the receiver of a message may not precisely know whom is the actual physical emitter of the message. We will also allow

that a broadcast can be simulated by several broadcasts. In order to do so we define the combination of two broadcast actions such that

$$\nu\tilde{x}\langle x \rhd L_1, \mathbb{L}_1\rangle@l_1 \otimes \nu\tilde{x}\langle x \rhd L_2, \mathbb{L}_2\rangle@l_2 = \nu\tilde{x}\langle x \rhd L, \mathbb{L}\rangle@l$$

where $L = L_1 \cup L_2$, l is any location name, and $\mathbb{L} = \mathbb{M}_1 \cup \mathbb{M}_2$ with

$$\mathbb{M}_1 = \{(\rho, k) \in \mathbb{L}_1 \mid k \in L_1 \setminus L_2\} \cup \{(\rho, k) \in \mathbb{L}_2 \mid k \in L_2 \setminus L_1\},$$

$$\mathbb{M}_2 = \{(1 - (1 - \rho_1) \cdot (1 - \rho_2), k) \mid k \in L_1 \cap L_2 \wedge (\rho_1, k) \in \mathbb{L}_1 \wedge (\rho_2, k) \in \mathbb{L}_2\}.$$

Intuitively, the resulting combination of two actions has the same effects as the original two. There are three cases to consider. If a location k is only in L_1, then the probability for location k receiving the broadcasted message x will not be changed by $\nu\tilde{x}\langle x \rhd L_2, \mathbb{L}_2\rangle@l_2$, similarly for locations only in L_2. For a location k appearing in both L_1 and L_2, the probability for k not receiving x is equal to $(1-\rho_1)\cdot(1-\rho_2)$ if $(\rho_1, k) \in \mathbb{L}_1$ and $(\rho_2, k) \in \mathbb{L}_2$, as a result the probability for a node at location k receiving x is equal to $1 - (1 - \rho_1) \cdot (1 - \rho_2)$. Obviously, $\otimes$ is associative and commutative. The following example shows how the operator $\otimes$ works.

Example 25. *Suppose that*

$$\alpha_1 = \langle x \rhd \{m, n\}, \{(0.7, m), (0.4, n)\}\rangle@k,$$

$$\alpha_2 = \langle x \rhd \{n, l\}, \{(0.6, n), (0.8, l)\}\rangle@k,$$

then $\alpha_1 \otimes \alpha_2 = \alpha$ *where*

$$\alpha = \langle x \rhd \{m, n, l\}, \{(0.7, m), (0.76, n), (0.8, l)\}\rangle@k.$$

Since the node at m *can only receive* x *from* k *with probability 0.7 in* α_1*, thus it can also receive* x *from* k *with the same probability in* α*, similarly for* l*. On the other hand since the node at* n *can receive* x *from* k *in both* α_1 *and* α_2 *with probabilities 0.4 and 0.6 respectively, therefore the probability from it receiving* x *from* k *in* α *is equal to* $1 - (1 - 0.4) \cdot (1 - 0.6) = 0.76$*.*

We extend the broadcast transitions in the following way:

$$E \xrightarrow{\langle x \rhd L^*, \mathbb{L}\rangle@l} \mu \text{ iff } E \stackrel{\alpha_1}{\Longrightarrow} \stackrel{\alpha_2}{\Longrightarrow} \ldots \stackrel{\alpha_n}{\Longrightarrow} \mu$$

with $\langle x \rhd L^*, \mathbb{L}\rangle@l = (\bigotimes_{1 \le i \le n} \alpha_i)$.

As in Chapter 2 we make use of the following finite sets of connectivity networks in the definition of our bisimulation:

$$\mathscr{C}_L = \{C \in \mathscr{C} \mid \forall l, k \in L.C(k,l) \neq \theta_{k \longmapsto l}\}.$$

Intuitively, $\mathscr{C}_L$ contains all the connectivity networks such that the probability of $Pro(k \longmapsto l)$ is known for all $l, k \in L$. Below follows the definition of weak bisimulation of networks where we use $C_{E,F,k}$ to range over $\mathscr{C}_{(l(E) \cup l(F) \cup \{k\})}$, and we let α_k range over all actions including λ except broadcast receptions from locations l where $l \neq k$.

Definition 16 (Weak Bisimulation)**.** *An equivalence relation $\mathcal{R} \subseteq \mathcal{N} \times \mathcal{N}$ is a weak bisimulation iff $E \mathcal{R} F$ implies that for each k and $C_{E,F,k}$, whenever*

$$E \propto C_{E,F,k} \xrightarrow{\alpha_k} \mu,$$

there exists

$$F \propto C_{E,F,k} \stackrel{\alpha_k}{\Longrightarrow}_c \mu'$$

such that $\mu \mathcal{R} \mu'$.

Let E and F be weakly bisimilar, written as $E \approx F$, if there exists a weak bisimulation $\mathcal{R}$ such that $E \mathcal{R} F$.

The cases when α_k is τ or λ are standard. When $\alpha_k = (x@L, \mathbb{L}) \lhd k$, any received message must be matched by receiving the same message with the same probabilities from the same sender. Observe that the source of the message cannot appear in $loc(E)$ due to the semantics in Table 3.3, as a consequence one may prove that $E \approx F$ implies $loc(E) = loc(F)$.

Example 26. *Given a $\mathcal{M}$ such that l and k can always connect to all locations except m with the same probability, and all locations can always connect to l and k with the same probability. Then*

$$\lfloor (x) \cdot \langle x \rangle \rfloor_l \parallel \lfloor 0 \rfloor_k \parallel \lfloor 0 \rfloor_m \approx \lfloor (x) \cdot \langle x \rangle \rfloor_k \parallel \lfloor 0 \rfloor_l \parallel \lfloor 0 \rfloor_m$$

but since l and k can receive messages from the node at location m with different probabilities

$$\lfloor (x) \cdot \langle x \rangle \rfloor_l \parallel \lfloor 0 \rfloor_k \not\approx \lfloor (x) \cdot \langle x \rangle \rfloor_k \parallel \lfloor 0 \rfloor_l$$

When a network is not stable, then all the Markovian transitions are blocking, and cannot affect the behaviors of the network. This is the so called *maximal progress assumption* which is a quite common in time (discrete and continuous) process calculi (32, 74, 75).

Example 27. *Consider two networks:*

$$E = \lfloor \langle x \rhd L \rangle \cdot p + \lambda \cdot q \rfloor_l,$$

$$F = \lfloor \langle x \rhd L \rangle \cdot p \rfloor_l,$$

since E is not stable due to $E \xrightarrow{\langle x \rhd L, \emptyset \rangle @ l}$, therefore the Markovian transition $E \xrightarrow{\lambda}$ can be omitted, obviously $E \approx F$.

When $\alpha_k = \nu \tilde{x} \langle x \rhd L^*, \mathbb{L} \rangle @ l$ any broadcasted message x must be matched by a broadcast action containing the same x, and x must be received at the same locations with the same probability, but the emitter need not be the same.

Example 28. *Given a $\mathcal{M}$ where l is disconnected from k forever, that is, location l can only receive messages from location k with probability 0. Then*

$$\lfloor \langle x \rhd l \rangle \rfloor_k \approx \lfloor 0 \rfloor_k$$

If $Pro(l \longmapsto k)$ is not always 0 then $\lfloor \langle x \rhd l \rangle \rfloor_k \not\approx \lfloor 0 \rfloor_k$, but if the node at l cannot receive then e.g.

$$\lfloor \langle x \rhd l \rangle \rfloor_k \parallel \lfloor 0 \rfloor_l \approx \lfloor 0 \rfloor_k \parallel \lfloor 0 \rfloor_l.$$

Additionally when $\alpha_k = \nu \tilde{x} \langle x \rhd L^*, \mathbb{L} \rangle @ l$, we also allow that a broadcast can be simulated by a series of broadcasts whose combination is equivalent to the original broadcast. This relies on the assumption that each message can only be received by a node at most once.

Example 29. *Given a $\mathcal{M}$ such that location l can receive messages from location k with probability either 1 or 0. Then*

$$\lfloor \langle x \rhd l \rangle \cdot \langle x \rhd l \rangle \rfloor_k \parallel \lfloor p \rfloor_l^M \approx \lfloor \langle x \rhd l \rangle \rfloor_k \parallel \lfloor p \rfloor_l^M$$

for any p. The reason is that after the process at location k receives the message x, it will remember it, and if it receives the same message for the second time, it will simply ignore it and stay unchanged.

In all cases in Definition 16 we use $C_{E,F,k}$ to eliminate all the possible unknown probabilities during the evolution of both E and F. Observe that unknown probabilities can only appear in derivatives on networks in case of broadcast and reception actions. The reason to include k is because k might be any location not appearing in either E or F, thus when E or F performs a reception from k, an unknown probability $\theta_{l\longmapsto k}$ with $l \in l(E) \cup l(F)$ may arise. Such an unknown probability may be eliminated by applying any $C_{E,F,k}$. When performing broadcasts the only possible unknown probability in a derivative from E and F is of the form $\theta_{m\longmapsto n}$ with $m, n \in l(E) \cup l(F)$, thus it can also be removed by applying any $C_{E,F,k}$.

Example 30. *Given a $\mathcal{M}$ such that $Pro(m \longmapsto n)$ is stable and always equal to 0.5 and two networks: $E = \{\{(0.5, m)\} \longmapsto n\}$ and $F = 0$. Without applying a $C_{E,F,k}$, we will conclude that $E \not\approx F$ since*

$$E \xrightarrow{(x@L^*,\{(0.5,m)\})\triangleleft n} \delta_E$$

which cannot be simulated by F. This is against our intuition since we know that $Pro(m \longmapsto n)$ is always equal to 0.5, thus F should be able to exploit this fact from the given $\mathcal{M}$. By applying any $C_{E,F,k}$ it is easy to check that $E \approx F$.

By applying $C_{E,F,k}$, we can make sure that

$$(E \propto C_{E,F,k})(m, n) = \theta_{m\longmapsto n} \text{ iff } (F \propto C_{E,F,k})(m, n) = \theta_{m\longmapsto n}$$

for any $m, n \in \mathcal{L}$ i.e. the probability of each connection is known in $E \propto C_{E,F,k}$ iff it is also known in $F \propto C_{E,F,k}$ even that their values may not coincide. Therefore we do not need to consider action $\mathbb{c} : \lambda$ in Definition 16, since we can make sure that all the actions like $\mathbb{c} : \lambda$ will be resolved to λ if $\mathbb{c}$ is true, otherwise $\mathbb{c}$ is false and $\mathbb{c} : \lambda$ is blocked.

Below we introduce several lemmas which will be useful for proving the congruence of $\approx$.

Lemma 9. *$E \xrightarrow{\nu x\langle x \triangleright L^*,\mathbb{L}\rangle@l} \mu$ iff $E \equiv \nu x E'$ and $E' \xrightarrow{\langle x \triangleright L^*,\mathbb{L}\rangle@l} \mu$.*

Proof. The *only if* direction follows by induction in the latest inference of $E \xrightarrow{\alpha} \mu$ and the *if* direction is due to (nSTR), and (nOPEN) in Table 3.3. □

Let us extend the operator $\otimes$ to receptions as follow:

$$(x@L_1, \mathbb{L}_1) \lhd l_1 \otimes (x@L_2, \mathbb{L}_2) \lhd l_2 = (x@L, \mathbb{L}) \lhd l$$

where $L = L_1 \cup L_2$, l is any location name, and $\mathbb{L} = \mathbb{M}_1 \cup \mathbb{M}_2$ with

$$\mathbb{M}_1 = \{(\rho, k) \in \mathbb{L}_1 \mid k \in L_1 \setminus L_2\} \cup \{(\rho, k) \in \mathbb{L}_2 \mid k \in L_2 \setminus L_1\}$$
$$\mathbb{M}_2 = \{(1 - (1 - \rho_1) \cdot (1 - \rho_2), k) \mid k \in L_1 \cap L_2 \wedge (\rho_1, k) \in \mathbb{L}_1 \wedge (\rho_2, k) \in \mathbb{L}_2\}$$

The following lemma says that we can separate a single reception into several receptions as long as their combination is the same as the original reception.

Lemma 10. *If* $E \xrightarrow{(x@L,\mathbb{L})\lhd l} \mu$, *then*

$$E \xrightarrow{(x@L_1,\mathbb{L}_1)\lhd l_1} \xrightarrow{(x@L_2,\mathbb{L}_2)\lhd l_2} \ldots \xrightarrow{(x@L_n,\mathbb{L}_n)\lhd l_n} \mu$$

whenever

$$\otimes_{1 \le i \le n}((x@L_i, \mathbb{L}_i) \lhd l_i) = (x@L, \mathbb{L}) \lhd l.$$

Proof. Suppose that there exists k and E' such that

$$E \equiv \nu\tilde{x}(\lfloor p \rfloor_k \parallel E')$$

where $k \in L$. We prove by induction on the number n of such k. The case when $n = 0$ is trivial since $\mu = \delta_E$. Assume that $n > 0$. Then it is not hard to see that

$$\mu \equiv \nu\tilde{x}(\{\rho : \lfloor p' \rfloor_k, 1 - \rho : \lfloor p \rfloor_k\} \parallel \mu')$$

where $(\rho, k) \in \mathbb{L}$, $p \xrightarrow{(x)} p'$ and $E' \xrightarrow{(x@L,\mathbb{L})\lhd l} \mu'$. By induction

$$E' \xrightarrow{(x@L_1,\mathbb{L}_1)\lhd l_1} \xrightarrow{(x@L_2,\mathbb{L}_2)\lhd l_2} \ldots \xrightarrow{(x@L_n,\mathbb{L}_n)\lhd l_n} \mu'$$

whenever

$$\otimes_{1 \le i \le n}((x@L_i, \mathbb{L}_i) \lhd l_i) = (x@L, \mathbb{L}) \lhd l.$$

Also note that the probability ρ is only determined by the probability of k receiving the message x, thus

$$\lfloor p \rfloor_k \parallel \mathcal{D}(E) \xrightarrow{(x@L_1,\mathbb{L}_1)\lhd l_1} \xrightarrow{(x@L_2,\mathbb{L}_2)\lhd l_2} \ldots \xrightarrow{(x@L_n,\mathbb{L}_n)\lhd l_n}$$
$$\{\rho : \lfloor p' \rfloor_k \parallel \mathcal{D}(E), 1 - \rho : \lfloor p \rfloor_k \parallel \mathcal{D}(E)\}.$$

As a result,

$$E \xrightarrow{(x@L_1,\mathbb{L}_1)\lhd l_1} \xrightarrow{(x@L_2,\mathbb{L}_2)\lhd l_2} \ldots \xrightarrow{(x@L_n,\mathbb{L}_n)\lhd l_n} \mu$$

which completes the proof. □

Let $\mu \propto C = \{(\mu(E) : E \propto C)\}$, the following lemma shows that we can attach any extra connectivity information to networks while preserving the weak bisimulation relation.

Lemma 11. *$E \parallel C \approx F \parallel C$ for any C provided that $E \approx F$*

Proof. It is enough to prove that

$$\mathcal{R} = \{(E \parallel C, F \parallel C) \mid E \approx F\}$$

is a weak bisimulation. Let $E' = E \parallel C$ and $F' = F \parallel C$. Assume that

$$E' \propto C_{E',F',l} \xrightarrow{(x@L,\mathbb{L})\lhd l} \mu_1'$$

for some $C_{E',F',l}$, then we need to prove that there exists

$$F' \propto C_{E',F',l} \xRightarrow{(x@L,\mathbb{L})\lhd l}_c \mu_2'$$

such that $\mu_1' \mathcal{R} \mu_2'$. It is not hard to see that for each $C_{E',F',l}$, there exists $C_{E,F,l}$ and C' such that

$$E' \propto C_{E',F',l} \equiv (E \propto C_{E,F,l}) \parallel C' \text{ and}$$
$$F' \propto C_{E',F',l} \equiv (F \propto C_{E,F,l}) \parallel C'.$$

It is trivial to show that

$$E \propto C_{E,F,l} \approx F \propto C_{E,F,l}$$

since $E \approx F$. If

$$E' \propto C_{E',F',l} \xrightarrow{\langle x \rhd L,\mathbb{L}\rangle@l} \mu_1',$$

then by (nLOS), (nCONN), and (nREC2) there exists

$$E \propto C_{E,F,l} \xrightarrow{\langle x \rhd K,\mathbb{M}\rangle@l} \mu_1$$

and $C' \xrightarrow{(x@K,\mathbb{N})\lhd l} C'$ such that $\mu_1 \parallel C' = \mu_1'$ (μ_1 contains no unknown probability since $E \propto C_{E,F,l}$ has enough connectivity information to resolve all the possible unknown probability.), $L = K \setminus \mathcal{Z}(\mathbb{N})$, and $\mathbb{L} = (\mathbb{M} \cup \mathbb{N}) \setminus \mathcal{Z}(\mathbb{N})$. Since

$$E \propto C_{E,F,l} \approx F \propto C_{E,F,l},$$

there exists

$$F \propto C_{E,F,l} \xRightarrow{\langle x \rhd K,\mathbb{M}\rangle@l}_c \mu_2$$

such that $\mu_1 \approx \mu_2$, thus there exists

$$F' \propto C_{E',F',l} \xRightarrow{(x@L,\mathbb{L})\lhd l}_c \mu_2' \equiv \mu_2 \parallel C'.$$

According to the definition of $\mathcal{R}$, we have $\mu_1' \mathcal{R} \mu_2'$, this completes the proof. □

The following theorem shows that the weak bisimulation is a congruence.

Theorem 13. $\approx$ *is a congruence.*

Proof. Due to Lemma 11 it is enough to prove that

$$\mathcal{R} = \{(\nu\tilde{x}(E \parallel G), \nu\tilde{x}(F \parallel G)) \mid E \approx F\}$$

is a weak bisimulation where G does not contain connectivity information i.e. $\mathcal{D}(G) = \emptyset$. Let

$$E_0 = \nu\tilde{x}(E \parallel G) \text{ and } F_0 = \nu\tilde{x}(F \parallel G),$$

we need to prove that for each k and $C_{E_0,F_0,k}$, if

$$E_0 \propto C_{E_0,F_0,k} \xrightarrow{\alpha_k} \mu_0,$$

there exists

$$F_0 \propto C_{E_0,F_0,k} \stackrel{\alpha_k}{\Longrightarrow}_c \mu_0'$$

such that $\mu_0 \mathcal{R} \mu_0'$. Since G contains no connectivity information,

$$E_0 \propto C_{E_0,F_0,k} \equiv \nu\tilde{x}((E \propto C_{E_0,F_0,k}) \parallel G) \equiv \nu\tilde{x}(((E \propto C_{E,F,k}) \parallel C) \parallel G)$$

for some $C_{E,F,k}$ and C, similarly for F_0. We consider the following cases.

1. $\alpha_k = \langle x \triangleright L, \mathbb{L}\rangle @ l$.
   Suppose that

   $$(E \propto C_{E,F,k}) \parallel C \xrightarrow{\langle x \triangleright K, \mathbb{K}\rangle @ l} \mu \text{ and } G \xrightarrow{(x @ K, \emptyset) \triangleleft l} \mathbb{G}$$

   such that $L = K \setminus loc(G)$, $\mathbb{L} = \mathbb{K} \setminus loc(G)$, and

   $$\mu_0 = \nu\tilde{x}(\mu \parallel (\mathbb{G} \propto \mathcal{D}(\{\mathbb{L} \longmapsto l\}))).$$

   Since

   $$(E \propto C_{E,F,k}) \parallel C \approx (F \propto C_{E,F,k}) \parallel C$$

   by Lemma 11, there exists

   $$(F \propto C_{E,F,k}) \parallel C \stackrel{\langle x \triangleright K, \mathbb{K}\rangle @ l}{\Longrightarrow}_c \mu'$$

   such that $\mu \approx \mu'$. By Lemma 10 we know that one reception can be divided into several receptions and vice versa as long as their accumulated results are same, so there exists

   $$F_0 \stackrel{\alpha_k}{\Longrightarrow}_c \mu_0' \equiv \nu\tilde{x}(\mu' \parallel (\mathbb{G} \propto \mathcal{D}(\{\mathbb{L} \longmapsto l\}))),$$

   thus $\mu_0 \mathcal{R} \mu_0'$.

2. $\alpha_k = (x@L, \mathbb{L}) \lhd k$.
   Suppose that

$$(E \propto C_{E,F,k}) \parallel C \xrightarrow{(x@L,\mathbb{L})\lhd k} \mu \text{ and } G \xrightarrow{(x@L,\emptyset)\lhd k} \mathbb{G}$$

   such that

$$\mu_0 = \nu\tilde{x}(\mu \parallel (\mathbb{G} \propto \mathcal{D}(\{\mathbb{L} \longmapsto l\}))).$$

   Since

$$(E \propto C_{E,F,k}) \parallel C \;\approx\; (F \propto C_{E,F,k}) \parallel C$$

   by Lemma 11, there exists

$$(F \propto C_{E,F,k}) \parallel C \xRightarrow{\langle x \triangleright L,\mathbb{L}\rangle@k}_c \mu'$$

   such that $\mu \;\approx\; \mu'$. By (nREC2), there exists

$$F_0 \xRightarrow{\langle x \triangleright L,\mathbb{L}\rangle@k}_c \mu'_0 \equiv \nu\tilde{x}(\mu' \parallel (\mathbb{G} \propto \mathcal{D}(\{\mathbb{L} \longmapsto l\}))),$$

   thus $\mu_0 \;\mathcal{R}\; \mu'_0$.

3. The other cases are similar.

□

The definition of our bisimulation depends on a given SMF $\mathcal{M}$, the more restricted the $\mathcal{M}$ the more bisimilar networks we can obtain. For instance, if we consider the extreme case where all the nodes are disconnected from each other all the time, that is, they cannot influence each other's behaviors, we then have $\lfloor p \rfloor_l \;\approx\; \lfloor q \rfloor_l$ for any p, q.

3.4.2 Weak Bisimulation on Distributions

Even though the weak bisimulation defined in Definition 16 may be considered natural and equate many networks that should obviously be considered similar, the bisimulation may also be considered to be too strict as illustrated by the following example:

Example 31. *Given a $\mathcal{M}$ such that $k \longmapsto l$ is either equal to 0.5 or 0.75 and $k \longmapsto m$ is always equal to 0 for $m \neq l$. Then intuitively*

$$E = \lfloor \langle y \triangleright k \rangle \cdot \langle y \triangleright k \rangle \rfloor_l \parallel \lfloor (x) \cdot p \rfloor_k^{\emptyset} \parallel \{\{(0.5, k)\} \longmapsto l\},$$

$$F = \lfloor \langle y \triangleright k \rangle \rfloor_l \parallel \lfloor (x) \cdot p \rfloor_k^{\emptyset} \parallel \{\{(0.75, k)\} \longmapsto l\}$$

are bisimilar, since in both E and F the message y can be received by p at location k with probability 0.75 eventually, even though in E we need two broadcasts in order to do so while in F only one broadcast is enough. But by Definition 16 $E \not\approx F$ since

$$E \xrightarrow{\tau} \begin{cases} 0.5 : \lfloor \langle y \rhd k \rangle \rfloor_l \parallel \lfloor (x) \cdot p \rfloor_k^{\emptyset} \parallel \{\{(0.5, k)\} \longmapsto l\} = E_1, \\ 0.5 : \lfloor \langle y \rhd k \rangle \rfloor_l \parallel \lfloor p\{y/x\} \rfloor_k^{\{y\}} \parallel \{\{(0.5, k)\} \longmapsto l\} = E_2 \end{cases}$$

where E_1 cannot be simulated by F or its derivatives. Essentially, E_1 corresponds to a distribution where x will be received or lost by the process at location k with probability 0.5.

In order to accommodate the problem illustrated by Example 31 and inspired by (5) we define a bisimulation over distributions instead of over single networks.

Let $\mu \xrightarrow{\alpha} \mu'$ iff for each $E_i \in Supp(\mu)$,

$$E_i \xrightarrow{\alpha} \mu_i \text{ and } \mu' = \sum_{E_i \in Supp(\mu). E_i \xrightarrow{\alpha} \mu_i} \mu(E_i) \cdot \mu_i.$$

The weak (combined) transitions of distributions can be defined similarly. Moreover, define $\mu \xrightarrow{\alpha}_\rho \mu'$ with $\rho \in (0, 1]$ iff there exists $\mu = \mu_1 + \mu_2$ such that $|\mu_1| = \rho$ and either $\alpha = \tau$ and $\mu' = \frac{1}{\rho} \cdot \mu_1$, or $\frac{1}{\rho} \cdot \mu_1 \xrightarrow{\alpha} \mu'$, similarly $\mu \xRightarrow{\alpha}_\rho \mu'$ iff there exists $\mu = \mu_1 + \mu_2$ such that $|\mu_1| = \rho$ and $\frac{1}{\rho} \cdot \mu_1 \xRightarrow{\alpha}_c \mu'$. Let $\mu \propto C$ be a distribution such that

$$(\mu \propto C)(E) = \mu(E \propto C)$$

for each $E \in Supp(\mu)$. Below follows the definition of the weak bisimulation over network distributions where $C_{\mu_1,\mu_2,k}$ ranges over $\mathscr{C}_{(l(\mu_1) \cup l(\mu_2) \cup \{k\})}$.

Definition 17 (Weak Bisimulation on Distributions)**.** *An equivalence relation $\mathcal{R} \subseteq \mathcal{ND} \times \mathcal{ND}$ is a weak bisimulation iff $\mu_1 \mathcal{R} \mu_2$ implies that for each k and $C_{\mu_1,\mu_2,k}$, whenever*

$$(\mu_1 \propto C_{\mu_1,\mu_2,k}) \xrightarrow{\alpha_k}_\rho \mu_1',$$

there exists

$$(\mu_2 \propto C_{\mu_1,\mu_2,k}) \xRightarrow{\alpha_k}_\rho \mu_2'$$

such that $\mu_1' \mathcal{R} \mu_2'$.

Let μ_1 and μ_2 be weakly bisimilar, written as $\mu_1 \approx_d \mu_2$ if there exists a weak bisimulation $\mathcal{R}$ such that $\mu_1 \mathcal{R} \mu_2$. Let E and F be weakly bisimilar, written as $E \approx_d F$, iff $\delta_E \approx_d \delta_F$.

Definition 17 can be seen as a conservative extension of Definition 16 dealing with relations over distributions. The only difference is that we replace the normal transition $\xrightarrow{\alpha_k}$ with $\xrightarrow{\alpha_k}_\rho$, since for a distribution we are only interested in the support which can perform an α_k at the same time. By using $\xrightarrow{\alpha_k}_\rho$ we only require that a fragment of the distribution is able to perform α_k simultaneously. If μ_1 can perform an action α_k with probability ρ, then μ_2 must be able to perform a weak transition with the same label and probability in order to simulate it, and their resulting distributions should still be related.

The following lemma shows a similar result for $\approx_d$ as Lemma 11.

Lemma 12. *$\mu \parallel \delta_C \approx_d \mu' \parallel \delta_C$ for any C provided that $\mu \approx_d \mu'$.*

Proof. It is enough to prove that

$$\mathcal{R} = \{(\mu \parallel \delta_C, \mu' \parallel \delta_C) \mid \mu \approx_d \mu'\}$$

is a weak bisimulation according to Definition 17. Let

$$\mu_0 = \mu \parallel \delta_C \text{ and } \mu'_0 = \mu' \parallel \delta_C,$$

and suppose that

$$\mu_0 \propto C_{\mu_0,\mu'_0,k} \xrightarrow{\alpha_k}_\rho \mu_1$$

for some k and $C_{\mu_0,\mu'_0,k}$, we need to prove that there exists

$$\mu'_0 \propto C_{\mu_0,\mu'_0,k} \xRightarrow{\alpha_k}_\rho \mu'_1$$

such that $\mu_1 \mathcal{R} \mu'_1$. It is not hard to see that there exists C' and $C_{\mu,\mu',k}$ such that

$$\mu_0 \propto C_{\mu_0,\mu'_0,k} \equiv (\mu \propto C_{\mu,\mu',k}) \parallel C'.$$

Obviously

$$(\mu \propto C_{\mu,\mu',k}) \approx_d (\mu' \propto C_{\mu,\mu',k})$$

since $\mu \approx_d \mu'$. If $\alpha_k = \langle x \triangleright L, \mathbb{L}\rangle @ l$, then there exists

$$(\mu \propto C_{\mu,\mu',k}) \xrightarrow{\langle x \triangleright K, \mathbb{M}\rangle @ l}_\rho \mu_2 \text{ and } C' \xrightarrow{(x @ K, \mathbb{N}) \triangleleft l} C'$$

such that $L = K \setminus \mathcal{Z}(\mathbb{N})$, $\mathbb{L} = (\mathbb{M} \cup \mathbb{N}) \setminus \mathcal{Z}(\mathbb{N})$, and $\mu_2 \equiv \mu_1 \parallel \delta_{C'}$ by (nSYN). Since

$$(\mu \propto C_{\mu,\mu',k}) \approx_d (\mu' \propto C_{\mu,\mu',k})$$

there exists

$$(\mu' \propto C_{\mu,\mu',k}) \xrightarrow{\langle x \triangleright K, \mathbb{M} \rangle @ l}_{\rho} \mu'_2$$

such that $\mu_2 \approx_d \mu'_2$, so

$$\mu'_0 \propto C_{\mu_0,\mu'_0,k} \stackrel{\alpha_k}{\Longrightarrow}_{\rho} \mu'_1 \equiv \mu'_2 \parallel \delta_{C'},$$

thus $\mu_1 \mathrel{\mathcal{R}} \mu'_1$. The other cases are similar. □

Let $\mu - E$ be the distribution such that $(\mu - E)(E) = 0$, and $(\mu - E)(F) = \mu(F)$ with $E \neq F$. The following lemma shows that whenever $\mu \approx_d \mu'$, there is a way to split μ' such that each part corresponds to each support of μ and vice versa.

Lemma 13. *If $\mu \approx_d \mu'$ where $Supp(\mu) = \{E_i\}_{1 \leq i \leq n}$, then there exists $\mu' \stackrel{\tau}{\Longrightarrow} \sum_{1 \leq i \leq n} \mu'_i$ such that $\delta_{E_i} \approx_d (\frac{1}{|\mu'_i|} \cdot \mu'_i)$ and vice versa.*

Proof. We prove by induction on n i.e. the size of $Supp(\mu)$. The case when $n = 1$ is trivial. Suppose that $n > 1$, if $\mu(E_n) = \rho > 0$, then $\mu \xrightarrow{\tau}_{\rho} \delta_{E_n}$. By Definition 17 there exists $\mu' \stackrel{\tau}{\Longrightarrow}_{\rho} \mu'_1$ such that $\delta_{E_n} \approx_d \mu'_1$ i.e. there exists $\mu' \stackrel{\tau}{\Longrightarrow} \mu'_1 + \mu'_2$ such that $|\mu'_1| = \rho$. We need to prove that

$$\frac{1}{1-\rho} \cdot (\mu - E_n) \approx_d \frac{1}{1-\rho} \cdot \mu'_2.$$

By contradiction suppose that

$$\frac{1}{1-\rho} \cdot (\mu - E_n) \not\approx_d \frac{1}{1-\rho} \cdot \mu'_2,$$

then there must exist

$$\frac{1}{1-\rho} \cdot (\mu - E_n) \xrightarrow{\tau}_{\rho'} \delta_{E_i}$$

which cannot be simulated by $\frac{1}{1-\rho} \cdot \mu'_2$, thus

$$\mu \xrightarrow{\tau}_{(\rho+\rho')} \frac{\rho}{\rho+\rho'} \cdot \delta_{E_n} + \frac{\rho'}{\rho+\rho'} \cdot \delta_{E_i}$$

which cannot be simulated by μ', this contradicts with the assumption that $\mu \approx_d \mu'$, therefore

$$\frac{1}{1-\rho} \cdot (\mu - E_n) \approx_d \frac{1}{1-\rho} \cdot \mu'_2.$$

By induction there exists

$$\frac{1}{1-\rho} \cdot \mu'_2 \stackrel{\tau}{\Longrightarrow} \sum_{1 \leq i \leq n-1} \mu'_i$$

such that $\delta_{E_i} \approx_d \mu'_i$, which completes the proof. □

As for $\approx$ also $\approx_d$ turns out to be a congruence.

Theorem 14. *$\approx_d$ is a congruence.*

Proof. It is enough to prove that

$$\mathcal{R} = \{(\mu_1 \parallel \mu_3, \mu_2 \parallel \mu_3) \mid \mu_1 \approx_d \mu_2\}$$

is a weak bisimulation. Let $\mu_{13} = \mu_1 \parallel \mu_3$ and $\mu_{23} = \mu_2 \parallel \mu_3$. Suppose that

$$\mu_{13} \propto C_{\mu_{13},\mu_{23},k} \xrightarrow{\alpha_k}_\rho \mu'_{13}$$

for some k and $C_{\mu_{13},\mu_{23},k}$, we need to prove that there exists

$$\mu_{23} \propto C_{\mu_{13},\mu_{23},k} \stackrel{\alpha_k}{\Longrightarrow}_\rho \mu'_{23}$$

such that $\mu'_{13}\ \mathcal{R}\ \mu'_{23}$. Since μ_3 contains no connectivity information,

$$\mu_{13} \propto C_{\mu_{13},\mu_{23},k} = (\mu_1 \propto C_{\mu_{13},\mu_{23},k}) \parallel \mu_3 \equiv ((\mu_1 \propto C_{\mu_1,\mu_2,k}) \parallel C) \parallel \mu_3$$

for some $C_{\mu_1,\mu_2,k}$ and C, similarly for μ_{23}. First we assume that $\mu_1 = \delta_E$ i.e. $|Supp(\mu)| = 1$, and there are several cases.

1. $\alpha_k = \langle x \triangleright L, \mathbb{L}\rangle @ l$.
   Suppose that

   $$(\mu_1 \propto C_{\mu_1,\mu_2,k}) \parallel C \xrightarrow{\langle x \triangleright K, \mathbb{K}\rangle @ l} \mu'_1 \text{ and } \mu_3 \xrightarrow{(x @ K, \emptyset) \lhd l}_\rho \mu'_3$$

   such that $L = K \setminus loc(\mu_3)$, $\mathbb{L} = \mathbb{K} \setminus loc(\mu_3)$, and

   $$\mu'_{13} = \mu'_1 \parallel (\mu'_3 \propto \mathcal{D}(\{\mathbb{L} \longmapsto l\})).$$

   Since

   $$(\mu_2 \propto C_{\mu_1,\mu_2,k}) \parallel C \approx_d (\mu_2 \propto C_{\mu_1,\mu_2,k}) \parallel C$$

   by Lemma 12, there exists

   $$(\mu_2 \propto C_{\mu_1,\mu_2,k}) \parallel C \stackrel{\langle x \triangleright K, \mathbb{K}\rangle @ l}{\Longrightarrow}_\rho \mu'_2$$

   such that $\mu'_1 \approx \mu'_2$. By Lemma 10 we know that one reception can be divided into several receptions and vice versa as long as their accumulated results are same, so there exists

   $$\mu_{23} \stackrel{\alpha_k}{\Longrightarrow}_\rho \mu'_{23} \equiv \mu'_2 \parallel (\mu'_3 \propto \mathcal{D}(\{\mathbb{L} \longmapsto l\})),$$

   thus $\mu'_{13}\ \mathcal{R}\ \mu'_{23}$.

2. $\alpha_k = (x@L, \mathbb{L}) \lhd k$.
   Suppose that
   $$(\mu_1 \propto C_{\mu_1,\mu_2,k}) \parallel C \xrightarrow{(x@L,\mathbb{L})\lhd k} \mu_1' \text{ and } \mu_3 \xrightarrow{(x@L,\emptyset)\lhd k}_\rho \mu_3'$$
   such that
   $$\mu_{13}' = \mu_1' \parallel (\mu_3' \propto \mathcal{D}(\{\mathbb{L} \longmapsto l\})).$$
   Since
   $$(\mu_1 \propto C_{\mu_1,\mu_3,k}) \parallel C \;\approx_d\; (\mu_2 \propto C_{\mu_1,\mu_2,k}) \parallel C$$
   by Lemma 12, there exists
   $$(\mu_2 \propto C_{\mu_1,\mu_2,k}) \parallel C \xRightarrow{\langle x \triangleright L,\mathbb{L}\rangle@k}_\rho \mu_2'$$
   such that $\mu_1' \;\approx_d\; \mu_2'$. By (nREC2), there exists
   $$\mu_{23} \xRightarrow{\langle x \triangleright L,\mathbb{L}\rangle@k}_\rho \mu_{23}' \equiv \mu_2' \parallel (\mu_3' \propto \mathcal{D}(\{\mathbb{L} \longmapsto l\})),$$
   thus $\mu_{13}' \;\mathcal{R}\; \mu_{23}'$ by induction.
3. The other cases are similar.

For now we have proved that if $|Supp(\mu_1)| = 1$, and $\mu_1 \;\approx_d\; \mu_2$, then
$$\mu_1 \parallel \mu_3 \;\approx_d\; \mu_2 \parallel \mu_3$$
for any μ_3. If $|Supp(\mu_1)| > 1$, then by Lemma 13 whenever $Supp(\mu_1) = \{E_i\}_{1\le i\le n}$, there exists $\mu_2 \xRightarrow{\tau} \sum_{1\le i\le n} \mu_{2i}$ such that
$$\delta_{E_i} \;\approx_d\; \frac{1}{|\mu_{2i}|} \cdot \mu_{2i}$$
for each $1 \le i \le n$. As proved before
$$\delta_{E_i} \parallel \mu_3 \;\approx_d\; \mu_{2i} \parallel \mu_3$$
for each i, thus $\mu_{13} \;\approx_d\; \mu_{23}$. □

Example 32. *Considering E and F in Example 31 where we showed $E \not\approx F$, according to the new bisimulation over distributions we now can show that $E \;\approx_d\; F$. The behavior of E and F are illustrated by Fig. 3.1 where E_1 and E_2 are as in Example 31,*
$$\begin{aligned}
E_3 &= \lfloor 0 \rfloor_l \parallel \lfloor (x) \cdot p \rfloor_k^{\emptyset} \parallel \{\{(0.5, k)\} \longmapsto l\},\\
E_4 &= \lfloor 0 \rfloor_l \parallel \lfloor p\{y/x\} \rfloor_k^{\{y\}} \parallel \{\{(0.5, k)\} \longmapsto l\},\\
F_3 &= \lfloor 0 \rfloor_l \parallel \lfloor (x) \cdot p \rfloor_k^{\emptyset} \parallel \{\{(0.75, k)\} \longmapsto l\},\\
F_4 &= \lfloor 0 \rfloor_l \parallel \lfloor p\{y/x\} \rfloor_k^{\{y\}} \parallel \{\{(0.75, k)\} \longmapsto l\}.
\end{aligned}$$

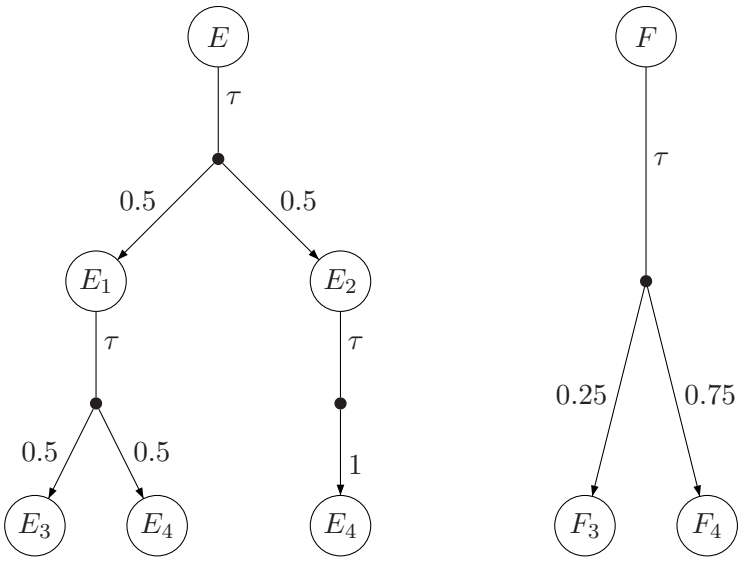

Figure 3.1: Illustration of weak bisimulation on distributions.

For instance it is not hard to see that

$$\delta_E \xrightarrow{\tau}_1 \mu = \{0.5 : E_1, 0.5 : E_2\},$$

hence we show that

$$\delta_F \xRightarrow{\tau}_1 \mu' = \{0.25 : F_3, 0.75 : F_4\}$$

such that $\mu \approx_d \mu'$. *By the definition of* $\rightarrow_\rho$, $\mu \xrightarrow{\tau}_{0.5} \delta_{E_1}$, *we will show how* μ' *can simulate this transition. Since*

$$\mu' = \{0.25 : F_3, 0.75 : F_4\},$$

we can split μ' *into* μ'_1 *and* μ'_2 *such that* $\mu' = \mu'_1 + \mu'_2$ *where*

$$\mu'_1 = \{0.25 : F_3, 0.25 : F_4\},$$

$$\mu'_2 = \{0.5 : F_4\},$$

therefore there exists $\mu' \xRightarrow{\tau}_{0.5} (\frac{1}{0.5} \cdot \mu'_1)$, *and obviously*

$$\delta_{E_1} \approx_d (\frac{1}{0.5} \cdot \mu'_1).$$

Thus even though E_1 *cannot be simulated by any of* F, F_3, *and* F_4, *it can be simulated by the distribution* $(\frac{1}{0.5} \cdot \mu'_1)$ *and vice versa. The other cases are similar, therefore we can conclude that* $E \approx_d F$.

Obviously $\approx_d$ is strictly coarser than $\approx$, thus we have the following theorem:

Theorem 15. $\approx \subset \approx_d$.

Proof. It is straightforward from Definition 16 and 17. □

3.5 Weak Simulations

3.5.1 Weak Simulation on States

We first introduce the weak simulation on networks which can be seen as an one direction weak bisimulation defined in Definition 16.

Below follows the definition of weak simulation.

Definition 18 (Weak Simulation)**.** *A relation $\mathcal{R} \subseteq \mathcal{N} \times \mathcal{N}$ is a weak bisimulation iff $E\ \mathcal{R}\ F$ implies that for each k and $C_{E,F,k}$, whenever*

$$E \propto C_{E,F,k} \xrightarrow{\alpha_k} \mu,$$

there exists

$$F \propto C_{E,F,k} \stackrel{\alpha_k}{\Longrightarrow}_c \mu'$$

such that $\mu\ \sqsubseteq_{\mathcal{R}}\ \mu'$.

Let E and F be weakly bisimilar, written as $E\ \stackrel{\mathcal{M}}{\lesssim}\ F$, if there exists a weak simulation $\mathcal{R}$ such that $E\ \mathcal{R}\ F$.

Lemma 14. *$E \parallel C\ \stackrel{\mathcal{M}}{\lesssim}\ F \parallel C$ for any C provided that $E\ \stackrel{\mathcal{M}}{\lesssim}\ F$.*

Proof. Similar with the proof of Lemma 11 and is omitted here. □

Theorem 16. *$\stackrel{\mathcal{M}}{\lesssim}$ is a congruence and preorder.*

Proof. We first prove that $\stackrel{\mathcal{M}}{\lesssim}$ is a preorder. The reflexivity is trivial, we only prove the transitivity here i.e. $E\ \stackrel{\mathcal{M}}{\lesssim}\ F$ and $F\ \stackrel{\mathcal{M}}{\lesssim}\ G$ implies that $E\ \stackrel{\mathcal{M}}{\lesssim}\ G$. In order to do so, we need another definition of weak simulation, called $\stackrel{\mathcal{M}}{\lesssim_1}$. The definition of $\stackrel{\mathcal{M}}{\lesssim_1}$ is almost the same as $\stackrel{\mathcal{M}}{\lesssim}$ except that $E \propto C_{E,F,k} \xrightarrow{\alpha_k} \mu$ is replaced by the weak transition $E \propto C_{E,F,k} \stackrel{\alpha_k}{\Longrightarrow}_c \mu$.

It can be proved that $\stackrel{\mathcal{M}}{\lesssim} = \stackrel{\mathcal{M}}{\lesssim_1}$. It is easy to see that $E\ \stackrel{\mathcal{M}}{\lesssim_1}\ F$ implies that $E\ \stackrel{\mathcal{M}}{\lesssim}\ F$ since $E \propto C_{E,F,k} \xrightarrow{\alpha_k} \mu$ is a special case of $E \propto C_{E,F,k} \stackrel{\alpha_k}{\Longrightarrow}_c \mu$. We prove that $E\ \stackrel{\mathcal{M}}{\lesssim}\ F$ implies $E\ \stackrel{\mathcal{M}}{\lesssim_1}\ F$, it is enough to show that

$$\mathcal{R} = \{(E, F) \in \mathscr{N} \times \mathscr{N} \mid E\ \stackrel{\mathcal{M}}{\lesssim}\ F\}$$

is a weak simulation under the new definition. For simplicity we will omit the parameter $C_{E,F,k}$ in the sequel. Suppose that $E \ \mathcal{R} \ F$ and $E \stackrel{\alpha_k}{\Longrightarrow}_c \mu$. If $\alpha_k = (x, \mathbb{L}) \lhd k$, we need to prove that there exists $F \stackrel{\alpha_k}{\Longrightarrow}_c \mu'$ such that $\mu \ \sqsubseteq_{\mathcal{R}} \ \mu'$. We are going to prove by induction on $E \stackrel{\alpha_k}{\Longrightarrow} \mu$. First assume that $E \stackrel{\alpha_k}{\Longrightarrow} \mu$, there are two cases to be considered:

1. $E \stackrel{\tau}{\rightarrow} \mu_1 \stackrel{\alpha_k}{\Longrightarrow} \mu$. Since $E \ \mathcal{R} \ F$ i.e. $E \ \precsim^{\mathcal{M}} \ F$, there exists $F \stackrel{\tau}{\Longrightarrow}_c \mu_1'$ such that $\mu_1 \ \sqsubseteq_{\mathcal{R}} \ \mu_1'$. By induction there exists

$$F \stackrel{\tau}{\Longrightarrow}_c \stackrel{\alpha_k}{\Longrightarrow} \mu'$$

   such that $\mu \ \sqsubseteq_{\mathcal{R}} \ \mu'$.

2. $E \stackrel{\alpha_k}{\rightarrow} \mu_1 \stackrel{\tau}{\Longrightarrow} \mu$. Since $E \ \precsim^{\mathcal{M}} \ F$, there exists $F \stackrel{\tau}{\Longrightarrow} \mu_1'$ such that $\mu_1 \ \sqsubseteq_{\mathcal{R}} \ \mu_1'$. The following proof is similar with Clause 1, and is omitted here.

If $\alpha_k = \nu\tilde{x}\langle x, \mathbb{L}\rangle@l$, there are also two cases:

1. $E \stackrel{\tau}{\rightarrow} \mu_1 \stackrel{\alpha_k}{\Longrightarrow} \mu$. This case is similar with the first clause when $\alpha_k = (x, \mathbb{L}) \lhd k$.

2. $E \xrightarrow{\nu\tilde{x}\langle x,\mathbb{L}_1\rangle@l_1} \mu_1 \xRightarrow{\nu\tilde{x}\langle x,\mathbb{L}_2\rangle@l_2} \mu$ such that

$$(\nu\tilde{x}\langle x, \mathbb{L}_1\rangle@l_1) \otimes (\nu\tilde{x}\langle x, \mathbb{L}_2\rangle@l_2) = \alpha_k.$$

   Since $E \ \precsim^{\mathcal{M}} \ F$, there exists

$$F \xRightarrow{\nu\tilde{x}\langle x,\mathbb{L}_1\rangle@l_1}_c \mu_1'$$

   such that $\mu_1 \ \sqsubseteq_{\mathcal{R}} \ \mu_1'$. As a result there exists

$$F \xRightarrow{\nu\tilde{x}\langle x,\mathbb{L}_1\rangle@l_1}_c \xRightarrow{\nu\tilde{x}\langle x,\mathbb{L}_2\rangle@l_2}_c \mu'$$

   such that $\mu \ \sqsubseteq_{\mathcal{R}} \ \mu'$.

When $E \stackrel{\alpha_k}{\Longrightarrow}_c \mu$, we know there exists $\{E \stackrel{\alpha_k}{\Longrightarrow}_c \mu_i\}_{1\leq i\leq n}$ and $\{w_i\}_{1\leq i\leq n}$ such that $\sum_{1\leq i\leq n} w_i = 1$ and $\sum_{1\leq i\leq n} w_i \cdot \mu_i = \mu$. Since we have proved that for each $E \stackrel{\alpha_k}{\Longrightarrow} \mu_i$, there exists $F \stackrel{\alpha_k}{\Longrightarrow}_c \mu_i'$ such that $\mu_i \ \sqsubseteq_{\mathcal{R}} \ \mu_i'$, thus there exists $F \stackrel{\alpha_k}{\Longrightarrow}_c \mu'$ such that $\mu \ \sqsubseteq_{\mathcal{R}} \ \mu'$.

Since we have proved that $\precsim^{\mathcal{M}} = \precsim_1^{\mathcal{M}}$, in order to show that $\precsim^{\mathcal{M}}$ is a preorder, it is equivalent to prove that $\precsim_1^{\mathcal{M}}$ is a preorder. Suppose that $E \ \precsim_1^{\mathcal{M}} \ F$ and $F \ \precsim_1^{\mathcal{M}} \ G$, we prove that $E \ \precsim_1^{\mathcal{M}} \ G$. According to the definition of $\precsim_1^{\mathcal{M}}$, there exists weak simulations $\mathcal{R}_1$ and $\mathcal{R}_2$ such that $E \ \mathcal{R}_1 \ F$ and $F \ \mathcal{R}_2 \ G$. Therefore whenever $E \xRightarrow{(x,\mathbb{L})\lhd k}_c \mu_1$, there

exists $F \xrightarrow{(x,\mathbb{L})\lhd k}_c \mu_2$ and $G \xrightarrow{(x,\mathbb{L})\lhd k}_c \mu_3$ such that $\mu_1 \sqsubseteq_{\mathcal{R}_1} \mu_2$ and $\mu_2 \sqsubseteq_{\mathcal{R}_2} \mu_3$. In other words, there exists Δ_1 and Δ_2 satisfying the conditions in Definition 7. Let

$$\mathcal{R} = \mathcal{R}_1 \circ \mathcal{R}_2 = \{(E', G') \mid \exists F'.(E' \ \mathcal{R}_1 \ F' \wedge F' \ \mathcal{R}_2 \ G')\},$$

then we need to find a Δ between μ_1 and μ_3 over $\mathcal{R}$. Let

$$\Delta(E, G) = \sum_{F \in \mathcal{N}} \Delta_1(E, F) \cdot \frac{\Delta_2(F, G)}{\mu_2(F)},$$

we show that Δ defined in this way does satisfy the conditions in Definition 7. Condition one is easy since $\Delta(E, G) > 0$ implies that there exists F such that $\Delta_1(E, F) > 0$ and $\Delta_2(F, G) > 0$, that is, $E \ \mathcal{R}_1 \ F$ and $F \ \mathcal{R}_2 \ G$, thus $E \ \mathcal{R} \ G$, and vice versa. Also

$$\begin{aligned}
\sum_{G \in \mathcal{N}} \Delta(E, G) &= \sum_{G \in \mathcal{N}} \sum_{F \in \mathcal{N}} \Delta_1(E, F) \cdot \frac{\Delta_2(F, G)}{\mu_2(F)} \\
&= \sum_{F \in \mathcal{N}} \Delta_1(E, F) \cdot \frac{1}{\mu_2(F)} \cdot (\sum_{G \in \mathcal{N}} \Delta_2(F, G)) \\
&= \sum_{F \in \mathcal{N}} \Delta_1(E, F) \\
&= \mu_1(E)
\end{aligned}$$

we prove that the second condition is satisfied too. The third condition is similar as the second one, and is omitted here. Therefore $\mu_1 \sqsubseteq_{\mathcal{R}} \mu_3$, this completes the proof.

Finally we prove that $\precsim^{\mathcal{M}}$ is a congruence, it is enough to show that

$$\mathcal{R} = \{(\nu\tilde{x}(E \parallel G), \nu\tilde{x}(F \parallel G)) \mid E \ \precsim^{\mathcal{M}} \ F\}$$

is a weak simulation. The following proof is similar with Theorem 13, and is omitted here. □

Since weak simulation is one direction weak bisimulation, and is strictly coarser than weak bisimulation, therefore there exists networks which are not weakly bisimilar with each other, but one network is able to simulation the other one, refer to the following example.

Example 33. *Consider the networks E and F in Example 31 where we have shown that $E \not\precsim F$, but it holds that $F \precsim^{\mathcal{M}} E$. The only non-trivial case is when*

$$F \xrightarrow{\tau} \left\{ \begin{array}{l} 0.75 : \lfloor 0 \rfloor_l \parallel \lfloor p\{y/x\} \rfloor_k^{\{y\}} \parallel \{\{(0.75, k)\} \longmapsto l\}, \\ 0.25 : \lfloor 0 \rfloor_l \parallel \lfloor (x) \cdot p \rfloor_k^{\emptyset} \parallel \{\{(0.75, k)\} \longmapsto l\} \end{array} \right\} \equiv \mu,$$

this can be simulated by the following weak transition of E:

$$E \xrightarrow{\tau} \left\{ \begin{array}{l} 0.5 : \lfloor \langle y \rhd k \rangle \rfloor_l \parallel \lfloor (x) \cdot p \rfloor_k^{\emptyset} \parallel \{\{(0.5, k)\} \longmapsto l\}, \\ 0.5 : \lfloor \langle y \rhd k \rangle \rfloor_l \parallel \lfloor p\{y/x\} \rfloor_k^{\{y\}} \parallel \{\{(0.5, k)\} \longmapsto l\} \end{array} \right\} \xrightarrow{\tau} \mu'$$

where

$$\mu' = \begin{cases} 0.75 : \lfloor 0 \rfloor_l \parallel \lfloor p\{y/x\} \rfloor_k^{\{y\}} \parallel \{\{(0.5, k)\} \longmapsto l\} \\ 0.25 : \lfloor 0 \rfloor_l \parallel \lfloor (x) \cdot p \rfloor_k^{\emptyset} \parallel \{\{(0.5, k)\} \longmapsto l\} \end{cases}$$

it is easy to see that $\mu \sqsubseteq_{\mathcal{R}} \mu'$, therefore $F \precapprox^{\mathcal{M}} E$. Note that this result still holds even that the node at k can receive messages from other locations with positive probability i.e. $k \longmapsto m$ is not always equal to 0 for $m \neq l$.

3.5.2 Weak Simulation on Distributions

In this section we give the definition of weak simulation on distributions. Based on Definition 17, the weak simulation can be given in a straightforward way as follows:

Definition 19 (Weak Simulation on Distributions)**.** *A relation $\mathcal{R} \subseteq \mathcal{ND} \times \mathcal{ND}$ is a weak simulation iff $\mu_1 \; \mathcal{R} \; \mu_2$ implies that for each k and $C_{\mu_1,\mu_2,k}$, whenever*

$$(\mu_1 \propto C_{\mu_1,\mu_2,k}) \xrightarrow{\alpha_k}_{\rho} \mu_1',$$

there exists

$$(\mu_2 \propto C_{\mu_1,\mu_2,k}) \xRightarrow{\alpha_k}_{\rho} \mu_2'$$

such that $\mu_1' \; \mathcal{R} \; \mu_2'$.

Let μ_1 be weakly simulated by μ_2, written as $\mu_1 \precapprox_d \mu_2$, if there exists a weak simulation $\mathcal{R}$ such that $\mu_1 \; \mathcal{R} \; \mu_2$. Let E be weakly simulated by F, written as $E \precapprox_d F$, iff $\delta_E \precapprox_d \delta_F$.

Lemma 15. *$\mu \parallel \delta_C \approx_d \mu' \parallel \delta_C$ for any C provided that $\mu \approx_d \mu'$.*

Proof. Similar to the proof of Lemma 12, and is omitted here. □

Lemma 16. *If $\mu \precapprox_d \mu'$ where $Supp(\mu) = \{E_i\}_{1 \leq i \leq n}$, then there exists*

$$\mu' \xRightarrow{\tau} \sum_{1 \leq i \leq n} \mu_i'$$

such that

$$\delta_{E_i} \precapprox_d (\frac{1}{|\mu_i'|} \cdot \mu_i')$$

and vice versa.

Proof. Similar to the proof of Lemma 13, and is omitted here. □

Similar with $\precsim^{\mathcal{M}}$, we can also show that $\precsim_d$ is a congruent preorder.

Theorem 17. *$\precsim_d$ is a congruence and preorder.*

Proof. We first prove that $\precsim_d$ is a preorder. The reflexivity is trivial, and we only prove the transitivity here i.e. $E \precsim_d F$ and $F \precsim_d G$ implies that $E \precsim_d G$. Similar as Theorem 16, we define another weak simulation, denoted as $\precsim'_d$, which is almost the same as $\precsim_d$ except that $(\mu_1 \propto C_{\mu_1,\mu_2,k}) \xrightarrow{\alpha_k}_\rho \mu'_1$ is replaced by $(\mu_1 \propto C_{\mu_1,\mu_2,k}) \stackrel{\alpha_k}{\Longrightarrow}_\rho \mu'_1$ in Definition 19.

It can be proved that $\precsim_d = \precsim'_d$. The proof of $\precsim'_d \subseteq \precsim_d$ is easy since $(\mu_1 \propto C_{\mu_1,\mu_2,k}) \xrightarrow{\alpha_k}_\rho \mu'_1$ is a special case of $(\mu_1 \propto C_{\mu_1,\mu_2,k}) \stackrel{\alpha_k}{\Longrightarrow}_\rho \mu'_1$. In order to prove that $\precsim_d \subseteq \precsim'_d$, it is enough to show that

$$\mathcal{R} = \{(\mu_1, \mu_2) \in \mathcal{ND} \times \mathcal{ND} \mid \mu_1 \precsim_d \mu_2\}$$

is a weak simulation under the new definition. Again we will omit the parameter $C_{\mu_1,\mu_2,k}$ for simplicity. Suppose that $\mu_1 \mathcal{R} \mu_2$ and $\mu_1 \stackrel{\alpha_k}{\Longrightarrow}_\rho \mu'_1$, we need prove that there exists $\mu_2 \stackrel{\alpha_k}{\Longrightarrow}_\rho \mu'_2$ such that $\mu'_1 \sqsubseteq_{\mathcal{R}} \mu'_2$. The proof is by induction on $\mu_1 \stackrel{\alpha_k}{\Longrightarrow}_\rho \mu'_1$.

1. $\alpha_k = (x, \mathbb{L}) \lhd k$. Then $\mu_1 \stackrel{\alpha_k}{\Longrightarrow}_\rho \mu'_1$ iff there exists

   $$\mu_1 \xrightarrow{\tau}_{\rho_1} \mu_{11} \stackrel{\alpha_k}{\Longrightarrow}_1 \mu'_{11}$$

   and

   $$\mu_1 \xrightarrow{\alpha_k}_{\rho_2} \mu_{12} \stackrel{\tau}{\Longrightarrow}_1 \mu'_{12}$$

   where $\rho_1 + \rho_2 = \rho$ and

   $$\mu'_1 = (\frac{\rho_1}{\rho} \cdot \mu'_{11} + \frac{\rho_2}{\rho} \cdot \mu'_{12}).$$

   Since $\mu_1 \precsim_d \mu'_1$, by Lemma 16 there exists $\mu_2 \stackrel{\tau}{\Longrightarrow}_{\rho_1} \mu_{21}$ and $\mu_2 \stackrel{\alpha_k}{\Longrightarrow}_{\rho_2} \mu_{22}$ such that $\mu_{11} \precsim_d \mu_{21}$ and $\mu_{12} \precsim_d \mu_{22}$. The following proof is straightforward by induction.

2. $\alpha_k = \nu\tilde{x}\langle x, \mathbb{L}\rangle@l$. Then $\mu_1 \stackrel{\alpha_k}{\Longrightarrow}_\rho \mu'_1$ iff there exists

   $$\{\mu_1 \xrightarrow{\nu\tilde{x}\langle x,\mathbb{M}_i\rangle@l}_{\rho_i} \mu_{1i} \stackrel{\nu\tilde{x}\langle x,\mathbb{N}_i\rangle@l}{\Longrightarrow}_1 \mu'_{1i}\}_{1\le i<n}$$

   and

   $$\mu_1 \xrightarrow{\tau}_{\rho_n} \mu_{1n} \stackrel{\alpha_k}{\Longrightarrow}_1 \mu'_{1n}$$

such that

$$(\nu\tilde{x}\langle x, \mathbb{M}_i\rangle@l) \otimes (\nu\tilde{x}\langle x, \mathbb{N}_i\rangle@l) = \alpha_k$$

for each $1 \leq i < n$,

$$\sum_{1\leq i\leq n} \rho_i = \rho \text{ and } \sum_{1\leq i\leq n} (\frac{\rho_i}{\rho} \cdot \mu'_{1i}) = \mu'_1.$$

The following proof is similar with Clause 1,and is omitted here.

3. $\alpha_k = \tau$. This case is similar with Clause 1, and is omitted here.

Since we have proved that $\precsim_d = \precsim'_d$, it is enough to show that $\precsim'_d$ is a preorder. The proof is similar with Theorem 16. The congruence of $\precsim_d$ can also be proved in a similar way as Theorem 14 based on Lemma 15 and 16. These proofs are omitted here. □

We give an example of weak simulation over distributions as follows:

Example 34. *Suppose that we have two networks:*

$$E = \lfloor 2 \cdot p + 2 \cdot (x) \cdot q + 3 \cdot q\{y/x\}\rfloor_l \parallel \lfloor 0\rfloor_k,$$

$$F = \lfloor 2 \cdot p + 5 \cdot (x) \cdot q\rfloor_l \parallel \lfloor\langle y \rhd l\rangle\rfloor_k.$$

Assume that in the given SMF $\mathcal{M}$*, the node at l can receive messages from k with probability 0.6. Let $C = \{\{(0.6, k)\} \longmapsto l\}$, then we have*

$$E \parallel C \precsim_d F \parallel C.$$

Intuitively, in E the node at k has received the message y, while in F the message y has not been received by l. Since $(F \parallel C)(k, l) = 0.6$, the node at k can also receive y and evolve into $\lfloor q\{y/x\}\rfloor_k$ with probability $\frac{5}{7} \cdot 0.6 = \frac{3}{7}$, which is the same as in E, similarly for other cases.

As in the bisimulation setting, $\precsim_d$ is strictly coarser than $\precsim^{\mathcal{M}}$.

Theorem 18. $\precsim^{\mathcal{M}} \subset \precsim_d$.

Proof. It is easy to see that $E \precsim^{\mathcal{M}} F$ implies $E \precsim_d F$ given Definition 18 and 19. To show that $E \precsim_d F$ does not always imply $E \precsim^{\mathcal{M}} F$, it is enough to give a counterexample. Note that Example 31 also works here, for the same reason $E \not\precsim^{\mathcal{M}} F$, but we can show $E \precsim_d F$. □

3.6 Removal of Memory

As we said in Section 3.1 even though we require that each message can only be received by each node for at most once in our semantics, this can be removed easily by omitting the parameter M associated with each node, and changing the semantics accordingly. As a result we also need to modify the definition of weak bisimulation. In this section we will show how to do so.

In order to remove the restriction, the only thing we need to do on the syntax level is to remove the parameter M, and leave others unchanged. On the semantics level we need to change several rules in Table 3.2 and 3.3. Most of the rules in Table 3.2 have nothing to do with the memory, thus can be kept without any change except (gIGN) and (gBRD) where we need to check if the coming message should be ignored or not. If $l \notin L \vee y \in M$ i.e. the broadcasted message is not intend to be received by the node at location l or the node at location l has received the same message before, so in both case the broadcasted message should be ignored, similarly for Rule (gBRD). Since we do not have memory M, we can simply remove the condition $y \in M$ in (gIGN) and $y \notin M$ in (gBRD), that is, the new rules will be as follows:

$$\frac{p \xrightarrow{\nu\tilde{y}\langle y \rhd L\rangle} p' \quad l \notin L}{p \parallel q \xrightarrow{\nu\tilde{y}\langle y \rhd L\rangle} p' \parallel q} \text{ (gIGN)}$$

$$\frac{p \xrightarrow{\nu\tilde{y}\langle y \rhd L\rangle} p' \quad q \xrightarrow{(y)} q' \quad \tilde{y} \cap fn(q) = \emptyset \quad l \in L}{p \parallel q \xrightarrow{\nu\tilde{y}\langle y \rhd L\rangle} p' \parallel q'} \text{ (gBRD)}$$

Four rules in Table 3.3 depend on the parameter M i.e. (nBRD1), (nBRD2), (nREC1), and (nIGN), thus they should be changed correspondingly. For (nREC1) and (nIGN) we can simply remove the conditions related to M in their premises as we did for (gBRD) and (gIGN). We should be more careful when dealing with rules (nBRD1) and (nBRD2). For sure we do not need to consider the update of the parameter M, and in addition the premises $l \in L^*$ in (nBRD1) and $l \notin L^*$ in (nBRD2) are needed in order to determine whether the broadcasted message have been received or not, thus we can update the parameter M correctly. But since we do not need to update M anymore, therefore the premises $l \in L^*$ and $l \notin L^*$ are also redundant now, so they can be removed. After doing this (nBRD1) and (nBRD2) will be identical.

$$\frac{l \notin L}{\lfloor p \rfloor_l \xrightarrow{(x@L,\emptyset)\lhd k} \lfloor p \rfloor_l} \text{(nIGN)}$$

$$\frac{p \xrightarrow{\nu\tilde{x}\langle x \rhd L^*\rangle} p'}{\lfloor p \rfloor_l \xrightarrow{\nu\tilde{x}\langle x \rhd L^*,\emptyset\rangle@l} \lfloor p' \rfloor_l} \text{(nBRD)}$$

$$\frac{p \xrightarrow{(x)} p' \quad l \in L^*}{\lfloor p \rfloor_l \xrightarrow{(x@L^*,\emptyset)\lhd k} \{(\theta_{l \longmapsto k} : \lfloor p' \rfloor_l), (1 - \theta_{l \longmapsto k} : \lfloor p \rfloor_l)\}} \text{(nREC1)}$$

In Definition 16 we allow that a single broadcast can be simulated by a series of broadcasts which can be combined together by operator $\otimes$. The definition of $\otimes$ depends on the assumption that each message can only be received by each node for at most once. Without this assumption we cannot define $\otimes$ as before, refer to the following example.

Example 35. *Given a network*

$$E = \lfloor (x) \cdot (y) \cdot p \rfloor_l \parallel C.$$

Suppose that $E(l,k) = \frac{3}{4}$*, then if there is a message* z *broadcasted from the node at location* k*,* E *can receive* z *and evolve into* $\lfloor (y) \cdot p\{z/x\} \rfloor_l \parallel C$ *with probability* $\frac{3}{4}$*. With the assumption "reception for at most once", this broadcast can be simulated by several broadcasts. For instance two broadcasts of* z *in a row from the node at location* m *can deliver* z *to* E *with probability* $\frac{3}{4}$ *if* $E(l,k) = \frac{1}{2}$*. But without this assumption we cannot do so, since* $\lfloor (y) \cdot p\{z/x\} \rfloor_l \parallel C$ *will not ignore the coming* z *as before, but will receive it and evolve into* $\lfloor p\{z/x\}\{z/y\} \rfloor_l \parallel C$ *with positive possibility, this cannot happen if* z *is only be broadcasted once.*

Based on these observation we should also change our definition of weak bisimulation. We first define a new operator $\oplus$ which plays a similar role as $\otimes$ in Definition 16 such that

$$\nu\tilde{x}\langle x \rhd L_1, \mathbb{L}_1\rangle@l_1 \oplus \nu\tilde{x}\langle x \rhd L_2, \mathbb{L}_2\rangle@l_2 = \nu\tilde{x}\langle x \rhd L, \mathbb{L}\rangle@l$$

where $L_1 \cap L_2 = \emptyset$, $L = L_1 \cup L_2$, and $\mathbb{L} = \mathbb{L}_1 \cup \mathbb{L}_2$, again l is not important and can be any location name. In order to apply $\oplus$, L_1 and L_2 should not contain common elements, the intuition to do so is clear from Example 35. Accordingly, we should extend the broadcast transitions in the following way:

$$E \xrightarrow{\langle x \rhd L^*, \mathbb{L}\rangle@l} \mu \text{ iff } E \xRightarrow{\alpha_1} \xRightarrow{\alpha_2} \ldots \xRightarrow{\alpha_n} \mu$$

where

$$\langle x \rhd L^*, \mathbb{L}\rangle @l = (\underset{1\leq i\leq n}{\oplus} \alpha_i).$$

The definition of weak bisimulation under the new framework , called $\approx_{\backslash M}$, is the same as Definition 16, we repeat it for completeness as follows:

Definition 20 (Weak Bisimulation)**.** *An equivalence relation $\mathcal{R} \subseteq \mathcal{N} \times \mathcal{N}$ is a weak bisimulation without M iff $E\ \mathcal{R}\ F$ implies that for each k and $C_{E,F,k}$, whenever*

$$E \propto C_{E,F,k} \xrightarrow{\alpha_k} \mu,$$

there exists

$$F \propto C_{E,F,k} \stackrel{\alpha_k}{\Longrightarrow}_c \mu'$$

such that $\mu\ \mathcal{R}\ \mu'$.

Let E and F be weakly bisimilar without M, written as $E \approx_{\backslash M} F$, if there exists a weak bisimulation $\mathcal{R}$ such that $E\ \mathcal{R}\ F$.

In the same way we can also define weak bisimulation on distributions as well as the weak simulations. We omit the details here.

3.7 A Leader Election Protocol

We illustrate the application of our calculus by modeling an adaption of the leader election protocol in (76). Before giving the model we first explain how this protocol works. It is assumed that each node has a unique ID i. A node may regularly initiate an election of a new leader; it will start the process of building a spanning tree by broadcasting a message *Election* to its neighbors and then wait for acknowledgement messages, *Ack*, from its children in the tree. An *Ack* message will contain the information about the node with the highest ID the child has found. When a node j receives an *Election* from another node i, it will set i as its parent and then propagate *Election* to its neighbors and then wait for the acknowledgements *Ack* from its children. In a state waiting for *Ack* messages a node keeps track of the highest ID received before it times out after a certain time limit. When timing out a node (not being the root of the spanning tree) reports the highest ID found to its parent via an *Ack* message and enters a state where it waits to be informed about the new leader found. When the initiator of the run of the protocol times out waiting for *Ack* messages it broadcasts the new leader, i.e.

Process 1 The model of the leader election protocol

$$
\begin{array}{lcl}
Node(i,l,m,p) & = & \lambda_{init} \cdot \langle E\_i \rhd I \rangle \cdot Init(i,l,m,p) \\
 & + & \sum_{x \neq i}(E\_x) \cdot \langle E\_i \rhd I \rangle \cdot waitAck(i,l,m,x) \\
Init(i,l,m,p) & = & \sum_{x \neq i}(A\_x) \cdot ([x > m]Init(i,l,x,p), Init(i,l,m,p)) \\
 & + & \lambda_{exp} \cdot \langle L\_m \rhd I \rangle \cdot Node(i,m,m,p) \\
waitAck(i,l,m,p) & = & \sum_{x \neq i}(A\_x) \cdot ([x > m]waitAck(i,l,x,p), waitAck(i,l,m,p)) \\
 & + & \lambda_{exp} \cdot \langle A\_m \rhd p \rangle \cdot waitLeader(i,l,m,p) \\
waitLeader(i,l,m,p) & = & \sum_{x \neq i}(L\_x) \cdot Node(i,x,m,p) \\
 & + & \lambda_{par} \cdot \langle L\_m \rhd I \rangle \cdot Node(i,m,m,p)
\end{array}
$$

the node with the highest ID found, to its neighbors via the message *Leader*. Notice that due to node mobility a child may disconnect from its parent before it sends the acknowledgement, the time out in this case prevents the parent getting stuck waiting for the acknowledgement forever. Similarly for a node waiting for announcements of a new leader, it will either receive the announcement in time, or it will time out and announce the node with highest ID it has found so far as the new leader.

The state of a node is represented by $Node(i,l,m,p)$ where i is the ID, l is the ID of its leader, m is the maximum ID known in a protocol run, and p is the ID of its parent. To model this protocol we define three types of messages (names) where I is a finite set of all the possible ID numbers: $\{E\_i \mid i \in I\}$ is the set of *Election* messages, $\{A\_m \mid m \in I\}$ is the set of *Ack* messages, and $\{L\_l \mid l \in I\}$ is the set of *Leader* messages which announces the elected leader. In (76) the messages in a given election are all assigned a unique index used to distinguish the protocol run from other runs. For simplicity we omit these details in the model of the protocol in this thesis.

To make the model more compact we extend the match operator in the following way: $[x > m]p, q$ denotes that the process will evolve into p if $x > m$, otherwise it will evolve into q, this operator can be defined using the standard operators in a straightforward way. The operator $\sum_{x \neq i}(E\_x)$ means that the input only accepts *Election* messages not from i, and ignores all the other messages, the operator can easily be encoded by a sequence of conditional operators prefixed by (x). We introduce similar operators for accepting just one type of protocol messages. The model of the protocol is given in Model 1 where λ_{init} and λ_{exp} denote the rate of initializing a new run of the protocol and the rate of timeout from waiting for the acknowledgements from

children respectively. If a node is not involved in any election, it will be at state *Node*. The node with ID i can initialize an election by broadcasting the message E_i to its neighbors, and evolve into *Init*. When the neighbor nodes receive the message E_i, they will join the election and evolve into *waitAck* after forwarding the *Election* message to their neighbors. While at *Init* or *waitAck*, a node will wait for the acknowledgements from its neighbors. In order not to get stuck and wait for the acknowledgements forever, we let each node stop waiting with rate λ_{exp}. When the node at *Init* stops waiting for the acknowledgements, it will announce m, the maximal ID found so far, as the new leader. Differently, when timing out nodes at *waitAck* will send an acknowledgement together with the parameter m to their parents, and then evolve into *waitLeader* waiting for the announcement of the new leader. It may happen that a node will timeout when waiting for the announcement from its parent while at *waitLeader*, in this case it will simply announce m as its leader and terminate the election. Each node at *waitLeader* will timeout with a certain delay by rate λ_{par}.

Next we will show how to define mobility rules for our example. For simplicity we assume that there are four locations in the network: l, k, m, and n where all the nodes are stationary except the node at l. Suppose that nodes at location k and l are always disconnected, thus the move of node at l will not affect the value of $\rho_{k \mapsto\!\!\!\!\rightarrow l}$ and $\rho_{l \mapsto\!\!\!\!\rightarrow k}$. There are two possible positions Pos_1 and Pos_2 for the node at location l such that when in Pos_1 it will be closer to the node at location m i.e. $\rho_{m \mapsto\!\!\!\!\rightarrow l} > \rho_{n \mapsto\!\!\!\!\rightarrow l}$ while in Pos_2 we have $\rho_{m \mapsto\!\!\!\!\rightarrow l} < \rho_{n \mapsto\!\!\!\!\rightarrow l}$. When the node at location l is at Pos_1, it will move to Pos_2 with rate 2, while in Pos_2 it will move to Pos_1 with rate 5. Moveover no matter how the node at location l moves, we can guarantee that $\rho_{m \mapsto\!\!\!\!\rightarrow l} + \rho_{n \mapsto\!\!\!\!\rightarrow l} = 1$ as long as $\rho_{m \mapsto\!\!\!\!\rightarrow n} = 1$ and $\rho_{n \mapsto\!\!\!\!\rightarrow m} = 1$. Since $\rho_{m \mapsto\!\!\!\!\rightarrow l}$ and $\rho_{n \mapsto\!\!\!\!\rightarrow l}$ are dependent, their mobility rules should be defined together in our SMF. Suppose that $\rho_{m \mapsto\!\!\!\!\rightarrow l} = 0.8$ and $\rho_{n \mapsto\!\!\!\!\rightarrow l} = 0.2$ when the node at location l moves to Pos_1, and $\rho_{m \mapsto\!\!\!\!\rightarrow l} = 0.3$ and $\rho_{n \mapsto\!\!\!\!\rightarrow l} = 0.7$ when it is at Pos_2. By letting $\mathcal{M}(C_1, C_2, \Bbbk) = 2$ and $\mathcal{M}(C_2, C_1, \Bbbk) = 5$ we complete the definition of the mobility rules with $C_1 = \{\{(0.8, m), (0.2, n)\} \longmapsto l\}$, $C_2 = \{\{(0.3, m), (0.7, n)\} \longmapsto l\}$, and $\Bbbk = (\rho_{m \mapsto\!\!\!\!\rightarrow n} = 1 \wedge \rho_{n \mapsto\!\!\!\!\rightarrow m} = 1)$. Note that more complicated rules can be defined, for instance when the condition $\Bbbk$ does not hold i.e. m and n are not close enough, we can let the $\rho_{m \mapsto\!\!\!\!\rightarrow l}$ and $\rho_{n \mapsto\!\!\!\!\rightarrow l}$ evolve into other values such that $\rho_{m \mapsto\!\!\!\!\rightarrow l} + \rho_{n \mapsto\!\!\!\!\rightarrow l} \neq 1$. For simplicity we will omit the details.

Process 2 An simplified model of the leader election protocol

$$
\begin{array}{lcl}
Node'(i) & = & \lambda_{init} \cdot \langle E\_i \rhd I \rangle \cdot Init'(i) + (E\_x) \cdot \langle E\_i \rhd I \rangle \cdot waitAck'(i) \\
Init'(i) & = & \lambda_{exp} \cdot \langle L\_i \rhd I \rangle \cdot Node'(i) \\
waitAck'(i) & = & \lambda_{exp} \cdot waitLeader'(i) \\
waitLeader'(i) & = & (L\_x) \cdot Node'(i) + \lambda_{par} \cdot \langle L\_i \rhd I \rangle \cdot Node'(i)
\end{array}
$$

It is not hard to see that in this example we use group broadcast often between nodes internally in the network, as a result we can abstract from the concrete execution of the model. Suppose we only care whether each node in a network has a leader or not, then the model can be simplified as Model 2 where the node which initializes the election always chooses itself as the new leader.

In Model 2, the acknowledgement messages $\langle A\_i \rhd I \rangle$ can be abstracted totally, and we can establish that:

$$\Big\|_{1 \leq i \leq I} \lfloor Node'(i) \rfloor_i \approx \Big\|_{1 \leq i \leq I} \lfloor Node(i, l, m, p) \rfloor_i \qquad (*)$$

Intuitively, (*) holds because all the group broadcasts will become internal and those group broadcasts dealing with acknowledgements used to find the node with the highest ID will be abstracted. Since we do not care about the specific ID of the leader, the broadcast actions $\langle A\_m \rhd p \rangle$ can be seen as internal. Essentially the node which initializes the election simply commutes between two states depending on whether it has a valid leader or not, while the nodes participating in an election simply commutes between three states depending on whether they have a valid leader, are part of an election waiting for acknowledgements from children, or are part of an election waiting for the announcement of the leader.

Since $\approx_d$ is strictly coarser than $\approx$ by Theorem 15, therefore by applying $\approx_d$ we expect to equate even more networks. Refer to the following example.

Example 36. *Let us consider a simple case where l is only connected to m, n such that $\mathcal{M}(C_1, C_1, true) = 0$ and $\mathcal{M}(C_2, C_2, true) = 0$ where*

$$C_1 = \{\{(\frac{1}{2}, l)\} \longmapsto m\} \parallel \{\{(\frac{1}{2}, l)\} \longmapsto n\},$$

$$C_2 = \{\{(\frac{3}{4}, l)\} \longmapsto m\} \parallel \{\{(0, l)\} \longmapsto n\}.$$

Assume that the processes at location m and n have received the new leader and are about to announce it to the neighbors, while the process at location l is waiting for the announcement of the new leader, then we can show that $E \approx_d F$ but $E \not\approx F$ where

$$E = \lfloor \langle L\_l \rhd I \rangle \cdot Node(m) \rfloor_m \parallel \lfloor \langle L\_l \rhd I \rangle \cdot Node(n) \rfloor_n \parallel \lfloor Node(l) \rfloor_l \parallel C_1,$$
$$F = \lfloor \langle L\_l \rhd I \rangle \cdot Node(m) \rfloor_m \parallel \lfloor \langle L\_l \rhd I \rangle \cdot Node(n) \rfloor_n \parallel \lfloor Node(l) \rfloor_l \parallel C_2.$$

and for simplicity we omit the parameters of each node except the ID.

3.8 Related Work

The most relevant work is the stochastic version of RBPT in (77) by Ghassemi et al., where the semantics deals with the stochastic behavior arising from data-line layer, physical layer, and mobility. We list its differences from our work as follows:

1. The mobility model of (77) is global and determined by three parameters: T_{Mac}, P_{rcv}, and P_{UP}, where T_{Mac} is the response time of MAC (Multi Access Control) protocol, P_{rcv} is the probability of a node receiving the messages successfully, and P_{UP} is the probability of one node being connected to another. These parameters are global i.e. they describe the mobility of every node. While in our work we can define mobility for arbitrary connections.

2. In (77), each action is associated with a rate which denotes the duration of the action. This approach can also be found in (29). But in our calculus the rate is not paired with actions, therefore the rate is used to denote the delay rather than duration of the actions. In other words, we follow the approach adopted in (32).

3. Each model in (66) gives rise to a Continuous Time Markov Chain (CTMC) by using Markovian network bisimilarity to collapse equivalent states, while this is not the case in our setting. Specially, each model in our calculus corresponds to a MA instead of CTMC.

Merro and Sibilio proposed a timed process calculus (TCWS) for wireless networks which may suffer from the problem of communication collisions. Differently, in TCWS the time is discrete instead of continuous, and moreover it is assumed that the network topology is static without considering mobility, thus TCWS is mainly applied to stationary networks.

Chapter 4

Probabilistic Automata

In this chapter we will discuss the characterizations of bisimulations and simulations w.r.t. PCTL* and its sublogics on probabilistic automata. Since PCTL* is a state-labeled logic i.e. it only refers to the labels of states not the labels of transitions, thus in this chapter and Chapter 5, we will consider state-labeled systems. As indicated in (4), the theories in Chapter 4 and 5 can be easily transformed to the action-labeled systems.

In Section 4.2 we first introduce some notations, and then we recall the definition of probabilistic automata and bisimulation relations by Segala (78). We also recall the logic PCTL* and its sublogics. Section 4.3 introduces the novel strong and strong branching bisimulations, and proves that they agree with PCTL* and PCTL equivalences, respectively. Section 4.4 extends them to weak (branching) bisimulations, and Section 4.5 extends the framework to simulations. We discuss the coarsest congruent bisimulations and simulations in Section 4.7, and the extension to countable states in Section 4.6. We conclude this chapter in Section 4.8 by discussing some related work.

4.1 Motivation

Probabilistic automata (PA) (1) have been successfully applied in formal verification of concurrent and stochastic systems. Efficient model checking algorithms have been studied, where properties are mostly expressed in the logic PCTL, introduced in (2) for Markov chains, and later extended in (3) for Markov decision processes, where PCTL is also extended to PCTL*.

To combat the infamous state space problem in model checking, various behavioral equivalences, including strong and weak bisimulations, are proposed for PAs. Indeed, they turn out to be a powerful tool for abstraction for PAs, since bisimilar states implies that they satisfy exactly the same PCTL formulae. Thus, bisimilar states can be grouped together, allowing one to construct smaller quotient automata before analyzing the model. Moreover, the nice compositional theory for PAs is exploited for compositional minimization (79), namely minimizing the automata before composing the components together.

For Markov chains, i.e., PAs without nondeterministic choices, the logical equivalence implies also bisimilarity, as shown in (54). Unfortunately, it does not hold in general, namely PCTL equivalence is strictly coarser than bisimulation – and their extension probabilistic bisimulation – for PAs. Even there is such a gap between behavior and logical equivalences, bisimulation based minimization is extensively studied in the literatures to leverage the state space explosion, for instance see (80, 81, 82).

The main reason for the gap can be illustrated by the following example. Consider the PAs in Fig. 4.1 assuming that s_1, s_2, s_3 are three absorbing states with different state properties. It is easy to see that s and r are PCTL equivalent: the additional middle transition out of r does not change the extreme probabilities, the interval of probabilities in which the three observing states can be reached is not changed. Existing bisimulations differentiate s and r, mainly because the middle transition out of r cannot be matched by any transition (or combined transition) of s. Bisimulation requires that the complete distribution of a transition must be matched, which is in this case too strong, as it differentiates states satisfying the same PCTL formulae.

In this chapter we will bridge this gap. We introduce novel notions of behavioral equivalences which characterize (both soundly and completely) PCTL, PCTL* and their sublogics. Summarizing, our contributions in this chapter are:

- A new bisimulation characterizing PCTL* soundly and completely. The bisimulation arises from a converging sequence of equivalence relations, each of which characterizes bounded PCTL*.

- Branching bisimulations which correspond to PCTL and bounded PCTL equivalences.

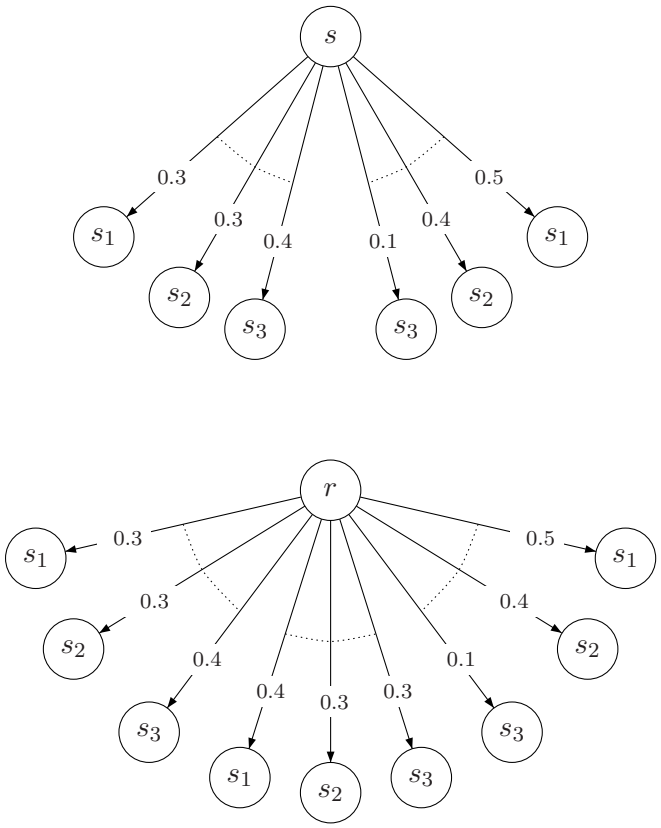

Figure 4.1: Counterexample of strong probabilistic bisimulation.

- We then extend our definitions to weak bisimulations, which characterize sublogics of PCTL and PCTL* with only unbounded path formulae.
- Further, we extend the framework to simulations as well as their characterizations.

4.2 Preliminaries

For a *finite* set S, a distribution is a function $\mu : S \to [0,1]$ satisfying $|\mu| := \sum_{s \in S} \mu(s) \leq 1$. We denote by $Dist(S)$ the set of distributions over S. We shall use $s, r, t, \ldots$ and $\mu, \nu \ldots$ to range over S and $Dist(S)$, respectively. The support of μ is defined by $Supp(\mu) = \{s \in S \mid \mu(s) > 0\}$. For an equivalence relation $\mathcal{R}$ over S, we write $\mu \; \mathcal{R} \; \nu$ if it holds that $\mu(C) = \nu(C)$ for all equivalence classes $C \in S/\mathcal{R}$. A distribution μ is called *Dirac* if $|Supp(\mu) \models 1$, and we let δ_s denote the Dirac distribution

with $\delta_s(s) = 1$. Given two distributions μ_1 and μ_2 such that $|\mu_1| + |\mu_2| \leq 1$, then $\mu_1 + \mu_2$ is a distribution such that $(\mu_1 + \mu_2)(s) = \mu_1(s) + \mu_2(s)$ for each $s \in S$. Let $\mu - C$ be a distribution such that $(\mu - C)(s) = \mu(s)$ if $s \notin C$, otherwise $(\mu - C)(s) = 0$, where $C \subseteq S$, we also write $\mu - \{s\}$ directly as $\mu - s$. Moreover $a \cdot \mu$ with $a \cdot |\mu| \leq 1$ is a distribution such that $(a \cdot \mu)(s) = a \cdot \mu(s)$ for each $s \in S$.

Let $\mathcal{R}$ be a relation over S, define $\mathcal{R}^{\uparrow}(C) = \{r \mid s\ \mathcal{R}\ r \wedge s \in C\}$ and $\mathcal{R}^{\downarrow}(C) = \{r \mid r\ \mathcal{R}\ s \wedge s \in C\}$. We say C is $\mathcal{R}$ upward closed iff $C = \mathcal{R}^{\uparrow}(C)$, and similarly C is $\mathcal{R}$ *downward closed* iff $C = \mathcal{R}^{\downarrow}(C)$. We use $\mathcal{R}^{\downarrow}(s)$ as the shorthand of $\mathcal{R}^{\downarrow}(\{s\})$, and $\mathcal{R}^{\downarrow} = \{\mathcal{R}^{\downarrow}(C) \mid C \subseteq S\}$ denotes the set of all $\mathcal{R}$ downward closed sets.

4.2.1 Probabilistic Automaton

We recall the notion of a probabilistic automaton introduced by Segala (78). We omit the set of actions, since they do not appear in the logic PCTL we shall consider later. Note that the bisimulation we shall introduce later can be extended to PA with actions directly.

Definition 21 (Probabilistic Automata)**.** *A* probabilistic automaton *is a tuple* $\mathcal{P} = (S, \rightarrow, IS, AP, L)$ *where*

- S *is a finite set of states;*
- $\rightarrow \subseteq S \times Dist(S)$ *is a transition relation;*
- $IS \subseteq S$ *is a set of initial states;*
- AP *is a set of atomic propositions;*
- $L : S \rightarrow 2^{AP}$ *is a labeling function.*

As usual we only consider image-finite PAs, i.e. $\{\mu \mid (s, \mu) \in \rightarrow\}$ is finite for each $s \in S$. A transition $(s, \mu) \in \rightarrow$ is denoted by $s \rightarrow \mu$. Moreover, we write $\mu \rightarrow \mu'$ iff for each $s \in supp(\mu)$ there exists $s \rightarrow \mu_s$ such that

$$\mu'(r) = \sum_{s \in supp(\mu)} \mu(s) \cdot \mu_s(r).$$

A *path* is a finite or infinite sequence $\omega = s_0 s_1 s_2 \ldots$ of states. For each $i \geq 0$ there exists a distribution μ such that $s_i \rightarrow \mu$ and $\mu(s_{i+1}) > 0$. We use $lstate(\omega)$ and $l(\omega)$ to denote the last state of ω and the length of ω respectively if ω is finite. The sets *Paths*

is the set of all paths, and $Paths(s_0)$ are those starting from s_0. Similarly, $Paths^*$ is the set of finite paths, and $Paths^*(s_0)$ are those starting from s_0. Also we use $\omega[i]$ to denote the $(i+1)$-th state for $i \geq 0$, $\omega|^i$ to denote the fragment of ω ending at $\omega[i]$, and $\omega|_i$ to denote the fragment of ω starting from $\omega[i]$.

When nondeterministic choices are involved, there does not exist a unique measure for the paths. As in (1, 83, 84) we introduce the definition of a *scheduler* to resolve nondeterminism. Intuitively, a scheduler decides how to choose the next transition based on the history execution of a PA by associating a distribution over all the available transitions at each step. Formally, a scheduler is a function

$$\pi : Paths^* \to Dist(\to)$$

such that $\pi(\omega)(s,\mu) > 0$ implies $s = lstate(\omega)$. A scheduler π is *deterministic* if it returns only Dirac distributions, that is, the next step is chosen deterministically. We use

$$Paths(s_0,\pi) = \{\omega \in Paths(s_0) \mid \forall i \geq 0. \exists \mu. \pi(\omega|^i)(\omega[i],\mu) > 0 \wedge \mu(\omega[i+1]) > 0\}$$

to denote the set of paths starting from s_0 respecting π. Similarly, $Paths^*(s_0,\pi)$ only contains finite paths.

The *cone* of a finite path ω, denoted by C_ω, is the set of paths having ω as their prefix, i.e.,

$$C_\omega = \{\omega' \mid \omega \leq \omega'\}$$

where $\omega' \leq \omega$ iff ω' is a prefix of ω. Fixing a starting state s_0 and a scheduler π, the measure $Prob_{\pi,s_0}$ of a cone C_ω, where $\omega = s_0 s_1 \ldots s_k$, is defined inductively as follows: $Prob_{\pi,s_0}(C_\omega)$ equals 1 if $k = 0$, and for $k > 0$,

$$Prob_{\pi,s_0}(C_\omega) = Prob_{\pi,s_0}(C_{\omega|^{k-1}}) \cdot \left(\sum_{(s_{k-1},\mu') \in \to} \pi(\omega|^{k-1})(s_{k-1},\mu') \cdot \mu'(s_k) \right)$$

Let $\mathcal{B}$ be the smallest algebra that contains all the cones and is closed under complement and countable unions [1], then $Prob_{\pi,s_0}$ can be extended to a unique measure on $\mathcal{B}$.

[1] By standard measure theory this algebra is a π-*algebra* and all its elements are the measurable sets of paths.

Given a preorder $\mathcal{R}$ over S, $(\mathcal{R}^{\downarrow})^i$ is the set of $\mathcal{R}$ *downward closed paths* of length i composed of $\mathcal{R}$ downward closed sets, and is equal to the *Cartesian* product of $\mathcal{R}^{\downarrow}$ with itself i times. Let

$$(\mathcal{R}^{\downarrow})^* = \bigcup_{i \geq 1} (\mathcal{R}^{\downarrow})^i$$

be the set of $\mathcal{R}$ *downward closed paths* of arbitrary length. Define $l(\Omega) = n$ for $\Omega \in (\mathcal{R}^{\downarrow})^n$. Let

$$\Omega = C_0 C_1 \dots C_n \in (\mathcal{R}^{\downarrow})^*$$

be the $\mathcal{R}$ *downward closed cone* C_Ω is defined as $C_\Omega = \{C_\omega \mid \omega \in \Omega\}$, where $\omega \in \Omega$ iff $\omega[i] \in C_i$ for $0 \leq i \leq n$.

For distributions μ_1 and μ_2, we define $\mu_1 \times \mu_2$ by

$$(\mu_1 \times \mu_2)((s_1, s_2)) = \mu_1(s_1) \times \mu_2(s_2).$$

Following (4) we also define the interleaving of PAs:

Definition 22 (Parallel Composition)**.** *Let* $\mathcal{P}_i = (S_i, \rightarrow_i, IS_i, AP_i, L_i)$ *be two* PA*s with* $i = 1, 2$*. The* parallel composition $\mathcal{P}_1 \parallel \mathcal{P}_2$ *is defined by:*

$$\mathcal{P}_1 \parallel \mathcal{P}_2 = (S_1 \times S_2, \rightarrow, IS_1 \times IS_2, AP_1 \times AP_2, L)$$

where

$$L((s_1, s_2)) = L_1(s_1) \times L_2(s_2)$$

and $(s_1, s_2) \rightarrow \mu$ *iff either*

- $s_1 \rightarrow \mu_1$ *and* $\mu = \mu_1 \times \delta_{s_2}$*, or*
- $s_2 \rightarrow \mu_2$ *and* $\mu = \delta_{s_1} \times \mu_2$*.*

The following example illustrates the application of the operator $\parallel$.

Example 37. *Suppose there are two states* s_0 *and* t_0 *as depicted in Fig. 4.2 (a) and (b) respectively, and their composition* $s_0 \parallel t_0$ *is given in Fig. 4.2 (c) where either* s_0 *or* t_0 *will perform first.*

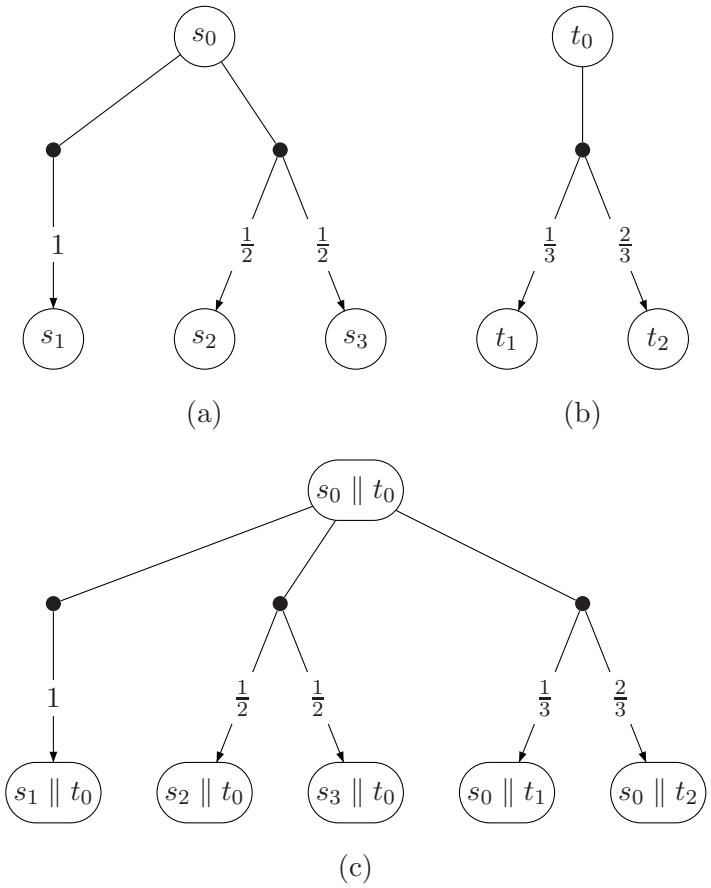

Figure 4.2: Parallel composition of s_0 and t_0.

4.2.2 PCTL* and its Sublogics

We introduce the syntax of PCTL (2) and PCTL* (3) which are probabilistic extensions of CTL and CTL* respectively. PCTL* over the set AP of atomic propositions are formed according to the following grammar:

$$\varphi ::= a \mid \varphi_1 \wedge \varphi_2 \mid \neg\varphi \mid \mathcal{P}_{\bowtie q}(\psi)$$
$$\psi ::= \varphi \mid \psi_1 \wedge \psi_2 \mid \neg\psi \mid \mathsf{X}\,\psi \mid \psi_1 \,\mathsf{U}\, \psi_2$$

where $a \in AP$, $\bowtie \in \{<, >, \leq, \geq\}$, $q \in [0, 1]$. We refer to φ and ψ as (PCTL*) state and path formulae, respectively.

The satisfaction relation $s \models \varphi$ for state formulae is defined as follows:

$$\begin{aligned}
s &\models a && \text{iff } a \in L(s)\\
s &\models \varphi_1 \wedge \varphi_2 && \text{iff } s \models \varphi_1 \wedge s \models \varphi_2\\
s &\models \neg\varphi && \text{iff } s \not\models \varphi\\
s &\models \mathcal{P}_{\bowtie q}(\psi) && \text{iff } \forall\pi.Prob_{\pi,s}(\{\omega \in Paths(s) \mid \omega \models \psi\}) \bowtie q
\end{aligned}$$

The satisfaction relation $\omega \models \psi$ for path formulae is defined exactly the same as for LTL formulae i.e.

$$\begin{aligned}
\omega &\models \varphi && \text{iff } \omega[0] \models \varphi\\
\omega &\models \psi_1 \wedge \psi_2 && \text{iff } \omega \models \psi_1 \wedge \omega \models \psi_2\\
\omega &\models \neg\psi && \text{iff } \omega \not\models \psi\\
\omega &\models \mathsf{X}\,\psi && \text{iff } \omega|_1 \models \psi\\
\omega &\models \psi_1 \,\mathsf{U}\, \psi_2 && \text{iff } \exists j \geq 0.(\omega|_j \models \psi_2 \wedge \forall 0 \leq k < j.(\omega|_k \models \psi_1))
\end{aligned}$$

Sublogics. The depth of path formula ψ of PCTL^* free of U operator, denoted by $Depth(\psi)$, is defined by the maximum number of embedded X operators appearing in ψ, that is,

- $Depth(\varphi) = 0$,
- $Depth(\psi_1 \wedge \psi_2) = \max\{Depth(\psi_1), Depth(\psi_2)\}$,
- $Depth(\neg\psi) = Depth(\psi)$ and
- $Depth(\mathsf{X}\,\psi) = 1 + Depth(\psi)$.

Then, we let PCTL^{*-} be the sublogic of PCTL^* without the until $(\psi_1 \,\mathsf{U}\, \psi_2)$ operator. Moreover, PCTL^{*-}_i is a sublogic of PCTL^{*-} where for each ψ we have $Depth(\psi) \leq i$.

The sublogic PCTL is obtained by restricting the path formulae to:

$$\psi ::= \mathsf{X}\,\varphi \mid \varphi_1 \,\mathsf{U}\, \varphi_2 \mid \varphi_1 \,\mathsf{U}^{\leq n}\, \varphi_2$$

Note the bounded until formula does not appear in PCTL^* as it can be encoded by nested next operator. PCTL^- is defined in a similar way as for PCTL^{*-}. Moreover we let PCTL^-_i be the sublogic of PCTL^- where only bounded until operator $\varphi_1 \,\mathsf{U}^{\leq j}\, \varphi_2$ with $j \leq i$ is allowed.

Logical equivalence. For a logic $\mathcal{L}$, we say that s and r are $\mathcal{L}$-equivalent, denoted by $s \sim_{\mathcal{L}} r$, if they satisfy the same set of formulae of $\mathcal{L}$, that is

$$s \models \varphi \text{ iff } r \models \varphi$$

for all formulae φ in $\mathcal{L}$. The logic $\mathcal{L}$ can be PCTL* or one of its sublogics.

4.2.3 Strong Probabilistic Bisimulation

In this section we introduce the definition of strong probabilistic bisimulation (1). Let $\{s \rightarrow \mu_i\}_{i \in I}$ be a collection of transitions of $\mathcal{P}$, and let $\{p_i\}_{i \in I}$ be a collection of probabilities with $\sum_{i \in I} p_i = 1$. Then $(s, \sum_{i \in I} p_i \mu_i)$ is called a *combined transition* and is denoted by $s \xrightarrow{}_{\mathsf{P}} \mu$ where $\mu = \sum_{i \in I} p_i \mu_i$.

Definition 23 (Strong Probabilistic Bisimulation)**.** *An equivalence relation $\mathcal{R} \subseteq S \times S$ is a strong probabilistic bisimulation iff $s \mathcal{R} r$ implies that $L(s) = L(r)$ and for each $s \rightarrow \mu$, there exists a combined transition $r \xrightarrow{}_{\mathsf{P}} \mu'$ such that $\mu \mathcal{R} \mu'$.*

We write $s \sim_{\mathsf{P}} r$ whenever there is a strong probabilistic bisimulation $\mathcal{R}$ such that $s \mathcal{R} r$.

It was shown in (1) that $\sim_{\mathsf{P}}$ is preserved by $\|$, that is,

$$s \sim_{\mathsf{P}} r \text{ implies } s \| t \sim_{\mathsf{P}} r \| t$$

for any t. Also strong probabilistic bisimulation is sound for PCTL which means that if $s \sim_{\mathsf{P}} r$ then for any state formula φ of PCTL, $s \models \varphi$ iff $r \models \varphi$. But the other way around is not true, i.e. strong probabilistic bisimulation is not complete for PCTL, as illustrated by the following example.

Example 38. *Consider again the two PAs in Fig. 4.1 and assume that $L(s) = L(r)$ and $L(s_1) \neq L(s_2) \neq L(s_3)$. In addition, s_1, s_2, and s_3 only have one transition to themselves with probability 1. The only difference between the left and right automata is that the right automaton has an extra step. It is not hard to see that $s \sim_{\mathsf{PCTL}^*} r$. By Definition 23 $s \nsim_{\mathsf{P}} r$ since the middle transition of r cannot be simulated by s even with combined transition. So we conclude that strong probabilistic bisimulation is not complete for PCTL* as well as for PCTL.*

It should be noted that PCTL* distinguishes more states in a PA than PCTL. Refer to the following example.

Example 39. *Suppose s and r are given by Fig. 4.1 where each of s_1, s_2, and s_3 is extended with a transition such that $s_1 \to \mu_1$ with $\mu_1(s_1) = 0.6$ and $\mu_1(s_4) = 0.4$, $s_2 \to \mu_2$ with $\mu_2(s_4) = 1$, and $s_3 \to \mu_3$ with $\mu_3(s_3) = 0.5$ and $\mu_3(s_4) = 0.5$. Here we assume that every state satisfies different atomic propositions except that $L(s) = L(r)$. Then it is not hard to see $s \sim_{\mathsf{PCTL}} r$ while $s \nsim_{\mathsf{PCTL}^*} r$. Consider the PCTL^* formula*

$$\varphi = \mathcal{P}_{\leq 0.38}(\mathsf{X}(L(s_1) \vee L(s_3)) \wedge \mathsf{X}\mathsf{X}(L(s_1) \vee L(s_3))),$$

it holds

$$s \models \varphi \text{ but } r \not\models \varphi.$$

Note that φ is not a well-formed PCTL formula. Indeed, states s and r are PCTL-equivalent.

We have the following theorem:

Theorem 19. *1. $\sim_{\mathsf{PCTL}}$, $\sim_{\mathsf{PCTL}^*}$, $\sim_{\mathsf{PCTL}^-}$, $\sim_{\mathsf{PCTL}_i^-}$, $\sim_{\mathsf{PCTL}^{*-}}$, $\sim_{\mathsf{PCTL}_i^{*-}}$, and $\sim_{\mathsf{P}}$ are equivalence relations for any $i \geq 1$.*

2. $\sim_{\mathsf{P}} \subseteq \sim_{\mathsf{PCTL}^*} \subseteq \sim_{\mathsf{PCTL}}$.

3. $\sim_{\mathsf{PCTL}^{*-}} \subseteq \sim_{\mathsf{PCTL}^-}$.

4. $\sim_{\mathsf{PCTL}_1^{*-}} = \sim_{\mathsf{PCTL}_1^-}$.

5. $\sim_{\mathsf{PCTL}_i^{*-}} \subseteq \sim_{\mathsf{PCTL}_i^-}$ for any $i > 1$.

6. $\sim_{\mathsf{PCTL}} \subseteq \sim_{\mathsf{PCTL}^-} \subseteq \sim_{\mathsf{PCTL}_{i+1}^-} \subseteq \sim_{\mathsf{PCTL}_i^-}$ for all $i \geq 0$.

7. $\sim_{\mathsf{PCTL}^*} \subseteq \sim_{\mathsf{PCTL}^{*-}} \subseteq \sim_{\mathsf{PCTL}_{i+1}^{*-}} \subseteq \sim_{\mathsf{PCTL}_i^{*-}}$ for all $i \geq 0$.

Proof. We take $\sim_{\mathsf{PCTL}}$ as an example and the others can be proved in a similar way. The reflexivity is trivial. If $s \sim_{\mathsf{PCTL}} r$, then we also have $r \sim_{\mathsf{PCTL}} s$ since s and r satisfy the same set of formulae, we prove the symmetry of $\sim_{\mathsf{PCTL}}$. Now we prove the transitivity, that is, for any s, r, t if we have $s \sim_{\mathsf{PCTL}} r$ and $r \sim_{\mathsf{PCTL}} t$, then $s \sim_{\mathsf{PCTL}} t$. It is also easy, since s and r satisfy the same set of formulae, and r and t satisfy the same set of formulae by $s \sim_{\mathsf{PCTL}} r$ and $r \sim_{\mathsf{PCTL}} t$, as result $s \models \varphi$ implies $t \models \varphi$ and vice versa for any φ, so $s \sim_{\mathsf{PCTL}} t$. We conclude that $\sim_{\mathsf{PCTL}}$ is an equivalence relation.

The proof of $\sim_{\mathsf{P}} \subseteq \sim_{\mathsf{PCTL}}$ can be found in (1) while the proof of $\sim_{\mathsf{P}} \subseteq \sim_{\mathsf{PCTL}^*}$ can be proved in a similar way. $\sim_{\mathsf{PCTL}^*} \subseteq \sim_{\mathsf{PCTL}}$ is trivial since PCTL is a subset of PCTL^*.

The proofs of Clause 3 and 5 are obvious since $\sim_{\mathsf{PCTL}^-}$ is a subset of $\sim_{\mathsf{PCTL}^{*-}}$ while $\sim_{\mathsf{PCTL}_i^-}$ is a subset of $\sim_{\mathsf{PCTL}_i^{*-}}$.

We now prove that $\sim_{\mathsf{PCTL}_1^{*-}} = \sim_{\mathsf{PCTL}_1^-}$. It is sufficient to prove that PCTL_1^- and PCTL_1^{*-} have the same expressiveness. $\sim_{\mathsf{PCTL}_1^{*-}} \subseteq \sim_{\mathsf{PCTL}_1^-}$ is easy since PCTL_1^- is a subset of PCTL_1^{*-}. We now show how formulae of PCTL_1^{*-} can be encoded by formulae of PCTL_1^-. It is not hard to see that the syntax of path formulae of PCTL_1^{*-} can be rewritten as:

$$\psi ::= \varphi \mid \mathsf{X}\varphi \mid \neg\psi \mid \psi_1 \wedge \psi_2$$

where we replace $\mathsf{X}\psi$ with $\mathsf{X}\varphi$ since PCTL_1^{*-} only allows path formulae whose depth is less or equal than 1. Since $\neg\mathsf{X}\varphi = \mathsf{X}\neg\varphi$, the syntax can refined further by deleting $\neg\psi$, that is,

$$\psi ::= \varphi \mid \mathsf{X}\varphi \mid \psi_1 \wedge \psi_2$$

Then the only left cases we need to consider are $\mathcal{P}_{\bowtie q}(\varphi)$, $\mathcal{P}_{\bowtie q}(\mathsf{X}\varphi_1 \wedge \mathsf{X}\varphi_2)$, and $\mathcal{P}_{\bowtie q}(\mathsf{X}\varphi_1 \wedge \varphi_2)$,

1. $s \models \mathcal{P}_{\geq q}(\varphi)$ iff $s \models \varphi$,
2. $s \models \mathcal{P}_{\geq q}(\mathsf{X}\varphi_1 \wedge \mathsf{X}\varphi_2)$ iff $s \models \mathcal{P}_{\geq q}(\mathsf{X}(\varphi_1 \wedge \varphi_2))$,
3. $s \models \mathcal{P}_{\geq q}(\mathsf{X}\varphi_1 \wedge \varphi_2)$ iff $s \models \varphi_2 \wedge \mathcal{P}_{\geq q}(\mathsf{X}\varphi_1)$.

Here we assume that $0 < q \leq 1$, other cases are similar and are omitted.

The proofs of Clauses 6 and 7 are straightforward. □

4.3 A Novel Strong Bisimulation

In this section we introduce a novel notion of strong bisimulation and strong branching bisimulation. We shall show that they agree with PCTL and PCTL^* equivalences, respectively. As a preparation step we introduce the strong 1-depth bisimulation.

4.3.1 Strong 1-depth Bisimulation

Definition 24 (Strong 1-depth Bisimulation)**.** *A relation $\mathcal{R} \subseteq S \times S$ is a strong 1-depth bisimulation if $s\ \mathcal{R}\ r$ implies that $L(s) = L(r)$ and for any $\mathcal{R}$ downward closed set C*

1. *for each $s \to \mu$, there exists $r \to \mu'$ such that $\mu'(C) \geq \mu(C)$,*
2. *for each $r \to \mu$, there exists $s \to \mu'$ such that $\mu'(C) \geq \mu(C)$.*

We write $s \sim_1 r$ *whenever there is a strong* 1*-depth bisimulation* $\mathcal{R}$ *such that* $s \mathcal{R} r$.

The – though very simple – definition requires only one step matching of the distributions out of s and r. The essential difference to the standard definition is: the quantification of the downward closed set comes before the quantification over transition. This is indeed the key of the new definition of bisimulations. The following theorem shows that $\sim_1$ agrees with $\sim_{\mathsf{PCTL}_1^-}$ and $\sim_{\mathsf{PCTL}_1^{*-}}$ which is also an equivalence relation:

Lemma 17. $\sim_{\mathsf{PCTL}_1^-} = \sim_1 = \sim_{\mathsf{PCTL}_1^{*-}}$.

Proof. According to Clause (4) of Theorem 19, it is enough to prove that

$$\sim_{\mathsf{PCTL}_1^-} = \sim_1 .$$

We defer the proof to Theorem 21. □

Note that in Definition 24 we consider all the $\mathcal{R}$ downward closed sets since it is not enough to only consider the $\mathcal{R}$ downward closed sets in $\{\mathcal{R}^{\downarrow}(s) \mid s \in S\}$, refer to the following counterexample.

Counterexample 1. *Suppose that there are four absorbing states* s_1, s_2, s_3, *and* s_4 *which are assigned with different atomic propositions. Suppose we have two processes* s *and* r *such that* $L(s) = L(r)$ *and*

$$s \to \mu_1 \qquad s \to \mu_2$$

$$r \to \nu_1 \qquad r \to \nu_2$$

where

$$\mu_1(s_1) = 0.5 \qquad \mu_1(s_2) = 0.5$$
$$\mu_2(s_3) = 0.5 \qquad \mu_2(s_4) = 0.5$$
$$\nu_1(s_1) = 0.5 \qquad \nu_1(s_3) = 0.5$$
$$\nu_2(s_2) = 0.5 \qquad \nu_2(s_4) = 0.5$$

If we only consider the $\mathcal{R}$ *downward closed sets in* $\{\mathcal{R}^{\downarrow}(s) \mid s \in S\}$ *where*

$$S = \{s, r, s_1, s_2, s_3, s_4\},$$

then we will conclude that $s \sim_1 r$, *but* $r \models \varphi$ *while* $s \not\models \varphi$ *where*

$$\varphi = \mathcal{P}_{\geq 0.5}(\mathsf{X}(L(s_1) \vee L(s_2))).$$

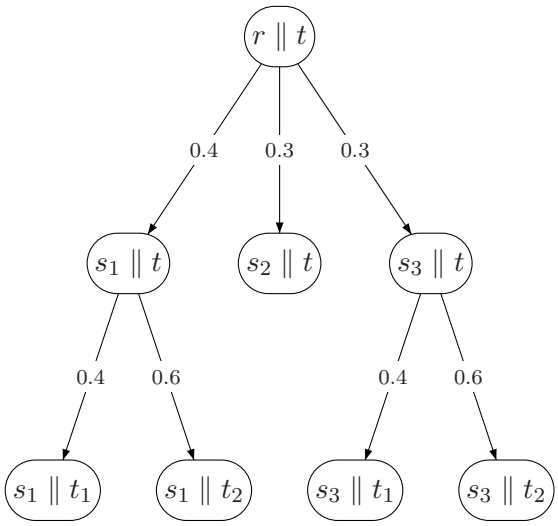

Figure 4.3: $\sim_i^b$ is not compositional when $i > 1$

It turns out that $\sim_1$ is preserved by $\parallel$, implying that $\sim_{\mathsf{PCTL}_1^-}$ and $\sim_{\mathsf{PCTL}_1^{*-}}$ are preserved by $\parallel$ as well.

Theorem 20. *$s \sim_1 r$ implies that $s \parallel t \sim_1 r \parallel t$ for any t.*

Proof. We need to prove that for each $\sim_1$ closed set C, if $s \parallel t \to \mu$ such that $\mu(C) > 0$, there exists $r \parallel t \to \mu'$ such that $\mu'(C) \geq \mu(C)$ and vice versa. This can be prove by structural induction on $s \parallel t$ and $r \parallel t$. By the definition of $\parallel$ operator, if $s \parallel t \to \mu$, then either $s \to \mu_s$ with $\mu = \mu_s \parallel \delta_t$, or $t \to \mu_t$ with $\mu = \delta_s \parallel \mu_t$. We only consider the case when $\mu = \mu_s \parallel \delta_t$ since the other one is similar. We have known that $s \sim_1 r$, so for each C' if $s \to \mu_s$ with $\mu_s(C') > 0$, then there exists $r \to \mu_r$ such that $\mu_r(C') \geq \mu_s(C')$. By induction, if $s' \sim_1 r'$ for $s', r' \in C'$, then $s' \parallel t \sim_1 r' \parallel t$. So for each C and $s \parallel t \to \mu$ with $\mu(C) > 0$, there exists $r \parallel t \to \mu'$ such that $\mu'(C) \geq \mu(C)$. □

Remark 1. *We note that for Kripke structure (*PA *with only Dirac distributions) $\sim_1$ agrees with the usual strong bisimulation by Milner (8).*

4.3.2 Strong Branching Bisimulation

Now we extend the relation $\sim_1$ to strong i-step bisimulations. Then, the intersection of all of these relations gives us the new notion of strong branching bisimulation, which we show to be the same as $\sim_{\mathsf{PCTL}}$. Recall Theorem 19 states that $\sim_{\mathsf{PCTL}}$ is strictly coarser than $\sim_{\mathsf{PCTL}^*}$, which we shall consider in the next section.

Following the approach in (85) we define $Prob_{\pi,s}(C, C', n, \omega)$ which denotes the probability from s to states in C' via states in C possibly in at most n steps under scheduler π, where ω is used to keep track of the path and only deterministic schedulers are considered in the following. Formally, $Prob_{\pi,s}(C, C', n, \omega)$ equals 1 if $s \in C'$, and else if $n > 0 \wedge (s \in C \setminus C')$, then

$$Prob_{\pi,s}(C, C', n, \omega) = \sum_{r \in supp(\mu')} \mu'(r) \cdot Prob_{\pi,r}(C, C', n-1, \omega r) \tag{4.1}$$

where $\pi(\omega)(s, \mu') = 1$, otherwise $Prob_{\pi,s}(C, C', n, \omega)$ equals to 0.

Strong i-depth branching bisimulation is a straightforward extension of strong 1-depth bisimulation, where instead of considering only one immediate step, we consider up to i steps. We let $\sim_1^b = \sim_1$ in the following.

Definition 25 (Strong i-depth Branching Bisimulation)**.** *A relation $\mathcal{R} \subseteq S \times S$ is a strong i-depth branching bisimulation with $i > 1$ if $s \mathcal{R} r$ implies $s \sim_{i-1}^b r$ and for any $\mathcal{R}$ downward closed sets C, C',*

1. *for each scheduler π, there exists a scheduler π' such that*

$$Prob_{\pi',r}(C, C', i, r) \geq Prob_{\pi,s}(C, C', i, s),$$

2. *for each scheduler π, there exists a scheduler π' such that*

$$Prob_{\pi',s}(C, C', i, s) \geq Prob_{\pi,r}(C, C', i, r).$$

We write $s \sim_i^b r$ whenever there is a strong i-depth branching bisimulation $\mathcal{R}$ such that $s \mathcal{R} r$. The strong branching bisimulation $\sim^b$ is defined as

$$\sim^b = \bigcap_{i \geq 1} \sim_i^b .$$

The following lemma shows that $\sim_i^b$ is an equivalence relation, and moreover, $\sim_i^b$ decreases until a fixed point is reached.

Lemma 18. *1. $\sim^b$ and $\sim_i^b$ are equivalence relations for any $i > 1$.*

2. *$\sim_j^b \subseteq \sim_i^b$ provided that $1 \leq i \leq j$.*

3. *There exists $i \geq 1$ such that $\sim_j^b = \sim_k^b$ for any $j, k \geq i$.*

Proof. We only show the proof of transitivity of $\sim_i^b$. Suppose that $s \sim_i^b t$ and $t \sim_i^b r$, we need to prove that $s \sim_i^b r$. By Definition 25, we know there exists strong i-depth branching bisimulations $\mathcal{R}_1$ and $\mathcal{R}_2$ such that $s \mathcal{R}_1 t$ and $t \mathcal{R}_2 r$. Let

$$\mathcal{R} = \mathcal{R}_1 \circ \mathcal{R}_2 = \{(s_1, s_3) \mid \exists s_2.(s_1 \mathcal{R}_1 s_2 \wedge s_2 \mathcal{R}_2 r)\},$$

it is enough to show that $\mathcal{R}$ is a strong i-depth bisimulation. Note $\mathcal{R}_1 \cup \mathcal{R}_2 \subseteq \mathcal{R}$, since for each $s_1 \mathcal{R}_1 s_2$ we also have $s_2 \mathcal{R}_2 s_2$ due to reflexivity, thus $s_1 \mathcal{R} s_2$, similarly we can show that $\mathcal{R}_2 \subseteq \mathcal{R}$. Therefore for any $\mathcal{R}$ downward closed sets C and C', they are also $\mathcal{R}_1$ and $\mathcal{R}_2$ downward closed. Therefore for each π, there exists π' such that

$$Prob_{\pi',t}(C, C', i) \geq Prob_{\pi,s}(C, C', i).$$

Since we also have $t \sim_i^b r$, thus there exists π'' such that

$$Prob_{\pi'',r}(C, C', i) \geq Prob_{\pi',t}(C, C', i) \geq Prob_{\pi,s}(C, C', i).$$

This completes the proof of transitivity.

The proof of Clause (2) is straightforward from Definition 27, since $s \sim_j^b r$ implies $s \sim_{j-1}^b r$ when $j > 1$.

It is straightforward from the Definition 25 that $\sim_i^b$ is getting more discriminating as i increases. In a PA only with finite states the maximum number of equivalence classes is equal to the number of states, as a result we can guarantee that $\sim_n^b = \sim^b$ where n is the total number of states. □

Let $\mathcal{R}$ be an equivalence over S. The set $C \subseteq S$ is said to be $\mathcal{R}$ closed iff $s \in C$ and $s \mathcal{R} r$ implies $r \in C$. $C_{\mathcal{R}}$ is used to denote the least $\mathcal{R}$ closed set which contains C.

Definition 26. *Two paths $\omega_1 = s_0 s_1 \ldots$ and $\omega_2 = r_0 r_1 \ldots$ are strong i-depth branching bisimilar, written as $\omega_1 \sim_i^b \omega_2$, iff $\omega_1[j] \sim_i^b \omega_2[j]$ for all $0 \leq j \leq i$.*

We first define the $\sim_i^b$ closed paths i.e. the set Ω of paths is $\sim_i^b$ *closed* if for any $\omega_1 \in \Omega$ and ω_2 such that $\omega_1 \sim_i^b \omega_2$, it holds that $\omega_2 \in \Omega$. Let

$$\mathcal{B}_{\sim_i^b} = \{\Omega \subseteq \mathcal{B} \mid \Omega \text{ is } \sim_i^b \text{ closed}\}.$$

By standard measure theory $\mathcal{B}_{\sim_i^b}$ is measurable. The $\sim_i$ for paths can be defined similarly and is omitted here.

Lemma 19. *$s \sim_{\mathsf{PCTL}} r$ iff $s \sim_n^b r$ for any $n \geq 1$, that is,*

$$\sim_{\mathsf{PCTL}} = \bigcap_{n \geq 1} \sim_n^b .$$

Proof. The proof is based on the fact that

$$\varphi_1 \,\mathsf{U}\, \varphi_2 = \varphi_1 \,\mathsf{U}^{\leq\infty}\, \varphi_2.$$

□

It is not hard to show that $\sim_i^b$ characterizes PCTL_i^-. Moreover, we show that $\sim^b$ agrees with PCTL equivalence.

Theorem 21. *$\sim_{\mathsf{PCTL}_i^-} = \sim_i^b$ for any $i \geq 1$, and moreover $\sim_{\mathsf{PCTL}} = \sim^b$.*

Proof. In the following, we will use

$$Sat(\varphi) = \{s \in S \mid s \models \varphi\}$$

to denote the set of states which satisfy φ. Similarly,

$$Sat(\psi) = \{\omega \in Paths(s_0) \mid \omega \models \psi\}$$

is the set of paths which satisfy ψ.

Let

$$\mathcal{R} = \{(s, r) \mid s \ \sim_{\mathsf{PCTL}_i^-} \ r\},$$

in order to prove that $s \ \sim_{\mathsf{PCTL}_i^-} \ r$ implies $s \ \sim_i^b \ r$ for any s and r, we need to show that for any $\mathcal{R}$ closed sets C, C' and scheduler π, there exists a scheduler π' such that

$$Prob_{\pi',r}(C, C', i, r) \geq Prob_{\pi,s}(C, C', i, s)$$

and vice versa provided that $s \ \mathcal{R} \ r$. Suppose there are n different equivalence classes in a finite PA. Let φ_{C_i,C_j} be a state formula such that

$$Sat(\varphi_{C_i,C_j}) \supseteq C_i \text{ and } Sat(\varphi_{C_i,C_j}) \cap C_j = \emptyset,$$

here $1 \leq i \neq j \leq n$ and $C_i, C_j \in S/\mathcal{R}$ are two different equivalence classes. Formula like φ_{C_i,C_j} always exists, otherwise there will not exist a formula which is fulfilled by states in C_i, but not fulfilled by states in C_j, that is, states in C_i and C_j satisfy the same set of formulae, this is against the assumption that C_i and C_j are two different equivalence classes. Let

$$\varphi_{C_i} = \bigwedge_{1 \leq j \neq i \leq n} \varphi_{C_i,C_j},$$

it is not hard to see that $Sat(\varphi_{C_i}) = C_i$. For a $\mathcal{R}$ closed set C, it holds

$$\varphi_C = \bigvee_{C' \in S/\mathcal{R} \wedge C' \subseteq C} \varphi_{C'},$$

then $Sat(\varphi_C) = C$. Now suppose $Prob_{\pi,s}(C, C', i, s) = q$, then we know

$$s \models \neg\mathcal{P}_{<q}\psi \text{ where } \psi = \varphi_C \,\mathsf{U}^{\leq j}\, \varphi_{C'}.$$

By assumption $r \models \neg\mathcal{P}_{<q}\psi$, so there exists a scheduler π' such that

$$Prob_{\pi',r}(C, C', i, r) \geq q,$$

that is,

$$Prob_{\pi',r}(C, C', i, r) \geq Prob_{\pi,s}(C, C', i, s).$$

The other case is similar and is omitted here.

The proof of $\sim_i^b \subseteq \sim_{\mathsf{PCTL}_i^-}$ is by structural induction on the syntax of state formula φ and path formula ψ of PCTL_i^-, that is, we need to prove the following two results simultaneously.

1. $s \sim_i^b r$ implies that $s \models \varphi$ iff $r \models \varphi$ for any state formula φ.
2. $\omega_1 \sim_i^b \omega_2$ implies that $\omega_1 \models \psi$ iff $\omega_2 \models \psi$ for any path formula ψ.

We only consider $\varphi = \mathcal{P}_{\leq q}(\psi)$ where $\psi = \varphi_1 \,\mathsf{U}^{\leq i}\, \varphi_2$, since other cases are similar. According to the semantics

$$s \models \varphi \text{ iff } \forall\pi. Prob_{\pi,s}(\{\omega \mid \omega \models \psi\}) \leq q.$$

By induction $\Omega = \{\omega \mid \omega \models \psi\}$ is $\sim_i^b$ closed. We need to show that $l(\Omega) = i$ and there exists two $\sim_i^b$ closed sets C, C' such that $\Omega = \bigcup_{0 \leq k < i} C^k C'$, this is straightforward by the semantics of $\mathsf{U}^{\leq i}$. We prove by contraction, and assume $s \models \varphi$ and $r \not\models \varphi$. Then for any π, we have $Prob_{\pi,s}(\Omega) \geq q$. Since $r \not\models \varphi$, there exists π' such that $Prob_{\pi',r}(\Omega) > q$, thus there does not exist π such that

$$Prob_{\pi,s}(C, C', i, s) \geq Prob_{\pi',r}(C, C', i, r),$$

which contradicts with assumption $s \sim_i^b r$. Therefore $r \models \varphi$, and $s \sim_{\mathsf{PCTL}_i^-} r$.

The proof of $\sim_{\mathsf{PCTL}} = \sim^b$ is straightforward by using Lemma 18 and Lemma 19. □

Intuitively, since $\sim_i^b$ decreases as i increases, for any PA $\sim_i^b$ will eventually converge to PCTL equivalence.

Recall $\sim_1^b$ is compositional by Theorem 20, which unfortunately is not the case for $\sim_i^b$ with $i > 1$. This is illustrated by the following example:

Counterexample 2. *$s \sim_i^b r$ does not imply $s \parallel t \sim_i^b r \parallel t$ for any t generally if $i > 1$.*

We have shown in Example 38 that $s \sim_{\mathsf{PCTL}} r$. If we compose s and r with t where t only has a transition to μ such that $\mu(t_1) = 0.4$ and $\mu(t_2) = 0.6$, then it turns out that

$$s \parallel t \not\sim_{\mathsf{PCTL}} r \parallel t.$$

Since there exists $\varphi = \mathcal{P}_{\leq 0.34}\psi$ with

$$\psi = ((L(s \parallel t) \vee L(s_1 \parallel t) \vee (L(s_3 \parallel t)))\, \mathsf{U}^{\leq 2} (L(s_1 \parallel t_2) \vee L(s_3 \parallel t_1)))$$

such that

$$s \parallel t \models \varphi \text{ but } r \parallel t \not\models \varphi,$$

as there exists a scheduler π such that the probability of paths satisfying ψ in $Prob_{\pi,r}$ equals 0.36. Fig. 4.3 shows the execution of r guided by the scheduler π, and we assume all the states in Fig. 4.3 have different atomic propositions except that $L(s \parallel t) = L(r \parallel t)$. It is similar for $\sim_{\mathsf{PCTL}^*}$.

Note that φ is also a well-formed state formula of PCTL_2^-, so $\sim_{\mathsf{PCTL}_i^-}$ as well as $\sim_i^b$ are not compositional if $i \geq 2$.

4.3.3 Strong Bisimulation

In this section we introduce a new notion of strong bisimulation and show that it characterizes $\sim_{\mathsf{PCTL}^*}$. Given a preorder $\mathcal{R}$, a $\mathcal{R}$ downward closed cone C_Ω and a measure $Prob$, the value of $Prob(C_\Omega)$ can be computed by summing up the values of all $Prob(C_\omega)$ with $\omega \in \Omega$. We let $\tilde{\Omega} \subseteq (\mathcal{R}^{\downarrow})^*$ be a set of $\mathcal{R}$ downward closed paths, then $C_{\tilde{\Omega}}$ is the corresponding set of $\mathcal{R}$ downward closed cones, that is, $C_{\tilde{\Omega}} = \cup_{\Omega \in \tilde{\Omega}} C_\Omega$. Define

$$l(\tilde{\Omega}) = Max\{l(\Omega) \mid \Omega \in \tilde{\Omega}\}$$

as the maximum length of Ω in $\tilde{\Omega}$. To compute $Prob(C_{\tilde{\Omega}})$, we cannot sum up the value of each $Prob(C_\Omega)$ such that $\Omega \in \widetilde{\Omega}$ as before since we may have a path ω such that $\omega \in \Omega_1$ and $\omega \in \Omega_2$ where $\Omega_1, \Omega_2 \in \widetilde{\Omega}$, so we have to remove these duplicate paths and make sure each path is considered once and only once as follows where we abuse the notation and write $\omega \in \widetilde{\Omega}$ iff $\exists \Omega.(\Omega \in \widetilde{\Omega} \wedge \omega \in \Omega)$:

$$Prob(C_{\widetilde{\Omega}}) = \sum_{\omega \in \widetilde{\Omega} \wedge \nexists \omega' \in \widetilde{\Omega}.\omega' \leq \omega} Prob(C_\omega) \tag{4.2}$$

Note Equation 4.2 can be extended to compute the probability of any set of cones in a given measure.

The definition of strong i-depth bisimulation is as follows:

Definition 27 (Strong i-depth Bisimulation)**.** *A relation $\mathcal{R} \subseteq S \times S$ is a strong i-depth bisimulation if $i > 1$ and $s\ \mathcal{R}\ r$ implies that $s \sim_{i-1} r$ and for any $\widetilde{\Omega} \subseteq (\mathcal{R}^{\downarrow})^*$ with $l(\widetilde{\Omega}) = i$*

1. *for each scheduler π, there exists π' such that*

$$Prob_{\pi',r}(C_{\widetilde{\Omega}}) \geq Prob_{\pi,s}(C_{\widetilde{\Omega}}),$$

2. *for each scheduler π, there exists π' such that*

$$Prob_{\pi',s}(C_{\widetilde{\Omega}}) \geq Prob_{\pi,r}(C_{\widetilde{\Omega}}).$$

We write $s \sim_i r$ whenever there is a i-depth strong bisimulation $\mathcal{R}$ such that $s\ \mathcal{R}\ r$. The strong bisimulation $\sim$ is defined as

$$\sim\ = \bigcap_{i \geq 1} \sim_i .$$

Similar to $\sim_i^b$, the relation $\sim_i$ forms a chain of equivalence relations where the strictness of $\sim_i$ increases as i increases, and $\sim_i$ will converge finally in a PA.

Lemma 20. *1. $\sim_i$ is an equivalence relation for any $i > 1$.*

2. $\sim_j \subseteq \sim_i$ provided that $1 \leq i \leq j$.

3. There exists $i \geq 1$ such that $\sim_j = \sim_k$ for any $j, k \geq i$.

Proof. 1. The proof is similar as the proof of Clause 1 of Lemma 18.

2. The proof is straightforward from Definition 27.

3. Since there are only finitely many states, thus there are only finitely many equivalence classes, such i always exists.

□

Let $\sim = \bigcap_{n \geq 1} \sim_n$, we have a lemma as follows:

Lemma 21. *$s \sim_{\mathsf{PCTL}^*} r$ iff $s \sim_n r$ for any $n \geq 1$, that is,*

$$\sim_{\mathsf{PCTL}^*} = \bigcap_{n \geq 1} \sim_n .$$

Proof. The proof is based on the fact that $\psi_1 \,\mathsf{U}\, \psi_2 = \psi_1 \,\mathsf{U}^{\leq \infty}\, \psi_2$. □

Below we show that $\sim_i$ characterizes $\sim_{\mathsf{PCTL}_i^{*-}}$ for all $i \geq 1$, and $\sim$ agrees with PCTL^* equivalence:

Theorem 22. *$\sim_{\mathsf{PCTL}_i^{*-}} = \sim_i$ for any $i \geq 1$, and moreover $\sim_{\mathsf{PCTL}^*} = \sim$.*

Proof. Let

$$\mathcal{R} = \{(s, r) \mid s \sim_{\mathsf{PCTL}_i^{*-}} r\},$$

we need to show that $\mathcal{R}$ is strong i-depth bisimulation in order to prove that $s \sim_{\mathsf{PCTL}_i^{*-}} r$ implies $s \sim_i r$ for any s and r. According to Definition 27, we need to show that for any $\widetilde{\Omega} \subseteq (\mathcal{R}^{\downarrow})^*$ with $l(\widetilde{\Omega}) = i$ and scheduler π, there exists a scheduler π' such that

$$Prob_{\pi',r}(C_{\widetilde{\Omega}}) \geq Prob_{\pi,s}(C_{\widetilde{\Omega}})$$

and vice versa provided that $s \,\mathcal{R}\, r$. Following the way in the proof of Theorem 21, we can construct a formula φ_C such that $Sat(\varphi_C) = C$ where C is a $\mathcal{R}$ closed set. Suppose $\Omega = C_0 C_1 \ldots C_j$ with $j \leq i$, then

$$\psi_\Omega = \varphi_{C_0} \wedge \mathsf{X}(\varphi_{C_1} \wedge \ldots \wedge \mathsf{X}(\varphi_{C_{j-1}} \wedge \mathsf{X}\, \varphi_{C_j}))$$

can be used to characterize Ω, that is, $Sat(\psi_\Omega) = C_\Omega$. Let $\psi = \bigvee_{\Omega \in \widetilde{\Omega}} \psi_\Omega$, then $Sat(\psi) = C_{\widetilde{\Omega}}$. As a result $s \models \neg \mathcal{P}_{<q} \psi$ where $q = Prob_{\pi,s}(C_{\widetilde{\Omega}})$. By assumption $r \models \neg \mathcal{P}_{<q} \psi$, so there exists a scheduler π' such that $Prob_{\pi',r}(C_{\widetilde{\Omega}}) \geq q$, that is,

$$Prob_{\pi',r}(C_{\widetilde{\Omega}}) \geq Prob_{\pi,s}(C_{\widetilde{\Omega}}).$$

The other case is similar and is omitted here.

The proof of $\sim_i \subseteq \sim_{\mathsf{PCTL}_i^{*-}}$ is by structural induction on the syntax of state formula φ and path formula ψ of PCTL_i^{*-}, that is, we need to prove the following two results simultaneously.

1. $s \sim_i r$ implies that $s \models \varphi$ iff $r \models \varphi$ for any state formula φ of PCTL_i^{*-}.
2. $\omega_1 \sim_i \omega_2$ implies that $\omega_1 \models \psi$ iff $\omega_2 \models \psi$ for any path formula ψ of PCTL_i^{*-}.

We only consider $\varphi = \mathcal{P}_{\leq q}(\psi)$ where $\psi = \psi_1 \,\mathsf{U}^{\leq i}\, \psi_2$, since other cases are similar. By induction $\widetilde{\Omega} = \{\omega \mid \omega \models \psi\}$ is $\sim_i$ closed, and also $l(\widetilde{\Omega}) = i$. We prove by contradiction, and assume that $s \models \varphi$ and $r \not\models \varphi$. According to the semantics $s \models \varphi$ iff $\forall \pi. Prob_{\pi,s}(\widetilde{\Omega}) \leq q$. If $r \not\models \varphi$, then there exists π' such that $Prob_{\pi',r}(\widetilde{\Omega}) > q$, consequently for such π' of r there does not exist π of s such that

$$Prob_{\pi,s}(\widetilde{\Omega}) \geq Prob_{\pi',r}(\widetilde{\Omega})$$

which contradicts with assumption that $s \sim_i r$, therefore $r \models \varphi$ and $s \sim_{\mathsf{PCTL}^{*-}_i} r$.

The proof of $\sim_{\mathsf{PCTL}^*} = \sim$ is straightforward by using Lemma 20 and Lemma 21. □

Recall by Lemma 20, there exists $i > 0$ such that $\sim_{\mathsf{PCTL}^*} = \sim_i$.

For the same reason as strong i-depth branching bisimulation, $\sim_i$ is not preserved by $\|$ when $i > 1$.

Counterexample 3. *$s \sim_i r$ does not imply $s \,\|\, t \sim_i r \,\|\, t$ for any t generally if $i > 1$. This can be shown by using the same arguments as in Counterexample 2.*

4.3.4 Taxonomy for Strong Bisimulations

Fig. 4.4 summaries the relationship among all these bisimulations and logical equivalences. The arrow $\rightarrow$ denotes $\subseteq$ and $\nrightarrow$ denotes $\nsubseteq$. We also abbreviate $\sim_{\mathsf{PCTL}}$ as PCTL, and it is similar for other logical equivalences. Congruent relations w.r.t. the $\|$ operator are shown in circles, and non-congruent relations are shown in boxes. Segala has considered another strong bisimulation in (1), which can be defined by replacing the $\xrightarrow{r}_{\mathsf{P}} \mu'$ with $r \rightarrow \mu'$ and thus is strictly stronger than $\sim_{\mathsf{P}}$. It is also worth mentioning that all the bisimulations shown in Fig. 4.4 coincide with the strong bisimulation defined in (54) in the DTMC setting which can be seen as a special case of PA (i.e., deterministic probabilistic automata).

4.4 Weak Bisimulations

As in (54) we use $\mathsf{PCTL}_{\setminus \mathsf{X}}$ to denote the subset of PCTL without next operator $\mathsf{X}\,\varphi$ and bounded until $\varphi_1 \,\mathsf{U}^{\leq n}\, \varphi_2$. Similarly, $\mathsf{PCTL}^*_{\setminus \mathsf{X}}$ is used to denote the subset of PCTL^* without next operator $\mathsf{X}\,\psi$. In this section we shall introduce weak bisimulations and study their relation to $\sim_{\mathsf{PCTL}_{\setminus \mathsf{X}}}$ and $\sim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}}$, respectively. Before this we should point

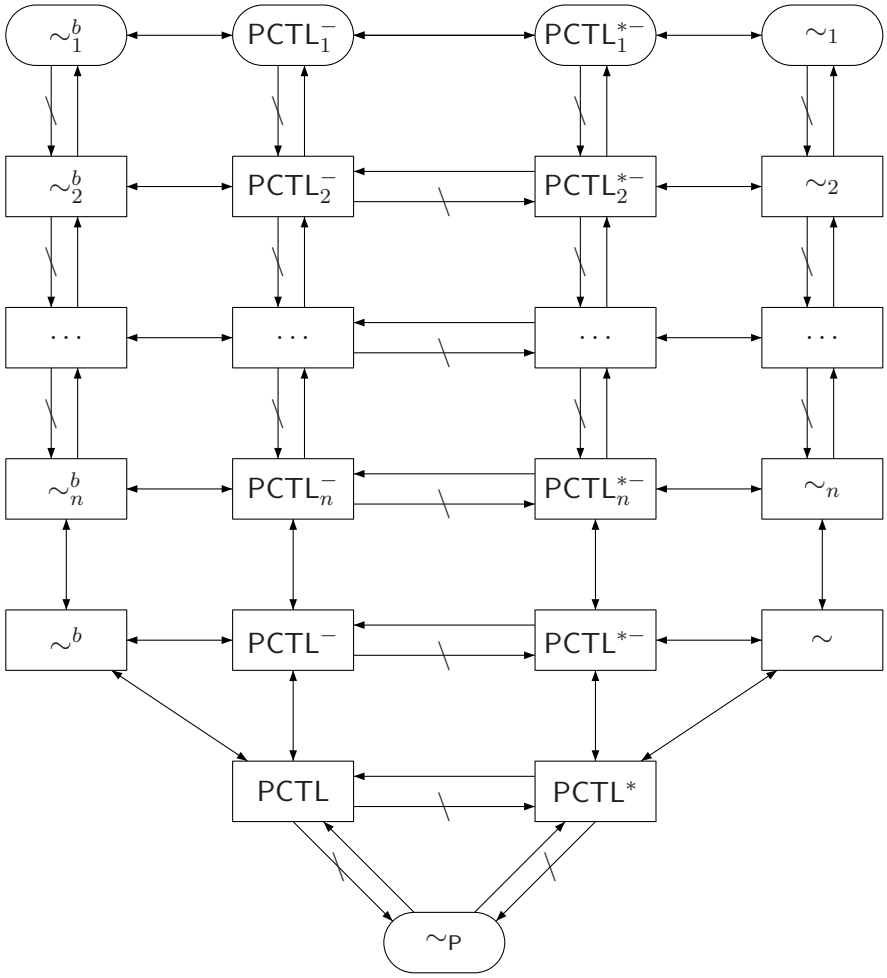

Figure 4.4: Relationship of different equivalences in strong scenario.

out that $\sim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}}$ implies $\sim_{\mathsf{PCTL}_{\setminus \mathsf{X}}}$ but the other direction does not hold. Refer to the following example.

Example 40. *Suppose s and r are given by Fig. 38 where each of s_1 and s_3 is attached with one transition respectively, that is, $s_1 \to \mu_1$ such that*

$$\mu_1(s_4) = 0.4 \text{ and } \mu_1(s_5) = 0.6,$$

$s_3 \to \mu_3$ such that

$$\mu_3(s_4) = 0.4 \text{ and } \mu_3(s_5) = 0.6.$$

In addition, s_2, s_4 and s_5 only have a transition with probability 1 to themselves, and all these states are assumed to have different atomic propositions. Then $s \sim_{\mathsf{PCTL}_{\setminus \mathsf{X}}} r$

but $s \not\sim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}} r$*, since we have a path formula*

$$\psi = ((L(s) \vee L(s_1)) \,\mathsf{U}\, L(s_5)) \vee ((L(s) \vee L(s_3)) \,\mathsf{U}\, L(s_4))$$

such that

$$s \models \mathcal{P}_{\leq 0.34}\psi \text{ but } r \not\models \mathcal{P}_{\leq 0.34}\psi,$$

since there exists a scheduler π *where the probability of path formulae satisfying* ψ *in* $Prob_{\pi,r}$ *is equal to*

$$Prob_{\pi,r}(ss_1s_5) + Prob_{\pi,r}(ss_3s_4) = 0.36.$$

Note ψ *is not a well-formed path formula of* $\mathsf{PCTL}_{\setminus \mathsf{X}}$.

4.4.1 Branching Probabilistic Bisimulation by Segala

Before introducing our weak bisimulations, we give the classical definition of branching probabilistic bisimulation proposed in (1). Given an equivalence relation $\mathcal{R}$, s can evolve into μ by a *branching transition*, written as $s \Rightarrow^{\mathcal{R}} \mu$, iff

- $\mu = \delta_s$, or
- $s \to \mu'$ and

$$\mu = \sum_{r \in (supp(\mu') \cap [s]) \wedge r \Rightarrow^{\mathcal{R}} \mu_r} \mu'(r) \cdot \mu_r + \sum_{r \in supp(\mu') \setminus [s]} \mu'(r) \cdot \delta_r$$

where $[s]$ denotes the equivalence class containing s. Stated differently, $s \Rightarrow^{\mathcal{R}} \mu$ means that s can evolve into μ only via states in $[s]$. Accordingly, *branching combined transition* $s \Rightarrow^{\mathcal{R}}_{\mathsf{P}} \mu$ can be defined based on the branching transition, i.e. $s \Rightarrow^{\mathcal{R}}_{\mathsf{P}} \mu$ iff there exists a collection of branching transitions $\{s \Rightarrow^{\mathcal{R}} \mu_i\}_{i \in I}$, and a collection of probabilities $\{p_i\}_{i \in I}$ with $\sum_{i \in I} p_i = 1$ such that $\mu = \sum_{i \in I} p_i \mu_i$.

We give the definition branching probabilistic bisimulation as follows:

Definition 28 (Branching Probabilistic Bisimulation)**.** *An equivalence relation* $\mathcal{R} \subseteq S \times S$ *is a branching probabilistic bisimulation iff* $s \,\mathcal{R}\, r$ *implies that* $L(s) = L(r)$ *and for each* $s \to \mu$*, there exists* $r \Rightarrow^{\mathcal{R}}_{\mathsf{P}} \mu'$ *such that* $\mu \,\mathcal{R}\, \mu'$.

We write $s \simeq_{\mathsf{P}} r$ *whenever there is a branching probabilistic bisimulation* $\mathcal{R}$ *such that* $s \,\mathcal{R}\, r$.

The following properties concerning branching probabilistic bisimulation are taken from (1):

Lemma 22 ((1)). *1.* $\simeq_{\mathsf{P}} \subseteq \sim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}} \subseteq \sim_{\mathsf{PCTL}_{\setminus \mathsf{X}}}$.

2. $\simeq_{\mathsf{P}}$ *is preserved by* $\|$.

4.4.2 A Novel Weak Branching Bisimulation

Similar to the definition of bounded reachability $Prob_{\pi,s}(C, C', n, \omega)$, we define the function $Prob_{\pi,s}(C, C', \omega)$ which denotes the probability from s to states in C' possibly via states in C. Again ω is used to keep track of the path which has been visited. Formally,

- if $s \in C'$, $Prob_{\pi,s}(C, C', \omega) = 1$;
- if $s \notin C$, $Prob_{\pi,s}(C, C', \omega) = 0$;
- otherwise

$$Prob_{\pi,s}(C, C', \omega) = \sum_{r \in supp(\mu')} \mu'(r) \cdot Prob_{\pi,r}(C, C', \omega r) \tag{4.3}$$

where $\pi(\omega)(s, \mu') = 1$.

The definition of weak branching bisimulation is as follows:

Definition 29 (Weak Branching Bisimulation). *A relation* $\mathcal{R} \subseteq S \times S$ *is a weak branching bisimulation if* $s \ \mathcal{R} \ r$ *implies that* $L(s) = L(r)$ *and for any* $\mathcal{R}$ *downward closed sets* C, C'

1. *for each scheduler* π*, there exists* π' *such that*

$$Prob_{\pi',r}(C, C', r) \geq Prob_{\pi,s}(C, C', s),$$

2. *for each scheduler* π*, there exists* π' *such that*

$$Prob_{\pi',s}(C, C', s) \geq Prob_{\pi,r}(C, C', r).$$

We write $s \approx^b r$ *whenever there is a weak branching bisimulation* $\mathcal{R}$ *such that* $s \ \mathcal{R} \ r$.

The following theorem shows that $\approx^{\mathrm{b}}$ is an equivalence relation. Also different from the strong cases where we use a series of equivalence relations to either characterize or approximate $\sim_{\mathsf{PCTL}}$ and $\sim_{\mathsf{PCTL}^*}$, in the weak scenario we show that $\approx^{\mathrm{b}}$ itself is enough

to characterize $\sim_{\mathsf{PCTL}_{\setminus \mathsf{X}}}$. Intuitively because in $\sim_{\mathsf{PCTL}_{\setminus \mathsf{X}}}$ only unbounded until operator is allowed in path formula which means we abstract from the number of steps to reach certain states.

Theorem 23. *1. $\approx^b$ is an equivalence relation.*

2. $\approx^b = \sim_{\mathsf{PCTL}_{\setminus \mathsf{X}}}$.

Proof. 1. The proof is similar as the proof of Clause 1 of Lemma 18.

2. In order to prove that $s \sim_{\mathsf{PCTL}_{\setminus \mathsf{X}}} r$ implies $s \approx^{\mathrm{b}} r$ for any s and r, we need to prove that

$$\mathcal{R} = \{(s, r) \mid s \sim_{\mathsf{PCTL}_{\setminus \mathsf{X}}} r\}$$

is a weak branching bisimulation. Therefore we need to show that for any $\mathcal{R}$ closed sets C, C' and any scheduler π of s, there exists a scheduler π' of r such that

$$Prob_{\pi',r}(C, C', r) \geq Prob_{\pi,s}(C, C', s)$$

and vice versa provided that $s \,\mathcal{R}\, r$. Following the way in the proof of Theorem 21, we can construct a formula φ_C such that $Sat(\varphi_C) = C$ where C is a $\mathcal{R}$ closed set. Let $\psi = \varphi_C \,\mathsf{U}\, \varphi_{C'}$, then it is not hard to see that $s \models \neg \mathcal{P}_{<q} \psi$ where $q = Prob_{\pi,s}(C, C', s)$. By assumption $r \models \neg \mathcal{P}_{<q} \psi$, so there exists a scheduler π' such that $Prob_{\pi',r}(C, C', r) \geq q$, that is,

$$Prob_{\pi',r}(C, C', r) \geq Prob_{\pi,s}(C, C', s).$$

The other case is similar and is omitted here.

The proof of $\approx^{\mathrm{b}} \subseteq \sim_{\mathsf{PCTL}_{\setminus \mathsf{X}}}$ is by structural induction on the syntax of state formula φ and path formula ψ of $\mathsf{PCTL}_{\setminus \mathsf{X}}$, that is, we need to prove the following two results simultaneously.

(a) $s \approx^{\mathrm{b}} r$ implies that $s \models \varphi$ iff $r \models \varphi$ for any state formula φ.

(b) $\omega_1 \approx^{\mathrm{b}} \omega_2$ implies that $\omega_1 \models \psi$ iff $\omega_2 \models \psi$ for any path formula ψ.

We only consider $\varphi = \mathcal{P}_{\leq q}(\psi)$ with $\psi = \varphi_1 \,\mathsf{U}\, \varphi_2$ since the other cases are similar. By induction $Sat(\varphi_1)$ and $Sat(\varphi_2)$ are $\approx^{\mathrm{b}}$ closed, moreover

$$Prob_{\pi,s}(\{\omega \mid \omega \models \psi\}) = Prob_{\pi,s}(Sat(\varphi_1), Sat(\varphi_2), s)$$

by Equation (4.3) for any π. We prove by contradiction, and assume that $s \models \varphi$ and $r \not\models \varphi$. According to the semantics,

$$s \models \varphi \text{ iff } \forall \pi. Prob_{\pi,s}(Sat(\varphi_1), Sat(\varphi_2), s) \leq q.$$

If $r \not\models \varphi$, then there exists π' of r such that

$$Prob_{\pi',r}(Sat(\varphi_1), Sat(\varphi_2), r) > q,$$

therefore for such π', there does not exist π of s such that

$$Prob_{\pi,s}(Sat(\varphi_1), Sat(\varphi_2), s) \geq Prob_{\pi',r}(Sat(\varphi_1), Sat(\varphi_2), r)$$

which contradicts with the assumption $s \approx^{\mathrm{b}} r$. As a result, it must hold that $r \models \varphi$, and $s \sim_{\mathsf{PCTL}_{\setminus \mathsf{X}}} r$.

□

As in the strong scenario, $\approx^{\mathrm{b}}$ suffers from the same problem as $\sim_i^b$ and $\sim_i$ with $i > 1$, that is, it is not preserved by $\|$.

Counterexample 4. *$s \approx^b r$ does not always imply $s \| t \approx^b r \| t$ for any t. This can be shown in a similar way as Counterexample 2 since the result will still hold even if we replace the bounded until formula with unbounded until formula in Counterexample 2.*

4.4.3 Weak Bisimulation

In order to define weak bisimulation we consider stuttering paths. Let Ω be a finite $\mathcal{R}$ downward closed path, then

$$C_{\Omega_{st}} = \begin{cases} C_\Omega & l(\Omega) = 1 \\ \bigcup\limits_{\forall 0 \leq i < n. \forall k_i \geq 0} C_{(\Omega[0])^{k_0} \ldots (\Omega[n-2])^{k_{n-2}} \Omega[n-1]} & l(\Omega) = n \geq 2 \end{cases} \tag{4.4}$$

is the set of $\mathcal{R}$ downward closed paths which contains all stuttering paths, where $\Omega[i]$ denotes the $(i+1)$-th element in Ω such that $0 \leq i < l(\Omega)$. Accordingly,

$$C_{\widetilde{\Omega}_{st}} = \bigcup_{\Omega \in \widetilde{\Omega}} C_{\Omega_{st}}$$

contains all the stuttering paths of each $\Omega \in \widetilde{\Omega}$. Given a measure $Prob$, $Prob(\widetilde{\Omega}_{st})$ can be computed by Equation (4.2).

Now we are ready to give the definition of weak bisimulation as follows:

Definition 30 (Weak Bisimulation)**.** *A relation $\mathcal{R} \subseteq S \times S$ is a weak bisimulation if $s\ \mathcal{R}\ r$ implies that $L(s) = L(r)$ and for any $\widetilde{\Omega} \subseteq (\mathcal{R}^{\downarrow})^*$*

1. *for each scheduler π, there exists π' such that*

$$Prob_{\pi',r}(C_{\widetilde{\Omega}_{st}}) \geq Prob_{\pi,s}(C_{\widetilde{\Omega}_{st}}),$$

2. *for each scheduler π, there exists π' such that*

$$Prob_{\pi',s}(C_{\widetilde{\Omega}_{st}}) \geq Prob_{\pi,r}(C_{\widetilde{\Omega}_{st}}).$$

We write $s \approx r$ whenever there is a weak bisimulation $\mathcal{R}$ such that $s\ \mathcal{R}\ r$.

The following theorem shows that $\approx$ is an equivalence relation. For the same reason as in Theorem 23, $\approx$ is enough to characterize $\sim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}}$ which gives us the following theorem.

Theorem 24. *1. $\approx$ is an equivalence relation.*

2. $\approx\ = \sim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}}$.

Proof. 1. The proof is similar with Clause 1 of Theorem 23 and is omitted here.

2. Let

$$\mathcal{R} = \{(s, r) \mid s \sim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}} r\},$$

in order to prove that $s \sim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}} r$ implies $s \approx r$ for any s and r, it is enough to show that $\mathcal{R}$ is a weak bisimulation. We need to show that for any $\widetilde{\Omega} \subseteq (\mathcal{R}^{\downarrow})^*$ and scheduler π, there exists a scheduler π' such that

$$Prob_{\pi',r}(C_{\widetilde{\Omega}_{st}}) \geq Prob_{\pi,s}(C_{\widetilde{\Omega}_{st}})$$

and vice versa provided that $s\ \mathcal{R}\ r$. Following the way in the proof of Theorem 21, we can construct a formula φ_C such that $Sat(\varphi_C) = C$ where C is a $\mathcal{R}$ closed set. Let $\psi_\Omega = \varphi_{C_0}\, \mathsf{U} \ldots \mathsf{U}\, \varphi_{C_n}$ where $\Omega = C_{C_0 \ldots C_n}$, then

$$\psi_{\widetilde{\Omega}} = \bigvee_{\Omega \in \widetilde{\Omega}} \psi_\Omega.$$

It is easy to see that $s \models \neg \mathcal{P}_{<q} \psi$ where $q = Prob_{\pi,s}(C_{\widetilde{\Omega}_{st}})$ and $\psi = \psi_{\widetilde{\Omega}}$. By assumption $r \models \neg \mathcal{P}_{<q} \psi$, so there exists a scheduler π' such that $Prob_{\pi',r}(C_{\widetilde{\Omega}_{st}}) \geq q$, that is,

$$Prob_{\pi',r}(C_{\widetilde{\Omega}_{st}}) \geq Prob_{\pi,s}(C_{\widetilde{\Omega}_{st}}).$$

The other case is similar and is omitted here.

The proof of $\approx \subseteq \sim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}}$ is by structural induction on the syntax of state formula φ and path formula ψ of $\mathsf{PCTL}^*_{\setminus \mathsf{X}}$, that is, we need to prove the following two results simultaneously.

(a) $s \approx r$ implies that $s \models \varphi$ iff $r \models \varphi$ for any state formula φ.

(b) $\omega_1 \approx \omega_2$ implies that $\omega_1 \models \psi$ iff $\omega_2 \models \psi$ for any path formula ψ.

To make the proof clearer, we rewrite the syntax of $\mathsf{PCTL}^*_{\setminus \mathsf{X}}$ as follows which is equivalent to the original definition.

$$\psi ::= \varphi \mid \psi_1 \vee \psi_2 \mid \neg\psi \mid \psi_1 \,\mathsf{U}\, \psi_2$$

We only consider $\varphi = \mathcal{P}_{\geq q}(\psi)$ here. We need to prove that for each π for each ψ, there exists $\widetilde{\Omega} \subseteq (\approx^{\downarrow})^{\infty}$ such that

$$Prob_{\pi,s}(\widetilde{\Omega}) = Prob_{\pi,s}(Sat(\psi)).$$

The proof is by structural induction on ψ as follows:

(a) $\psi = \varphi'$. By induction $Sat(\varphi')$ is $\approx$ closed. Let $\widetilde{\Omega} = \{Sat(\varphi')\}$, then

$$Prob_{\pi,s}(\widetilde{\Omega}) = Prob_{\pi,s}(Sat(\psi)).$$

(b) $\psi = \psi_1 \vee \psi_2$. By induction there exists $\widetilde{\Omega}'$ and $\widetilde{\Omega}''$ such that

$$Prob_{\pi,s}(Sat(\psi_1)) = Prob_{\pi,s}(C_{\widetilde{\Omega}'_{st}}),$$

$$Prob_{\pi,s}(Sat(\psi_2)) = Prob_{\pi,s}(C_{\widetilde{\Omega}''_{st}}).$$

It is not hard to see that $\widetilde{\Omega} = \widetilde{\Omega}' \cup \widetilde{\Omega}''$ will be enough.

(c) $\psi = \psi_1 \,\mathsf{U}\, \psi_2$. By induction there exists $\widetilde{\Omega}'$ and $\widetilde{\Omega}''$ such that

$$Prob_{\pi,s}(Sat(\psi_1)) = Prob_{\pi,s}(C_{\widetilde{\Omega}'_{st}}),$$

$$Prob_{\pi,s}(Sat(\psi_2)) = Prob_{\pi,s}(C_{\widetilde{\Omega}''_{st}}).$$

Let

$$\widetilde{\Omega} = \{\Omega'\Omega'' \mid \Omega' \in \widetilde{\Omega}' \wedge \Omega'' \in \widetilde{\Omega}''\},$$

then

$$Prob_{\pi,s}(\widetilde{\Omega}) = Prob_{\pi,s}(Sat(\psi)).$$

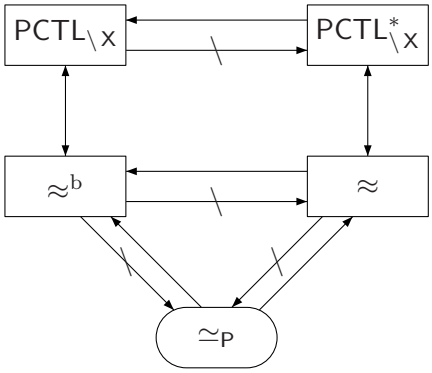

Figure 4.5: Relationship of different equivalences in weak scenario.

(d) $\psi = \neg\psi'$. $s \models \mathcal{P}_{\geq q}(\psi)$ iff $s \models \mathcal{P}_{<1-q}(\psi')$, so ψ can be reduced to another formula without $\neg$ operator.

The following proof is routine and is omitted here.

□

Not surprisingly $\approx$ is not preserved by $\|$.

Counterexample 5. *$s \approx r$ does not always imply $s \| t \approx r \| t$ for any t. This can be shown by using the same arguments as in Counterexample 4.*

4.4.4 Taxonomy for Weak Bisimulations

As in the strong cases we summarize the relation of the equivalences in the weak scenario in Fig. 4.5 where all the denotations have the same meaning as Fig. 4.4. Compared to Fig. 4.4, Fig. 4.5 is much simpler because the step-indexed bisimulations are absent. As in strong cases, here we do not consider the standard definition of branching bisimulation which is a strict subset of $\simeq_P$ and can be defined by replacing $\Rightarrow_P^{\mathcal{R}}$ with $\Rightarrow^{\mathcal{R}}$ in Definition 28. Again not surprisingly all the relations shown in Fig. 4.5 coincide with the weak bisimulation defined in (54) in the DTMC setting.

4.5 Simulations

In Section 4.3 and 4.4 we discuss bisimulations and their characterizations. Usually two states s and r are bisimilar iff s can mimic stepwise all the transitions of r and vice versa.

In this section we relax the conditions of bisimulations, and only requires one direction mimicking, which introduces us the definitions of simulations. Simulations are preorders on the states, which has been used widely for verification purpose (1, 8, 54, 70, 71). Intuitively, if r simulates s, then r can be seen as a correct implementation of s. Since s is more abstract and contains less details, it is much easier to be analyzed. We also discuss the characterization of simulations w.r.t. the safe fragments of PCTL and PCTL*. First let us introduce the safe fragment of PCTL*, denoted by PCTL$^*_{safe}$, which is a fragment of PCTL* without negative operators except for the atomic propositions, and is defined by the following syntax:

$$\varphi ::= a \mid \neg a \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \vee \varphi_2 \mid \mathcal{P}_{\leq q}(\psi)$$
$$\psi ::= \varphi \mid \psi_1 \wedge \psi_2 \mid \psi_1 \vee \psi_2 \mid \mathsf{X}\,\psi \mid \psi_1 \,\mathsf{U}\, \psi_2$$

where $a \in AP$ and $q \in [0,1]$. Accordingly the safe fragment of PCTL, denoted by PCTL$_{safe}$, is a sub logic of PCTL$^*_{safe}$ where only the path formula is constrained to be the following form:

$$\psi ::= \mathsf{X}\,\varphi \mid \varphi_1 \,\mathsf{U}\, \varphi_2 \mid \varphi_1 \,\mathsf{U}^{\leq n}\, \varphi_2.$$

We write $s \prec_{\mathsf{PCTL}^*_{safe}} r$ iff $r \models \varphi$ implies that $s \models \varphi$ for any φ of PCTL$^*_{safe}$, and similarly for other sublogics.

We first recall the definition of *weight function* defined in Definition 7.

Definition 31 (Weight Function)**.** *Let $\mathcal{R} = S \times S$ be a relation over S. A weight function for μ and ν w.r.t. $\mathcal{R}$ is a function $\Delta : S \times S \mapsto [0,1]$ such that:*

- *$\Delta(s,r) > 0$ implies that $s\ \mathcal{R}\ r$,*
- *$\mu(s) = \sum_{r \in S} \Delta(s,r)$ for any $s \in S$,*
- *$\nu(r) = \sum_{s \in S} \Delta(s,r)$ for any $r \in S$.*

We write $\mu \sqsubseteq_{\mathcal{R}} \nu$ iff there exists a weight function for μ and ν w.r.t. $\mathcal{R}$.

Below follows the definition of strong probabilistic simulation.

Definition 32 (Strong Probabilistic Simulation)**.** *A relation $\mathcal{R} \subseteq S \times S$ is a strong probabilistic simulation iff $s\ \mathcal{R}\ r$ implies that $L(s) = L(r)$ and for each $s \to \mu$, there exists a combined transition $\stackrel{r}{\to}_{\mathsf{P}} \mu'$ such that $\mu \sqsubseteq_{\mathcal{R}} \mu'$.*

We write $s \prec_{\mathsf{P}} r$ whenever there is a strong probabilistic simulation $\mathcal{R}$ such that $s\ \mathcal{R}\ r$.

It was shown in (1) that $\sqsubseteq_{\mathcal{R}}$ is congruent, i.e. $s \prec_{\mathsf{P}} r$ implies that $s \parallel t \prec_{\mathsf{P}} r \parallel t$ for any t. But not surprisingly, it turns out that the strong probability simulation is too fine w.r.t $\prec_{\mathsf{PCTL}_{safe}}$ and $\prec_{\mathsf{PCTL}^*_{safe}}$ which can be seen from Example 38. Similarly we have the correspondent theorem of Theorem 19 in the simulation scenario where we only consider the safe fragment of the logics, thus the subscription s is often omitted for readability.

Theorem 25. *1.* $\prec_{\mathsf{PCTL}}$, $\prec_{\mathsf{PCTL}^*}$, $\prec_{\mathsf{PCTL}^-}$, $\prec_{\mathsf{PCTL}^-_i}$, $\prec_{\mathsf{PCTL}^{*-}}$, $\prec_{\mathsf{PCTL}^{*-}_i}$, *and* $\prec_{\mathsf{P}}$ *are preorders for any* $i \geq 1$.

2. $\prec_{\mathsf{P}} \subseteq \prec_{\mathsf{PCTL}^*} \subseteq \prec_{\mathsf{PCTL}}$.

3. $\prec_{\mathsf{PCTL}^{*-}} \subseteq \prec_{\mathsf{PCTL}^-}$.

4. $\prec_{\mathsf{PCTL}^{*-}_1} = \prec_{\mathsf{PCTL}^-_1}$.

5. $\prec_{\mathsf{PCTL}^{*-}_i} \subseteq \prec_{\mathsf{PCTL}^-_i}$ *for any* $i > 1$.

6. $\prec_{\mathsf{PCTL}} \subseteq \prec_{\mathsf{PCTL}^-} \subseteq \prec_{\mathsf{PCTL}^-_{i+1}} \subseteq \prec_{\mathsf{PCTL}^-_i}$ *for all* $i \geq 0$.

7. $\prec_{\mathsf{PCTL}^*} \subseteq \prec_{\mathsf{PCTL}^{*-}} \subseteq \prec_{\mathsf{PCTL}^{*-}_{i+1}} \subseteq \prec_{\mathsf{PCTL}^{*-}_i}$ *for all* $i \geq 0$.

Proof. For Clause (1) we only prove that $\prec_{\mathsf{PCTL}}$ is a preorder since the others are similar. The reflexivity is trivial as $s \prec_{\mathsf{PCTL}} s$ for any s. Suppose that $s \prec_{\mathsf{PCTL}} t$ and $t \prec_{\mathsf{PCTL}} r$, then we need to prove that $s \prec_{\mathsf{PCTL}} r$ in order to the transitivity. According to the definition of $\prec_{\mathsf{PCTL}}$, we need to prove that $r \models \varphi$ implies $s \models \varphi$ for any φ. Suppose that $r \models \varphi$ for some φ, then $t \models \varphi$ because of $t \prec_{\mathsf{PCTL}} r$, moreover since $s \prec_{\mathsf{PCTL}} t$, hence $s \models \varphi$ which completes the proof.

The proof of Clause (2) can be found in (1). Since we have shown in Theorem 19 that PCTL^-_1 and PCTL^{*-}_1 have the same expressiveness, thus the proof of Clause (4) is straightforward. The proofs of all the other clauses are trivial. □

4.5.1 Strong i-depth Branching Simulation

Following Section 4.3.2 we can define strong i-depth branching simulation which can be characterized by $\prec_{\mathsf{PCTL}^-_i}$. Let $s \prec^{\mathrm{b}}_0 r$ iff $L(s) = L(r)$, then

Definition 33 (Strong i-depth Branching Simulation)**.** *A relation* $\mathcal{R} \subseteq S \times S$ *is a strong* i*-depth branching simulation with* $i \geq 1$ *iff* $s \mathcal{R} r$ *implies that* $s \prec^{b}_{i-1} r$ *and for any* $\mathcal{R}$ *downward closed sets* C, C'*, and any scheduler* π*, there exists* π' *such that*

$$Prob_{\pi',r}(C, C', i) \geq Prob_{\pi,s}(C, C', i).$$

We write $s \prec_i^b r$ *whenever there is a strong* i*-depth branching simulation* $\mathcal{R}$ *such that* $s \mathcal{R} r$*. The strong branching simulation* $\prec^b$ *is defined as*

$$\prec^b = \bigcap_{i \geq 0} \prec_i^b .$$

Below we show the similar properties of strong i-depth branching simulations.

Lemma 23. *1.* $\prec^b$ *and* $\prec_i^b$ *are preorders for any* $i \geq 0$*.*

2. $\prec_j^b \subseteq \prec_i^b$ *provided that* $0 \leq i \leq j$*.*

3. There exists $i \geq 0$ *such that* $\prec_j^b = \prec_k^b$ *for any* $j, k \geq i$*.*

Proof. 1. The reflexivity is trivial, we only prove the transitivity. Suppose that $s_1 \prec_i^b s_2$ and $s_2 \prec_i^b s_3$, we need to prove that $s_1 \prec_i^b s_3$. By Definition 33 there exists strong simulation $\mathcal{R}_1$ and $\mathcal{R}_2$ such that $s_1 \mathcal{R}_1 s_2$ and $s_2 \mathcal{R}_2 s_3$. Let

$$\mathcal{R} = \mathcal{R}_1 \circ \mathcal{R}_2 = \{(s_1, s_3) \mid \exists s_2.(s_1 \mathcal{R}_1 s_2 \wedge s_2 \mathcal{R}_2 s_3)\},$$

it is enough to prove that $\mathcal{R}$ is strong i-depth branching simulation. Due to the reflexivity, any $\mathcal{R}$ downward closed set C is also $\mathcal{R}_1$ and $\mathcal{R}_2$ downward closed. Therefore for any $\mathcal{R}$ downward closed sets C, C' and any scheduler π, then there exists π' such that

$$Prob_{\pi', s_2}(C, C', i) \geq Prob_{\pi, s_1}(C, C', i)$$

according to Definition 33. Similarly, there exists π'' such that

$$Prob_{\pi'', s_3}(C, C', i) \geq Prob_{\pi', s_2}(C, C', i) \geq Prob_{\pi, s_1}(C, C', i),$$

and $\mathcal{R}$ is indeed a strong i-depth branching simulation. This completes the proof.

2. It is straightforward from Definition 33.

3. Since there are only finite states, thus only finite equivalence classes, such i always exists.

□

Our strong i-depth branching simulation coincides with $\prec_{\mathsf{PCTL}_i^-}$ for each i, therefore $\prec_{\mathsf{PCTL}}$ is equivalent to $\prec^b$ as shown by the following theorem.

Theorem 26. $\prec_{\mathsf{PCTL}_i^-} = \prec_i^b$ *for any* $i \geq 1$*, and moreover* $\prec_{\mathsf{PCTL}} = \prec^b$*.*

Proof. We first prove that $\prec_{\mathsf{PCTL}_i^-}$ implies $\prec_i^{\mathrm{b}}$. Let

$$\mathcal{R} = \{(s, r) \mid s \prec_{\mathsf{PCTL}_i^-} r\},$$

it is enough to prove that $\mathcal{R}$ is a strong i-depth branching simulation. Suppose that $s \mathcal{R} r$, we need to prove that for any $\mathcal{R}$ downward closed sets C, C' and any scheduler π of s, there exists π' of r such that

$$Prob_{\pi',r}(C, C', i) \geq Prob_{\pi,s}(C, C', i).$$

Note that $Sat(\varphi)$ is a $\mathcal{R}$ downward closed set for any φ. Since the states space is finite, for each $\mathcal{R}$ downward closed set C, there exists φ_C such that $Sat(\varphi_C) = C$. Assume that there exists $\mathcal{R}$ downward closed sets C, C' and π such that

$$Prob_{\pi',r}(C, C', i) < Prob_{\pi,s}(C, C', i)$$

for all schedulers π' of r. Then there exists q such that

$$r \models \mathcal{P}_{\leq q}(\psi) \text{ but } s \not\models \mathcal{P}_{\leq q}(\psi)$$

where $\psi = \varphi_C \,\mathsf{U}^{\leq i}\, \varphi_{C'}$, this contradicts with the assumption that $s \prec_{\mathsf{PCTL}_i^-} r$. Therefore $\mathcal{R}$ is a strong i-depth branching bisimulation.

In order to prove that $\prec_i^{\mathrm{b}}$ implies $\prec_{\mathsf{PCTL}_i^-}$, we need to prove that whenever $s \prec_i^{\mathrm{b}} r$ and $r \models \varphi$, we also have $s \models \varphi$. We prove by structural induction on φ, and only consider the case when $\varphi = \mathcal{P}_{\leq q}(\varphi_1 \,\mathsf{U}^{\leq i}\, \varphi_2)$ since all the others are trivial. By induction $Sat(\varphi_1)$ and $Sat(\varphi_2)$ are $\prec_i^{\mathrm{b}}$ downward closed, therefore if

$$r \models \mathcal{P}_{\leq q}(\varphi_1 \,\mathsf{U}^{\leq i}\, \varphi_2) \text{ but } s \not\models \mathcal{P}_{\leq q}(\varphi_1 \,\mathsf{U}^{\leq i}\, \varphi_2),$$

then there exists π of s such that there does not exist π' such that

$$Prob_{\pi',r}(Sat(\varphi_1), Sat(\varphi_2), i) \geq Prob_{\pi,s}(Sat(\varphi_1), Sat(\varphi_2), i)$$

which contradicts with the assumption that $s \prec_i^{\mathrm{b}} r$. □

In Counterexample 2 we have shown the $\sim_i^b$ is not compositional for $i > 1$, using the same arguments we can show that $\prec_i^{\mathrm{b}}$ is not compositional either for $i > 1$, thus we have

Theorem 27. *$s \prec_1^b r$ implies that $s \parallel t \prec_1^b r \parallel t$ for any t, while $\prec_i^b$ with $i > 1$ is not compositional in general.*

Proof. Let

$$\mathcal{R} = \{(s \parallel t, r \parallel t) \mid s \prec_1^{\mathrm{b}} r\},$$

it is enough to show that $\mathcal{R}$ is a strong 1-depth simulation. Let C, C' be two $\mathcal{R}$ downward closed sets, there are several cases we need to consider:

1. If $s \parallel t \notin C$, then $Prob_{\pi, s\parallel t}(C, C', 1) = 0$. Since C is $\mathcal{R}$ downward closed, $r \parallel t \notin C$ by induction, thus there exists π' such that

$$Prob_{\pi', r\parallel t}(C, C', 1) \geq Prob_{\pi, s\parallel t}(C, C', 1).$$

2. If $s \parallel t \in C$, and for each scheduler π, there exists $s \parallel t \to \mu$ such that $\mu(C') = Prob_{\pi, s\parallel t}(C, C', 1)$. According to Definition 22, $s \parallel t \to \mu$ iff either $s \to \mu_s$ such that $\mu_s \parallel \delta_t = \mu$, or $t \to \mu_t$ such that $\delta_s \parallel \mu_t = \mu$. We only consider the first case, since the other one is similar. Since $\mu_s \parallel \delta_t = \mu$, there exists $\mathcal{R}$ downward closed set C'' such that $\mu_s(C'') = \mu(C')$. The following proof is then straightforward.

Note that Counterexample 2 also applies here, thus $\prec_i^{\mathrm{b}}$ is not compositional when $i > 1$. □

Remark 2. *The safe fragment of* PCTL *we adopt in this chapter is slightly different from (54) where two new operators* $\widetilde{\mathsf{X}}$ *and* $\widetilde{\mathsf{U}}$ *are introduced, called weak next and until respectively, and the* $\mathcal{P}_{\leq q}(\psi)$ *is replaced by* $\mathcal{P}_{\geq q}(\psi)$*. The semantics of* $\widetilde{\mathsf{X}}$ *and* $\widetilde{\mathsf{U}}$ *are defined as follows where* $|\omega|$ *denotes the length of* ω*:*

$$\omega \models \widetilde{\mathsf{X}}\varphi \text{ iff } (|\omega| < 1 \vee \omega[i] \models \varphi)$$
$$\omega \models \varphi_1 \widetilde{\mathsf{U}} \varphi_2 \text{ iff } (\omega \models \varphi_1 \,\mathsf{U}\, \varphi_2 \vee \forall i \leq |\omega| \ .\omega[i] \models \varphi_1)$$

Similarly we can also define the weak counterpart of bounded until $\widetilde{\mathsf{U}}^{\leq n}$*. Due to duality between* X, $\mathsf{U}^{\leq n}$, U *and their weak counterparts, these two variants of safe* PCTL *are essentially equivalent, refer to (54) for detail discussion.*

Let PCTL_{live} *denote the liveness fragment of* PCTL *in (54) which is the same as* PCTL_{safe} *except that* $\mathcal{P}_{\leq q}(\psi)$ *is replaced with* $\mathcal{P}_{\geq q}(\psi)$*. We say* $s \prec_{\mathsf{PCTL}_{live}} r$ *iff* $s \models \varphi$ *implies* $r \models \varphi$ *for any state formula of* PCTL_{live}*. Even though it has been shown in (54) that* $\prec_{\mathsf{PCTL}_{safe}}$ *and* $\prec_{\mathsf{PCTL}_{live}}$ *are equivalent for* DTMC*, the result is not true for* PA*. Refer to the following example.*

Example 41. *Consider the two states* s_0 *and* r_0 *shown in Fig. 4.6, where we assume that all the states have different labels except that* $L(s_0) = L(r_0)$*. It is easy to check that* $s_0 \prec_{\mathsf{P}} r_0$*, thus* $s_0 \prec_{\mathsf{PCTL}_{safe}} r_0$ *according to Clause 2 of Theorem 25, but we*

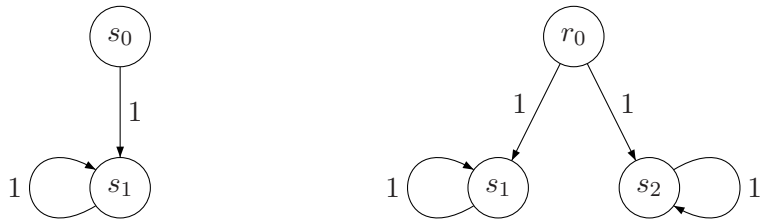

Figure 4.6: $s_0 \not\preceq_{\mathsf{PCTL}_{live}} r_0$.

have $s_0 \not\preceq_{\mathsf{PCTL}_{live}} r_0$. *Let* $\varphi = \mathcal{P}_{\geq 1}(L(s_0) \,\mathsf{U}\, L(s_1))$ *which is a valid state formula of* PCTL_{live}, *it is obvious that* $s_0 \models \varphi$, *but* $r_0 \not\models \varphi$ *since the minimal probability of* r_0 *reaching state* s_1 *is equal to 0 i.e. by choosing the transition to* s_2.

4.5.2 Strong i-depth Simulation

In this section we introduce strong i-depth simulation which can be characterized by $\preceq_{\mathsf{PCTL}_i^{*-}}$. Below follows the definition of strong i-depth simulation where $\preceq_0 = \preceq_0^{\mathrm{b}}$.

Definition 34 (Strong i-depth Simulation)**.** *A relation* $\mathcal{R} \subseteq S \times S$ *is a strong* i*-depth simulation with* $i \geq 1$ *iff* $s \;\mathcal{R}\; r$ *implies that* $s \preceq_{i-1} r$ *and for any* $\widetilde{\Omega} \subseteq (\mathcal{R}^{\downarrow})^*$ *with* $l(\widetilde{\Omega}) = i$ *and any scheduler* π, *there exists* π' *such that*

$$Prob_{\pi',r}(C_{\widetilde{\Omega}}) \geq Prob_{\pi,s}(C_{\widetilde{\Omega}}).$$

We write $s \preceq_i r$ *whenever there is a* i*-depth strong simulation* $\mathcal{R}$ *such that* $s \;\mathcal{R}\; r$. *The strong simulation* $\preceq$ *is defined as*

$$\preceq \;=\; \bigcap_{i \geq 0} \preceq_i .$$

Below we show the similar properties of strong i-depth simulations.

Lemma 24. *1.* $\preceq$ *and* $\preceq_i$ *are preorders for any* $i \geq 0$.

2. $\preceq_j \subseteq \preceq_i$ *provided that* $0 \leq i \leq j$.

3. There exists $i \geq 0$ *such that* $\preceq_j = \preceq_k$ *for any* $j, k \geq i$.

Proof. 1. This clause can be proved in a similar way as Clause (1) of Lemma 23.

2. According to Definition 34, as i is growing, $\preceq_i$ is getting finer.

3. The proof is based on the fact that the states are finitely many, with the similar argument as in Clause (3) of Lemma 23.

□

Our strong i-depth simulation coincides with $\prec_{\mathsf{PCTL}_i^{*-}}$ for each i, therefore $\prec_{\mathsf{PCTL}^*}$ is equivalent to $\prec$ as shown by the following theorem.

Theorem 28. *$\prec_{\mathsf{PCTL}_i^{*-}} = \prec_i$ for any $i \geq 1$, and moreover $\prec_{\mathsf{PCTL}^*} = \prec$.*

Proof. We first prove that $s \prec_{\mathsf{PCTL}_i^{*-}} r$ implies $s \prec_i r$ for any s and r. Let

$$\mathcal{R} = \{(s,r) \mid s \prec_{\mathsf{PCTL}_i^{*-}} r\},$$

we need to show that for any $\widetilde{\Omega} \subseteq (\mathcal{R}^{\downarrow})^*$ with $l(\widetilde{\Omega}) \leq i$ and scheduler π, there exists a scheduler π' such that

$$Prob_{\pi',r}(C_{\widetilde{\Omega}}) \geq Prob_{\pi,s}(C_{\widetilde{\Omega}})$$

whenever $s \,\mathcal{R}\, r$. By induction, there exists a formula φ_C such that $Sat(\varphi_C) = C$ where C is $\mathcal{R}$ downward closed set. Suppose $\Omega = C_0 C_1 \ldots C_j$ with $j \leq i$, then

$$\psi_\Omega = \varphi_{C_0} \wedge \mathsf{X}(\varphi_{C_1} \wedge \ldots \wedge \mathsf{X}(\varphi_{C_{j-1}} \wedge \mathsf{X}\,\varphi_{C_j}))$$

can be used to characterize Ω, that is, $Sat(\psi_\Omega) = C_\Omega$. Let $\psi = \bigvee_{\Omega \in \widetilde{\Omega}} \psi_\Omega$, then $Sat(\psi) = C_{\widetilde{\Omega}}$. We prove by contradiction. Suppose that there does not exist π' such that

$$Prob_{\pi',r}(C_{\widetilde{\Omega}}) \geq Prob_{\pi,s}(C_{\widetilde{\Omega}}),$$

then there exists q such that $r \models \mathcal{P}_{\leq q}\psi$, but $s \not\models \mathcal{P}_{\leq q}\psi$ which contradicts with the assumption that $s \prec_{\mathsf{PCTL}_i^{*-}} r$, so there exists a scheduler π' such that

$$Prob_{\pi',r}(C_{\widetilde{\Omega}}) \geq q = Prob_{\pi,s}(C_{\widetilde{\Omega}}).$$

The other case is similar and is omitted here.

The proof of $\prec_i \subseteq \prec_{\mathsf{PCTL}_i^{*-}}$ is by structural induction on the syntax of state formula φ and path formula ψ of safe PCTL_i^{*-}, that is, we need to prove the following two results simultaneously.

1. $r \models \varphi$ implies $s \models \varphi$ for any state formula φ provided that $s \prec_i r$.
2. $\omega_2 \models \psi$ implies $\omega_1 \models \psi$ for any path formula ψ provided that $\omega_1 \prec_i \omega_2$.

We only consider $\varphi = \mathcal{P}_{\leq q}(\psi)$ here. Suppose that $r \models \varphi$, i.e.

$$\forall \pi. Prob_{\pi,r}(\{\omega \mid \omega \models \psi\}) \leq q,$$

we need to show that $s \models \varphi$. We prove by contradiction, and assume that $s \not\models \varphi$, i.e. there exists π such that

$$Prob_{\pi,s}(\{\omega \mid \omega \models \psi\}) > q.$$

By induction $\{\omega \mid \omega \models \psi\}$ is $\prec_i$ downward closed, that is, there exists $\widetilde{\Omega} = \{\omega \mid \omega \models \psi\}$, and moreover $l(\widetilde{\Omega}) \leq i$ since the depth of ψ is at most i. Since $r \models \varphi$, there does not exists π' such that

$$Prob_{\pi',r}(C_{\widetilde{\Omega}}) \geq Prob_{\pi,s}(C_{\widetilde{\Omega}}) = q,$$

which contradicts the assumption that $s \prec_i r$, thus it holds that $s \models \varphi$. □

Similarly, we can show that $\prec_i$ is not compositional either for $i > 1$, thus we have

Theorem 29. *$s \prec_1 r$ implies that $s \parallel t \prec_1 r \parallel t$ for any t, while $\prec_i$ with $i > 1$ is not compositional in general.*

Proof. According to Theorem 26 and 28, and Clause (4) of Theorem 25, $\prec_1^{\mathrm{b}} = \prec_1$, thus the result is straightforward according to Theorem 27. □

4.5.3 Weak Simulations

Given the results for weak bisimulations from Section 4.4, the characterization of weak simulations is straightforward. Let us first introduce the definition of branching probabilistic simulation by Segala as follows:

Definition 35 (Branching Probabilistic Simulation)**.** *A relation $\mathcal{R} \subseteq S \times S$ is a branching probabilistic simulation iff $s\ \mathcal{R}\ r$ implies that $L(s) = L(r)$ and for each $s \to \mu$, there exists $r \Rightarrow_{\mathsf{P}}^{\mathcal{R}} \mu'$ such that $\mu\ \mathcal{R}\ \mu'$.*

We write $s \preceq_{\mathsf{P}} r$ whenever there is a branching probabilistic simulation $\mathcal{R}$ such that $s\ \mathcal{R}\ r$.

From (1) we know that $\preceq_{\mathsf{P}}$ is compositional, but it is too fine for $\precsim_{\mathsf{PCTL}_{\setminus \mathsf{X}}}$ as well as $\precsim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}}$, therefore along the line of weak bisimulations, we come out similar results for weak simulations. Below follows the definition of weak branching simulation.

Definition 36 (Weak Branching Simulation)**.** *A relation $\mathcal{R} \subseteq S \times S$ is a weak branching simulation iff $s\ \mathcal{R}\ r$ implies that $L(s) = L(r)$ and for any $\mathcal{R}$ downward closed sets C, C' and any scheduler π, there exists π' such that*

$$Prob_{\pi',r}(C, C', r) \geq Prob_{\pi,s}(C, C', s).$$

We write $s \precsim^b r$ whenever there is a weak branching simulation $\mathcal{R}$ such that $s\ \mathcal{R}\ r$.

Due to Counterexample 4, $\precsim^{\mathrm{b}}$ is not compositional, but it coincides with $\precsim_{\mathsf{PCTL}_{\setminus \mathsf{X}}}$ as shown by the following theorem.

Theorem 30. *$\precsim^b$ is a preorder, and $\precsim^b = \precsim_{\mathsf{PCTL}_{\setminus \mathsf{X}}}$.*

Proof. 1. The reflexibility of $\precsim^{\mathrm{b}}$ is trivial. We only prove the transitivity of $\precsim^{\mathrm{b}}$. Suppose that $s \precsim^{\mathrm{b}} r$ and $r \precsim^{\mathrm{b}} t$, then for any $\precsim^{\mathrm{b}}$ downward closed sets C, C' and scheduler π, there exists π' such that

$$Prob_{\pi',r}(C, C', r) \geq Prob_{\pi,s}(C, C', s).$$

Since we also have $r \precsim^{\mathrm{b}} t$, so there exists π'' such that

$$Prob_{\pi'',t}(C, C', t) \geq Prob_{\pi',r}(C, C', r) \geq Prob_{\pi,s}(C, C', s).$$

This proves the transitivity of $\precsim^{\mathrm{b}}$.

2. In order to prove that $s \precsim_{\mathsf{PCTL}_{\setminus \mathsf{X}}} r$ implies $s \precsim^{\mathrm{b}} r$ for any s and r, it is enough to show that

$$\mathcal{R} = \{(s, r) \mid s \precsim_{\mathsf{PCTL}_{\setminus \mathsf{X}}} r\}$$

is a weak branching simulation i.e. we need to prove that for any $\mathcal{R}$ downward closed sets C, C' and scheduler π, there exists a scheduler π' such that

$$Prob_{\pi',r}(C, C', r) \geq Prob_{\pi,s}(C, C', s)$$

provided that $s\ \mathcal{R}\ r$. Let φ_C be a formula such that $Sat(\varphi_C) = C$ where C is a $\mathcal{R}$ downward closed set. We prove by contradiction. Suppose that there does not exist π' such that

$$Prob_{\pi',r}(C, C', r) \geq Prob_{\pi,s}(C, C', s),$$

then there exists q such that $r \models \mathcal{P}_{\leq q}\psi$ where $\psi = \varphi_C \,\mathsf{U}\, \varphi_{C'}$, but $s \not\models \mathcal{P}_{\leq q}\psi$, which contradicts with the assumption that $s \precsim_{\mathsf{PCTL}_{\setminus \mathsf{X}}} r$. Therefore there must exist a scheduler π' such that

$$Prob_{\pi',r}(C, C', r) \geq Prob_{\pi,s}(C, C', s).$$

The other case is similar and is omitted here.

The proof of $\precsim^{\mathrm{b}} \subseteq \precsim_{\mathsf{PCTL}_{\setminus \mathsf{X}}}$ is by structural induction on the syntax of state formula φ and path formula ψ of safe $\mathsf{PCTL}_{\setminus \mathsf{X}}$, that is, we need to prove the following two results simultaneously.

(a) $r \models \varphi$ implies $s \models \varphi$ for any state formula φ provided that $s \precsim^{\mathrm{b}} r$.

(b) $\omega_2 \models \psi$ implies that $\omega_1 \models \psi$ for any path formula ψ provided that $\omega_1 \precsim^{\mathrm{b}} \omega_2$.

We only consider $\varphi = \mathcal{P}_{\leq q}(\psi)$ where $\psi = \varphi_1 \,\mathsf{U}\, \varphi_2$ since the other cases are similar. Suppose that $r \models \varphi$, we need to prove that $s \models \varphi$. We prove by contradiction, and assume that $s \not\models \varphi$, then there exists π such that

$$Prob_{\pi,s}(\{\omega \mid \omega \models \psi\}) > q.$$

By induction $Sat(\varphi_1)$ and $Sat(\varphi_2)$ are $\precsim^{\mathrm{b}}$ downward closed, thus

$$Prob_{\pi,s}(Sat(\varphi_1), Sat(\varphi_2), s) = Prob_{\pi,s}(\{\omega \mid \omega \models \psi\}) > q.$$

Since $r \models \varphi$, there does not exist π' such that

$$Prob_{\pi,r}(Sat(\varphi_1), Sat(\varphi_2), r) \geq Prob_{\pi,s}(Sat(\varphi_1), Sat(\varphi_2), s)$$

which contradicts with the assumption that $s \precsim^{\mathrm{b}} r$, thus $s \models \varphi$, and $s \precsim_{\mathsf{PCTL}_{\setminus \mathsf{X}}} r$. □

The weak simulation equivalent to $\precsim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}}$ can also be obtained in a straightforward way by adapting Definition 30.

Definition 37 (Weak Simulation)**.** *A relation $\mathcal{R} \subseteq S \times S$ is a weak simulation iff $s \,\mathcal{R}\, r$ implies that $L(s) = L(r)$ and for any $\widetilde{\Omega} \subseteq (\mathcal{R}^{\downarrow})^*$ and any scheduler π, there exists π' such that*

$$Prob_{\pi',r}(C_{\widetilde{\Omega}_{st}}) \geq Prob_{\pi,s}(C_{\widetilde{\Omega}_{st}}).$$

We write $s \precsim r$ whenever there is a weak simulation $\mathcal{R}$ such that $s \,\mathcal{R}\, r$.

Again $\precsim$ is not compositional, but it coincides with $\precsim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}}$, therefore we have the following theorem.

Theorem 31. *$\precsim$ is a preorder, and $\precsim = \precsim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}}$.*

Proof. 1. The proof is similar as the proof of Clause 1 of Lemma 23.

2. In order to prove that $\precsim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}} \subseteq \precsim$, it is enough to show that

$$\mathcal{R} = \{(s,r) \mid s \precsim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}} r\}$$

is a weak branching simulation i.e. we need to prove that for any $\widetilde{\Omega} \subseteq (\mathcal{R}^{\downarrow})^*$ and scheduler π, there exists a scheduler π' such that

$$Prob_{\pi',r}(C_{\widetilde{\Omega}_{st}}) \geq Prob_{\pi,s}(C_{\widetilde{\Omega}_{st}})$$

provided that $s \mathcal{R} r$. By induction $C_{\widetilde{\Omega}_{st}}$ is $\mathcal{R}$ downward closed, thus there exists ψ such that $Sat(\psi) = C_{\widetilde{\Omega}_{st}}$. We prove by contradiction. Suppose that there does not exist π' such that

$$Prob_{\pi',r}(C_{\widetilde{\Omega}_{st}}) \geq Prob_{\pi,s}(C_{\widetilde{\Omega}_{st}}),$$

then there exists q such that $r \models \mathcal{P}_{\leq q}(\psi)$, but apparently $s \not\models \mathcal{P}_{\leq q}\psi$, which contradicts with the assumption that $s \precsim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}} r$. Therefore there must exist a scheduler π' such that

$$Prob_{\pi',r}(C_{\widetilde{\Omega}_{st}}) \geq Prob_{\pi,s}(C_{\widetilde{\Omega}_{st}}).$$

The proof of $\precsim \subseteq \precsim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}}$ is by structural induction on the syntax of state formula φ and path formula ψ of safe $\mathsf{PCTL}^*_{\setminus \mathsf{X}}$, that is, we need to prove the following two results simultaneously.

(a) $r \models \varphi$ implies $s \models \varphi$ for any state formula φ provided that $s \precsim r$.

(b) $\omega_2 \models \psi$ implies that $\omega_1 \models \psi$ for any path formula ψ provided that $\omega_1 \precsim \omega_2$.

We only consider $\varphi = \mathcal{P}_{\leq q}(\psi)$ since the other cases are similar. Suppose that $r \models \varphi$, we need to prove that $s \models \varphi$. We prove by contradiction, and assume that $s \not\models \varphi$, then there exists π such that

$$Prob_{\pi,s}(\{\omega \mid \omega \models \psi\}) > q.$$

By induction $\{\omega \mid \omega \models \psi\}$ is $\precsim$ downward closed, thus there exists $\widetilde{\Omega}_{st}$ such that $\widetilde{\Omega}_{st} = \{\omega \mid \omega \models \psi\}$. Since $r \models \varphi$, there does not exist π' such that

$$Prob_{\pi,r}(\widetilde{\Omega}_{st}) \geq Prob_{\pi,s}(\widetilde{\Omega}_{st}) = q$$

which contradicts with the assumption that $s \precsim r$, thus $s \models \varphi$, and $s \precsim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}} r$. □

4.5.4 Simulation Kernel and Summary of Simulation

Let $\mathcal{R}^{-1}$ denote the reverse of $\mathcal{R}$, then $\mathcal{R} \cap \mathcal{R}^{-1}$ is the simulation kernel. In this section we will show the relation between the simulation kernels and their correspondent bisimulations. Not surprisingly, the simulation kernels are coarser than the bisimulations as shown in the following theorem.

Theorem 32. *1.* $\sim_i^b \subseteq (\prec_i^b \cap (\prec_i^b)^{-1})$.

2. $\sim_i \subseteq (\prec_i \cap \prec_i^{-1})$.

3. $\approx^b \subseteq (\precapprox^b \cap (\precapprox^b)^{-1})$.

4. $\approx \subseteq (\precapprox \cap \precapprox^{-1})$.

Proof. We only prove the first clause here, since the others are quite similar. The proof of $\sim_i^b \subseteq \prec_i^{\mathrm{b}} \cap (\prec_i^{\mathrm{b}})^{-1}$ is trivial and omitted here. To show that $\prec_i^{\mathrm{b}} \cap (\prec_i^{\mathrm{b}})^{-1}$ is strictly coarser than $\sim_i^b$, it is enough to give a counterexample. Suppose we have three states s_1, s_2, and s_3 such that $s_1 \prec_i^{\mathrm{b}} s_2 \prec_i^{\mathrm{b}} s_3$ but $s_3 \not\prec_i^{\mathrm{b}} s_2 \not\prec_i^{\mathrm{b}} s_1$. Let s and r be two states such that $L(s) = L(r)$. In addition s has three transitions: $s \to \delta_{s_1}$, $s \to \delta_{s_2}$, $s \to \delta_{s_3}$, and r only has two transitions: $s \to \delta_{s_1}$, $s \to \delta_{s_3}$. Then it should be easy to check that $s \prec_i^{\mathrm{b}} r$ and $r \prec_i^{\mathrm{b}} s$, the only non-trivial case is when $s \to \delta_{s_2}$. Since $s_2 \prec_i^{\mathrm{b}} s_3$, thus there exists $r \to \delta_{s_3}$ such that $\delta_{s_2} \sqsubseteq_{\prec_i^{\mathrm{b}}} \delta_{s_3}$. But obviously $s \not\prec_i^b r$, since the transition $s \to \delta_{s_2}$ cannot be simulated by any transition of r. □

We summarize the preorders in strong and weak scenarios in Fig. 4.7 and 4.8 respectively, note we omit the subscript s denoting safe fragment for the logic preorders as before.

4.6 Countable States

For now we only consider finite PAs i.e. only contain finite states. In this section we will show that these results also apply for PAs with countable states. Assume S is a countable set of states S. We adopt the method used in (56) to deal with strong branching bisimulation since all the other cases are similar. First we recall some standard notations from topology theory. Given a metric space (S, d) where d is a metric, a sequence $\{s_i \mid i \geq 0\}$ converges to s iff for any $\epsilon > 0$, there exists n such that

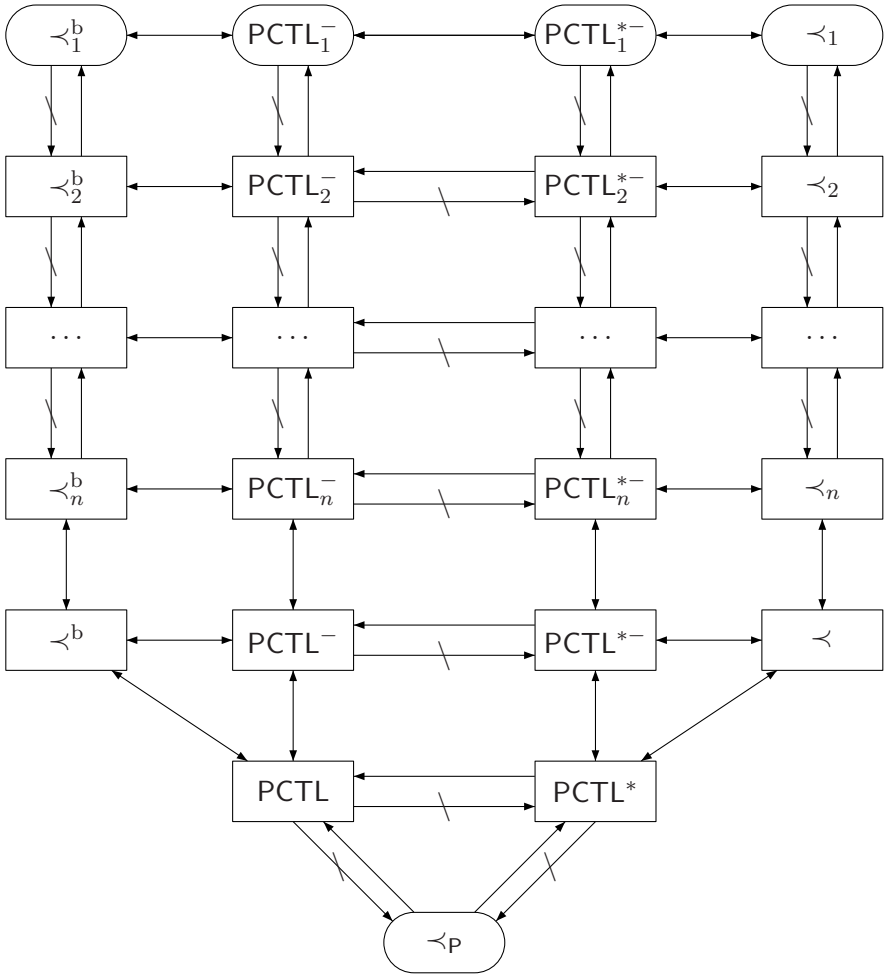

Figure 4.7: Relationship of different preorders in strong scenario.

$d(s_m, s) < \epsilon$ for any $m \geq n$. A metric space is compact if every infinite sequence has a convergent subsequence.

Below follows the definition of metric over distributions from (56).

Definition 38 (Metric)**.** *Given two distributions $\mu, \nu \in Dist(S)$, the metric d is defined by*

$$d(\mu, \nu) = Sup_{C \in S} |\mu(C) - \nu(C)| \ .$$

Since the metric is defined over distributions while in Definition 28 we did not consider distributions explicitly, thus we need to adapt the definition of $Prob_{\pi,s}(C, C', n)$ in the following way: $s \stackrel{n,C}{\Longrightarrow} \mu$ iff either

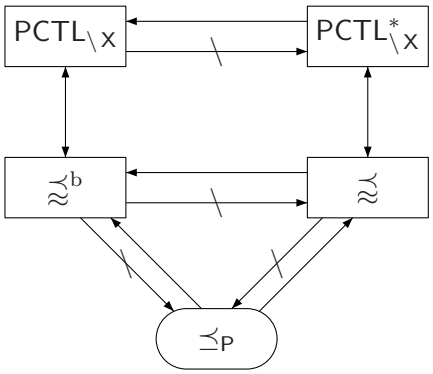

Figure 4.8: Relationship of different preorders in weak scenario.

- $\mu = \delta_s$, or
- $s \to \nu$ such that

$$\sum_{\forall r \in Supp(\nu).r \xrightarrow{n-1,C} \nu_r} \nu(r) \cdot \nu_r = \mu.$$

It is obvious that for each π, C, C', and n, there exists $s \xrightarrow{n,C} \mu$ such that $\mu(C') = Prob_{\pi,s}(C, C', n)$.

Now we can define the compactness of probabilistic automata as in (56) with a slight difference.

Definition 39 (Compactness)**.** *Given a probabilistic automaton $\mathcal{P}$, $\mathcal{P}$ is i-compact iff*

$$\{\mu \mid s \xrightarrow{i,C} \mu\}$$

is compact under metric d for each $s \in S$ and $\sim_i^b$ closed set C.

As mentioned in (56, 86), the convex closure does not change the compactness, thus we can extend $\xrightarrow{n,C}$ to allow combined transitions in a standard way without changing anything, but for simplicity we omit this. A probabilistic automaton is *compact* iff it is i-compact for any $i \geq 1$.

We introduce the definition of *capacity* as follows.

Definition 40 (Capacity)**.** *Given a set of states S and a π-algebra $\mathcal{B}$, a capacity on $\mathcal{B}$ is a function $Cap : \mathcal{B} \to (R^+ \cup \{0\})$ such that*[1]*:*

[1] R^+ is the set of positive real numbers.

1. $Cap(\emptyset) = 0$,
2. *whenever* $C_1 \subseteq C_2$ *with* $C_1, C_2 \in \mathcal{B}$, *then* $Cap(C_1) \leq Cap(C_2)$,
3. *whenever there exists* $C_1 \subseteq C_2 \subseteq \ldots$ *such that* $\cup_{i\geq 1} C_i = C$, *or* $C_1 \supseteq C_2 \supseteq \ldots$ *such that* $\cap_{i\geq 1} C_i = C$, *then*

$$\lim_{i\to\infty} Cap(C_i) = Cap(C).$$

A capacity Cap is sub-additive *iff*

$$Cap(C_1 \cup C_2) \leq Cap(C_1) + Cap(C_2)$$

for any $C_1, C_2 \in \mathcal{B}$.

Different from (56), the value of $Prob_{\pi,s}(C, C', n)$ depends on both C and C'. Let

$$PreCap^{C}_{s,n}(C') = Sup_{\pi} Prob_{\pi,s}(C, C', n),$$

$$PostCap^{C'}_{s,n}(C) = Sup_{\pi} Prob_{\pi,s}(C, C', n)$$

i.e. given a C', $PreCap^{C}_{s,n}$ will return the maximum probability from s to C' in at most n steps via only states in C, similar for $PostCap^{C'}_{s,n}$. The following lemma shows that both $PreCap^{C}_{s,n}$ and $PostCap^{C'}_{s,n}$ are sub-additive capacities.

Lemma 25. *$PreCap^{C}_{s,n}$ and $PostCap^{C'}_{s,n}$ are sub-additive capacities on $\mathcal{B}$ where $\mathcal{B}$ is the π-algebra only containing $\sim^b_i$ closed sets.*

Proof. Refer to the proof of Lemma 5.2 in (56). □

Now we can show that the following results are still valid as long as the given probabilistic automaton is compact even when it contains infinitely countable states.

Theorem 33. *Given a compact probabilistic automata,*

1. $\sim^b_n = \sim_{\mathsf{PCTL}^-_n}$,
2. *there exists* $n \geq 0$ *such that* $\sim^b_n = \sim_{\mathsf{PCTL}}$.

Proof. 1. The proof of $\sim^b_n \subseteq \sim_{\mathsf{PCTL}^-_n}$ is similar with the proof of Theorem 21, and is omitted here. We prove that $\sim_{\mathsf{PCTL}^-_n} \subseteq \sim^b_n$ in the sequel following the proof of Theorem 6.10 in (56). Let

$$\mathcal{R} = \{(s, r) \mid s \sim_{\mathsf{PCTL}^-_n} r\},$$

we need to prove that $\mathcal{R}$ is a strong i-depth branching bisimulation. In order to do so, we need to prove that for any $(s,r) \in \mathcal{R}$,

$$PreCap^{C}_{s,n}(C') = PreCap^{C}_{r,n}(C')$$

for each $\mathcal{R}$ closed sets C and C'. Since both C and C' may be countable union of equivalence classes while each equivalence class can only be characterized by countable many formulas, therefore we have

$$C = \cup^{\infty}_{i=1}(\cap^{\infty}_{j=1}C_{i,j}) \text{ and } C' = \cup^{\infty}_{i=1}(\cap^{\infty}_{j=1}C'_{i,j})$$

where $\cap^{\infty}_{j=1}C_{i,j}$ corresponds the i-th equivalence class in C, and $C_{i,j}$ corresponds the set of states determining by the j-th formula satisfied by i-th equivalence class, similar for $\cap^{\infty}_{j=1}C'_{i,j}$ and $C'_{i,j}$. Similar as (56), let

$$B_k = \cap^{\infty}_{j=1}(\cup^{k}_{i=1}C_{i,j}), A^{l}_{k} = \cap^{l}_{j=1}(\cup^{k}_{i=1}C_{i,j}),$$

$$B'_k = \cap^{\infty}_{j=1}(\cup^{k}_{i=1}C'_{i,j}), A'^{l}_{k} = \cap^{l}_{j=1}(\cup^{k}_{i=1}C'_{i,j}).$$

It is easy to see that B_k and B'_k are increasing sequences of $\mathcal{R}$ closed sets such that $\cup^{\infty}_{k=1}B_k = C$, and $\cup^{\infty}_{k=1}B'_k = C'$, while A^{l}_{k} and A'^{l}_{k} are decreasing sequences of $\mathcal{R}$ closed sets such that $\cap^{\infty}_{l=1}A^{l}_{k} = B_k$ and $\cap^{\infty}_{l=1}A'^{l}_{k} = B'_k$. Both A^{l}_{k} and A'^{l}_{k} only contain conjunction and disjunction of finite formulas, thus can be described by PCTL^{-}_{i}. The following proof is straightforward due to $s \sim_{\mathsf{PCTL}^{-}_{i}} r$ and Lemma 25.

2. Suppose that $\sim_{\mathsf{PCTL}} \subset \sim^{b}_{n}$ for any $n \geq 0$ which means that there exists s and r such that $s \sim^{b}_{n} r$ for any $n \geq 0$, but $s \nsim_{\mathsf{PCTL}} r$. As a result there exists C, C' and π such that

$$\lim_{i\to\infty} Prob_{\pi,s}(C, C', i) > 0,$$

but there does not exist π' such that

$$\lim_{i\to\infty} Prob_{\pi',r}(C, C', i) \geq \lim_{i\to\infty} Prob_{\pi,s}(C, C', i).$$

In other words,

$$\lim_{i\to\infty} Prob_{\pi',r}(C, C', i) < \lim_{i\to\infty} Prob_{\pi,s}(C, C', i)$$

for any π' which indicates that there exists $n \geq 0$ such that

$$Prob_{\pi',r}(C, C', n) < Prob_{\pi,s}(C, C', n)$$

for any π', therefore $s \nsim_{\mathsf{PCTL}^{-}_{i}} r$ which contradicts with our assumption.

□

In a similar way we can extend the results of this section to strong bisimulations and weak bisimulations, we skip their proofs here. For the simulations, we need to do more work, since there may be uncountable many downward closed sets. We prove along the line of (57). The following lemma is similar as Lemma 5.1 in (57) with only slight differences: i) we consider downward closed sets instead of upward closed sets, ii) we do not require $\mathcal{R}$ to be a preorder, but these do not change the proof.

Lemma 26 (Lemma 5.1 (57))**.** *Let $\mathcal{R} \subseteq S \times S$ be a relation, and $C \subseteq S$ be a $\mathcal{R}$ downward closed set, then C is a union of equivalence classes of $\equiv_{\mathcal{R}}$ where $\equiv_{\mathcal{R}}$ is the largest equivalence relation contained in $\mathcal{R}$.*

Given a $\mathcal{R}$ downward closed set C, we say C is *finitely generated* if there exists a finite set of equivalence classes of $\{C_i \in S/\equiv_{\mathcal{R}}\}_{i\in I}$ such that $C = \cup_{i\in I} C_i$. Since the set of the equivalence classes in $S/\equiv_{\mathcal{R}}$ is countable, thus the set of finitely generated $\mathcal{R}$ downward closed set is also countable (57). The following lemma shows an alternative definition of $\prec_i^{\mathrm{b}}$ in Definition 33 where we only focus on finitely generated downward closed sets:

Lemma 27. *A relation $\mathcal{R} \subseteq S\times S$ is a strong i-depth branching simulation with $i \geq 1$ iff $s\ \mathcal{R}\ r$ implies that $s\ \prec_{i-1}^{b}\ r$ and for any finitely generated $\mathcal{R}$ downward closed sets C, C', and any scheduler σ, there exists σ' such that $Prob_{\sigma',r}(C, C', i) \geq Prob_{\sigma,s}(C, C', i)$.*

We write $s\ \prec_i^b\ r$ whenever there is a strong i-depth branching simulation $\mathcal{R}$ such that $s\ \mathcal{R}\ r$.

Proof. The proof is similar as the proof of Lemma 5.2 in (57). Let $(\prec_i^{\mathrm{b}})'$ denote the new definition, we need to prove that $s\ \prec_i^{\mathrm{b}}\ r$ iff $s\ (\prec_i^{\mathrm{b}})'\ r$. Since finitely generated $\mathcal{R}$ downward closed sets are special cases of $\mathcal{R}$ downward closed sets, it is trivial to see that $s\ \prec_i^{\mathrm{b}}\ r$ implies $s\ (\prec_i^{\mathrm{b}})'\ r$. We prove that $s\ (\prec_i^{\mathrm{b}})'\ r$ implies $s\ \prec_i^{\mathrm{b}}\ r$ by contradiction. Suppose that for any finitely generated $\mathcal{R}$ downward closed sets C, C' and σ, there exists σ' such that $Prob_{\sigma',r}(C, C', i) \geq Prob_{\sigma,s}(C, C', i)$, but there exists $\mathcal{R}$ downward closed sets C, C' and σ such that $Prob_{\sigma',r}(C, C', i) < Prob_{\sigma,s}(C, C', i)$ for any σ'. Let σ be a scheduler such that $Prob_{\sigma',r}(C, C', i) < Prob_{\sigma,s}(C, C', i)$ for any σ' and $\epsilon = Prob_{\sigma,s}(C, C', i) - Prob_{\sigma',r}(C, C', i) > 0$. According to Lemma 26, there exists sets of equivalences classes: $\{C_j \in S/\equiv_{\mathcal{R}}\}_{j\in J}$ and $\{C_k \in S/\equiv_{\mathcal{R}}\}_{k\in K}$ such that $C = \cup_{j\in J} C_i$ and $C' = \cup_{k\in K} C_k$ where J, K are (infinite) sets of indexes. Define two sequences of finitely generated $\mathcal{R}$ downward closed sets:

$$\{C_{\leq j} = \cup_{j'\in J\wedge j'\leq j} \mid j \in J\},$$

$$\{C_{\leq k} = \cup_{k' \in K \wedge k' \leq k} \mid k \in K\}.$$

Obviously both $Prob_{\sigma,s}(C, C_{\leq k}, i)$ and $Prob_{\sigma,s}(C_{\leq j}, C', i)$ are monotone, non-decreasing and converge to $Prob_{\sigma,s}(C, C', i)$ for any C and C'. Therefore there exists $j \in J$ and $k \in K$ such that

$$Prob_{\sigma,s}(C_{\leq j}, C', i) > Prob_{\sigma,s}(C, C', i) - \frac{\epsilon}{4}, \text{ and}$$

$$Prob_{\sigma,s}(C_{\leq j}, C_{\leq k}, i) > Prob_{\sigma,s}(C_{\leq j}, C', i) - \frac{\epsilon}{4}.$$

This implies

$$Prob_{\sigma,s}(C_{\leq j}, C_{\leq k}, i) > Prob_{\sigma,s}(C, C', i) - \frac{\epsilon}{2}$$

$$= Prob_{\sigma',r}(C, C', i) + \frac{\epsilon}{2} > Prob_{\sigma',r}(C, C', i) \geq Prob_{\sigma,s}(C_{\leq j}, C_{\leq k}, i),$$

which contradicts with the assumption. □

By Lemma 27 it is enough to consider all the finitely generated $\prec_i^{\flat}$ downward closed sets in Definition 39 which is countable. The extension of Theorem 26 to the countable state space is then routine, and is omitted here. Moreover the definitions of other variants of simulations in Section 4.5 can be adopted to only consider finitely generated downward closed sets too, thus their logic characterizations can also be extended to countable states.

4.7 The Coarsest Congruent (Bi)Simulations

Before we have shown that $\sim_{\mathsf{P}}$ is congruent but cannot be characterized by $\sim_{\mathsf{PCTL}}$ completely since it is too fine. On the other hand, there exists $\sim_n^b$ which can be characterized by $\sim_{\mathsf{PCTL}}$, but it is not congruent generally, this indicates that $\sim_{\mathsf{PCTL}}$ is essentially not congruent. Therefore a natural question one may ask is that what is the largest subset of $\sim_{\mathsf{PCTL}}$ which is congruent. The following theorem shows that $\sim_{\mathsf{P}}$ is such coarsest congruent relation in $\sim_{\mathsf{PCTL}}$ assuming that the given probabilistic automaton is compact.

Theorem 34. *$\sim_{\mathsf{P}}$ is the coarsest congruent equivalence relation in $\sim_{\mathsf{PCTL}}$.*

Proof. We prove by contradiction. Suppose that there exists $\sim_{\mathsf{P}} \subset \simeq \subset \sim_{\mathsf{PCTL}}$ such that $\simeq$ is congruent. Since $\sim_{\mathsf{P}} \subset \simeq$, there exists s and r such that $s \simeq r$ but $s \not\sim_{\mathsf{P}} r$. According to Definition 23 there exists $s \to \mu$ such that there does not exist $r \to_{\mathsf{P}} \nu$

with $\mu \sim_{\mathsf{P}} \nu$. The idea is to show that there always exists t such that $s \parallel t \not\sim_{\mathsf{PCTL}} r \parallel t$ in this case, then it is enough to give a formula φ such that $r \parallel t \models \varphi$, but $s \parallel t \not\models \varphi$.

Let $Supp(\mu) = \{s_1, s_2, \ldots\}$ and $\mu(s_i) = a_i$[1] with $i \geq 1$. Without losing of generality we assume that there exists $s \to \mu$ such that for any two (combined) transitions of r: $r \to_{\mathsf{P}} \nu_1$ and $r \to_{\mathsf{P}} \nu_2$, there does not exist $0 \leq w_1, w_2 \leq 1$ such that $w_1 + w_2 = 1$ and $\mu \sim_{\mathsf{P}} (w_1 \cdot \nu_1 + w_2 \cdot \nu_2)$ (every combined transition of r can be seen as a combined transition of two other combined transitions of r). Let $\nu_1(s_i) = b_i$ and $\nu_2(s_i) = c_i$ in the following, then there must exist $i \neq j \geq 1$ such that there does not exist $0 \leq w_1, w_2 \leq 1$ such that $w_1 \cdot b_i + w_2 \cdot c_i = a_i$ and $w_1 \cdot b_j + w_2 \cdot c_j = a_j$ with $w_1 + w_2 = 1$, otherwise we will have $\mu \sim_{\mathsf{P}} (w_1 \cdot \nu_1 + w_2 \cdot \nu_2)$ which contradicts with the assumption. There are nine possible cases in total depending on the relation between a_i, a_j and b_i, c_i, b_j, c_j. Most of the cases are trivial except when $a_i \in [b_i, c_i]$ and $a_j \in [c_j, b_j]$. [2] For instance if $a_i > b_i, c_i$, r will evolve into s_i with probability less than a_i which is not the case for s, thus $s \not\sim_{\mathsf{PCTL}} r$ which contradicts with the assumption. Considering the following inequations where ρ_1 and ρ_2 are two variables with values in $[0, 1]$:

$$a_i \cdot \rho_1 + a_j \cdot \rho_2 < b_i \cdot \rho_1 + b_j \cdot \rho_2, \tag{4.5}$$

$$a_i \cdot \rho_1 + a_j \cdot \rho_2 < c_i \cdot \rho_1 + c_j \cdot \rho_2 \tag{4.6}$$

which can be transformed into the following forms:

$$(a_i - b_i) \cdot \rho_1 < (b_j - a_j) \cdot \rho_2, \tag{4.7}$$

$$(a_i - c_i) \cdot \rho_1 < (c_j - a_j) \cdot \rho_2. \tag{4.8}$$

Note that $(a_i - b_i)$, $(a_i - c_i)$, $(b_j - a_j)$, and $(c_j - a_j)$ cannot be 0 at the same time, so there always exists $0 \leq \rho_1, \rho_2 \leq 1$ such that $a_i \cdot \rho_1 + a_j \cdot \rho_2$ is either greater or smaller than both of $b_i \cdot \rho_1 + b_j \cdot \rho_2$ and $c_i \cdot \rho_1 + c_j \cdot \rho_2$. By simple calculation whenever $\rho_1 \in (\frac{b_j - a_j}{a_i - b_i} \cdot \rho_2, \frac{a_j - c_j}{c_i - a_i} \cdot \rho_2)$ (it is not possible for $\frac{b_j - a_j}{a_i - b_i} = \frac{a_j - c_j}{c_i - a_i}$, otherwise there exists $0 \leq w_1, w_2 \leq 1$ such that $w_1 \cdot b_i + w_2 \cdot c_i = a_i$ and $w_1 \cdot b_j + w_2 \cdot c_j = a_j$ with $w_1 + w_2 = 1$), then $a_i \cdot \rho_1 + a_j \cdot \rho_2$ is smaller than $b_i \cdot \rho_1 + b_j \cdot \rho_2$ and $c_i \cdot \rho_1 + c_j \cdot \rho_2$. Let t be a state such that it can only evolve into t_1 with probability ρ_1 and t_2 with probability ρ_2 where $\rho_1 + \rho_2 = 1$ and $\rho_1 \in (\frac{b_j - a_j}{a_i - b_i} \cdot \rho_2, \frac{a_j - c_j}{c_i - a_i} \cdot \rho_2)$, obviously such t always exists. Assume that all the states have distinct labels except for s and r, moreover let

$$\psi = ((L(s \parallel\!\mid t) \vee L(s_i \parallel\!\mid t) \vee (L(s_j \parallel\!\mid t)))\, \mathsf{U}^{\leq 2} (L(s_i \parallel\!\mid t_1) \vee L(s_j \parallel\!\mid t_2))),$$

[1] For simplicity we assume that $s_i (i \geq 1)$ belong to different equivalence classes.

[2] We assume here that $c_i \geq b_i$ and $b_j \geq c_j$

it is not hard to see that the minimum probability of the paths of $s \parallel t$ satisfying ψ is at most $a_i \cdot \rho_1 + a_j \cdot \rho_2$ i.e. when $s \parallel t$ first performs the transition $s \to \mu$ of s and then performs the transition $t \to \{\rho_1 : t_1, \rho_2 : t_2\}$ of t. Let $r \to_{\mathsf{P}} \nu$ be the transition such that when $r \parallel t$ first performs it and then performs $t \to \{\rho_1 : t_1, \rho_2 : t_2\}$, the probability of the paths of $r \parallel t$ satisfying ψ is minimal. Since $\nu(s_i) \cdot \rho_1 + \nu(s_j) \cdot \rho_2 > a_i \cdot \rho_1 + a_j \cdot \rho_2$, we have $r \parallel t \models \mathcal{P}_{\geq q}\psi$ but $s \parallel t \not\models \mathcal{P}_{\geq q}\psi$ where $q = \nu(s_i) \cdot \rho_1 + \nu(s_j) \cdot \rho_2$. In other words $s \parallel t \not\sim_{\mathsf{PCTL}} r \parallel t$, as a result $s \parallel t \not\simeq r \parallel t$, so $\simeq$ is not congruent. When all the states do not have distinct labels, we can always construct formulas to distinguish them, since the probabilistic automaton is compact and these states are in different equivalence classes by assumption, the following proof is the same. This completes our proof. □

Theorem 34 can be extended to identify the coarsest congruent weak bisimulation in $\sim_{\mathsf{PCTL}_{\setminus \mathsf{X}}}$, and the coarsest congruent strong and weak simulations in $\prec_{\mathsf{PCTL}}$ and $\precsim_{\mathsf{PCTL}_{\setminus \mathsf{X}}}$ respectively.

Theorem 35. *1. $\simeq_{\mathsf{P}}$ is the coarsest congruent equivalence relation in $\sim_{\mathsf{PCTL}_{\setminus \mathsf{X}}}$,*

2. $\prec_{\mathsf{P}}$ is the coarsest congruent preorder in $\prec_{\mathsf{PCTL}}$,

3. $\preceq_{\mathsf{P}}$ is the coarsest congruent preorder in $\precsim_{\mathsf{PCTL}_{\setminus \mathsf{X}}}$.

Proof. The proof is similar with the proof of Theorem 34 and we only sketch the proof of Clause (2) here. In order to prove that $\prec_{\mathsf{P}}$ is the coarsest congruent preorder in $\prec_{\mathsf{PCTL}}$, we need to show that for any $\preceq$ such that $\prec_{\mathsf{P}} \subset \preceq \subset \prec_{\mathsf{PCTL}}$, it holds that $\preceq$ is not congruent i.e. there exists s, r, and t such that $s \preceq r$, but $s \parallel t \not\preceq r \parallel t$. First assume that $\preceq$ is a congruence, and we then prove by contradiction as in Theorem 34 and show that if $s \preceq r$ and $s \not\prec_{\mathsf{P}} r$, there exists t such that $s \parallel t \not\prec_{\mathsf{PCTL}} r \parallel t$, thus $s \parallel t \not\preceq r \parallel t$ which contradicts with the assumption that $\preceq$ is a congruence. Since $s \not\prec_{\mathsf{P}} r$, then there exists $s \to \mu$ such that there does not exist $r \to_{\mathsf{P}} \nu$ with $\mu \sqsubseteq_{\prec_{\mathsf{P}}} \nu$. With the same argument as in Theorem 34 and Lemma 27, there exists t and ψ such that $r \parallel t \models \mathcal{P}_{\geq q}\psi$ but $s \parallel t \not\models \mathcal{P}_{\geq q}\psi$ i.e. $s \parallel t \not\prec_{\mathsf{PCTL}} r \parallel t$, thus $\preceq$ is not congruent. □

4.8 Related Work

For Markov chains, i.e., deterministic probabilistic automata, the logic PCTL characterizes bisimulations, and PCTL without X operator characterizes weak bisimula-

tions (54, 87). As pointed out in (1), probabilistic bisimulation is sound, but not complete for PCTL for PAs. In the literature, various extensions of the Hennessy-Milner logic (88) are considered for characterizing bisimulations. Larsen and Skou (49) considered such an extension of Hennessy-Milner logic, which characterizes bisimulation for *alternating automaton* (49), or labeled Markov processes (56) (PAs but with continuous state space). For probabilistic automata, Jonsson *et al.* (89) considered a two-sorted logic in the Hennessy-Milner style to characterize strong bisimulations. In (57), the results are extended for characterizing also simulations.

Weak bisimulation was first defined in the context of PAs by Segala (1), and then formulated for alternating models by Philippou *et al.* (53). The seemingly very related work is by Desharnais et al. (56), where it is shown that PCTL* is sound and complete w.r.t. weak bisimulation for alternating automata. The key difference is that the model they have considered is not the same as probabilistic automata considered in this chapter. Briefly, in alternating automata, states are either nondeterministic like in transition systems, or stochastic like in discrete-time Markov chains. As discussed in (90), a probabilistic automaton can be transformed to an alternating automaton by replacing each transition $s \to \mu$ by two consecutive transitions $s \to s'$ and $s' \to \mu$ where s' is the new inserted state. Surprisingly, for alternating automata, Desharnais et al. have shown that weak bisimulation – defined in the standard manner – characterizes PCTL* formulae. The following example illustrates why it works in that setting, but fails for probabilistic automata.

Example 42. *Refer to Fig. 4.1, we need to add three additional states s_{μ_1}, s_{μ_2}, and s_{μ_3} in order to transform s and r to alternating automata. The resulting automata are shown in Fig. 4.9. Suppose that s_1, s_2, and s_3 are three absorbing states with different atomic propositions, so they are not (weak) bisimilar, as a result s_{μ_1}, s_{μ_2} and s_{μ_3} are not (weak) bisimilar either since they can evolve into s_1, s_2, and s_3 with different probabilities. Therefore s and r are not (weak) bisimilar. Let*

$$\varphi = \mathcal{P}_{\geq 0.4}(\mathsf{X}\, L(s_1)) \wedge \mathcal{P}_{\geq 0.3}(\mathsf{X}\, L(s_2)) \wedge \mathcal{P}_{\geq 0.3}(\mathsf{X}\, L(s_3)),$$

it is not hard to see that $s_{\mu_2} \models \varphi$ but $s_{\mu_1}, s_{\mu_3} \not\models \varphi$, so $s \models \mathcal{P}_{\leq 0}(\mathsf{X}\, \varphi)$ while $r \not\models \mathcal{P}_{\leq 0}(\mathsf{X}\, \varphi)$. When working in the setting of probabilistic automata, s_{μ_1}, s_{μ_2}, and s_{μ_3} will not be considered as states, so we cannot use the above arguments for alternating automata anymore.

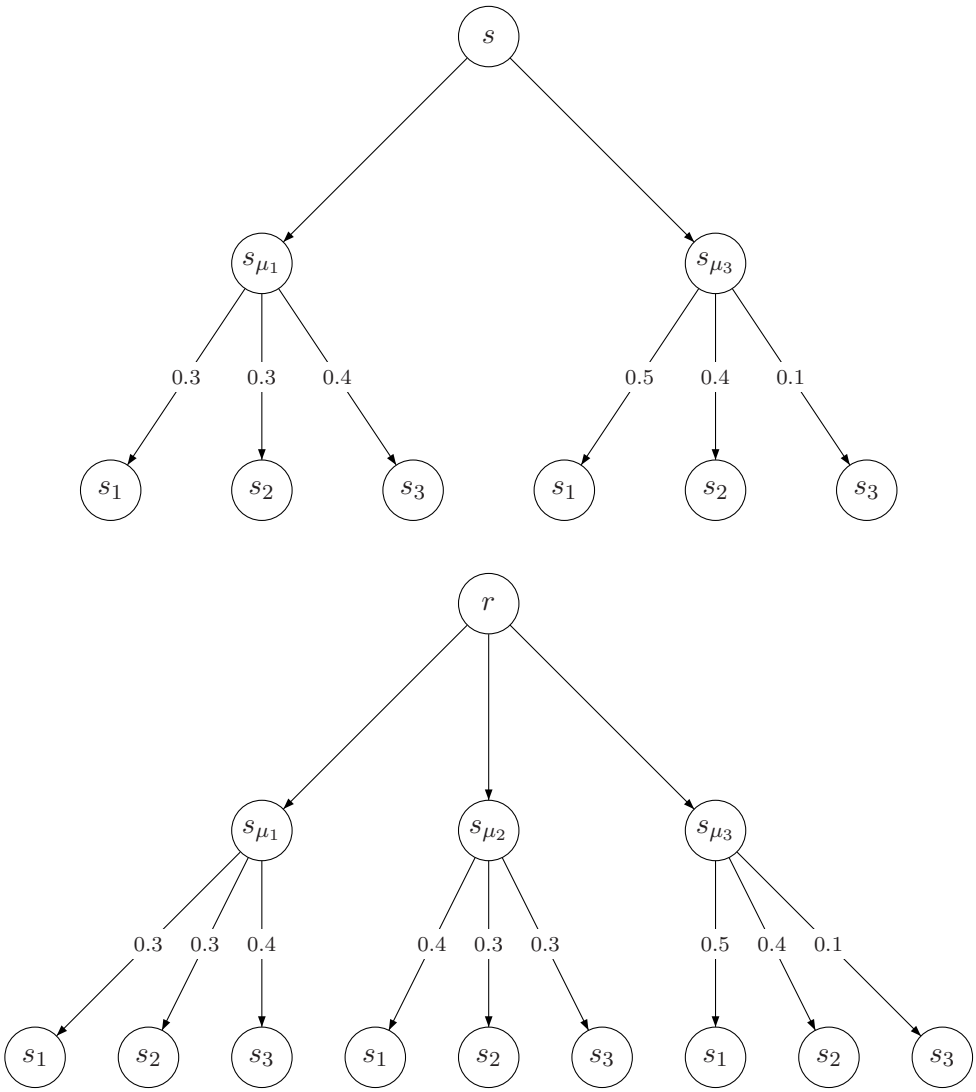

Figure 4.9: Alternating automata.

In the definition of $\sim_1$ and $\prec_1$, we choose first the downward closed set C before the successor distribution to be matched, which is the key for achieving our new notion of bisimulations and simulations. This approach was also adopted in (91) to define the priori ϵ-bisimulation and simulation. It turns out that when $\epsilon = 0$, the priori ϵ-bisimulation coincides with $\sim_1$. The priori ϵ-bisimulation was shown to be sound and complete w.r.t. an extension of Hennessy-Milner logic, similarly for the priori ϵ-simulation. Finally, the priori ϵ-bisimulation was also used to define pseudo-metric between PAs in (91, 92). The definition of priori 0-simulation in (91), denoted as $\prec_1'$,

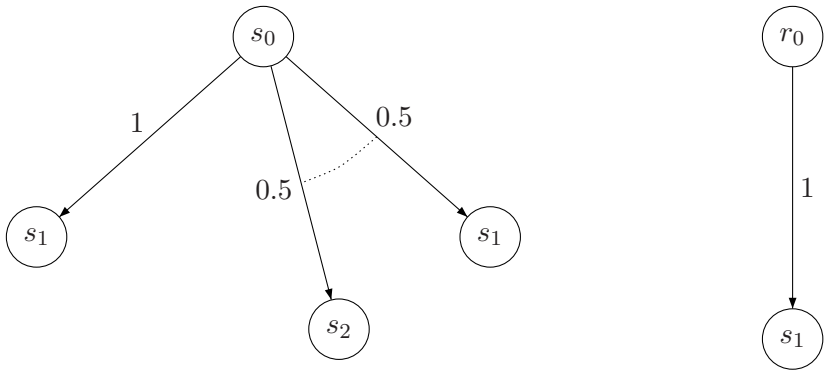

Figure 4.10: $\prec'_i \neq \prec_{\mathsf{PCTL}_1^-}$.

is however not equivalent to $\prec_1$. In the definition of $\prec'_1$, the upward closed sets are considered while in the definition of $\prec_1$ we consider downward closed sets. If we adopt the definition of $\prec'_1$ here, Theorem 26 will not be valid anymore. Refer to the following example.

Example 43. *Consider the two states s_0 and r_0 in Fig. 4.10 where all the states have different labels except that $L(s_0) = L(r_0)$, and the transitions of s_1 and s_2 are omitted. Moreover we assume that $s_2 \prec'_1 s_1$, but $s_1 \not\prec'_1 s_2$. Let $\mathcal{R} = \{(s_0, r_0), (s_1, s_1), (s_2, s_1)\}$, in order to show that $\mathcal{R}$ is a priori 0-simulation, we need to check that for each $\mathcal{R}$ upward closed set C and $s_0 \to \mu$, there exists $r_0 \to \nu$ such that $\mu(C) \leq \nu(C)$. The only non-trivial cases are when $C = \{s_1\}$ or $\{s_2, s_1\}$, thus $s_0 \prec'_1 r_0$. But we will show that $s_0 \not\prec_{\mathsf{PCTL}_1^-} r_0$. By contradiction, assume that $\prec'_1 = \prec_{\mathsf{PCTL}_1^-}$. Let $\varphi = \mathcal{P}_{\leq 0}(\mathsf{X}\,\varphi_{s_2})$ where φ_{s_2} is a formula such that $s_2 \models \varphi_{s_2}$ but $s_1 \not\models \varphi_{s_2}$. Since $s_1 \not\prec'_1 s_2$, such formula always exists by assumption. It is easy to see that $r_0 \models \varphi$, but $s_0 \not\models \varphi$ since the maximal probability from s_0 to s_2 in one step is equal to 0.5, thus we get contradiction, and $\prec'_1 \neq \prec_{\mathsf{PCTL}_1^-}$.*

Chapter 5

Continuous-time MDP

In Chapter 4 we show the characterizations of bisimulations and simulations w.r.t. PCTL* and its sublogics on probabilistic automata. In this chapter we will extend the work to continuous case i.e. we will show the characterizations of bisimulations and simulations w.r.t. CSL and its sublogics on continuous-time Markov decision processes (CTMDP).

We first motivate the work in Section 5.1, and then in Section 5.2 we recall the definition of CTMDPs and the logic CSL. In Section 5.3 we propose a parallel composition operator for CTMDPs. Strong and weak bisimulation relations and the corresponding logical characterization results are studied in Section 5.4. In Section 5.5, we present the sequence of i-depth bisimulations. The work is extended to simulations in Section 5.6. In Section 5.7, we discuss how the (bi)simulations on CTMDPs relate to those in probabilistic automata and Markov chains. Section 5.8 summarizes the chapter. We conclude this chapter by discussing some related work in Section 5.9.

5.1 Motivation

Recently, continuous-time Markov decision processes (CTMDP) have received extensive attentions in the model checking community, see for example (37, 54, 93, 94, 95, 96, 97, 98). Analysis techniques for CTMDPs suffer especially from the infamous state space explosion problem. Thus, as for other stochastic models, strong bisimulations have been proposed for CTMDPs in (37), which were shown to be sound w.r.t. the continuous-time stochastic logic (CSL). This result guarantees that one can first reduce the CTMDP

using bisimulations before analyzing the CTMDPs, as in the standard setting. On the other hand, as indicated in the paper (37), strong bisimulation is not complete w.r.t. CSL, i.e., logically equivalent states might not be bisimilar.

CTMDPs can be considered as extending the Markov decision processes (MDPs) with exponentially sojourn time distributions, and this subsumes models such as labeled transition systems and Markov chains as well. While linear and branching time equivalences and preorders are studied for these submodels (42, 43, 54, 99), this has not been studied for CTMDPs. In this chapter we study the branching time equivalences and preorders for CTMDP, and the logical characterization problem of these relations w.r.t. CSL.

We start with a slightly coarser notion of strong bisimulations, and then propose the notion of *weak bisimulations* for CTMDPs. We study the relationship between weak bisimulations and the logical equivalence induced by $\mathsf{CSL}_{\setminus \mathsf{X}}$, the sub-logic of CSL without the next operator. Our first contribution is to identify a subclass of CTMDPs under which our weak bisimulation coincides with $\mathsf{CSL}_{\setminus \mathsf{X}}$ equivalence. We discuss then how this class of CTMDPs can be efficiently determined.

Recently, in (99), we have introduced a sequence of i-depth bisimulations, which are shown to be converging to the logical equivalence w.r.t. probabilistic CTL (PCTL). As a second part of this chapter, we propose strong and weak i-depth bisimulations for CTMDPs, and provide logical characterization results for them. We show that, for general CTMDPs with finitely many states, the strong and weak i-depth bisimulations converge to equivalence relations which are exactly the CSL and $\mathsf{CSL}_{\setminus \mathsf{X}}$ equivalences, respectively.

Further, we extend the definitions to (weak) simulations, and study their relationship to the logical preorders w.r.t. the (weak) safety CSL respectively. As CTMDPs can be considered as combining MDPs and CTMCs, we will discuss the downward compatibility of the relations with those for MDPs and CTMCs.

As another notable contribution, we propose a novel – and very simple – parallel composition operator for CTMDPs. We show that both strong and weak bisimulations are congruence relations w.r.t. this new operator. As a direct consequence of this result, (weak) bisimulation compositional minimization reduction technique can be applied for analyzing the CTMDPs.

Summarizing, in this chapter we introduce various (weak) simulation and bisimulation relations, and develops for the first time a taxonomy of logical characterizations of these relations on CTMDPs:

- We introduce a new notion of weak bisimulation for CTMDPs. We identify a subclass of CTMDPs and show the sound and complete characterization for $\mathsf{CSL}_{\setminus \mathsf{X}}$.
- We present a sequence of i-depth (weak) bisimulations and the corresponding logical characterization results.
- We extends the definitions and logical characterization results to (weak) simulations and i-depth (weak) simulations.
- We introduce a novel parallel operator for CTMDPs, and study the congruence property of strong and weak bisimulations and simulations with respect to it.

5.2 Preliminaries

We first recall the definition of continuous-time Markov decision process as follows.

5.2.1 Continuous-time Markov Decision Process.

Definition 41 (Continuous-time Markov Decision Process)**.** *A tuple* $\mathcal{C} = (S, \rightarrow, AP, L, s_0)$ *is a continuous-time Markov decision process (*CTMDP*) where*

- S *is a finite but non-empty set of states;*
- $\rightarrow \subseteq S \times R^+ \times Dist(S)$ *is a finite transition relation where* R^+ *is the set of positive real numbers;*
- AP *is a finite set of atomic propositions;*
- $L : S \mapsto 2^{AP}$ *is labeling function;*
- $s_0 \in S$ *is the initial state.*

Let

$$Suc(s) = \{r \mid \exists (s \xrightarrow{\lambda} \mu).\mu(r) > 0\}$$

denote the successor states of s, and $Suc^*(s)$ the transitive closure. To avoid timelock, we assume w.l.o.g. that $Suc(s) \neq \emptyset$ for each $s \in S$. A state s is said to be *absorbing*, denoted as $s_\perp$, iff

$$\forall(s' \in Suc^*(s)).L(s') = L(s).$$

A continuous-time Markov chain (CTMC) is a CTMDP satisfying the condition that: $s \xrightarrow{\lambda} \mu$ and $s \xrightarrow{\lambda'} \mu'$ imply $\lambda = \lambda'$ and $\mu = \mu'$.

Below we recall the notion of *uniformization* for CTMDPs (95, 100). Essentially, by uniformizing each state will have a unique exit rate while preserving certain properties.

Definition 42 (Uniformization)**.** *Given a* CTMDP $\mathcal{C} = (S, \rightarrow, AP, L, s_0)$*, the uniformized* CTMDP *is denoted as* $\bar{\mathcal{C}} = (\bar{S}, \rightarrow', AP, \bar{L}, \bar{s_0})$ *where*

- $\bar{S} = \{\bar{s} \mid s \in S\}$*;*
- $\bar{L}(\bar{s}) = L(s)$ *for each* $s \in S$*;*
- $(\bar{s}, E, \bar{\mu}) \in \rightarrow'$ *iff there exists* $(s, \lambda, \mu) \in \rightarrow$ *and*

$$\bar{\mu} = \frac{\lambda}{E} \cdot \mu' + (1 - \frac{\lambda}{E}) \cdot \delta_{\bar{s}}$$

where $\mu'(\bar{r}) = \mu(r)$ *for each* $r \in Supp(\mu)$ *and*

$$E = \max\{\lambda \mid (s, \lambda, \mu) \in \rightarrow\}$$

is the maximum rate in the original CTMDP*.*

A CTMDP $\mathcal{C}$ *is uniformized iff for any* $(s_1, \lambda_1, \mu_1) \in \rightarrow$ *and* $(s_2, \lambda_2, \mu_2) \in \rightarrow$*,* $\lambda_1 = \lambda_2$*.*

5.2.2 Path and Measurable Scheduler

Let $\mathcal{C} = (S, \rightarrow, AP, L, s_0)$ be a given CTMDP. Let

$$Paths^{n+1}(\mathcal{C}) = S \times (R^+ \times S)^n$$

denote the set of paths with length $n + 1$ of $\mathcal{C}$. The set of all the finite paths of $\mathcal{C}$ is the union of all the $Paths^n(\mathcal{C})$ with $n > 0$, that is,

$$Paths^*(\mathcal{C}) = \cup_{n>0} Paths^n(\mathcal{C}).$$

In addition $Paths^\infty(\mathcal{C}) = S \times (R^+ \times S)^\infty$ contains all the infinite paths and

$$Paths(\mathcal{C}) = Paths^*(\mathcal{C}) \cup Paths^\infty(\mathcal{C})$$

is the set of all the paths of $\mathcal{C}$. Intuitively, a path is comprised of alternation of state and its sojourn time. To simplify the discussion we introduce some notations some of which are from Chapter 4 and overloaded here. Given a path $\omega = s_0, t_0, s_1, t_1 \cdots s_{n-1} \in Paths^n(\mathcal{C})$, $|\omega| = n$ is the length of ω, $\omega\downarrow = s_{n-1}$ is the last state of ω, $\omega|^i = s_0, t_0, \cdots, s_i$ is the prefix of ω ending at the i-th state, and $\omega|_i = s_i, t_i, s_{i+1}, \cdots$ is the suffix of ω starting from the i-th state, and $\omega^\frown(t_{n-1}, s_n)$ is the path obtained by extending ω with t_{n-1}, s_n. Let $\omega[i] = s_i$ and $time(\omega, i) = t_i$ denote the i-th state and the time spent in the i-th state respectively where $i < n$, while $\omega@t$ is the state at time point t in ω, that is, $\omega@t = \omega[j]$ where j is the smallest index such that $\sum_{i=0}^{j} t_i > t$. Moreover,

$$Steps(s) = \{(rate, \mu) \mid (s, rate, \mu) \in \rightarrow\}$$

is the set of all available choices in state s. Let $\{I_i \subseteq [0, \infty)\}_{0 \leq i < k}$ denote a set of intervals, then

$$C(s_0, I_0, \cdots, I_{k-1}, s_k)$$

is the *cylinder set* of paths $\omega \in Paths^\infty(\mathcal{C})$ such that $\omega[i] = s_i$ and $time(\omega, i) \in I_i$. Let $\mathfrak{F}_{Paths^\infty(\mathcal{C})}$ be the smallest σ algebra on $Paths^\infty(\mathcal{C})$ containing all the cylinder sets. Refer to (37) for more details.

Non-deterministic choices in CTMDPs are resolved by schedulers, which generates a distribution over the available transitions based on the existing path. We consider measurable timed history-dependent randomized schedulers (37, 101).

Definition 43 (Scheduler)**.** *A scheduler*

$$\pi : Paths^*(\mathcal{C}) \times R^+ \times Dist(S) \mapsto [0, 1]$$

is measurable if $\pi(\omega, \lambda, \mu) > 0$ *implies* $(\lambda, \mu) \in Dist(Steps(\omega\downarrow))$ *and*

$$\pi(\cdot, tr) : Paths^*(\mathcal{C}) \mapsto [0, 1]$$

are measurable for all $tr \in 2^{(R^+ \times Dist(S))}$.

Given a scheduler π a unique probability measure Pr_{π,s_0} can be defined on the σ algebra $\mathfrak{F}_{Paths^\infty(\mathcal{C})}$ by: $Pr_{\pi,s_0}(C(s_0)) = 1$ and $Pr_{\pi,s_0}(C(s_0, I_0, \cdots, s_n, I_n, s_{n+1}))$ equals:

$$\int_{\omega \in C(s_0, I_0, \cdots, s_n)} \left(\sum_{(\lambda,\mu) \in Steps(s_n)} \pi(\omega|^n, \lambda, \mu) \cdot \mu(s_{n+1}) \cdot (e^{-\lambda \cdot a} - e^{-\lambda \cdot b}) \right) (dPr_{\pi,s_0}(\omega|^n))$$

where $I_n = [a, b]$.

5.2.3 Continuous Stochastic Logic

Continuous stochastic logic (CSL) is introduced to reason about continuous-time Markov chains (102), and to reason about CTMDP later on in (37). It contains both state[1] and path formulas whose syntax is defined by the following BNFs:

$$\varphi ::= a \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid \mathcal{P}_{\bowtie p}(\psi)$$
$$\psi ::= \mathsf{X}^I\,\varphi \mid \varphi\,\mathsf{U}^I\,\varphi \mid \varphi\,\mathsf{U}^I_n\,\varphi$$

where $a \in AP$, $p \in [0,1]$, $I \subseteq [0,\infty)$ is a non-empty closed interval and $\bowtie \in \{<, \leq, \geq, >\}$. We also introduce a bounded until operator $\varphi\,\mathsf{U}^I_n\,\varphi$ a restricted version of the general until operator $\varphi\,\mathsf{U}^I\,\varphi$.

We use $s \models \varphi$ to denote that s satisfies the state formula φ while $\omega \models \psi$ denotes that ω satisfies the path formula ψ. Below we give the satisfaction relation for the state and path formulas:

$$\begin{aligned}
s &\models a \text{ iff } a \in L(s)\\
s &\models \neg\varphi \text{ iff } s \not\models \varphi\\
s &\models \varphi_1 \wedge \varphi_2 \text{ iff } s \models \varphi_1 \wedge s \models \varphi_2\\
s &\models \mathcal{P}_{\bowtie p}(\psi) \text{ iff } \forall\pi.Pr_{\pi,s_0}(\{\omega \in Paths^\infty \mid \omega \models \psi\}) \bowtie p\\
\omega &\models \mathsf{X}^I\,\varphi \text{ iff } \omega[1] \models \varphi \wedge time(\omega,0) \in I\\
\omega &\models \varphi_1\,\mathsf{U}^I\,\varphi_2 \text{ iff } \exists t \in I.(\omega@t \models \varphi_2 \wedge (\forall t' < t.\omega@t' \models \varphi_1))\\
\omega &\models \varphi_1\,\mathsf{U}^I_n\,\varphi_2 \text{ iff } \exists i \leq n \wedge t \in I.(\omega@t = \omega[i]\\
&\qquad \wedge \omega@t \models \varphi_2 \wedge (\forall t' < t.\omega@t' \models \varphi_1))
\end{aligned}$$

Logic Equivalences. We say s and r be CSL-equivalent, denoted by $s \sim_{\mathsf{CSL}} r$, if they satisfy the same set of formulas of CSL, that is, $s \models \varphi$ iff $r \models \varphi$ for all state formulas φ. Similarly for sub-logics of CSL. In the following, we let

- CSL^- denote the sub-logic of CSL without unbounded until operator,
- $\mathsf{CSL}_{\setminus \mathsf{U}_n}$ denote the sub-logic without bounded until,
- $\mathsf{CSL}_{\setminus \mathsf{X}}$ denote the sub-logic without next and bounded until, and

[1] The steady-state operator is omitted here for simplicity of presentation.

- CSL_i be the sub-logic such that all the bounded until operators are like $\varphi_1 \,\mathsf{U}_j^I\, \varphi_2$ with $j \leq i$.

The subscripts i.e. $-, \mathsf{X}, \mathsf{U}_n$, and i can be applied to CSL at the same time (for instance CSL_i^-).

5.3 Parallel Composition for CTMDPs

Compositional theory plays an extremely important role in verification, as composition based minimization and verification are effective methods for solving the state space problem. For all sub-models of CTMDPs, including CTMCs and probabilistic automata, their compositional theories have been studied extensively in the literature (32, 78, 103, 104). Surprisingly, to the best of our knowledge, the parallel operator has not been defined for CTMDPs. Indeed, thus far, CTMDPs are considered as non-compositional. In this section, we define a novel parallel composition operator for CTMDPs – directly inspired by the parallel composition for CTMCs (32). We will show that the strong and weak bisimulations we introduce are compositional w.r.t. our parallel composition.

Definition 44 (Parallel Composition)**.** *Let* $\mathcal{C}_i = (S_i, \to_i, AP_i, L_i, s_i)$ *with* $i = 1, 2$ *be two* CTMDP*s, and* $\mu_1 \parallel \mu_2$ *be a distribution such that*

$$(\mu_1 \parallel \mu_2)(s_1 \parallel s_2) = \mu_1(s_1) \cdot \mu_2(s_2).$$

The parallel composition $C_1 \parallel C_2$ *is defined by:*

$$C_1 \parallel C_2 = (S_1 \parallel S_2, \to, AP_1 \times AP_2, L, s_1 \parallel s_2)$$

where

- $S_1 \parallel S_2 = \{s \parallel s' \mid s \in S_1 \wedge s' \in S_2\}$,
- $L(s \parallel s') = L(s) \times L(s')$, *and*
- $(s \parallel s', \lambda, \mu) \in \to$ *whenever there exists* $(s, \lambda_1, \mu_1) \in \to_1$ *and* $(s', \lambda_2, \mu_2) \in \to_2$ *such that* $\lambda = \lambda_1 + \lambda_2$ *and*

$$\mu = \frac{\lambda_1}{\lambda} \cdot (\mu_1 \parallel \delta_{s'}) + \frac{\lambda_2}{\lambda} \cdot (\delta_s \parallel \mu_2).$$

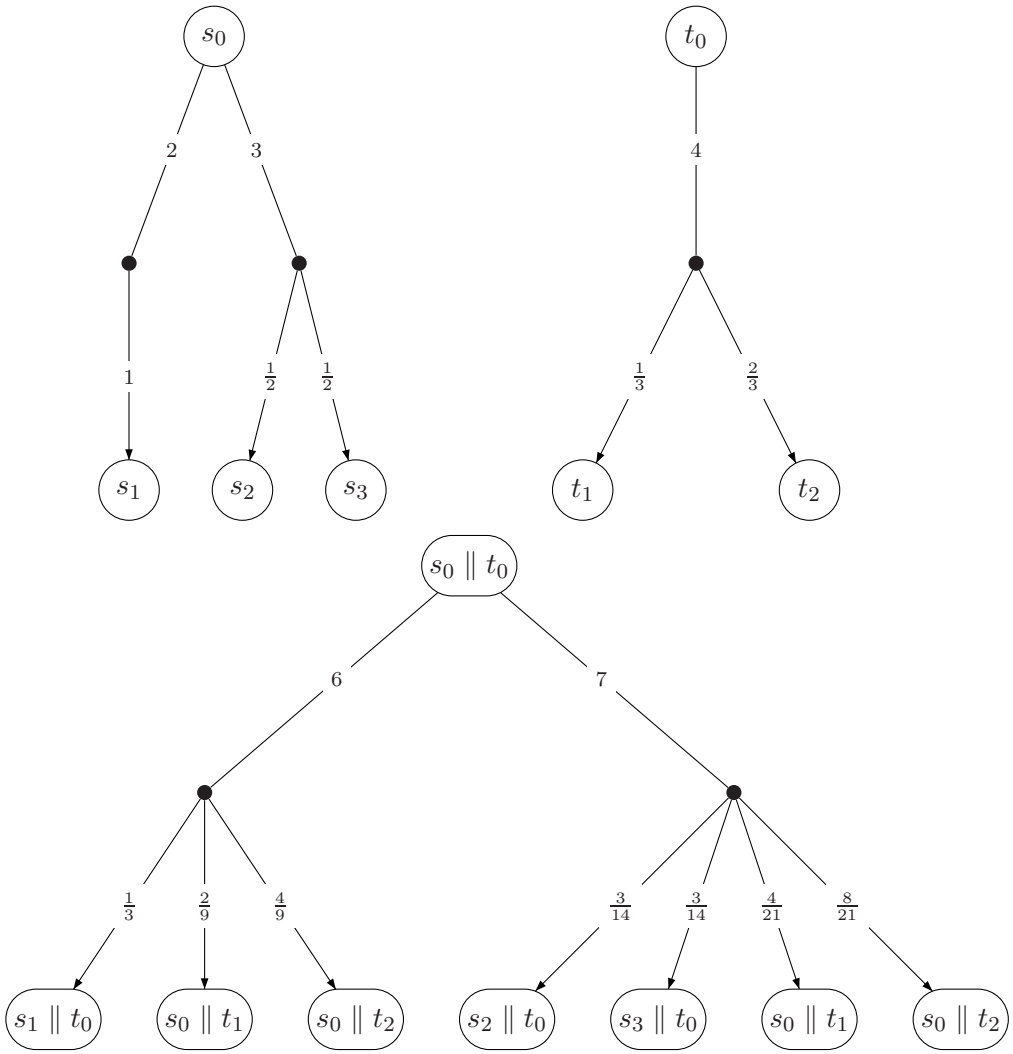

Figure 5.1: Parallel composition of s_0 and t_0.

In Definition 44 we have not considered labels of the transitions, but the composition operator can be easily extended to deal with labels in a standard way. The following example illustrates how the composition operator works.

Example 44. *Given two processes s_0 and t_0 as in Fig. 5.1 (a) and (b) respectively, where s_0 has two non-deterministic transitions labeled with 2 and 3, and t_0 only has one transition with rate 4, then the parallel composition $s_0 \parallel t_0$ of s_0 and t_0 according to Definition 44 is described as in Fig. 5.1 (c).*

Discussion. The parallel composition is inspired by the parallel operator introduced for CTMCs in (32). The extension is conservative, i.e., restricting to CTMCs, our parallel composition agrees with that for CTMCs. The parallel operator have been extended for both interactive Markov chains (IMCs) in (32) and Markov Automata (MAs) (104). In both IMCs and MAs, for each state at most one transition is labeled with Markovian rate $s \xrightarrow{\lambda} \mu$, that is, *no nondeterministic choices* between Markovian transitions are allowed. But nondeterministic choices between transitions labeled with actions are allowed.

Transformation between IMCs, CTMDPs and MAs have been studied in (105), which allows techniques developed for one model to be exploited in the others, see for example (96, 98). However, similar to the discrete setting (90), such transformation does not preserve bisimulation relations that shall be introduced in the next section.

5.4 Bisimulations for CTMDPs

5.4.1 Strong Bisimulation

In this section we recall the notion of strong bisimulation for CTMDPs, introduced in (37), where $s \xrightarrow{\lambda}_{\mathsf{P}} \mu$ iff there exists $\{s \xrightarrow{\lambda} \mu_i\}_{i\in I}$ and $\{p_i\}_{i\in I}$ such that $p_i \in (0,1]$ for each $i \in I$, $\sum_{i\in I} p_i = 1$, and $\sum_{i\in I} p_i \cdot \mu_i = \mu$. We assume that there is a given CTMDP $\mathcal{C} = (S, \to, AP, L, s_0)$ throughout this chapter in the following.

Definition 45 (Strong Bisimulation)**.** *Let $\mathcal{R} \subseteq S \times S$ be an equivalence relation. $\mathcal{R}$ is a strong bisimulation if $s\ \mathcal{R}\ r$ implies that $L(s) = L(r)$ and for each $s \xrightarrow{\lambda} \mu$, there exists $r \xrightarrow{\lambda}_{\mathsf{P}} \mu'$ such that $\mu\ \mathcal{R}\ \mu'$.*

We write $s \sim r$ whenever there exists a strong bisimulation $\mathcal{R}$ such that $s\ \mathcal{R}\ r$.

The above bisimulation relation is slightly coarser than the one considered in (37), where $r \xrightarrow{\lambda}_{\mathsf{P}} \mu'$ is replaced by strong transition $r \xrightarrow{\lambda} \mu'$. The idea of combining transitions with the same exit rate is borrowed from (1). The theorem shows that strong bisimulation is sound, but not complete for CSL equivalence:

Theorem 36 ((37))**.** $\sim\ \subset\ \sim_{\mathsf{CSL}}$.

Note the proof in (37) can be directly adapted to our slightly more general strong bisimulation. The inclusion is sound but not complete which is illustrated below:

Example 45. *Suppose that we have two states s and r such that s can evolve into s_1 either with rate 3 or 5 while r can evolve into s_1 with rate 3, 4, or 5. Also we assume that $L(s) = L(r)$ and s_1 is an absorbing state with $L(s_1) \neq L(s)$. It is easy to see that s and r are* CSL*-equivalent, but they are not strongly bisimilar.*

In Example 45 $s \sim r$ would hold if one allows combining transitions with different exit rates, but unfortunately this does not work generally, refer to Example 46.

Example 46. *Suppose that we let $s \xrightarrow{\lambda}_{\mathsf{P}} \mu$ iff there exists $\{s \xrightarrow{\lambda_i} \mu_i\}_{i\in I}$ and $\{p_i\}_{i\in I}$ such that $\sum_{i\in I} p_i = 1$, $\sum_{i\in I} p_i \cdot \lambda_i = \lambda$ and $\sum_{i\in I} p_i \cdot \mu_i = \mu$. Given two states s and r such that*

$$s \xrightarrow{3} \mu_1, s \xrightarrow{4} \mu_2, s \xrightarrow{5} \mu_3$$
$$r \xrightarrow{3} \mu_1, r \xrightarrow{5} \mu_3$$

where

$$\mu_1(s_1) = 0.3, \mu_1(s_2) = 0.7$$
$$\mu_2(s_1) = 0.4, \mu_2(s_2) = 0.6$$
$$\mu_3(s_1) = 0.5, \mu_3(s_2) = 0.5$$

For simplicity again we assume that s_1, s_2, and s_3 are absorbing states and all the states have different atomic propositions except $L(s) = L(r)$, then s and r should be bisimilar. But there exists a formula φ such that $r \models \varphi$ and $s \not\models \varphi$. For instance let $\psi = \mathsf{X}^I\, s_1$ with $I = [a, \infty)$, then the maximum probability of the paths starting from s satisfying ψ is

$$\max\{0.3 \cdot e^{-3a}, 0.4 \cdot e^{-4a}, 0.5 \cdot e^{-5a}\}.$$

If $e^{-a} \in (\frac{3}{4}, \frac{4}{5})$, then maximum probability is $0.4 \cdot e^{-4a}$ which is obviously greater than the maximum probability of the paths of r satisfying ψ.

Below we show that the bisimulation relation is a congruence w.r.t. the parallel operator we introduced in Section 5.3:

Theorem 37. *$s \sim r$ implies that $s \parallel t \sim r \parallel t$ for any t.*

Proof. Let

$$\mathcal{R} = \{(s \parallel t, r \parallel t) \mid s \sim r\},$$

it is enough to show that $\mathcal{R}$ is a strong bisimulation. Suppose that $(s \parallel t)\ \mathcal{R}\ (r \parallel t)$, and $s \parallel t \xrightarrow{\lambda} \mu$. By Definition 44 there exists $s \xrightarrow{\lambda_1} \mu_1$ and $t \xrightarrow{\lambda_2} \nu$ such that $\lambda = \lambda_1 + \lambda_2$ and

$$\mu = \frac{\lambda_1}{\lambda} \cdot (\mu_1 \parallel \delta_t) + \frac{\lambda_2}{\lambda} \cdot (\delta_s \parallel \nu).$$

Since $s \sim r$, there exists $r \xrightarrow{\lambda_1}_{\mathsf{P}} \mu_1'$ such that $\mu_1 \sim \mu_1'$, thus

$$(\mu_1 \parallel \delta_t) \mathcal{R} (\mu_1' \parallel \delta_t) \text{ and } (\delta_s \parallel \nu) \mathcal{R} (\delta_r \parallel \nu).$$

As a result there exists

$$r \parallel t \xrightarrow{\lambda}_{\mathsf{P}} \mu' \equiv \frac{\lambda_1}{\lambda} \cdot (\mu_1' \parallel \delta_t) + \frac{\lambda_2}{\lambda} \cdot (\delta_r \parallel \nu),$$

so $\mu \mathcal{R} \mu'$ which completes the proof. □

5.4.2 Weak Bisimulation

In this section we will introduce a novel notion of *weak bisimulation* for CTMDPs in the sense that it only preserves $\mathsf{CSL}_{\setminus \mathsf{X}}$ equivalence. Our definition of weak bisimulation is directly motivated by the two examples in the previous section, together with the well-known fact that uniformization does not alter reachabilities for CTMDPs (96, 98, 100). Even though we have seen that strong bisimulation is sound but not complete w.r.t. CSL equivalence, we can show that the two relations do agree on a subclass of uniformized CTMDPs. As a result, the weak bisimulation is both sound and complete for the sub-logic $\mathsf{CSL}_{\setminus \mathsf{X}}$ for the same subclass of CTMDPs (not necessarily uniformed). The section ends up with a discussion about why the results do not hold for general CTMDPs, and motivates the study of a sequence of bisimulations in next section.

Below follows the definition of weak bisimulation.

Definition 46 (Weak bisimulation)**.** *We say that states s and r are weakly bisimilar, denoted by $s \approx r$, whenever $\bar{s} \sim \bar{r}$ in the uniformized* CTMDP $\bar{\mathcal{C}}$.

Our weak bisimulation is a conservative extension of strong bisimulation. The following lemma establishes a few properties:

Lemma 28. *1. $\sim \subseteq \approx$,*

2. for uniformized CTMDP*, $\sim = \approx$.*

3. $s \sim_{\mathsf{CSL}_{\setminus \mathsf{X}}} r$ in $\mathcal{C}$ iff $s \sim_{\mathsf{CSL}} r$ in $\bar{\mathcal{C}}$.

Proof. To show that $\sim$ implies $\approx$, we observe that for each $s \xrightarrow{\lambda} \mu$, we have

$$\bar{s} \xrightarrow{E} (\frac{E - \lambda}{E} \cdot \delta_s + \frac{\lambda}{E} \cdot \mu),$$

similar for $s \xrightarrow{\lambda}_{\mathsf{P}} \mu$. The following proof is trivial.

The proof of Clause 2 is straightforward from Definition 46.

We first prove that if $\mathcal{C}$ is a CTMC, then $s \sim_{\mathsf{CSL}_{\setminus \mathsf{X}}} r$ in $\mathcal{C}$ iff $s \sim_{\mathsf{CSL}} r$ in $\bar{\mathcal{C}}$. Since uniformization preserves the satisfiability of $\mathsf{CSL}_{\setminus \mathsf{X}}$, thus $\bar{s} \sim_{\mathsf{CSL}_{\setminus \mathsf{X}}} \bar{r}$. Let

$$\mathcal{R} = \{(\bar{s}, \bar{r}) \mid \bar{s} \sim_{\mathsf{CSL}_{\setminus \mathsf{X}}} \bar{r}\},$$

we first prove that $\mathcal{R}$ is a strong bisimulation. Let λ denote the exit rate of $\bar{s}$ and $\bar{r}$, and $\lambda_{\bar{s}}$ denote the rate from $\bar{s}$ to states in $[\bar{s}]_{\mathcal{R}}$ i.e. $\bar{s} \xrightarrow{\lambda} \mu$ and $\lambda_{\bar{s}} = \lambda \cdot \mu([\bar{s}]_{\mathcal{R}})$, where $[\bar{s}]_{\mathcal{R}} = \{\bar{s} \mid \bar{s}\ \mathcal{R}\ \bar{r}\}$ is the equivalence class of $\mathcal{R}$ containing $\bar{s}$. The case when $\lambda_{\bar{s}} = \lambda$ is trivial, we assume that $\lambda > \lambda_{\bar{s}}$, then for each $C \in \bar{S}/\mathcal{R}$ such that $\bar{s} \notin C$, the probability of the path of $\bar{s}$ satisfying $\varphi_{\bar{s}}\, \mathsf{U}^{[a,b]}\, \varphi_C$ is equal to

$$\frac{\lambda_C}{\lambda - \lambda_{\bar{s}}} \cdot (e^{-\lambda_C \cdot a} - e^{-\lambda_C \cdot b})$$

where $\lambda_C = \lambda \cdot \mu(C)$. Since $\bar{s} \sim_{\mathsf{CSL}_{\setminus \mathsf{X}}} \bar{r}$, it must be the case such that $\bar{r} \xrightarrow{\lambda} \nu$ with $\mu(C) = \nu(C)$ i.e. $\mu\ \mathcal{R}\ \nu$, thus $\mathcal{R}$ is a strong bisimulation. According to (54), $\bar{s} \sim_{\mathsf{CSL}} \bar{r}$.

We now generalize the result to CTMDP. If $s \sim_{\mathsf{CSL}_{\setminus \mathsf{X}}} r$, then $\bar{s} \sim_{\mathsf{CSL}_{\setminus \mathsf{X}}} \bar{r}$. Since in a uniformized CTMDP, every execution of $\mathcal{C}$ guided by a given scheduler can be seen as a CTMC, thus $\bar{s} \sim_{\mathsf{CSL}} \bar{r}$ based on the above result. □

Now we shall show that, different from the strong bisimulation, $\approx$ coincides with $\sim_{\mathsf{CSL}_{\setminus \mathsf{X}}}$ in a subclass of CTMDPs, which is defined in the following.

Definition 47 (2-step Recurrent)**.** *Let $\mathcal{R}$ be an equivalence relation on S. A state s is said to be* 2-step recurrent *w.r.t. $\mathcal{R}$ iff s is not absorbing, and moreover $|Suc(s)| > 2$ and*

$$\exists(s \xrightarrow{\lambda} \mu).(\exists(s' \in Supp(\mu)).(\forall(s' \xrightarrow{\lambda'} \nu).\nu(C) = 1))$$

where $C = (\cup_{t \in Supp(\mu)}[t]_{\mathcal{R}}) \cup [s]_{\mathcal{R}}$. We say $\mathcal{C}$ is 2-step recurrent *w.r.t. $\mathcal{R}$, iff there exists a state $s \in S$ which is 2-step recurrent w.r.t. $\mathcal{R}$.*

The non 2-step recurrent states can be seen as an extension of the well-known *non-absorbing states*, those that can evolve into other equivalence classes. Non 2-step recurrent states extend non-absorbing states further by excluding those non-absorbing states that can evolve into other equivalence classes only through their parent and the parents' equivalent states. Moreover, we say that s (or $\mathcal{C}$) is *2-step recurrent* iff it is 2-step recurrent w.r.t. $\sim_{\mathsf{CSL}_{\setminus \mathsf{X}}}$. Intuitively, the term 2-step recurrent requires that s

has more than 2 successors and there exists a transition $s \to \mu$ such that some states in $Supp(\mu)$ must only return back to states equivalent to s or states in $Supp(\mu)$ directly. We show below $\approx$ coincides with $\mathsf{CSL}_{\setminus \mathsf{X}}$ for CTMDPs without 2-step recurrent states.

Theorem 38. $\approx \subseteq \sim_{\mathsf{CSL}_{\setminus \mathsf{X}}}$. *If $\mathcal{C}$ is not 2-step recurrent,* $\approx = \sim_{\mathsf{CSL}_{\setminus \mathsf{X}}}$.

Proof. In the following the parameter E will be omitted in the transition, i.e. we simply write $s \to \mu$ for $s \xrightarrow{E} \mu$.

First we show that $\approx \subseteq \sim_{\mathsf{CSL}_{\setminus \mathsf{X}}}$. Let $\mathcal{C}$ be a CTMDP and assume $s \approx r$. By the definition of weak bisimulation, we have $s \approx r$ in $\bar{\mathcal{C}}$. By Theorem 36, $s \sim_{\mathsf{CSL}} r$ in $\bar{\mathcal{C}}$. Applying the third claus of Lemma 28, it holds that $s \sim_{\mathsf{CSL}_{\setminus \mathsf{X}}} r$ in $\mathcal{C}$.

Now we prove that $\sim_{\mathsf{CSL}_{\setminus \mathsf{X}}}$ implies $\approx$ whenever $\mathcal{C}$ is not 2-step recurrent. By definition, it is the same to prove that $\sim_{\mathsf{CSL}}$ implies $\sim$ in a uniformized CTMDP. In the following we assume that the given CTMDP is uniformized and assume that the rate is equal to 1 for simplicity without losing generality. Let

$$\mathcal{R} = \{(s, r) \mid s \ \sim_{\mathsf{CSL}} \ r\}$$

which is obviously an equivalence relation, we are going to show that $\mathcal{R}$ is a strong bisimulation. By contradiction we assume that $\mathcal{R}$ is not a strong bisimulation, then there exists $(s, r) \in \mathcal{R}$ such that either i) $L(s) \neq L(r)$, or ii) there exists a $s \to \mu$ such that there does not exist $r \to_{\mathsf{P}} \nu$ with $\mu \ \mathcal{R} \ \nu$. In both cases, if we can find a formula φ such that $s \models \varphi$ but $r \not\models \varphi$ or the other way around, then we can obtain a contradiction. Case i) is easy and we only focus on ii) here. Suppose there exists a transition $s \to \mu$, since $\mathcal{C}$ is not 2-step recurrent, there are three different cases to consider.

1. $s_\perp$ i.e. s is an absorbing state. This case is trivial since all the derivations of s will stay in the same equivalence class $[s]_{\mathcal{R}}$.

2. $Suc(s) \leq 2$ i.e. there exists at most two equivalence [1]classes $C_1, C_2 \in S/\mathcal{R}$ such that $\mu(C_1 \cup C_2) = 1$, in the other words, $\mu(C_1) = 1 - \mu(C_2)$. The reason to consider this special case is that for each μ, if there exists μ_1 and μ_2 such that $\mu_1(C_1) \leq \mu(C_1) \leq \mu_2(C_1)$, then we can make sure that there exists w_1, w_2 such that $w_1 + w_2 = 1$ and $w_1 \cdot \mu_1(C_1) + w_2 \cdot \mu_2(C_1) = \mu(C_1)$, therefore

$$\begin{aligned} & w_1 \cdot \mu_1(C_2) + w_2 \cdot \mu_2(C_2) \\ &= w_1 \cdot (1 - \mu_1(C_1)) + w_2 \cdot (1 - \mu_2(C_1)) \\ &= w_1 + w_2 - (w_1 \cdot \mu_1(C_1) + w_2 \cdot \mu_2(C_1)) \\ &= 1 - \mu(C_1) = \mu(C_2) \end{aligned}$$

[1]The $Sucs = 1$ can be covered by taking $C_2 = \emptyset$ in the proof.

thus $(w_1 \cdot \mu_1 + w_2 \cdot \mu_2) = \mu$ as we expect. This cannot be generalized to the case where $Suc(s) > 2$.

Let φ_C be the master formula of an equivalence class $C \in S/\mathcal{R}$ such that $Sat(\varphi_C) = C$. Since $s \sim_{\mathsf{CSL}} r$, and

$$s \models P_{\geq 1}(\mathsf{X}^{[0,\infty)}(\varphi_{C_1} \vee \varphi_{C_2}))$$

obviously, thus

$$r \models P_{\geq 1}(\mathsf{X}^{[0,\infty)}(\varphi_{C_1} \vee \varphi_{C_2})),$$

that is, $Suc(r) \subseteq C_1 \cup C_2$ which means r can only move to states in $C_1 \cup C_2$ too. Secondly, we prove that there exists $r \to \nu_1$ and $r \to \nu_2$ such that $\nu_1(C_1) \leq \mu(C_1) \leq \nu_2(C_1)$. Assume there does not exists $r \to \nu_2$ such that $\nu_2(C_1) \geq \mu(C_1)$, in the other words, for all $r \to \nu$ we have $\nu(C_1) < \mu(C_1)$, so there exists q such that

$$r \models P_{\leq q}(\mathsf{X}^{[0,\infty)}\, \varphi_{C_1}) \text{ but } \not\models P_{\leq q}(\mathsf{X}^{[0,\infty)}\, \varphi_{C_1})$$

which contradicts with the assumption that $s \sim_{\mathsf{CSL}} r$. Similarly, we can show that there exists $r \to \nu_1$ such that $\nu_1(C_1) \leq \mu(C_1)$. Based on the discussion above, we can guarantee that there always exists w_1 and w_2 such that $w_1 + w_2 = 1$ and

$$(w_1 \cdot \nu_1 + w_2 \cdot \nu_2)\ \mathcal{R}\ \mu.$$

3. We consider the – most involved – remaining case: $Suc(s) > 2$ and for all $s' \in Supp(\mu)$, there exists t and $s' \to \mu'$ such that $\mu'(t) > 0$ where t is in a different equivalence class from which s and the states in $Supp(\mu)$ belong to.

   We prove by contraction. Assume that there does not exists $r \to_{\mathsf{P}} \nu$ such that $\mu\ \mathcal{R}\ \nu$. Note every combined transition of r can be seen as a combined transition of two other combined transitions of r. We fix two arbitrarily fixed (combined) transitions of r: $r \to_{\mathsf{P}} \nu_1$ and $r \to_{\mathsf{P}} \nu_2$, thus

$$\forall 0 \leq w_1, w_2 \leq 1.(w_1 + w_2 = 1 \wedge (\mu, w_1 \cdot \nu_1 + w_2 \cdot \nu_2) \notin \mathcal{R}) \tag{5.1}$$

   Let $Supp(\mu) = \{s_1, s_2, \ldots, s_n\}$. For simplicity we assume that $s_1, \ldots, s_n$ belong to different equivalence classes. For $1 \leq i \leq n$, define:

$$\mu(s_i) = a_i, \nu_1(s_i) = b_i, \qquad \text{and } \nu_2(s_i) = c_i\ .$$

   Then there must exist $1 \leq k \neq j \leq n$ such that there does not exist $0 \leq w_1, w_2 \leq 1$ with $w_1 + w_2 = 1$ such that

$$w_1 \cdot b_k + w_2 \cdot c_k = a_k \text{ and } w_1 \cdot b_j + w_2 \cdot c_j = a_j,$$

otherwise $(\mu, (w_1\nu_1 + w_2\nu_2)) \in \mathcal{R}$ which contradicts Eq. 5.1. The idea now is then to construct a formula φ which is satisfied by s but not r, depending on the relation between a_k, a_j and b_k, c_k, b_j, c_j. There are nine possible cases in total depending on whether $a_k \in [b_k, c_k]$ and/or $a_j \in [b_j, c_j]$. Most of the cases are trivial except when $a_k \in [b_k, c_k]$ and $a_j \in [c_j, b_j]$ with $c_k \geq b_k$ and $b_j \geq c_j$. [1] The formula for this case is given by:

$$\varphi = (r \vee s \vee s_k)\, \mathsf{U}^{[a,b]} (s_j \vee s'_k)$$

where s'_k is the successor of s_k not equivalent to s and the states in $Supp(\mu)$, and the names of states are used as the abbreviations of the state formulas characterizing the equivalence classes where they are located. Suppose there exists $s_k \to \mu_k$ with $\mu_k(s'_k) = \rho$, and define:

$$\rho_1 = \rho \cdot (a \cdot e^{-a} + e^{-a} - b \cdot e^{-b} - e^{-b})$$
$$\rho_2 = e^{-a} - e^{-b}$$

then

- the probability of s satisfying φ by choosing transitions $s \to \mu$ and $s_k \to \mu_k$ is equal to
$$p(s, \mu) := a_j \cdot \rho_2 + a_k \cdot \rho_1$$
- the probability of r satisfying φ by choosing the combined transition of $r \to \nu_1$ and $r \to \nu_1$ and $s_k \to \mu_k$ is either
$$p(r, \nu_1) := b_j \cdot \rho_2 + b_k \cdot \rho_1$$
or
$$p(r, \nu_2) = c_j \cdot \rho_2 + c_k \cdot \rho_1.$$

Now it is sufficient to prove that we can find $0 \leq a \leq b$ such that $p(s, \mu) > p(r, \nu_1)$ and $p(s, \mu) > p(r, \nu_2)$. We claim [2] that it is the case once we can guarantee

$$\frac{\rho_1}{\rho_2} \in (\frac{b_j - a_j}{a_k - b_k}, \frac{a_j - c_j}{c_k - a_k}),$$

which can be seen as follows:

[1] For instance if $a_k > b_k, c_k$, s will evolve into s_k with higher probability than r, so φ is easy to give.

[2] By solving two equations:$a_k \cdot \rho_1 + a_j \cdot \rho_2 > b_k \cdot \rho_1 + b_j \cdot \rho_2$, and $a_k \cdot \rho_1 + a_j \cdot \rho_2 > c_k \cdot \rho_1 + c_j \cdot \rho_2$, such ρ_1 and ρ_2 always exists due to that there does not exists w_1, w_2 such that $w_1 \cdot b_k + w_2 \cdot c_k = a_k$ and $w_1 \cdot b_j + w_2 \cdot c_j = a_j$.

- Let $b = \infty$, then $\frac{\rho_1}{\rho_2} = \rho \cdot (a+1)$ and it is easy to see that there exists a, b such that $\frac{\rho_1}{\rho_2} \in [\rho, \infty)$.
- On the other hand let $a = 0$, then

$$\rho_1 = \rho \cdot (1 - e^{-b} - b \cdot e^{-b})$$

and $\rho_2 = 1 - e^{-b}$, so

$$\frac{\rho_1}{\rho_2} = \rho \cdot (1 - \frac{b \cdot e^{-b}}{1 - e^{-b}}),$$

note here that $\frac{b \cdot e^{-b}}{1-e^{-b}} \in (0,1)$ since $\frac{b \cdot e^{-b}}{1-e^{-b}}$ can be arbitrary close to 1 when b is close to 0, and on the other hand, $\frac{b \cdot e^{-b}}{1-e^{-b}}$ is arbitrary close to 0 as b increases. As a result $\frac{\rho_1}{\rho_2} \in (0, \rho)$.

- it is not possible for

$$\frac{b_j - a_j}{a_k - b_k} = \frac{a_j - c_j}{c_k - a_k},$$

otherwise there exists $0 \leq w_1, w_2 \leq 1$ such that

$$w_1 \cdot b_k + w_2 \cdot c_k = a_k \text{ and } w_1 \cdot b_j + w_2 \cdot c_j = a_j$$

with $w_1 + w_2 = 1$.

Thus there always exists $0 \leq a \leq b$ such that s will satisfy φ with higher probability than r for some a, b, therefore $s \not\sim_{\mathsf{CSL}} r$, and we have a contradiction. All the other cases are similar and omitted here.

□

In the proof we only need to use unbounded until, $\wedge$ (to construct the master formula of each equivalence class), and $\vee$. Thus, the following sub-logic is sufficient to characterize weak bisimulation for CTMDPs which are not 2-step recurrent:

$$\varphi ::= a \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \mathcal{P}_{\bowtie p}(\psi)$$
$$\psi ::= \varphi \, \mathsf{U}^I \, \varphi$$

Below we show that, as for strong bisimulations, the weak bisimulation relation is a congruence w.r.t. the parallel operator we introduced in Section 5.3. Moreover, for CTMDPs which are not 2-step recurrent, $\sim_{\mathsf{CSL}_{\setminus \mathsf{X}}}$ is a congruence as well.

Theorem 39. *1. $s \approx r$ implies that $s \parallel t \approx r \parallel t$ for any t.*

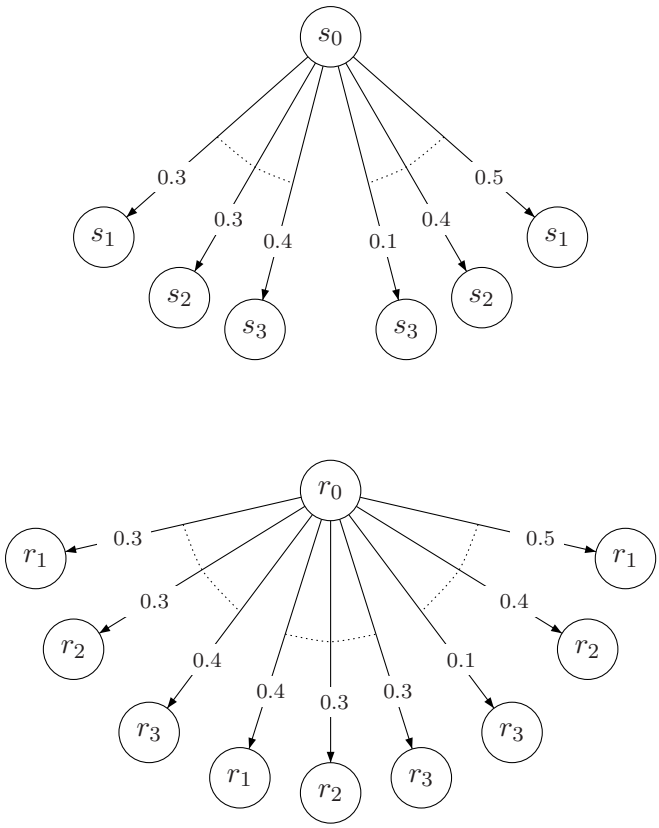

Figure 5.2: Counter example of strong probabilistic bisimulation.

2. *if $\mathcal{C}$ is not 2-step recurrent, $s \sim_{\mathsf{CSL}_{\setminus \mathsf{X}}} r$ implies that $s \parallel t \sim_{\mathsf{CSL}_{\setminus \mathsf{X}}} r \parallel t$ for any t.*

Proof. We prove Clause 1 first. Since $s \approx r$, by Definition 46 $\bar{s} \sim \bar{r}$. According to Theorem 37 $\bar{s} \parallel \bar{t} \sim \bar{r} \parallel \bar{t}$ for any t. It is easy to check that $\bar{s} \parallel \bar{t} = \overline{s \parallel t}$, as a result $\overline{s \parallel t} \sim \overline{r \parallel t}$ which implies that $s \parallel t \approx r \parallel t$ for any t.

The proof of Clause 2 is straightforward based on Clause 1. □

General CTMDPs. The following example explains the necessity to consider CTMDPs without 2-step recurrent states in Theorem 38. It is shown that when 2-step recurrent states are involved, $\sim_{\mathsf{CSL}_{\setminus \mathsf{X}}} \subseteq \approx$ does not always hold.

Example 47. *Suppose we are given two states s_0 and r_0 of a CTMDP depicted in Fig. 5.2.*

First assume s_i and r_i are absorbing states for each $1 \leq i \leq 3$. In this case, it is easy to check that s_0 and r_0 are 2-step recurrent states where all the states have different

atomic propositions except $L(s_i) = L(r_i)$ *for each* $0 \leq i \leq 3$. [1] *Then there does not exist a* CSL *formula which can distinguish them, as a result they are* CSL *equivalent. On the other hand,* s_0 *and* r_0 *are not bisimilar, as for the middle transition of* r_0, s_0 *has no way to simulate it even with combined transition.*

Now suppose that s_2 *and* r_2 *are not absorbing, for instance they can evolve into* s_0 *and* r_0 *with probability 1 respectively, then still they are* CSL *equivalent. But interestingly, if the non-absorbing states are* s_3 *and* r_3 *instead but with the same transitions, then* $s_0 \not\sim_{\mathsf{CSL}} r_0$. *Considering the formula*

$$\psi = (L(s_0) \vee L(s_3))\, \mathsf{U}^{[0,\infty)}\, L(s_1),$$

the maximum probability of the paths of s_0 *satisfying* ψ *is* $\frac{5}{9}$ *while this probability in* r_0 *is* $\frac{4}{7} > \frac{5}{9}$, *thus* $s_0 \models P_{\leq \frac{5}{9}}\psi$ *but* $r_0 \not\models P_{\leq \frac{5}{9}}\psi$. *Note that even we let* s_2 *and* s_3 *have such transition,* s_0 *and* r_0 *are still 2-step recurrent by Definition 47.*

The key idea behind the difference illustrated in Example 47 is that the bisimulation relation only takes one step into consideration. This restriction might be the best one can hope for the completeness results.

5.4.3 Determining 2-step Recurrent CTMDPs

In Theorem 38, the completeness holds only for CTMDPs which are not 2-step recurrent. This section discusses a simple procedure for checking it. The following lemma holds by applying the definition directly:

Lemma 29. *Given two equivalence relations* $\mathcal{R}$ *and* $\mathcal{R}'$ *over* S *such that* $\mathcal{R} \subseteq \mathcal{R}'$, *then if* $\mathcal{C}$ *is 2-step recurrent w.r.t.* $\mathcal{R}$, *then it is 2-step recurrent w.r.t.* $\mathcal{R}'$, *or equivalently if* $\mathcal{C}$ *is not 2-step recurrent w.r.t.* $\mathcal{R}'$, *then it is not 2-step recurrent w.r.t.* $\mathcal{R}$.

Proof. Straightforward from Definition 47 and the fact the $[s]_{\mathcal{R}} \subseteq [s]_{\mathcal{R}'}$ provided that $\mathcal{R} \subseteq \mathcal{R}'$. □

Lemma 29 suggests a simple way to check whether a given CTMDP $\mathcal{C}$ is 2-step recurrent w.r.t. $\sim_{\mathsf{CSL}_{\setminus \mathsf{X}}}$. We know that

$$\sim \subset \approx \subseteq \sim_{\mathsf{CSL}_{\setminus \mathsf{X}}} \subseteq \mathcal{R},$$

where

$$\mathcal{R} = \{(s, r) \mid L(s) = L(r)\}.$$

[1] Assume that $\mathcal{R} = \{(s, r) \mid L(s) = L(r)\}$, and same for the following examples.

By Lemma 29, we can first check whether $\mathcal{C}$ is 2-step recurrent w.r.t. $\mathcal{R}$, if it is not, we know that $\mathcal{C}$ is not 2-step recurrent either w.r.t. $\sim_{\mathsf{CSL}_{\setminus \mathsf{X}}}$. Otherwise we continue to check whether $\mathcal{C}$ is 2-step recurrent w.r.t. $\sim$ or $\approx$, if the answer is yes, then $\mathcal{C}$ is 2-step recurrent too w.r.t. $\sim_{\mathsf{CSL}_{\setminus \mathsf{X}}}$. Both $\sim$ and $\approx$ can be computed in polynomial time, see (106) for detail.

In the remaining cases, namely when $\mathcal{C}$ is 2-step recurrent w.r.t. $\approx$, but not w.r.t. $\mathcal{R}$, we cannot conclude anything, thus the relation $\sim_{\mathsf{CSL}_{\setminus \mathsf{X}}}$ shall be computed first for this purpose. The decision algorithm for $\sim_{\mathsf{CSL}_{\setminus \mathsf{X}}}$ falls, however, out of the scope of this dissertation.

5.5 Characterization of CSL in General CTMDPs

In (99) we have defined a sequence of strong bisimulations to characterize probabilistic CTL (PCTL) as well as its sub-logics. Following that approach, in this section we show that such strong bisimulations can be used to characterize CSL and its sub-logics as well, for general CTMDPs.

5.5.1 Strong i-depth Bisimulation

For the interval $I = [a, b]$, define $I \ominus x = [a - x, b - x]$ if $a \geq x$, and $I \ominus x = [0, b - x]$ if $a < x \leq b$. First, we define the notation $Prob_{\pi,s}(C, C', n, I, \omega)$, denoting the probability of reaching C', from state s, via only states in C within time in the interval $I \subseteq [0, \infty)$ and in at most n steps under scheduler π, where ω is used to keep track of the path. Formally, $p = Prob_{\pi,s}(C, C', n, [a, b], \omega)$ is defined as follows:

1. if $(n = 0) \wedge (a = 0) \wedge (s \in C')$, p is equal to 1

2. else if $(s \in C \wedge s \notin C') \wedge (n > 0)$, p is equal to

$$\sum_{(\lambda,\mu)\in Steps(\omega\downarrow)} \pi(\omega, \lambda, \mu) \cdot \Big(\int_0^b \lambda \cdot e^{-\lambda x} \cdot \sum_{s'\in Supp(\mu)} \mu(s') \cdot Prob_{\pi,s'}(C, C', n-1, [a, b] \ominus x, \omega\frown(x, s'))dx \Big),$$

3. else if $(s \in C \cap C') \wedge (n > 0)$, p is equal to

$$\sum_{(\lambda,\mu)\in Steps(\omega\downarrow)} \pi(\omega,\lambda,\mu) \cdot \Big(e^{-\lambda a} + \int_0^a \lambda \cdot e^{-\lambda x} \cdot \sum_{s'\in Supp(\mu)} \mu(s') \cdot Prob_{\pi,s'}(C, C', n-1, [a,b] \ominus x, \omega\frown(x,s'))dx\Big),$$

4. otherwise p is equal to 0.

The above definition has the same flavor as the definitions in (37, 102) – extended with bounds on the discrete steps. The first clause is trivial. For the second clause, $s \in C \wedge s \notin C'$ and we have still steps $n > 0$. The term $\pi(\omega, \lambda, \mu)$ denotes the probability that the pair (λ, μ) is chosen by the scheduler π under consideration. Further, $\lambda \cdot e^{-\lambda x}$ is the density of leaving s at time x. Once s is left, the successor s' is taken with probability $\mu(s')$, from which we have $n-1$ steps and $[a,b] \ominus x$ time left. The path is then augmented with the pair (x, s'). For the third clause with $(s \in C \cap C') \wedge (n > 0)$, either we stay in state s more than a time units with probability

$$\int_a^\infty \lambda \cdot e^{-\lambda x} dx = e^{-\lambda a},$$

otherwise we should continue, and the argument is the same as the previous case. For all the other cases, it is obvious that the result equals 0. Below follows the definition of strong i-depth bisimulation where $s \sim_0 r$ iff $L(s) = L(r)$:

Definition 48 (Strong i-depth Bisimulation)**.** *A relation $\mathcal{R} \subseteq S \times S$ is a strong i-depth bisimulation with $i > 0$ if $s\ \mathcal{R}\ r$ implies $s \sim_{i-1} r$ and for any $\mathcal{R}$ downward closed sets C, C' and I,*

1. *for each scheduler π, there exists a scheduler π' such that*

$$Prob_{\pi',r}(C, C', i, I, r) \leq Prob_{\pi,s}(C, C', i, I, s),$$

2. *for each scheduler π, there exists a scheduler π' such that*

$$Prob_{\pi',s}(C, C', i, I, s) \leq Prob_{\pi,r}(C, C', i, I, r).$$

We write $s \sim_i r$ whenever there is a strong i-depth bisimulation $\mathcal{R}$ such that $s\ \mathcal{R}\ r$.

It is not hard to show that $\sim_i$ is an equivalence relation.

Lemma 30. *$\sim_i$ is an equivalence relation for all $i \geq 0$.*

Proof. The reflexivity and symmetry are easy to show, we only prove the transitivity here. Suppose that $s \sim_i t$ and $t \sim_i r$, we should prove that $s \sim_i r$. By Definition 48 there exists two strong i-depth bisimulation $\mathcal{R}_1$ and $\mathcal{R}_2$ such that $s\ \mathcal{R}_1\ t$ and $t\ \mathcal{R}_2\ r$. Let

$$\mathcal{R} = \mathcal{R}_1 \circ \mathcal{R}_2 = \{(s_1, s_3) \mid \exists s_2.(s_1\ \mathcal{R}_1\ s_2 \wedge s_2\ \mathcal{R}_2\ r)\},$$

it is enough to show that $\mathcal{R}$ is a strong i-depth bisimulation. Note $\mathcal{R}_1 \cup \mathcal{R}_2 \subseteq \mathcal{R}$, since for each $s_1\ \mathcal{R}_1\ s_2$ we also have $s_2\ \mathcal{R}_2\ s_2$ due to reflexivity, thus $s_1\ \mathcal{R}\ s_2$, similarly we can show that $\mathcal{R}_2 \subseteq \mathcal{R}$. Therefore for any $\mathcal{R}$ downward closed sets C and C', they are also $\mathcal{R}_1$ and $\mathcal{R}_2$ downward closed. As a result for each I and π, there exists π' such that

$$Prob_{\pi',t}(C, C', i, I, t) \leq Prob_{\pi,s}(C, C', i, I, s)$$

since $s \sim_i t$. Furthermore, since $t \sim_i r$ there exists π'' such that

$$Prob_{\pi'',r}(C, C', i, I, r) \leq Prob_{\pi',t}(C, C', i, I, t).$$

This completes the proof. □

Similarly we can show that $\sim_i$ is both sound and complete for $\sim_{\mathsf{CSL}_i^-}$, and also in an arbitrary CTMDP there exists a n such that $\sim_n = \sim_{\mathsf{CSL}}$, therefore we have the following theorem.

Theorem 40. *1.* $\sim_i = \sim_{\mathsf{CSL}_i^-}$.

2. There exists n such that $\sim_n = \sim_{\mathsf{CSL}^-} = \sim_{\mathsf{CSL}}$.

3. $\sim_i$ *with* $i \geq 1$ *is not in general a congruence (w.r.t. the operator* $\|$ *in Definition 44).*

Proof. Let

$$Sat(\varphi) = \{s \in S \mid s \models \varphi\}$$

denote the set of states satisfying φ, and

$$Sat(\psi) = \{\omega \in Paths^{\infty} \mid \omega \models \psi\}$$

denote the set of paths satisfying ψ. We prove that $\sim_{\mathsf{CSL}_i^-} \subseteq \sim_i$ first. Let

$$\mathcal{R} = \{(s, r) \mid s \sim_{\mathsf{CSL}_i^-} r\},$$

it is enough to show that $\mathcal{R}$ is a strong i-depth bisimulation. It is a standard technique to construct a state formula φ_C such that $Sat(\varphi_C) = C$ where C is $\mathcal{R}$ downward closed.

Suppose that there exists π, C, C' and I such that there does not exist a scheduler π' with

$$Prob_{\pi',r}(C, C', i, I, r) \leq Prob_{\pi,s}(C, C', i, I, s)$$

where C, C' are $\mathcal{R}$ downward closed sets, and $I \subseteq [0, \infty)$ is an interval. In other words

$$Prob_{\pi',r}(C, C', i, I, r) > Prob_{\pi,s}(C, C', i, I, s)$$

for any π'. Let $Pr_{\pi,s}(\varphi_1 \,\mathsf{U}_i^I\, \varphi_2)$ denote the probability of the paths of s satisfying $\varphi_1 \,\mathsf{U}_i^I\, \varphi_2$ guarded by the scheduler π, it is not hard to see that

$$Pr_{\pi,s}(\varphi_C \,\mathsf{U}_i^I\, \varphi_{C'}) = Prob_{\pi,s}(C, C', i, I, s).$$

As a result there exists q such that

$$r \models \mathcal{P}_{\geq q}(\varphi_C \,\mathsf{U}_i^I\, \varphi_{C'}) \text{ but } s \not\models \mathcal{P}_{\geq q}(\varphi_C \,\mathsf{U}_i^I\, \varphi_{C'})$$

which contradicts with our assumption, therefore there does exist π' such that

$$Prob_{\pi',r}(C, C', i, I, r) \leq Prob_{\pi,s}(C, C', i, I, s),$$

thus $s \;\mathcal{R}\; r$.

In order to prove that $\sim_i \subseteq \sim_{\mathsf{CSL}_i^-}$, we need to show that for all states s and r, $s \models \varphi$ implies $r \models \varphi$ and vice versa whenever $s \;\sim_i\; r$, where φ is any state formula of CSL_i^-. We only consider formula $P_{\leq q}(\psi)$ here since all the others are trivial. Suppose $\psi = \mathsf{X}^I\, \varphi$ where $I = [a, b]$. We show that the next operator can be encoded by bounded until. First consider the case when $s \notin Sat(\varphi)$, then $Pr_{\pi,s}(\mathsf{X}^I\, \varphi) = Pr_{\pi,s}(\varphi_s \,\mathsf{U}_1^I\, \varphi)$ for any scheduler π. Suppose that $s \in Sat(\varphi)$. Since

$$Pr_{\pi,s}(\mathsf{X}^I\, \varphi) = \sum_{(\lambda,\mu) \in Supp(\pi(s))} \pi(s)(\lambda, \mu) \cdot (e^{-\lambda a} - e^{-\lambda b}) - Pr_{\pi,s}(\mathsf{X}^I\, \neg\varphi),$$

so we can use the above result to encode $Pr_{\pi,s}(\mathsf{X}^I\, \neg\varphi)$ as well. As a result we only need to consider the case when $\psi = \varphi_1 \,\mathsf{U}_i^I\, \varphi_2$. Suppose that $s \models P_{\geq q}(\psi)$, that is, $\forall \pi. Pr_{\pi,s}(\varphi_1 \,\mathsf{U}_i^I\, \varphi_2) \geq q$. Since

$$Pr_{\pi,s}(\varphi_1 \,\mathsf{U}_i^I\, \varphi_2) = Prob_{\pi,s}(Sat(\varphi_1), Sat(\varphi_2), i, I, s)$$

for any scheduler π, then we have

$$\forall \pi. Prob_{\pi,s}(Sat(\varphi_1), Sat(\varphi_2), i, I, s) \geq q.$$

Again we prove by contradiction, assume that $r \not\models P_{\geq q}\psi$, then there exists π' such that

$$Prob_{\pi',r}(Sat(\varphi_1), Sat(\varphi_2), i, I, r) < q,$$

since $s \sim_i r$, then there should exist π such that

$$Prob_{\pi,s}(Sat(\varphi_1), Sat(\varphi_2), i, I, s) \leq Prob_{\pi',r}(Sat(\varphi_1), Sat(\varphi_2), i, I, r) < q,$$

this contradicts with the fact that $s \models P_{\geq q}\psi$, so $r \models P_{\geq q}\psi$, this completes our proof.

The proof of Clause 2 is trivial since there are at most n equivalence classes where n is the number of states in a CTMDP, thus $\sim_n = \sim_{\mathsf{CSL}^-} = \sim_{\mathsf{CSL}}$.

For the counterexample of the last clause please refer to Example 51. □

The following example illustrates that $\sim_i$ is both sound and complete for $\sim_{\mathsf{CSL}_i^-}$ even for general CTMDPs.

Example 48. *Refer to s_0 and r_0 in Example 47. If s_j and r_j are absorbing states with $1 \leq j \leq 3$, then it can be proved that $s_0 \sim_i r_0$, thus $s_0 \sim_{\mathsf{CSL}_i^-} r_0$ for any $i \geq 0$. Similarly for the case when s_2 and r_2 are not absorbing but can evolve into s_0 and r_0 with probability 1 respectively. Suppose now the non-absorbing states are s_3 and r_3 with same transitions, then we show that there exists n such that $s_0 \not\sim_n r_0$. Let $C = \{s_0, s_3, r_0, r_3\}$, $C' = \{s_1, r_1\}$, and $I = [0, \infty)$, then it is easy to see that*

$$Prob_{\pi_l,s_0}(C, C', 2n+1, I, s_0) = 0.3 \cdot \sum_{i=0}^{n} 0.4^i$$

where π_l always chooses the left transition when at s_0. Similarly

$$Prob_{\pi_r,s_0}(C, C', 2n+1, I, s_0) = 0.5 \cdot \sum_{i=0}^{n} 0.1^i$$

where π_r always chooses the right transition when at s_0. Given a π_m which always chooses the middle transition of r_0 when at r_0, then

$$Prob_{\pi_m,r_0}(C, C', 2n+1, I, r_0) = 0.4 \cdot \sum_{i=0}^{n} 0.3^i.$$

Observe that

$$\lim_{n\to\infty} Prob_{\pi_m,r_0}(C, C', 2n+1, I, r_0) = \frac{4}{7}$$

which is greater than

$$\lim_{n\to\infty} Prob_{\pi_l,s_0}(C, C', 2n+1, I, s_0) = \frac{1}{2}$$

and

$$\lim_{n\to\infty} Prob_{\pi_r,s_0}(C, C', 2n+1, I, s_0) = \frac{5}{9},$$

thus there must exists n such that it holds

$$Prob_{\pi_m,r_0}(C, C', n, I, r_0) > Prob_{\pi_l,s_0}(C, C', n, I, s_0)$$

and

$$Prob_{\pi_m,r_0}(C, C', n, I, r_0) > Prob_{\pi_r,s_0}(C, C', n, I, s_0),$$

thus $s_0 \not\sim_n r_0$.

Recall that $\mathsf{CSL}_{\setminus \mathsf{U}_n}$ denotes the sub-logic of CSL without bounded until. The following lemma shows that the intersection of $\sim$ and $\sim_1$ is sound and complete for this sub-logic:

Lemma 31. *If $\mathcal{C}$ is not 2-step recurrent, we have*

1. $\approx \cap \sim_1 = \sim_{\mathsf{CSL}_{\setminus \mathsf{U}_n}}$,
2. $\sim_{\mathsf{CSL}_{\setminus \mathsf{U}_n}}$ *is not in general a congruence.*

Proof. By Theorem 38 $\approx = \sim_{\mathsf{CSL}_{\setminus \mathsf{X}}}$ in a CTMDP without 2-step recurrent states, and moreover by Theorem 40 $\sim_1 = \sim_{\mathsf{CSL}_1^-}$. Let CSL_0^- denote the sub-logic of CSL without (bounded and unbounded) until operator. We are going to show that $\mathsf{CSL}_0^- = \mathsf{CSL}_1^-$. The proof of $\sim_{\mathsf{CSL}_1^-} \subseteq \sim_{\mathsf{CSL}_0^-}$ is trivial. We show that $\sim_{\mathsf{CSL}_0^-} \subseteq \sim_{\mathsf{CSL}_1^-}$. The only case we need to consider is $\varphi = P_{\leq q}(\varphi_1 \,\mathsf{U}_1^I\, \varphi_2)$. We prove by structural induction on φ. Suppose that $s \models \varphi$ and $s \models \varphi_1 \wedge \neg\varphi_2$, if we choose transition $s \xrightarrow{\lambda} \mu$, then the probability of the paths of s satisfying $\varphi_1 \,\mathsf{U}_1^I\, \varphi_2$ is equal to

$$\mu(Sat(\varphi_2)) \cdot (e^{-\lambda a} - e^{-\lambda b})$$

where $I = [a, b]$, note the probability of the paths of s satisfying $\mathsf{X}^I\, \varphi_2$ is also equal to

$$\mu(Sat(\varphi_2)) \cdot (e^{-\lambda a} - e^{-\lambda b}),$$

in other words, if $s \models \varphi_1 \wedge \neg\varphi_2$, then $s \models \varphi$ iff $s \models P_{\leq q}(\mathsf{X}^I\, \varphi_2)$. Since $s \sim_{\mathsf{CSL}_0^-} r$, then $r \models P_{\leq q}(\mathsf{X}^I\, \varphi_2)$, by induction $r \models \varphi_1 \wedge \neg\varphi_2$, thus $r \models \varphi$. The other cases are similar and omitted here. Therefore $\approx \cap \sim_1$ is both sound and complete for $\sim_{\mathsf{CSL}_{\setminus \mathsf{U}_n}}$.

Since $\sim_1$ is not congruent, the first clause implies clause 2 directly. □

The example below shows that Lemma 31 does not hold in CTMDPs with 2-step recurrent states:

Example 49. *Again considering s_0 and r_0 in Example 47, if s_i and r_i are absorbing states for $1 \leq i \leq 3$, then both s_0 and r_0 are 2-step recurrent states by Definition 47. As we said before $s_0 \sim_{\mathsf{CSL}} r_0$, thus $s_0 \sim_{\mathsf{CSL}_{\setminus \mathsf{U}_n}} r_0$, but $s_0 \not\approx r_0$.*

5.5.2 Weak i-depth Bisimulation

Following the idea of defining weak bisimulations in Section 5.4.2, in this section, we introduce weak i-depth bisimulations.

Definition 49 (Weak i-depth Bisimulation)**.** *We say that states s and r are weak i-depth bisimilar, denoted by $s \approx_i r$, whenever $\bar{s} \sim_i \bar{r}$ in the uniformized* CTMDP *$\bar{\mathcal{C}}$.*

Due to that $\mathsf{CSL}_{\setminus \mathsf{X}}$ satisfaction is preserved after uniformization, we have the following characterization results for $\mathsf{CSL}_{\setminus \mathsf{X}}$ in arbitrary CTMDP.

Theorem 41. *1. There exists n such that $\approx_n = \sim_{\mathsf{CSL}_{\setminus \mathsf{X}}}$.*

2. $\approx_1$ is congruent, and $\approx_i$ with $i > 1$ is not in general a congruence.

Proof. The proof of the first clause is based on Theorem 40. We first shows that $s \approx r$ implies that $s \sim_{\mathsf{CSL}_{\setminus \mathsf{X}}} r$ i.e. $\approx \subseteq \sim_{\mathsf{CSL}_{\setminus \mathsf{X}}}$. Since $s \approx r$, then $\bar{s} \sim \bar{r}$, thus $\bar{s} \sim_{\mathsf{CSL}_{\setminus \mathsf{X}}} \bar{r}$ by Theorem 40. Since uniformization does not change the satisfaction of $\mathsf{CSL}_{\setminus \mathsf{X}}$, therefore $s \sim_{\mathsf{CSL}_{\setminus \mathsf{X}}} r$. To show that $\sim_{\mathsf{CSL}_{\setminus \mathsf{X}}} \subseteq \approx$, we prove that $s \sim_{\mathsf{CSL}_{\setminus \mathsf{X}}} r$ implies that $s \approx r$. It is easy to see that $\sim_{\mathsf{CSL}_{\setminus \mathsf{X}}} = \sim_{\mathsf{CSL}}$ in a uniformized CTMDP, thus $s \sim_{\mathsf{CSL}_{\setminus \mathsf{X}}} r$ implies that $\bar{s} \sim_{\mathsf{CSL}} \bar{r}$. By Theorem 40 $\bar{s} \sim \bar{r}$, therefore $s \approx r$.

We prove that $\approx_1$ is congruent. By Definition 49, $s \approx_1 r$ iff $\bar{s} \sim_1 \bar{r}$, so we only need to show that $\sim_1$ is congruent in uniformized CTMDPs. It is enough to show that

$$\mathcal{R} = \{(s \parallel t, r \parallel t) \mid s \sim_1 r\}$$

is a strong 1-step bisimulation. Note that in a uniformized CTMDP $s \sim_1 r$ iff for each $\sim_1$-closed set and $s \to \mu$, there exists $r \to \nu$ such that $\nu(C) \leq \mu(C)$ and vice versa. Suppose that $s \parallel t \to \mu$, by Definition 44, there exists $s \to \mu_s$ and $t \to \mu_t$ such that

$$\mu = \frac{1}{2} \cdot (\mu_s \parallel \delta_t) + \frac{1}{2} \cdot (\delta_s \parallel \mu_t),$$

the following proof is straightforward. □

We have seen that $\sim_{\mathsf{CSL}_{\setminus \mathsf{X}}}$ is a congruence in CTMDPs that are not 2-step recurrent. Since $\approx_i$ with $i > 1$ are not congruent in general, it follows that $\sim_{\mathsf{CSL}_{\setminus \mathsf{X}}}$ is also not congruent in general.

5.6 Simulations

In this section we introduce (weak) simulations, and i-depth (weak) simulations. Further, we extend the characterization results to these simulation relations.

5.6.1 Strong and Weak Simulations

We extend the strong (weak) bisimulations to strong (weak) simulations for CTMDPs, respectively:

Definition 50 (Simulation)**.** *Let $\mathcal{R} \subseteq S \times S$, $\mathcal{R}$ is a strong simulation if $s\ \mathcal{R}\ r$ implies that for each $s \to \mu$, there exists $r \to_{\mathsf{P}} \mu'$ such that $\mu \sqsubseteq_{\mathcal{R}} \mu'$.*

We write $s \prec r$ whenever there exists a strong simulation $\mathcal{R}$ such that $s\ \mathcal{R}\ r$.

We say that s is weak simulated by r, denoted by $s \precapprox r$, whenever $\bar{s} \prec \bar{r}$ in the uniformized CTMDP *$\bar{\mathcal{C}}$.*

The relation $\prec$ is then a preorder. To characterize $\prec$, we use the *safe* fragment of CSL (54), denoted as CSL_s, which is defined by the following BNFs:

$$\varphi ::= a \mid \neg a \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \mathcal{P}_{\geq p}(\psi)$$
$$\psi ::= \mathsf{X}^I\, \varphi \mid \varphi\, \mathsf{U}^I_n\, \varphi \mid \varphi\, \mathsf{U}^I\, \varphi$$

As usual, $\mathsf{CSL}_{s\setminus\mathsf{X}}$ is obtained from CSL_s by removing the next operator. Below we present the logical characterization results for strong and weak simulations with respect to CSL_s and $\mathsf{CSL}_{s\setminus\mathsf{X}}$, and their relationship:

Theorem 42. *1. $\prec \subseteq \prec_{\mathsf{CSL}_s}$.*

2. if $\mathcal{C}$ is uniformized and not 2-step recurrent, $\prec_{\mathsf{CSL}_s} = \prec$.

3. $\precapprox \subseteq \prec_{\mathsf{CSL}_{s\setminus\mathsf{X}}}$.

4. if $\mathcal{C}$ is not 2-step recurrent, $\prec_{\mathsf{CSL}_{s\setminus\mathsf{X}}} = \precapprox$.

Proof. In order to show that $\prec_{\mathsf{CSL}_s} \subseteq \prec$ when $\mathcal{C}$ is not 2-step recurrent, it is sufficient to show that

$$\mathcal{R} = \{(s, r) \mid s \prec_{\mathsf{CSL}_s} r\}$$

is a strong simulation. Suppose that $s\ \mathcal{R}\ r$ and $s \to_{\mathsf{P}} \mu$, we need to show that there exists $r \to_{\mathsf{P}} \nu$ such that $\mu \sqsubseteq_{\mathcal{R}} \nu$. Similar with the proof of Theorem 38, if there does not exist $r \to_{\mathsf{P}} \nu$ such that $\mu \sqsubseteq_{\mathcal{R}} \nu$, then a path formula ψ and π can be found such

that $Pr_{r,\pi'}(\psi) > Pr_{s,\pi}(\psi)$ for all π'. Therefore there exists q such that $r \models P_{\geq q}\psi$ but $s \not\models P_{\geq q}\psi$, which contradicts our assumption that $s \prec_{\mathsf{CSL}_s} r$.

Now suppose that $s \prec r$, we are going to show that $s \prec_{\mathsf{CSL}_s} r$, that is, $r \models \varphi$ implies $s \models \varphi$ for any φ of CSL_s by structural induction on φ. First we show for each π of s, two $\prec$ downward closed sets C, C', and $I = [a, b]$, there exists π' of r such that

$$Prob_{\pi',r}(C, C', I, r) \leq Prob_{\pi,s}(C, C', I, s).$$

Since C and C' are $\prec$ downward closed, there exists φ_C and $\varphi_{C'}$ such that $Sat(\varphi_C) = C$ and $Sat(\varphi_{C'}) = C'$. There are several cases we need to consider.

1. $s \models \varphi_C$ and $s \not\models \varphi_{C'}$.
   Then

$$Prob_{\pi,s}(C, C', I, s) = \sum_{(\lambda,\mu') \in Supp(\pi(s))} \pi(s)(\lambda, \mu')$$
$$\cdot \int_0^b \lambda \cdot e^{-\lambda x} \cdot \sum_{t \in Supp(\mu')} \mu'(t) \cdot Prob_{\pi,t}(C, C', I \ominus x, s\frown(x, t))dx,$$

   thus there exists $s \to_{\mathsf{P}} \mu$ such that

$$Prob_{\pi,s}(C, C', I, s)$$
$$= \int_0^b \lambda \cdot e^{-\lambda x} \cdot \sum_{t \in Supp(\mu)} \mu(t) \cdot Prob_{\pi,t}(C, C', I \ominus x, s\frown(x, t))dx.$$

   By induction if $s \models \varphi_C$ and $s \not\models \varphi_{C'}$, then $r \not\models \varphi_{C'}$ and either $r \models \varphi_C$ or $r \not\models \varphi_C$, the case when $r \not\models \varphi_C$ is trivial, since $Prob_{\pi',r}(C, C', I, r) = 0$ for all π'. Suppose that $r \models \varphi_C$ and $r \not\models \varphi_C$, since $s \prec r$, there exists $r \to_{\mathsf{P}} \nu$ such that $\mu \sqsubseteq_{\prec} \nu$, in other words, $\nu(C) \leq \mu(C)$ for each $\prec$ downward closed set C, hence there exists π' such that

$$\int_0^b \lambda \cdot e^{-\lambda x} \cdot \sum_{t \in Supp(\nu)} \nu(t) \cdot Prob_{\pi',t}(C, C', I \ominus x, r\frown(x, t))dx$$
$$\leq \int_0^b \lambda \cdot e^{-\lambda x} \cdot \sum_{t \in Supp(\mu)} \mu(t) \cdot Prob_{\pi,t}(C, C', I \ominus x, s\frown(x, t))dx$$

   by induction. By definition there exists $\{\nu_i\}_{1 \leq i \leq n}$ and $\{p_i\}_{1 \leq i \leq n}$ such that $\sum_{1 \leq i \leq n} p_i = 1$ and $\sum_{1 \leq i \leq n} p_i \cdot \nu_i = \nu$. Let π' choose transition (λ, ν_i) with

probability p_i at state r, then it is not hard to see that

$$\begin{aligned}
&\int_0^b \lambda \cdot e^{-\lambda x} \cdot \sum_{t \in Supp(\nu)} \nu(t) \cdot Prob_{\pi',t}(C, C', I \ominus x, r \frown (x,t)) dx \\
&= \sum_{(\lambda,\nu') \in Supp(\pi'(r))} \pi'(r)(\lambda, \nu') \\
&\cdot \left(\int_0^b \lambda \cdot e^{-\lambda x} \cdot \sum_{t \in Supp(\nu')} \nu'(t) \cdot Prob_{\pi',t}(C, C', I \ominus x, r \frown (x,t)) dx \right),
\end{aligned}$$

thus there exists π' such that $Prob_{\pi',r}(C, C', I, r) \leq Prob_{\pi,s}(C, C', I, s)$.

2. $s \models \varphi_C$ and $s \models \varphi_{C'}$.
Then

$$\begin{aligned}
Prob_{\pi,s}(C, C', I, s) &= e^{-\lambda a} + \sum_{(\lambda,\mu') \in Supp(\pi(s))} \pi(s)(\lambda, \mu') \\
&\cdot \left(\int_0^a \lambda \cdot e^{-\lambda x} \cdot \sum_{t \in Supp(\mu')} \mu'(t) \cdot Prob_{\pi,t}(C, C', I \ominus x, s \frown (x,t)) dx \right),
\end{aligned}$$

and there exists $s \to_{\mathsf{P}} \mu$ such that

$$\begin{aligned}
&Prob_{\pi,s}(C, C', I, s) = e^{-\lambda a} \\
&+ \int_0^a \lambda \cdot e^{-\lambda x} \cdot \sum_{t \in Supp(\mu)} \mu(t) \cdot Prob_{\pi,t}(C, C', I \ominus x, s \frown (x,t)) dx.
\end{aligned}$$

By induction there are four cases: either

- $r \models \varphi_C$ and $r \models \varphi_{C'}$, or
- $r \not\models \varphi_C$ and $r \models \varphi_{C'}$, or
- $r \models \varphi_C$ and $r \not\models \varphi_{C'}$, or
- $r \not\models \varphi_C$ and $r \not\models \varphi_{C'}$.

The first case is similar with Clause 1, and is omitted here. If $r \not\models \varphi_C$ and $r \models \varphi_{C'}$, then

$$Prob_{\pi,s}(C, C', I, s) = Prob_{\pi',r}(C, C', I, r) = 1$$

if $a = 0$, otherwise $Prob_{\pi',r}(C, C', I, r) = 0$, thus such π' always exists. When

$r \models \varphi_C$ and $r \not\models \varphi_{C'}$, there exists $r \to_{\mathsf{P}} \nu$ such that

$$\begin{aligned}
&\int_0^b \lambda \cdot e^{-\lambda x} \cdot \sum_{t \in Supp(\nu)} \nu(t) \cdot Prob_{\pi',t}(C, C', I \ominus x, r \frown (x,t))dx \\
=&\int_0^a \lambda \cdot e^{-\lambda x} \cdot \sum_{t \in Supp(\nu)} \nu(t) \cdot Prob_{\pi',t}(C, C', I \ominus x, r \frown (x,t))dx \\
&+ \int_a^b \lambda \cdot e^{-\lambda x} \cdot \sum_{t \in Supp(\nu)} \nu(t) \cdot Prob_{\pi',t}(C, C', I \ominus x, r \frown (x,t))dx \\
\leq&\int_a^b \lambda \cdot e^{-\lambda x} dx + \int_0^a \lambda \cdot e^{-\lambda x} \cdot \sum_{t \in Supp(\nu)} \nu(t) \cdot Prob_{\pi',t}(C, C', I \ominus x, r \frown (x,t))dx \\
\leq&\int_a^\infty \lambda \cdot e^{-\lambda x} dx + \int_0^a \lambda \cdot e^{-\lambda x} \cdot \sum_{t \in Supp(\nu)} \nu(t) \cdot Prob_{\pi',t}(C, C', I \ominus x, r \frown (x,t))dx \\
=&e^{-\lambda a} + \int_0^a \lambda \cdot e^{-\lambda x} \cdot \sum_{t \in Supp(\nu)} \nu(t) \cdot Prob_{\pi',t}(C, C', I \ominus x, r \frown (x,t))dx \\
\leq&e^{-\lambda a} + \int_0^a \lambda \cdot e^{-\lambda x} \cdot \sum_{t \in Supp(\mu)} \mu(t) \cdot Prob_{\pi,t}(C, C', I \ominus x, s \frown (x,t))dx
\end{aligned}$$

Let π' be a scheduler which chooses transition (λ, ν_i) with probability p_i, then

$$Prob_{\pi',r}(C, C', I, r) \leq Prob_{\pi,s}(C, C', I, s).$$

The last case is trivial since $Prob_{\pi,r}(C, C', I, r) = 0$ for all π.

3. The other cases are trivial.

In all cases we have proved that for each π, C, C', and I, there always exists π' such that

$$Prob_{\pi',r}(C, C', I, r) \leq Prob_{\pi,s}(C, C', I, s).$$

Suppose that $r \models P_{\geq q}(\varphi_1 \,\mathsf{U}^I\, \varphi_2)$, that is,

$$Prob_{\pi',r}(Sat(\varphi_1), Sat(\varphi_2), I, r) \geq q$$

for all π'. If $s \not\models P_{\geq q}(\varphi_1 \,\mathsf{U}^I\, \varphi_2)$ which means there exists π such that

$$Prob_{\pi,s}(Sat(\varphi_1), Sat(\varphi_2), I, s) < q,$$

then there does not exist π' such that

$$Prob_{\pi',r}(Sat(\varphi_1), Sat(\varphi_2), I, r) \leq Prob_{\pi,s}(Sat(\varphi_1), Sat(\varphi_2), I, s)$$

which contradicts the assumption that $s \prec r$, hence $s \models P_{\geq q}(\varphi_1 \,\mathsf{U}^I\, \varphi_2)$.

Since uniformization does not change the satisfaction of $\mathsf{CSL}_{\setminus \mathsf{X}}$, thus the proof of Clause 3) and 4) is straightforward according to Definition 50. □

Example 47 can applies here as well showing that Theorem 42 does not hold in general CTMDPs. Let R^{-1} denote the reverse of the relation R. The following theorem shows the compositional properties and their relation to bisimulations:

Theorem 43. *1. $s \prec r$ implies that $s \parallel t \prec r \parallel t$ for any t.*

2. $s \precapprox r$ implies that $s \parallel t \precapprox r \parallel t$ for any t.

3. If $\mathcal{C}$ is uniformized, $\prec = \precapprox$, and $\prec_{\mathsf{CSL}_s} = \prec_{\mathsf{CSL}_{s\setminus \mathsf{X}}}$.

4. If $\mathcal{C}$ is not 2-step recurrent, $s \prec_{\mathsf{CSL}_{s\setminus \mathsf{X}}} r$ implies that $s \parallel t \prec_{\mathsf{CSL}_{s\setminus \mathsf{X}}} r \parallel t$ for any t.

5. $\sim \subset (\prec \cap \prec^{-1})$.

6. $\approx \subset (\precapprox \cap \precapprox^{-1})$.

Proof. 1. Let

$$\mathcal{R} = \{(s \parallel t, r \parallel t) \mid s \prec r\},$$

it is enough to show that $\mathcal{R}$ is a strong simulation. Suppose that $(s \parallel t)\ \mathcal{R}\ (r \parallel t)$, and $s \parallel t \xrightarrow{\lambda} \mu$. By Definition 44 there exists $s \xrightarrow{\lambda_1} \mu_1$ and $t \xrightarrow{\lambda_2} \nu$ such that $\lambda = \lambda_1 + \lambda_2$,

$$\mu = \frac{\lambda_1}{\lambda} \cdot (\mu_1 \parallel \delta_t) + \frac{\lambda_2}{\lambda} \cdot (\delta_s \parallel \nu).$$

Since $s \prec r$, there exists $r \xrightarrow{\lambda_1}_{\mathsf{P}} \mu_1'$ such that $\mu_1 \sqsubseteq_{\mathcal{R}} \mu_1'$, thus

$$(\mu_1 \parallel \delta_t) \sqsubseteq_{\mathcal{R}} (\mu_1' \parallel \delta_t) \text{ and } (\delta_s \parallel \nu) \sqsubseteq_{\mathcal{R}} (\delta_r \parallel \nu)$$

by induction. As a result there exists

$$r \parallel t \xrightarrow{\lambda}_{\mathsf{P}} \mu' \equiv \frac{\lambda_1}{\lambda} \cdot (\mu_1' \parallel \delta_t) + \frac{\lambda_2}{\lambda} \cdot (\delta_r \parallel \nu),$$

so $\mu \sqsubseteq_{\mathcal{R}} \mu'$ which completes the proof.

2. Suppose that $s \precapprox r$, then according to Definition 50, $\bar{s} \prec \bar{r}$. Due to Theorem 37, we have $\bar{s} \parallel \bar{t} \prec \bar{r} \parallel \bar{t}$. As a result $\overline{s \parallel t} \prec \overline{r \parallel t}$, therefore $s \parallel t \precapprox r \parallel t$.

3. The proof is $\prec = \precsim$ is directly from Definition 50. Since uniformization preserves $\mathsf{CSL}_{s\backslash \mathsf{X}}$, thus $\mathsf{CSL}_s = \mathsf{CSL}_{s\backslash \mathsf{X}}$ in a uniformized CTMDP.

4. The proof is straightforward based on Clause 2) and Theorem 42.

5. The proof of $\sim \subseteq (\prec \cap \prec^{-1})$ is trivial and omitted here. To show that $(\prec \cap \prec^{-1})$ is strictly coarser than $\sim$, it is enough to give a counterexample. Suppose we have three states s_1, s_2, and s_3 such that $s_1 \prec s_2 \prec s_3$ but $s_3 \not\prec s_2 \not\prec s_1$. Let s and r be two states such that $L(s) = L(r)$. In addition s has three transitions: $s \xrightarrow{1} \delta_{s_1}$, $s \xrightarrow{1} \delta_{s_2}$, $s \xrightarrow{1} \delta_{s_3}$, and r only has two transitions: $s \xrightarrow{1} \delta_{s_1}$, $s \xrightarrow{1} \delta_{s_3}$. Then it should be easy to check that $s \prec r$ and $r \prec s$, the only non-trivial case is when $s \xrightarrow{1} \delta_{s_2}$. Since $s_2 \prec s_3$, thus there exists $r \xrightarrow{1} \delta_{s_3}$ such that $\delta_{s_2} \sqsubseteq_{\prec} \delta_{s_3}$. But obviously $s \not\prec r$, since the transition $s \xrightarrow{1} \delta_{s_2}$ cannot be simulated by any transition of r.

6. The counterexample adopted in the proof of Clause 3) in Theorem 43 also applies here, thus the proof is similar and omitted.

□

5.6.2 Strong and Weak i-depth Simulations

In this section we introduce the one side strong and weak i-depth bisimulations. Below follows their definitions where $s \prec_0 r$ iff $L(s) = L(r)$:

Definition 51 (i-depth Simulations)**.** *A relation $\mathcal{R} \subseteq S \times S$ is a strong i-depth simulation with $i > 0$ if $s \mathcal{R} r$ implies $s \prec_{i-1} r$ and for any $\mathcal{R}$ downward closed sets C, C', I and π, there exists a scheduler π' such that*

$$Prob_{\pi',r}(C, C', i, I, r) \leq Prob_{\pi,s}(C, C', i, I, s).$$

We write $s \prec_i r$ whenever there is a strong i-depth simulation $\mathcal{R}$ such that $s \mathcal{R} r$. We say that s is weak simulated by r, denoted by $s \precsim_i r$, whenever $\bar{s} \prec_i \bar{r}$ in the uniformed CTMDP *$\bar{\mathcal{C}}$.*

The following theorem shows the properties of $\prec_i$ and $\precsim_i$, especially there exists n such that $\prec_n$ and $\precsim_n$ are enough to characterize CSL_s and $\mathsf{CSL}_{s\backslash \mathsf{X}}$ respectively.

Theorem 44. *1. $\prec_i$ is preorder, and $\prec_i = \prec_{\mathsf{CSL}^-_{si}}$.*

2. There exists n such that

$$\prec_n = \prec_{\mathsf{CSL}^-_s} = \prec_{\mathsf{CSL}_s}$$

and $\precsim_n = \prec_{\mathsf{CSL}_{s\backslash \mathsf{X}}}$ in any CTMDP.

3. $\prec_i$ *with* $i \geq 1$ *and* $\precsim_i$ *with* $i > 1$ *are not congruences while* $\precsim_1$ *is a congruence.*

Proof. We first show that $\prec_i$ is a preorder. The reflexivity is trivial and we only show the proof of transitivity. Suppose that $s \prec_i t$ and $t \prec_i r$, we need to prove that $s \prec_i r$. By Definition 51 there exists two strong i-depth simulation such that $s \mathcal{R}_1 t$ and $t \mathcal{R}_2 r$. Let

$$\mathcal{R} = \mathcal{R}_1 \circ \mathcal{R}_2 = \{(s_1, s_3) \mid \exists s_2.(s_1 \prec_i s_2 \wedge s_2 \prec_i s_3)\},$$

it is enough to show that $\mathcal{R}$ is a strong i-depth simulation. Similar with the proof of Lemma 30 it can be shown that $\mathcal{R}_1 \cup \mathcal{R}_2 \subseteq \mathcal{R}$, thus for each $\mathcal{R}$ downward closed set C, it is also $\mathcal{R}_1$ and $\mathcal{R}_2$ downward closed. The following proof is straightforward, and is omitted here.

To prove that $\sim_{\mathsf{CSL}^-_{si}} \subseteq \prec_i$, it is enough to show that

$$\mathcal{R} = \{(s, r) \mid s \sim_{\mathsf{CSL}^-_{si}} r\}$$

is a strong i-depth simulation. By definition given a $\mathcal{R}$ downward closed set C, there exists φ_C such that $Sat(\varphi_C) = C$. Suppose that $s \mathcal{R} r$ and for two $\mathcal{R}$ downward closed sets C, C' and $I \subseteq [0, \infty)$, there exists π such that

$$Prob_{\pi',r}(C, C', i, I, r) > Prob_{\pi,s}(C, C', i, I, s)$$

for any π'. Since

$$Pr_{\pi,s}(\psi) = Prob_{\pi,s}(C, C', i, I, s)$$

where $\psi = \varphi_C \, \mathsf{U}^I_i \, \varphi_{C'}$, thus there exists q such that $r \models P_{\geq q}\psi$ but $s \not\models P_{\geq q}\psi$ which contradicts with the assumption that $s \sim_{\mathsf{CSL}^-_{si}} r$, so there must exist π' such that

$$Prob_{\pi',r}(C, C', i, I, r) \leq Prob_{\pi,s}(C, C', i, I, s).$$

To show that $\prec_i \subseteq \sim_{\mathsf{CSL}^-_{si}}$, we need to prove that if $s \prec_i r$, then $r \models \varphi$ implies $s \models \varphi$ for any φ of CSL^-_{si}. We only consider the case when $\varphi = P_{\geq q}(\varphi_1 \, \mathsf{U}^I_i \, \varphi_2)$ since all the other operators are either similar or trivial. Suppose that $r \models \varphi$, in other words, $Pr_{\pi,s}(\varphi) \geq q$ for any scheduler π. Let

$$C = \{s \in S \mid s \models \varphi_1\}$$

and

$$C' = \{s \in S \mid s \models \varphi_2\},$$

it is obvious that C and C' are $\prec_i$ downward closed by induction. Then

$$Prob_{\pi,r}(C, C', i, I, r) \geq q$$

for any scheduler π. Assume that $s \not\models \varphi$, that is, there exists π' such that

$$Prob_{\pi',s}(C, C', i, I, s) < q.$$

By definition of $\prec_i$, there should exist π such that

$$Prob_{\pi,r}(C, C', i, I, r) \leq Prob_{\pi',s}(C, C', i, I, s) < q$$

which contradicts with the fact that $r \models \varphi$, thus $s \models \varphi$.

Since in a finite system we only have finite equivalence classes, thus the same argument applied in Theorem 40 also works here.

Similar as the proof of Clause 3 of Theorem 40, Example 51 can be used as a counterexample here too, thus $\prec_i$ with $i \geq 1$ is not congruent in general.

Now we prove that there exists n such that $\precsim_n = \prec_{\mathsf{CSL}_{\setminus \mathsf{X}}}$. We first shows that $s \precsim_n r$ implies that $s \prec_{\mathsf{CSL}_{\setminus \mathsf{X}}} r$ i.e. $\precsim_n \subseteq \prec_{\mathsf{CSL}_{\setminus \mathsf{X}}}$. Since $s \precsim_n r$, then $\bar{s} \prec_n \bar{r}$, thus $\bar{s} \prec_{\mathsf{CSL}_{\setminus \mathsf{X}}} \bar{r}$ as shown before. Since uniformization does not change the satisfaction of $\mathsf{CSL}_{\setminus \mathsf{X}}$, therefore $s \prec_{\mathsf{CSL}_{\setminus \mathsf{X}}} r$. To show that $\prec_{\mathsf{CSL}_{\setminus \mathsf{X}}} \subseteq \precsim_n$, we prove that $s \prec_{\mathsf{CSL}_{\setminus \mathsf{X}}} r$ implies that $s \precsim_n r$. It is easy to see that $\prec_{\mathsf{CSL}_{\setminus \mathsf{X}}} = \prec_{\mathsf{CSL}}$ in a uniformized CTMDP, thus $s \prec_{\mathsf{CSL}_{\setminus \mathsf{X}}} r$ implies that $\bar{s} \prec_{\mathsf{CSL}} \bar{r}$. Therefore $\bar{s} \sim \bar{r}$ i.e. $s \precsim r$.

We prove that $\precsim_1$ is congruent. By Definition 51, $s \precsim_1 r$ iff $\bar{s} \prec_1 \bar{r}$, so we only need to show that $\prec_1$ is congruent in uniformized CTMDPs. It is enough to show that

$$\mathcal{R} = \{(s \parallel t, r \parallel t) \mid s \prec_1 r\}$$

is a strong 1-step simulation. Note that in a uniformized CTMDP, we can change the definition of strong 1-step simulation as follows: $s \mathcal{R} r$ implies that for any $\mathcal{R}$ download closed set C and $s \to \mu$ such that $\mu(C) > 0$, there exists $r \to \nu$ such that $\nu(C) \leq \mu(C)$. Suppose that for a $\mathcal{R}$ download closed set C, and $s \parallel t \to \mu$ with $\mu(C) > 0$, there exists $s \to \mu_1$ and $t \to \mu_2$ such that

$$\frac{1}{2} \cdot (\mu_1 \parallel \delta_t) + \frac{1}{2} \cdot (\delta_s \parallel \mu_2) = \mu,$$

thus there exists $\mathcal{R}$ downward closed sets C_1 and C_2 such that

$$\frac{1}{2} \cdot \mu_1(C_1) + \frac{1}{2} \cdot \mu_2(C_2) = \mu(C)$$

where

$$(\{s' \parallel t \mid s' \in C_1\} \cup \{r \parallel t' \mid t' \mid C_2\}) \subseteq C.$$

Since $s \prec_1 r$, there exists $r \to \nu_1$ such that $\nu_1(C_1) \leq \mu_1(C_1)$, by induction there exists $r \to \nu$ such that

$$\frac{1}{2} \cdot \mu_1(C_1) + \frac{1}{2} \cdot \mu_2(C_2) \leq \frac{1}{2} \cdot \nu_1(C_1) + \frac{1}{2} \cdot \mu_2(C_2)$$

i.e. $\nu(C) \leq \mu(C)$. This completes our proof. □

As a direct consequence, $\prec_{\mathsf{CSL}_{s\setminus \mathsf{X}}} = \precsim_i$ is not congruent for $i > 1$. Below we prove a few properties of i-depth simulations, along Theorem 43:

Theorem 45. *1. If $\mathcal{C}$ is uniformized, $\prec_i = \precsim_i$.*

2. $\sim_i \subset (\prec_i \cap \prec_i^{-1})$.

3. $\approx_i \subset (\precsim_i \cap \precsim_i^{-1})$.

Proof. 1. According to Definition 51, $\prec_i = \precsim_i$ in a uniformized CTMDP.

2. The proof of $\sim_i \subseteq (\prec_i \cap \prec_i^{-1})$ is trivial. Note that the counterexample used in Clause 5) of Theorem 43 also applies here, thus $\sim_i \subset (\prec_i \cap \prec_i^{-1})$.

3. Similar as Clause 2), the proof of $\approx_i \subseteq (\precsim_i \cap \precsim_i^{-1})$ is trivial, and moreover the counterexample used in Clause 5) of Theorem 43 also applies here, thus $\approx_i \subset (\precsim_i \cap \precsim_i^{-1})$.

□

Extending Lemma 31 to simulations, we can also characterize $\mathsf{CSL}_{s\setminus \mathsf{U}_n}$ i.e. the safe CSL without bounded until.

Lemma 32. *If $\mathcal{C}$ is not 2-step recurrent, we have*

1. $\precsim \cap \prec_1 = \prec_{\mathsf{CSL}_{s\setminus \mathsf{U}_n}}$.

2. $\prec_{\mathsf{CSL}_{s\setminus \mathsf{U}_n}}$ is not a congruence.

Proof. First we can show that $\prec_{\mathsf{CSL}_1^-} = \prec_{\mathsf{CSL}_0^-}$. The proof is similar with the proof of $\sim_{\mathsf{CSL}_1^-} = \sim_{\mathsf{CSL}_0^-}$ in Lemma 31, and is omitted here. Therefore $\precsim \cap \prec_{\mathsf{CSL}_1^-}$ coincides with $\sim_{\mathsf{CSL}_{\setminus \mathsf{U}_n}}$. □

5.7 Relation to Probabilistic Automata and Markov Chains

In this section we discuss the relation of our bisimulations with those in the embedded time-abstract models.

5.7.1 Relation to Bisimulation of Probabilistic Automata

Let $\mathcal{C}$ be a CTMDP, the *embedded probabilistic automata* $\mathcal{M}_{\mathcal{C}}$ is obtained by removing the rates on the transition relations. In Chapter 4, probabilistic bisimulation $\sim_{\mathsf{P}}$, and strong i-depth branching bisimulations $\sim_i^b$ are defined in Definition 23 and 25 respectively. The following lemma is obvious from the definitions:

Lemma 33. *1. $s \sim r$ implies $s \sim_{\mathsf{P}} r$ in $\mathcal{M}_{\mathcal{C}}$.*

2. If $\mathcal{C}$ is uniformized, then $s \sim_{\mathsf{P}} r$ in $\mathcal{M}_{\mathcal{C}}$ implies $s \sim r$.

3. $s \sim_i r$ implies $s \sim_i^b r$ in $\mathcal{M}_{\mathcal{C}}$.

4. If $\mathcal{C}$ is uniformized, then $s \sim_i^b r$ in $\mathcal{M}_{\mathcal{C}}$ implies $s \sim_i r$.

The other direction for the first clause does not hold generally. For PAs, we know that $\sim_{\mathsf{P}}$ is only sound but not complete for PCTL, so it is a surprise that the strong probabilistic bisimulation in the continuous setting with minor variant is both sound and complete for CSL in the uniformized CTMDPs without 2-step recurrent states according to Definition 46 and Theorem 38. Refer to Example 50 for an intuitive explanation.

Example 50. *Considering two states s_0 and r_0 of a PA in Fig. 5.2. Suppose that s_i and r_i can evolve into t with probability 1 where $1 \leq i \leq 3$ and t is absorbing. Also all the states have different atomic propositions except $L(s_i) = L(r_i)$ for $0 \leq i \leq 3$. It is easy to check that s_0 and r_0 are PCTL-equivalent, but $s_0 \not\sim_{\mathsf{P}} r_0$ since the middle transition of r_0 has no way to be simulated by any (combined) transition of s_0. Assume that s_0 and r_0 as two states of a CTMDP where each transition has rate 1, then obviously the CTMDP is not 2-step recurrent by Definition 47. We can show that actually s_0 and r_0 are not CSL-equivalent. Let*

$$\psi = (s_0 \vee s_1)\, \mathsf{U}^{[a,b]} (s_3 \vee t)$$

where a state is used as a shorthand of the atomic propositions it satisfies. If s_0 chooses the transition on the left first, then the probability of the paths satisfying ψ is equal to

$$0.4 \cdot (e^{-a} - e^{-b}) + 0.3 \cdot (a \cdot e^{-a} + e^{-a} - b \cdot e^{-b} - e^{-b}).$$

The probability for other transitions can be obtained in a similar way by substituting 0.3 and 0.4 with corresponding probabilities. Since the interval $[a, b]$ can be chosen

arbitrarily, so we can choose the intervals such that the probability of path satisfying ψ when choosing the middle transition of r is larger than the other two cases. For instance here we can choose interval $[\frac{1}{2}, \infty)$, then the maximum probability of paths of r_0 satisfying ψ is $0.9 \cdot e^{-\frac{1}{2}}$ while the corresponding maximum probability of s_0 is only $0.85 \cdot e^{-\frac{1}{2}}$, so essentially s_0 and r_0 are not CSL-equivalent.

Different from the discrete case where $\sim_1^b$ is congruent, in the continuous case even $\sim_1$ is not congruent, refer to the following example.

Example 51. *Considering s and r in Example 45, s and r are CSL-equivalent, thus $s \sim_1 r$. Suppose we have t such that t can only evolve into t_1 with rate 2. We can show that actually*

$$s \parallel t \not\sim_1 r \parallel t$$

where all the states have different atomic propositions except $L(s) = L(r)$. Let $\psi = s\, \mathsf{U}_1^I (s_1 \parallel t)$ with $I = [a, \infty)$, then the probability of the paths of $s \parallel t$ satisfying ψ by choosing the left transition is equal to $\frac{3}{5} \cdot e^{-5a}$, similarly the probability is equal to $\frac{2}{3} \cdot e^{-6a}$ and $\frac{5}{7} \cdot e^{-7a}$ by choosing the middle and left transition respectively. By solving the inequations:

$$\frac{2}{3} \cdot e^{-6a} > \frac{3}{5} \cdot e^{-5a} \text{ and } \frac{2}{3} \cdot e^{-6a} > \frac{5}{7} \cdot e^{-7a},$$

we can see that if $e^{-a} \in (\frac{15}{14}, \frac{10}{9})$, the probability by choosing the middle transition is maximum which is greater than the correspondent probability of r, thus $s \parallel t \not\sim_1 r \parallel t$, and $\sim_1$ is not congruent.

5.7.2 Relation to (Weak) Bisimulation for CTMCs

For CTMCs each state has a unique Markovian transition, which will be denoted by $s \xrightarrow{\lambda_s} \mu_s$. The notion of weak bisimulation can be found in (54) for CTMCs, repeated as follows:

Definition 52 (Weak Bisimulation CTMC)**.** *For CTMCs, an equivalence relation $\mathcal{R}$ is a weak bisimulation iff for all $s\ \mathcal{R}\ r$ it holds (i) $L(s) = L(r)$, and (ii) $\lambda_s \cdot \mu_s(C) = \lambda_r \cdot \mu_r(C)$ for all equivalence classes $C \neq [s]_{\mathcal{R}}$. States s, r are weakly bisimilar, denoted by $s \approx_{\mathsf{CTMC}} r$, iff there exists a weak bisimulation $\mathcal{R}$ such that $s\ \mathcal{R}\ r$.*

Strong bisimilarity for CTMCs is defined if in addition $\lambda_s \cdot \mu_s(C) = \lambda_r \cdot \mu_r(C)$ holds for $C = [s]_{\mathcal{R}} = [r]_{\mathcal{R}}$ as well. States s, r are strongly bisimilar, denoted by $s \sim_{\mathsf{CTMC}} r$, iff there exists a strong bisimulation $\mathcal{R}$ such that $s\ \mathcal{R}\ r$.

Below we prove that, restricted to CTMCs, our strong and weak bisimulations agree with the strong and weak bisimulations for CTMCs:

Lemma 34. *For* CTMC*s, it holds that* $\sim = \sim_{\mathsf{CTMC}}$ *and* $\approx = \approx_{\mathsf{CTMC}}$.

Proof. The proof of $\sim = \sim_{\mathsf{CTMC}}$ is trivial, since in a CTMC there is only one transition for each state, thus we can simply replace $\to_{\mathsf{P}}$ with $\to$. The condition $\lambda_s \cdot \mu_s(C) = \lambda_r \cdot \mu_r(C)$ for each C coincides with the condition: i) $\lambda_s = \lambda_r$, and ii) $\mu_s \; \mathcal{R} \; \mu_r$.

We first prove that $\approx$ implies $\approx_{\mathsf{CTMC}}$. Let

$$\mathcal{R} = \{(s, r) \mid s \;\approx\; r\}$$

is a weak bisimulation referring to Definition 52. Suppose that $s \xrightarrow{\lambda_s} \mu_s$, we need to prove that $r \xrightarrow{\lambda_r} \mu_r$ such that $\lambda_s \cdot \mu_s(C) = \lambda_r \cdot \mu_r(C)$ for all $C \in S/\mathcal{R}$ with $C \neq [s]_{\mathcal{R}} = [r]_{\mathcal{R}}$. According to Definition 46, $s \;\approx\; r$ if $\bar{s} \;\sim\; \bar{r}$. By Definition 42, if $s \xrightarrow{\lambda_s} \mu_s$, then $\bar{s} \xrightarrow{E} \mu$ such that

$$\mu = \frac{E - \lambda_s}{E} \cdot \delta_{\bar{s}} + \frac{\lambda_s}{E} \cdot \bar{\mu_s}$$

where $\bar{\mu_s}$ is defined as expected. Therefore there exists $\bar{r} \xrightarrow{E} \nu$ such that $\mu \;\sim\; \nu$ where

$$\nu = \frac{E - \lambda_r}{E} \cdot \delta_{\bar{r}} + \frac{\lambda_r}{E} \cdot \bar{\mu_r}.$$

Obviously if there exists $C \in S/\mathcal{R}$ with $C \neq [s]_{\mathcal{R}} = [r]_{\mathcal{R}}$ such that $\lambda_s \cdot \mu_s(C) \neq \lambda_r \cdot \mu_r(C)$, then $\mu(\bar{C}) \neq \nu(\bar{C})$ since

$$\mu(\bar{C}) = \frac{\lambda_s}{E} \cdot \mu_s(C) \text{ and } \nu(\bar{C}) = \frac{\lambda_r}{E} \cdot \mu_r(C),$$

thus it is impossible for $\mu \;\sim\; \nu$.

To show that $\approx_{\mathsf{CTMC}}$ implies $\approx$, it is enough to show that

$$\mathcal{R} = \{(s, r) \mid s \;\approx_{\mathsf{CTMC}}\; r\}$$

is a weak bisimulation according to Definition 46, that is, we need show that

$$\mathcal{R} = \{(\bar{s}, \bar{r}) \mid s \;\approx_{\mathsf{CTMC}}\; r\}$$

is a strong bisimulation by Definition 45. Suppose that $\bar{s} \xrightarrow{E} \mu$, then there exists $s \xrightarrow{\lambda_s} \mu_s$ such that

$$\mu = \frac{E - \lambda_s}{E} \cdot \delta_{\bar{s}} + \frac{\lambda_s}{E} \cdot \bar{\mu_s}.$$

Since $s \approx_{\mathsf{CTMC}} r$, there exists $r \xrightarrow{\lambda_r} \mu_r$ such that $\lambda_s \cdot \mu_s(C) = \lambda_r \cdot \mu_r(C)$ for all equivalence class $C \neq [s]_{\approx_{\mathsf{CTMC}}} = [r]_{\approx_{\mathsf{CTMC}}}$. Therefore there exists $\bar{r} \xrightarrow{E} \nu$ such that

$$\nu = \frac{E - \lambda_r}{E} \cdot \delta_{\bar{r}} + \frac{\lambda_r}{E} \cdot \bar{\mu_r}$$

and $\mu(\bar{C}) = \nu(\bar{C})$ for all equivalence class $\bar{C} \neq [\bar{s}]_{\mathcal{R}} = [\bar{r}]_{\mathcal{R}}$, since $\mu(\bar{C}) = \frac{\lambda_s}{E} \cdot \mu_s(C)$ and $\nu(\bar{C}) = \frac{\lambda_r}{E} \cdot \mu_r(C)$ i.e. $\mu \; \mathcal{R} \; \nu$. □

The lemma above shows that $\sim$ and $\approx$ are conservative extensions of the strong bisimulation and the weak bisimulation for CTMCs in (54), and so are their logical characterization results except that they only work in a subset of CTMDPs.

5.7.3 Relation to (Weak) Simulations for CTMCs

The strong and weak simulations were introduced in (54), we recall the definition of the strong simulation as follows.

Definition 53 (Strong Simulation CTMC)**.** *For CTMCs , a relation $\mathcal{R}$ is a strong simulation iff for all $s \; \mathcal{R} \; r$ it holds (i) $L(s) = L(r)$, (ii) $\mu_s \sqsubseteq_{\mathcal{R}} \mu_r$, and (iii) $\lambda_s \leq \lambda_r$.*

State s is strongly simulated by r, denoted by $s \prec_{\mathsf{CTMC}} r$, iff there exists a strong simulation $\mathcal{R}$ such that $s \; \mathcal{R} \; r$.

The following relation holds for simulations:

Lemma 35. *For CTMCs, $\prec \subset \prec_{\mathsf{CTMC}}$. If the CTMC is uniformized,*

$$\prec = \prec_{\mathsf{CTMC}} = \precapprox .$$

Proof. According to Definition 50 and 53, the only difference between $\prec$ and $\prec_{\mathsf{CTMC}}$ is that $s \prec r$ requires that $\lambda_s = \lambda_r$ while $s \prec_{\mathsf{CTMC}} r$ only requires that $\lambda_s \leq \lambda_r$, thus $\prec \subseteq \prec_{\mathsf{CTMC}}$. In a uniformized CTMC, $\lambda_s = \lambda_r$ for any s and r, thus $\prec = \prec_{\mathsf{CTMC}} = \precapprox$. □

The simulation relation $\prec_{\mathsf{CTMC}}$ in (54) is strictly coarser than ours. In (54), it is shown that $\prec_{\mathsf{CTMC}}$ characterizes a sublogic of $\prec_{\mathsf{CSL}_s}$, denoted by $\prec_{\mathsf{CSL}_s^0}$, in which all intervals are of the form $[0, b]$, i.e., the left endpoint is always 0. The following example illustrates this difference:

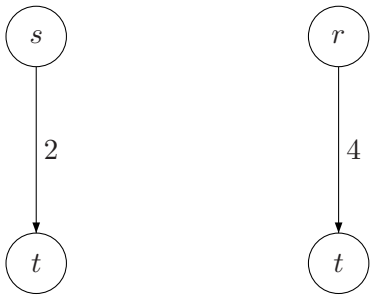

Figure 5.3: $\prec_{\mathsf{CTMC}}$ is too coarse (transition of t is omitted).

Example 52. *Considering the states s, r and t in Fig. 5.3 where $L(s) = L(r) \neq L(t)$, and t is an absorbing state. According to Definition 53, it is easy to check that*

$$s \prec_{\mathsf{CTMC}} r \text{ but } s \not\prec_{\mathsf{CSL}_s} r.$$

Let

$$\psi = (s \,\mathsf{U}^{[a,b]}\, t)$$

then the probability for the paths of s and r satisfying ψ is equal to

$$(e^{-2a} - e^{-2b}) \text{ and } (e^{-4a} - e^{-4b})$$

respectively, when $a = 0$ and $b > 0$,

$$(1 - e^{-2b}) < (1 - e^{-4b}),$$

while when $a > 0$ and $b = \infty$, $e^{-2a} > e^{-4a}$. In other words, there exists φ and φ' such that $s \models \varphi$, $r \not\models \varphi$ and $s \not\models \varphi'$, $r \models \varphi'$. Essentially, neither $s \prec_{\mathsf{CSL}_s} r$, nor $r \prec_{\mathsf{CSL}_s} s$ holds.

The various strong simulation definitions in this chapter can be slightly adapted such that they correspond to the safe sublogic as in (54). However, the same does not hold for weak simulations. We recall the definition of weak simulation on CTMC introduced in (54). Let $Post(s) = Supp(\mu_s)$ denote the successors of s. Bellow follows the definition of weak simulation where $i = 1, 2$:

Definition 54 (Weak Simulation CTMC)**.** *Given a CTMC, let $\mathcal{R} \subseteq S \times S$ be a weak simulation iff for $s_1 \,\mathcal{R}\, s_2$: $L(s_1) = L(s_2)$ and there exists functions $\eta_i : S \to [0, 1]$ and sets $U_i, V_i \subseteq S$ where*

$$U_i = \{u_i \in Post(s_i) \mid \eta_i(u_i) > 0\},$$

$$V_i = \{v_i \in Post(s_i) \mid \eta_i(v_i) < 1\}$$

such that:

1. $v_1 \mathrel{\mathcal{R}} s_2$ *for all* $v_1 \in V_1$, *and* $s_1 \mathrel{\mathcal{R}} v_2$ *for all* $v_2 \in V_2$.
2. *There exists a function* $\Delta : S \times S \to [0,1]$ *such that:*
   (a) $\Delta(u_1, u_2) > 0$ *implies* $u_i \in U_i$ *and* $u_1 \mathrel{\mathcal{R}} u_2$.
   (b) *If* $K_i > 0$, *then*
   $$K_1 \cdot \sum_{u_2 \in U_2} \Delta(w, u_2) = \eta_1(w) \cdot \mu_{s_1}(w)$$
   and
   $$K_2 \cdot \sum_{u_1 \in U_1} \Delta(u_1, w) = \eta_2(w) \cdot \mu_{s_2}(w)$$
   for all states $w \in S$ *where* $K_i = \sum_{u_i \in U_i} \eta_i(u_i) \cdot \mu_{s_i}(u_i)$.
   (c) $\sum_{u_1 \in U_1} \eta(u_1) \cdot \lambda_{s_1} \cdot \mu_{s_1}(u_1) \leq \sum_{u_2 \in U_2} \eta(u_2) \cdot \lambda_{s_2} \cdot \mu_{s_2}(u_2)$.

s_1 *is weakly simulated by* s_2, *written as* $s_1 \mathrel{\precsim_{\mathsf{CTMC}}} s_2$, *iff there exists a weak simulation* $\mathcal{R}$ *such that* $s_1 \mathrel{\mathcal{R}} s_2$.

The relation $\precsim_{\mathsf{CTMC}}$ is shown to be sound w.r.t. the sublogic $\mathsf{CSL}^0_{s\setminus \mathsf{X}}$ (obtained from CSL^0_s by removing the next operator). The completeness was conjectured, but remains *open*. In the following example we show that, on the contrary, the completeness *does not hold*.

Example 53. *Consider states* s_0 *and* r_0 *in Example 53 and shown in Fig. 5.5. We first show that* $s_0 \mathrel{\precsim_{\mathsf{CSL}^0_{s\setminus \mathsf{X}}}} r_0$. *It is easy to check that* $v_1 \mathrel{\precsim_{\mathsf{CSL}^0_{s\setminus \mathsf{X}}}} s_0$, *thus the transition from* s_0 *to* v_1 *is invisible. For the transition from* s_0 *to* u_1, r_0 *can perform exactly the same transition, thus no formula* φ *of* $\mathsf{CSL}^0_{s\setminus \mathsf{X}}$ *exists such that* $s_0 \models \varphi$ *but* $r_0 \not\models \varphi$. *Secondly, we show that* $s_0 \mathrel{\not\precsim_{\mathsf{CTMC}}} r_0$. *Obviously* $v_1 \mathrel{\precsim_{\mathsf{CTMC}}} r_0$, *but* $u_1 \mathrel{\not\precsim_{\mathsf{CTMC}}} r_0$, $s_0 \mathrel{\not\precsim_{\mathsf{CTMC}}} r_1$, *and* $s_0 \mathrel{\not\precsim_{\mathsf{CTMC}}} u_1$ *because* s_0, r_1, *and* u_1 *have different labels. Thus the only possible partition is letting* $U_1 = \{u_1\}$, $V_1 = \{v_1\}$, *and* $U_2 = \{r_1, u_1\}$, $V_2 = \emptyset$ *i.e.* $\eta_1(v_1) = 0$, $\eta_1(u_1) = 1$, $\eta_2(r_1) = \eta_2(u_1) = 1$. *According to Definition 54* $K_1 = 0.5$ *and* $K_2 = 1$. *Since* $u_1 \mathrel{\not\precsim_{\mathsf{CTMC}}} r_1$, *thus* $\Delta(u_1, r_1) = 0$, *but then* $K_2 \cdot \Delta(u_1, r_1) = 0 \neq 0.5 = \eta_2(r_1) \cdot \mu_{r_0}(r_1)$ *which contradicts the condition of Definition 54, thus* $s_0 \mathrel{\not\precsim_{\mathsf{CTMC}}} r_0$.

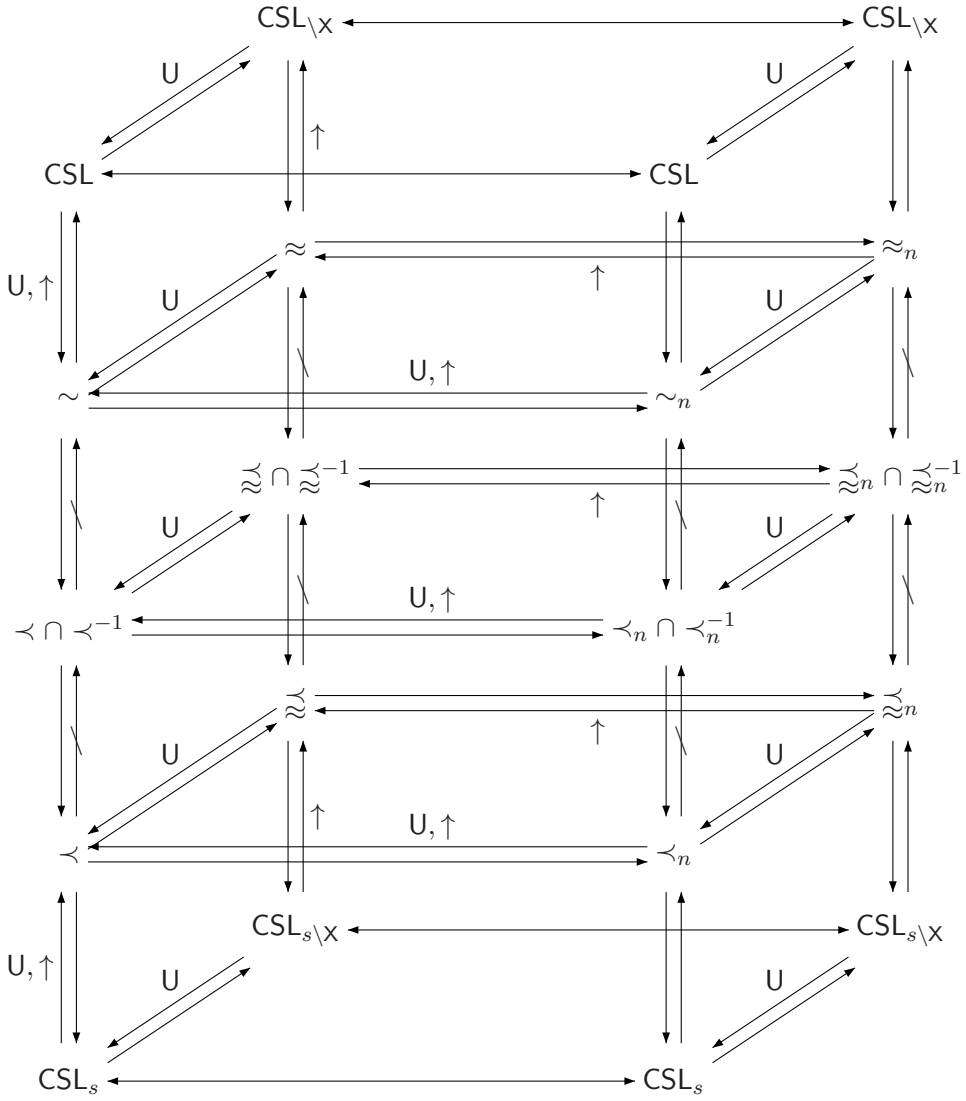

Figure 5.4: Relationship of various bisimulation and simulation relations

5.8 Summary

The spectrum of the branching time relations and the logic equivalences are summarized in Fig. 5.4. The arrow $\to$ should be interpreted as "imply". The labels U and $\uparrow$ denote that the implication is only valid in a uniformized CTMDP, and a CTMDP without 2-step recurrent states respectively. We write $\mathcal{L}$ directly for $\sim_{\mathcal{L}}$ for readability where $\mathcal{L}$ is a sub-logic of CSL. The index n appearing on the right plane is chosen according to Theorem 40 and 44. Thus $\sim_k = \sim_n$ for all $k \geq n$, and similar holds for other relations, and for a smaller index, the relation will be coarser.

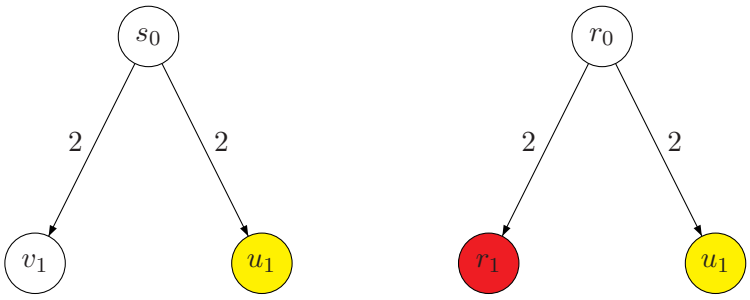

Figure 5.5: A counterexample for the completeness of $\precsim_{\mathsf{CTMC}}$.

5.9 Related Work

Logical characterizations of bisimulation have been studied extensively for stochastic models. For CTMCs the logic CSL characterizes bisimulations, while CSL without next-state formulas characterizes weak bisimulations (54). Our results in this chapter is a conservative extension for both strong and weak bisimulations. In (61), the results are extended to CTMCs with continuous state spaces.

For CTMDPs, the first logical characterization result is presented in (37). It is shown that strong bisimulation is sound, but not complete w.r.t. CSL equivalence. For the non-completeness please refer to Example 45 of this chapter. In this chapter, we introduced the weak bisimulation relation for CTMDPs. For a subclass of CTMDPs, i.e. without 2-step recurrent states, we have shown that the weak bisimulation is also complete for $\mathsf{CSL}_{\setminus \mathsf{X}}$-equivalence.

For probabilistic automata PA, Hennessy-Milner logic has been extended to characterize bisimulations in (55, 57, 89). In (56), Desharnais *et al.* have shown that weak bisimulation agrees with PCTL^* equivalence for PAs. The most related paper for PAs is our previous paper in (99), in which we have introduced bisimulations and i-depth bisimulations for characterizing logical equivalence induced by PCTL and sub-logics. This leads to the study of the i-depth bisimulation relations for CTMDPs in this chapter. For uniformized CTMDPs, we have shown that they agree with the equivalences in the discrete setting.

Chapter 6

Markov Automata

In this Chapter we address related issues of another stochastic model called Markov automata, which is the combination of PA and IMC. We first propose the late semantics of MAs based on which we then define the late weak bisimulation. It is shown that the late weak bisimulation is strictly coarser than the weak bisimulations defined in (5) and (6).

In Section 6.2 we give the definition of MA as well as its early and late semantics. The novel weak bisimulation is proposed with its compositionality being discussed in Section 6.3. In Section 6.4, we extend the results to early and weak simulations. Section 6.5 we investigate the relations between our weak bisimulations with the weak bisimulations introduced in (5) and (6). In Section 6.6 we briefly discuss how time-divergent MA are dealt with previously, and show that our late weak bisimulation is also the coarsest reduction barbed congruence.

6.1 Motivation

Recently, Markov automata (MA) have been proposed in (5) as a compositional behavioral model supporting both probabilistic transitions and exponentially distributed random delays. MA can be considered as a combination of probabilistic automata (PA) (78) and interactive Markov chains (IMC) (32). A PA is obtained by disallowing random delays, whereas an IMC is obtained by restricting to degenerative probabilistic transitions.

As the main result in (5), the authors have proposed the notion of weak bisimulation relation, which is shown to be congruent w.r.t. parallel composition. Moreover, the proposed weak bisimulation conservatively extends that for probabilistic automata (53, 78) and IMCs (32). However, as pointed out in the conclusion in (5),

> *"a good notion of equality is tightly linked to the practically relevant issue of constructing a small (quotient) model that contains all relevant information needed to analyze the system".*

Indeed, an example is given in the conclusion illustrating that an even *weaker version* of weak bisimulation would be expected.

In this chapter we address this problem by proposing such a weaker bisimulation. We start with discussing the example presented in the conclusion of (5). An extended version is shown in Fig. 6.1, where:

- In part (a) we have a Markovian transition out of state s labeled with rate 2λ, meaning that the sojourn time in state s is exponentially distributed with rate 2λ. Thus the probability of leaving it within time a is $1 - e^{-2\lambda a}$. From s' we have a probabilistic transition labeled with τ, leading to t_1 and t_2 with equal probability. Note the dashed arrows denote probabilistic transitions.

- Part (c) is similar to part (a), in the sense that first a probabilistic transition out of r is enabled, followed with a Markovian transition with rate 2λ.

- Part (b) has only Markovian transitions. Starting with state t, the sojourn time is exponentially distributed with rate 2λ. If the transition is taken, there is a race between the transition to t_1 and t_2 respectively. The probability that the transition to state t_1 wins the race is thus $\frac{1}{2}$. As a result, the overall probability of reaching state t_1 within time a is $(1-e^{-2\lambda a}) \cdot \frac{1}{2}$. Note that from t no probabilistic transitions can be reached.

The weak bisimulation defined in (5), written as $\approx_{ehz}$, identifies s and t: $s \approx_{ehz} t$. Intuitively $s \approx_{ehz} t$ because both s and t will leave their original states after an exponential delay with rate 2λ, and after leaving s and t they will reach either t_1 with probability 0.5, or t_2 with probability 0.5.

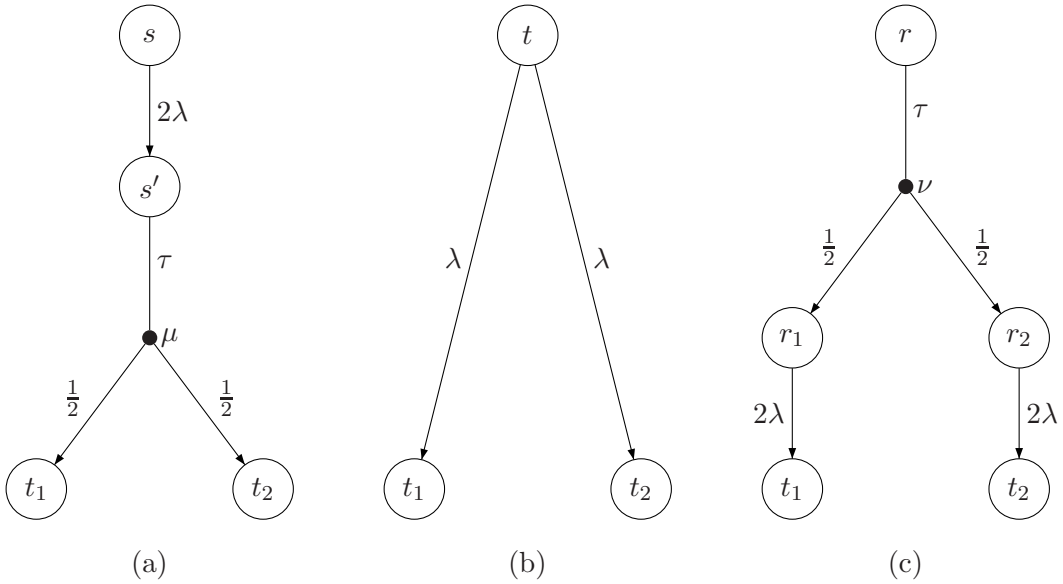

Figure 6.1: Examples of Markov automata.

However the weak bisimulation distinguishes t and r, i.e., $t \not\approx_{ehz} r$. Different from s, r will make a probabilistic choice first, and then move to either t_1 or t_2 after an exponential delay with rate 2λ. Thus the difference between s and r is just the order of the probabilistic choice and the Markovian transition. If one does not consider the intermediate states, but only the probability and time of reaching the states t_1 and t_2, obviously, all of the three states s, t, r are behaving the same.

In this chapter, we propose *early* and *late* semantics for Markovian transitions reflecting the example above. Under early semantics, Markovian transitions are considered as a sequence of sojourn time distributions followed with probabilistic choices. The core contribution in this chapter is the notion of *late weak bisimulation*, which is obtained by interpreting Markovian transitions as a sequence of probabilistic choices followed by sojourn time distributions, as illustrated in the example. However, the late semantics is much more involved to define for MA, especially if from state t also other probabilistic transitions labeled with α *would have been* enabled. In that case, under the late semantics this additional α-probabilistic transition *should also have been* enabled after the probabilistic choices, even after potential internal transitions from t_1 or t_2. We show that late weak bisimulation is strictly coarser than early weak bisimulation.

Both early and late weak bisimulations are defined over the derived structure of MA, namely through Markov labeled transition systems (MLTS), which is introduced by Deng and Hennesy in (6). Moreover, they have proposed another notion of weak bisimulation, denoted by $\approx_{dh}$, for MA. The weak bisimulation $\approx_{dh}$ enjoys the nice property of being a *reduction barbed congruence* (107), i.e., it is compositional, barb-preserving (simple experiments are preserved) and reduction-closed (nondeterministic choices are in some sense preserved). The relationship between $\approx_{ehz}$ and $\approx_{dh}$ is however unclear. In this chapter we clarify these relationships. We show that the *early weak bisimulation* induced under our early semantics gives rise to the weak bisimulation $\approx_{ehz}$, as well as $\approx_{dh}$. Thus, the proposed weak bisimulations $\approx_{ehz}$ and $\approx_{dh}$ agree with each other, and are strictly finer than our late weak bisimulation for MA. Since our late weak bisimulation is defined over the derived MLTS as well, applying a result in (6), even being coarser, our late weak bisimulation is a reduction barbed congruence as well.

Summarizing, the contributions of this chapter are as follows:

- For MA, we propose early and late semantics for Markovian transitions. Based on this notion, we propose early and late weak bisimulations. The latter is shown to be strictly coarser.
- We prove that our early weak bisimulation agrees with both the weak bisimulation proposed by Eisentraut, Hermanns and Zhang in (5), and with the weak bisimulation proposed by Deng and Hennesy in (6).
- We propose early and late weak simulations along the same line, and clarify the relation to weak simulations proposed in the literature.

6.2 Markov Automata

In this section we first introduce some notations and recall the definition of Markov automata. Then we introduce two different semantics: early and late semantics for Markov automata.

6.2.1 Preliminaries

Given a distribution μ, if $\mu(S) = 1$, it is called a *full distribution*, otherwise it is a *sub distribution*. Let $ADist(S)$ denote the set of all (sub or full) distributions over S,

ranged over by $\mu, \nu, \ldots$ too. To be clear, we will use $Dist(S)$ to denote the set of all full distributions. We often write $\{\mu(s) : s \mid s \in Supp(\mu)\}$ alternatively for a distribution μ. For instance, $\{0.4 : s_1, 0.6 : s_2\}$ denotes a distribution μ such that $\mu(s_1) = 0.4$ and $\mu(s_2) = 0.6$.

We first recall the definition of Markov automata introduced in (5). Then, we give the early and late semantics of Markov automata in terms of Markov labeled transition systems.

Definition 55 (Markov Automata)**.** *An* MA $\mathcal{M}$ *is a tuple* $(S, Act_\tau, \rightarrow, \twoheadrightarrow, s_0)$*, where*

- S *is a finite but non-empty set of states,*
- $Act_\tau = Act \dot{\cup} \{\tau\}$ *is a set of actions including internal action* τ*,*
- $\rightarrow \subset S \times Act_\tau \times Dist(S)$ *is a finite set of probabilistic transitions,*
- $\twoheadrightarrow \subset S \times R^+ \times S$ *is a finite set of Markovian transitions, and*
- $s_0 \in S$ *is the initial state.*

Again let $\alpha, \beta, \gamma, \ldots$ range over the actions in Act_τ, λ range over the rates in R^+. Moreover, let $\alpha_r, \beta_r, \gamma_r, \ldots$ range over $Act_\tau \cup R^+$. A state $s \in S$ is stable, written as $s\downarrow$, if $s \stackrel{\tau}{\not\twoheadrightarrow}$, similarly μ is stable, written as $\mu\downarrow$, iff $s\downarrow$ for each $s \in Supp(\mu)$. As in (5, 32), the *maximal progress assumption* is assumed, meaning that if state s is not stable, no Markovian transitions can be executed.

Let

$$rate(s, s') = \sum \{\lambda \mid s \stackrel{\lambda}{\twoheadrightarrow} s'\}$$

denote the rate from s to s'. Also the function *rate* is overloaded such that

$$rate(s) = \sum_{s' \in S} rate(s, s')$$

which denotes the exit rate of s. For a stable state s, the sojourn time at s is exponentially distributed with rate equal to $rate(s)$, and the probability of one of the Markovian transitions being taken within time $[0, a]$ is equal to $1 - e^{-rate(s)a}$.

MA extend the well-known probabilistic automata (PA) (78) and interactive Markov chains (IMC) (32). Precisely, if the set of Markovian transitions is empty, i.e., $\twoheadrightarrow = \emptyset$, we obtain PA. On the other side, if distributions are all Dirac, i.e., $\rightarrow \subset S \times Act_\tau \times \delta_S$ with $\delta_S = \{\delta_s \mid s \in S\}$, we obtain IMCs. Following (6), MA will be studied indirectly through the Markov labeled transition system:

Definition 56 (Markov Labeled Transition System)**.** *A Markov labeled transition system (*MLTS*) L is a triple $(S, Act_\tau, \rightarrow)$ where S and Act_τ are the same as in Definition 55, and*

$$\rightarrow \subseteq \ S \times (Act_\tau \cup R^+) \times Dist(S)$$

is a finite set of transitions satisfying $s \xrightarrow{\lambda_1} \mu_1$ and $s \xrightarrow{\lambda_2} \mu_2$ implies that $s \xrightarrow{\tau}\!\!\!\!\!\!\rightarrow$, $\lambda_1 = \lambda_2$, and $\mu_1 = \mu_2$.

Different from the definition of MA, in Definition 56 we require that $s \xrightarrow{\lambda_1} \mu_1$ and $s \xrightarrow{\lambda_2} \mu_2$ implies that $s \xrightarrow{\tau}\!\!\!\!\!\!\rightarrow$, $\lambda_1 = \lambda_2$, and $\mu_1 = \mu_2$. This means that each state in an MLTS can only have at most one Markovian transition, but after the Markovian transition, it will evolve into a distribution instead of a single state as in MA. This is not a restriction, but just expresses the race condition explicitly. In MLTS the *maximal progress assumption* is also embedded in the definition, i.e. $s \xrightarrow{\lambda} \mu$ implies that $s \xrightarrow{\tau}\!\!\!\!\!\!\rightarrow$.

As usual, a transition $\xrightarrow{\alpha_r}$ can be lifted to distributions, that is, $\mu \xrightarrow{\alpha_r} \mu'$ iff for each $s \in Supp(\mu)$ there exists $s \xrightarrow{\alpha_r} \mu_s$ such that $\sum_{s \in Supp(\mu)} \mu(s) \cdot \mu_s = \mu'$.

6.2.2 Early Semantics of Markov Automata

Definition 57 (Early Semantics)**.** *Let $\mathcal{M} = (S, Act_\tau, \rightarrow, \twoheadrightarrow, s_0)$ be an* MA*. The early semantics of $\mathcal{M}$ is defined as an* MLTS*, denoted by $^\bullet\mathcal{M} = (S, Act_\tau, \bullet\!\!\longrightarrow)$, where $\rightarrow \subseteq \bullet\!\!\longrightarrow$ and*

$$s \bullet\!\!\xrightarrow{\lambda} \mu, \text{ iff } s{\downarrow} \wedge \lambda = rate(s) \wedge \forall s' \in Supp(\mu).\mu(s') = \frac{rate(s, s')}{rate(s)}.$$

In the equation above we require that s is stable as usual due to the maximal progress assumption. As an example for the MA in Fig. 6.1(b), $t \xrightarrow{2\lambda} \{(\frac{1}{2} : t_1), (\frac{1}{2} : t_2)\}$ according to the early semantics.

To define the late semantics for MA, we need the notion of weak transitions which shall be introduced in this section. In order to abstract from the internal action of L, we let $s \xRightarrow{\alpha_r} \mu$ denote that a distribution μ is reached through a sequence of steps which are internal except one of which is equal to α_r. Formally, the weak transitions for MLTSs are defined as follows:

Definition 58 (Weak Transitions for MLTS)**.** *The weak transition relation $\xRightarrow{\alpha_r}$ is the least relation such that, $s \xRightarrow{\alpha_r} \mu$ iff*

1. *$\alpha_r = \tau$ and $\mu = \delta_s$, or*

2. *there exists a step* $s \xrightarrow{\beta_r} \mu'$ *such that* $\mu = \sum_{s' \in Supp(\mu')} \mu'(s') \cdot \mu_{s'}$, *where* $s' \stackrel{\tau}{\Longrightarrow} \mu_{s'}$ *if* $\beta_r = \alpha_r$, *otherwise* $s' \stackrel{\alpha_r}{\Longrightarrow} \mu_{s'}$ *and* $\beta_r = \tau$.

Intuitively, through the weak transition, s reaches the distribution μ through an *history-dependent scheduler*, very much the way it is introduced in (78). In more detail, the first clause says that in case $\alpha_r = \tau$, we can stop at s. Otherwise, from s the action β_r is chosen leading to the distribution μ', such that:

- if $\beta_r = \alpha_r$, then each state s' in the support of μ' reaches $\mu_{s'}$ only through a sequence of τ actions,
- if $\beta_r = \tau$, then each state s' in the support of μ' reaches $\mu_{s'}$ through a weak transition $s' \stackrel{\alpha_r}{\Longrightarrow} \mu_{s'}$

Stated differently, we unfold a tree with the root s, the successor states are determined by the action chosen from the node. It is history dependent as each state s may occur in different nodes in the tree, and each time a different transition may be chosen. We say that the weak transition $s \stackrel{\alpha_r}{\Longrightarrow} \mu$ is a *deterministic weak transition* if in addition it satisfies the property that each state picks always the same transition whenever it is visited. In the sequel we shall use $s \stackrel{\alpha_r}{\Longrightarrow}_D \mu$ to denote deterministic weak transitions, which will be used later in defining the late semantics. Note that only finitely many deterministic weak transitions exist, see (80).

The weak transition defined in Definition 58 can be lifted to distributions in a straightforward way as for strong transitions. Equivalently, weak transitions can be formalized elegantly using trees as in (56), or using infinite sum (108). The advantage of this definition will be clear in proving the equivalence results of all the existing weak bisimulations.

6.2.3 Late Semantics of Markov Automata

When defining the early semantics of an MA in Definition 57, a stable state with Markovian transition is equipped with a transition labeled with its exit rate λ, followed by a distribution depending on the race condition. As discussed in the introduction, in the late semantics, we switch the interpretation, namely the state first evolves into a distribution according to the race condition, followed by a Markovian transition labeled with λ.

In the late semantics we introduce the set of states

$$[\![S]\!] := \{[\![s,t]\!] \mid s,t \in S \wedge s{\downarrow} \wedge rate(s) > 0\}.$$

The outgoing transitions from these new states are defined by: $[\![s,t]\!]$ be a state such that i) $[\![s,t]\!] \xrightarrow{\lambda} t$ where $\lambda = rate(s)$, and ii) $[\![s,t]\!] \xrightarrow{\alpha} \mu$ iff $s \xrightarrow{\alpha} \mu$. Intuitively, $[\![s,t]\!]$ is a new state having exactly the same non-Markovian transitions as s, and can evolve into t via a Markovian transition with rate equal to $rate(s)$. Moreover, for a distribution μ over S, we let $[\![s,\mu]\!]$ denote the corresponding distribution over $[\![S]\!]$ satisfying $[\![s,\mu]\!]([\![s,t]\!]) = \mu(t)$ for all $t \in S$. The late semantics is defined as follows.

Definition 59 (Late Semantics)**.** *Let $\mathcal{M} = (S, Act_\tau, \to, \twoheadrightarrow, s_0)$ be an* MA*. Moreover, let the* MLTS $^\bullet\mathcal{M} = (S, Act_\tau, \bullet\!\!\longrightarrow)$ *be its early semantics. The late semantics of $\mathcal{M}$, denoted by $\mathcal{M}^\bullet = (S \cup [\![S]\!], Act_\tau, \longrightarrow\!\!\bullet)$, is the smallest* MLTS *such that for each $s \in S$*

1. *$s \bullet\!\!\xrightarrow{\alpha} \mu$ implies that $s \xrightarrow{\alpha}\!\!\bullet\ \mu$,*
2. *$s \bullet\!\!\xrightarrow{\lambda}\bullet\!\!\xRightarrow{\tau}_D \mu$ implies that $s \xrightarrow{\tau}\!\!\bullet\ [\![s,\mu]\!]$ and for all $[\![s,t]\!] \in Supp([\![s,\mu]\!])$, $[\![s,t]\!] \xrightarrow{\lambda}\!\!\bullet\ \delta_t$ and $[\![s,t]\!] \xrightarrow{\alpha}\!\!\bullet\ \nu$ iff $s \bullet\!\!\xrightarrow{\alpha} \nu$.*

The idea of Definition 59 is to postpone the exponentially distributed sojourn time distribution of s after the probability choices. The first case is trivial where all other non-Markovian transitions from s will be then copied. If $s \bullet\!\!\xrightarrow{\lambda}\bullet\!\!\xRightarrow{\tau}_D \mu$, then it can be seen that μ is obtained by applying the race condition after the Markovian transition. As a result in the late semantics we can let s choose the successors according to the race condition first, and then perform other delayed actions. Therefore $s \xrightarrow{\tau}\!\!\bullet\ [\![s,\mu]\!]$ where for each $[\![s,t]\!] \in Supp([\![s,\mu]\!])$, there exists a $t \in Supp(\mu)$ such that all the delayed non-Markovian transition of s is enabled at $[\![s,t]\!]$ i.e. $[\![s,t]\!] \xrightarrow{\alpha}\!\!\bullet\ \nu$ iff $s \bullet\!\!\xrightarrow{\alpha} \nu$, moreover $[\![s,t]\!]$ will leave for δ_t via Markovian transition with rate λ i.e. $[\![s,t]\!] \xrightarrow{\lambda}\!\!\bullet\ \delta_t$. Essentially, for each $t \in Supp(\mu)$ and s we introduce a new state $[\![s,t]\!] \in [\![S]\!]$ such that all the delayed non-Markovian transition of s and the delayed Markovian transition to t are enabled at $[\![s,t]\!]$. The following two examples illustrate how the late semantics works.

Example 54. *For the* MA *t in Fig. 6.1(b), by adopting the late semantics, we have*

$$t \xrightarrow{\tau}\!\!\bullet\ \{\frac{1}{2} : [\![t,t_1]\!], \frac{1}{2} : [\![t,t_2]\!]\}$$

in the resulting MLTS *where the only possible transitions for* $[\![t, t_1]\!]$ *and* $[\![t, t_2]\!]$ *are* $[\![t, t_1]\!] \xrightarrow{2\lambda}\!\bullet\ \delta_{t_1}$ *and* $[\![t, t_2]\!] \xrightarrow{2\lambda}\!\bullet\ \delta_{t_2}$. *Considering the* MA *in Fig. 6.1(a), since*

$$s \xrightarrow{2\lambda}\!\bullet\ \delta_{s'} \stackrel{\tau}{\Longrightarrow}_D \{(\frac{1}{2} : t_1), (\frac{1}{2} : t_2)\},$$

according to Definition 59 we will also have

$$s \xrightarrow{\tau}\!\bullet\ \{\frac{1}{2} : [\![s, t_1]\!], \frac{1}{2} : [\![s, t_2]\!]\},$$

in the resulting late semantics MLTS. *Thus, the three systems are equivalent w.r.t. the late semantics. Note for states without Markovian transitions like r in Fig. 6.1 (c), we do not need to introduce extra states for them.*

Example 55. *Suppose we have an* MA *shown in Fig. 6.2(b). It is not hard to see that* $s_0 \xrightarrow{3\lambda}\!\bullet\ \mu$ *such that* $\mu = \{\frac{1}{3} : s_3, \frac{2}{3} : s_4\}$ *according to the early semantics which is illustrated by the* MLTS *in Fig. 6.2(a). Instead if we adopt the late semantics, we can move the probabilistic choice upward, and thus postpone the execution of other actions. Specifically, we allow* s_0 *to have a transition* $s_0 \xrightarrow{\tau}\!\bullet\ [\![s_0, \mu]\!]$ *where*

$$[\![s_0, \mu]\!] = \{\frac{1}{3} : [\![s_0, s_3]\!], \frac{2}{3} : [\![s_0, s_4]\!]\},$$

moreover $[\![s_0, s_3]\!]$ *and* $[\![s_0, s_4]\!]$ *are two new states where all the delayed actions including the Markovian action are enabled i.e.* α *and* 3λ *in this cased. Formally,* $[\![s_0, s_3]\!] \xrightarrow{\alpha}\!\bullet\ \delta_{s_1}$ *and* $[\![s_0, s_4]\!] \xrightarrow{\alpha}\!\bullet\ \delta_{s_1}$ *because of* $s_0 \xrightarrow{\alpha}\!\bullet\ \delta_{s_1}$, *moreover* $[\![s_0, s_3]\!] \xrightarrow{3\lambda}\!\bullet\ \delta_{s_3}$ *and* $[\![s_0, s_4]\!] \xrightarrow{3\lambda}\!\bullet\ \delta_{s_4}$ *because of* $rate(s_0) = 3\lambda$. *The correspondent* MLTS *of* s_0 *according to the late semantics is shown in Fig. 6.2(c).*

A few remarks are in order:

1. We have used deterministic weak transitions $\stackrel{\tau}{\Longrightarrow}_D$ to define the late semantics. Using weak transitions would do the same job, but induces then late semantics with infinitely many transitions. As the deterministic weak transition in Definition 59 involves only internal τ transitions, the algorithm in (80) can be used directly for constructing the late semantics. The resulting late semantics can have exponentially many transitions.

2. Notice that in Definition 59 we consider each deterministic weak τ transition after the Markovian transition in the second clause. Indeed, it is not enough

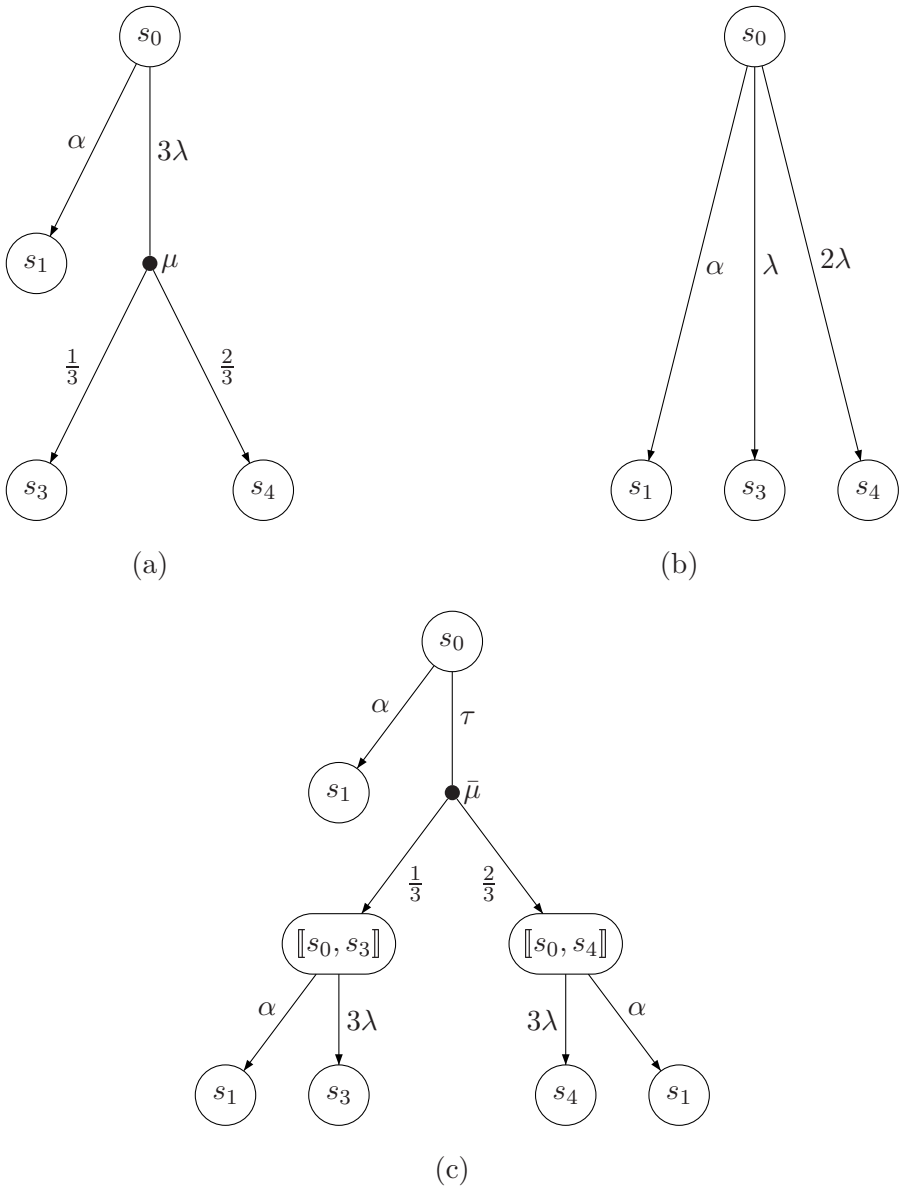

Figure 6.2: Illustration of early and late semantics.

to only consider strong τ transitions. Intuitively, by using deterministic weak τ transition we can postpone the execution of the exponentially distributed sojourn time distribution after any probabilistic internal transitions, not just that with one step. Refer to Example 59 in the next section for more details.

3. The size of $[\![S]\!]$ is in the worst case $|S|^2$. By the definition of late semantics, we only need to consider states $[\![s, t]\!]$ such that $s\downarrow$, and t is reachable from s via τ

transitions after the Markovian transition. Thus, in a real model the size of $[\![S]\!]$ is expected to be much smaller.

6.3 Weak Bisimulations

Before we introduce early and late weak bisimulations, we define some notations about transitions for MLTS. For a given MLTS $L = (S, Act_\tau, \to)$, we define $\xrightarrow{\alpha_r}_\rho$ and $\stackrel{\alpha_r}{\Longrightarrow}_\rho$ as following:

Definition 60. *1.* $\mu \xrightarrow{\alpha_r}_\rho \mu'$ *with* $\rho \in (0,1]$ *iff there exists a* $\mu = \mu_1 + \mu_2$ *such that* $\rho = |\mu_1|$ *and either* $\alpha_r = \tau$ *and* $\mu' = \frac{1}{\rho} \cdot \mu_1$, *or* $\frac{1}{\rho} \cdot \mu_1 \xrightarrow{\alpha_r} \mu'$,

2. $\mu \stackrel{\alpha_r}{\Longrightarrow}_\rho \mu'$ *with* $\rho \in (0,1]$ *iff there exists a* $\mu = \mu_1 + \mu_2$ *such that* $\rho = |\mu_1|$ *and* $\frac{1}{\rho} \cdot \mu_1 \stackrel{\alpha_r}{\Longrightarrow} \mu'$.

Intuitively, the index ρ is the part of the distribution of μ which makes the move to μ', which is scaled by $\frac{1}{\rho}$ such that μ' is a full distribution. Note that the condition "$\alpha_r = \tau$ and $\mu' = \frac{1}{\rho} \cdot \mu_1$" in clause 1 of Definition 60 is necessary, refer to the Example 56 for a detail discussion. In the following let

$$Suc(\mu) = \{\nu \mid \exists \rho > 0.(\mu \xrightarrow{\alpha_r}_\rho \nu)\}$$

denote the *successors* of ν, and $Suc^*(\mu)$ be the transitive closure, called the *derivatives* of μ.

6.3.1 Early and Late Weak Bisimulations

Below follows the definition of our weak bisimulation for MLTSs.

Definition 61 (Weak Bisimulation)**.** *Let* $L = (S, Act_\tau, \to)$ *be an* MLTS. *A relation* $\mathcal{R} \subseteq Dist(S) \times Dist(S)$ *is a weak bisimulation over* L *iff* $\mu \mathcal{R} \nu$ *implies that*

1. whenever $\mu \xrightarrow{\alpha_r}_\rho \mu'$, *there exists a* $\nu \stackrel{\alpha_r}{\Longrightarrow}_\rho \nu'$ *such that* $\mu' \mathcal{R} \nu'$,

2. whenever $\nu \xrightarrow{\alpha_r}_\rho \nu'$, *there exists a* $\mu \stackrel{\alpha_r}{\Longrightarrow}_\rho \mu'$ *such that* $\mu' \mathcal{R} \nu'$.

μ *and* ν *are weakly bisimilar, written as* $\mu \approx^L \nu$, *iff there exists a weak bisimulation* $\mathcal{R}$ *such that* $\mu \mathcal{R} \nu$. *Moreover* $s \approx^L r$ *iff* $\delta_s \approx^L \delta_r$.

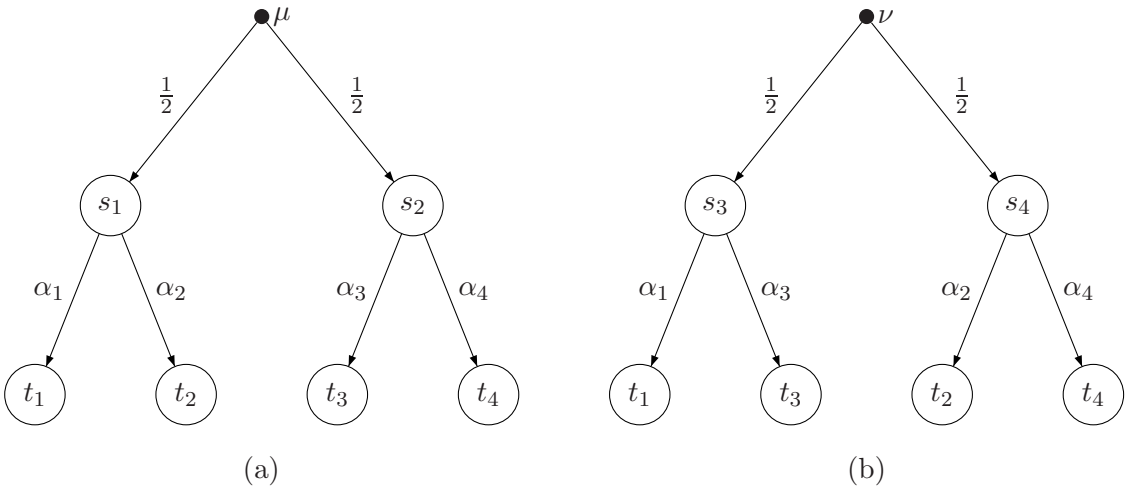

Figure 6.3: Two distributions which should not be weakly bisimilar.

Intuitively, if two distributions μ and ν are weakly bisimilar, then whenever μ is able to make a transition labeled with α_r with probability ρ, ν must be able to mimic the transition with the same probability such that their resulting distributions should be weakly bisimilar as well. As mentioned before, the condition "$\alpha_r = \tau$ and $\mu' = \frac{1}{\rho} \cdot \mu_1$" in clause 1 of Definition 60 cannot be omitted, refer to the following counterexample.

Example 56. *Suppose there are two distributions μ and ν given in Fig. 6.3 (a) and (b) respectively where $\alpha_i (1 \leq i \leq 4)$ are pairwise different, then if we omit the condition "$\alpha_r = \tau$ and $\mu' = \frac{1}{\rho} \cdot \mu_1$" in Definition 60, μ only has four strong transitions: $\mu \xrightarrow{\alpha_1}_{\frac{1}{2}} \delta_{t_1}$, $\mu \xrightarrow{\alpha_2}_{\frac{1}{2}} \delta_{t_2}$, $\mu \xrightarrow{\alpha_3}_{\frac{1}{2}} \delta_{t_3}$, and $\mu \xrightarrow{\alpha_4}_{\frac{1}{2}} \delta_{t_4}$, each of which can be simulated by ν and vice versa. Therefore we will conclude that μ and ν are weakly bisimilar according to Definition 61. This is against intuition since μ can evolve into s_1 with probability $\frac{1}{2}$ where only transitions labeled with α_1 and α_2 are possible, this cannot be simulated by ν.*

Definition 61 is defined upon MLTSs. For MA, below we shall introduce early and late weak bisimulations based on the early and late semantics, respectively:

Definition 62 (Early and Late Weak Bisimulation)**.** *Let $\mathcal{M} = (S, Act_\tau, \rightarrow, \twoheadrightarrow, s_0)$ be an* MA*. Then, $\mu, \nu \in Dist(S)$ are*

1. *early weakly bisimilar, written as $\mu \overset{\bullet}{\approx} \nu$, iff $\mu \approx^{\bullet_{\mathcal{M}}} \nu$,*
2. *late weakly bisimilar, written as $\mu \overset{\bullet}{\approx} \nu$, iff $\mu \approx^{\mathcal{M}_\bullet} \nu$.*

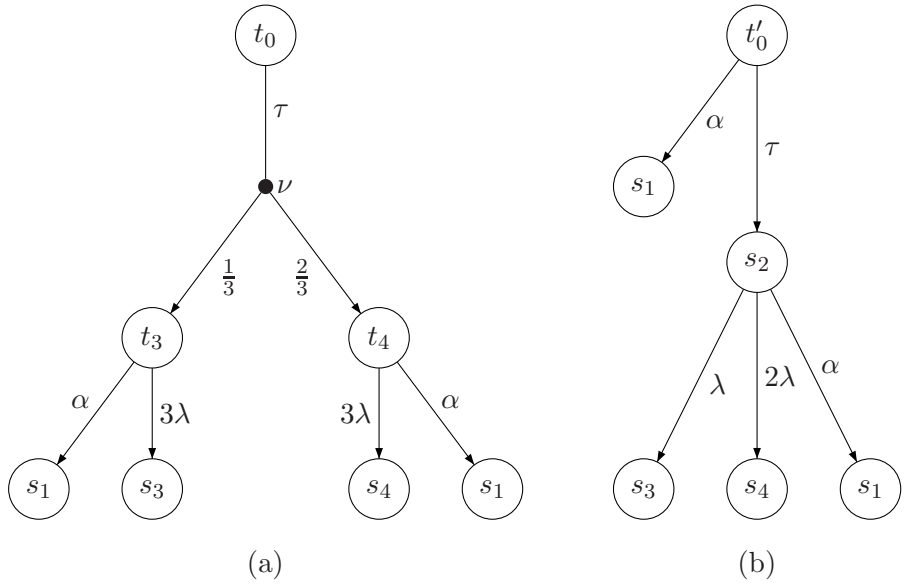

Figure 6.4: Example of late weakly bisimilar states.

In the above definition, we skip the superscript $\mathcal{M}$ in ${}^{\bullet}\approx$ and $\approx^{\bullet}$, as we assume there is a given MA $\mathcal{M} = (S, Act_\tau, \rightarrow, \twoheadrightarrow, s_0)$, if not mentioned explicitly, throughout the remaining parts.

Example 57. *Recall the example given in Fig. 6.1, we have shown that* $s \,{}^{\bullet}\!\approx\, t$*, but* $s \,{}^{\bullet}\!\not\approx\, r$ *since* δ_r *can evolve into* ν *via a* τ *transition where* ν *cannot be simulated by* δ_s *or any derivative of it. But by considering the late semantics,* s *will also have a transition similar to* r*, that is,* $s \xrightarrow{\tau}\!\!\bullet\, [\![s, \mu]\!]$ *which is obviously able to simulate* ν *since* $s \xrightarrow{2\lambda}\!\!\bullet \Longrightarrow_D \mu$*, thus we have* $s \,\approx^{\bullet}\, r$*.*

Example 58. *Suppose we are given an* MA *where the states* t_0 *and* t'_0 *behave following the way described in Fig. 6.4(a) and (b) respectively. Then it can be shown that* $t_0 \,\approx^{\bullet}\, t'_0$*. For instance for* s_2 *in Fig. 6.4(b), since*

$$s_2 \xrightarrow{3\lambda}\!\!\bullet \Longrightarrow_D \mu = \{(\frac{1}{3} : s_3), (\frac{2}{3} : s_4)\}$$

according to the early semantics, we have $s_2 \xrightarrow{\tau}\!\!\bullet\, [\![s_2, \mu]\!]$ *according to the late semantics. It is easy to check that* $\nu \,\approx^{\bullet}\, [\![s_2, \mu]\!]$*. The other cases can be checked in a similar way, therefore by Definition 62* $t_0 \,\approx^{\bullet}\, t'_0$*. Notice that* $t_0 \,\not\approx^{\bullet\mathcal{M}}\, t'_0$ *i.e.* $t_0 \,{}^{\bullet}\!\not\approx\, t'_0$*, since* ν *cannot be simulated by any derivative of* t'_0*. By interpreting* t'_0 *using early semantics,* s_2 *can*

only evolve into $\{(\frac{1}{3} : s_3), (\frac{2}{3} : s_4)\}$ *via Markovian transition with rate* 3λ. *Therefore* $t_0 \overset{\bullet}{\not\approx} t_0'$.

In Definition 59 we consider each deterministic weak τ transition after the Markovian transition, since it turns out that it is not enough to only consider strong τ transition, refer to the following counterexample.

Example 59. *Let us consider* s *and* r *in Fig. 6.1(a) and (c) again, if we only consider strong* τ *transition in Definition 59 i.e. replacing* $s \xrightarrow{\lambda} \xRightarrow{\tau}_D \mu$ *in the second clause by* $s \xrightarrow{\lambda} \xrightarrow{\tau} \mu$, *then still* $s \overset{\bullet}{\approx} r$. *But this does not work in general, for instance if we change* s *a little bit by adding another intermediate state* s'' *such that* $s' \xrightarrow{\tau} s''$ *and* $s'' \xrightarrow{\tau} \mu$, *then* $s \xrightarrow{2\lambda} \xrightarrow{\tau} \delta_{s''}$, *thus we will have* $s \xrightarrow{\tau} [\![s, \delta_{s''}]\!]$ *where* $[\![s, s'']\!] \xrightarrow{2\lambda} \delta_{s''}$. *Since* s *is the only state with Markovian transition in Fig. 6.1 (a), hence all the other states will have the same transitions in the late semantics* MLTS. *It is not hard to see that* $s \overset{\bullet}{\not\approx} r$ *according to Definition 62, since neither* δ_{r_1} *nor* δ_{r_2} *can be simulated by any derivative of* s, *this is against our intuition.*

6.3.2 Properties of Early and Late Weak Bisimulations

In Definition 61 we have used strong transitions on the left side of Clauses 1 and 2. As in the standard setting for transition systems, in the lemma below we show that the weak bisimulation does not change if we replace the strong transitions by weak transitions. This simple replacement is very useful for proving the transitivity, which we shall see later.

Lemma 36. *Let* $L = (S, Act_\tau, \rightarrow)$ *be an* MLTS. *A relation* $\mathcal{R} \subseteq Dist(S) \times Dist(S)$ *is a weak bisimulation iff* $\mu \; \mathcal{R} \; \nu$ *implies that*

1. *whenever* $\mu \xRightarrow{\alpha_r}_\rho \mu'$, *there exists a* $\nu \xRightarrow{\alpha_r}_\rho \nu'$ *such that* $\mu' \; \mathcal{R} \; \nu'$,
2. *whenever* $\nu \xRightarrow{\alpha_r}_\rho \nu'$, *there exists a* $\mu \xRightarrow{\alpha_r}_\rho \mu'$ *such that* $\mu' \; \mathcal{R} \; \nu'$.

Proof. Let

$$\mathcal{R} = \{(\mu, \nu) \mid \mu \approx^L \nu\},$$

and suppose that $\mu \; \mathcal{R} \; \nu$ and $\mu \xRightarrow{\alpha_r}_\rho \mu'$, we are going to show that there exists a $\nu \xRightarrow{\alpha_r}_\rho \nu'$ such that $\mu' \; \mathcal{R} \; \nu'$ by structural induction. According to the definition of $\xRightarrow{\alpha_r}_\rho$, there exists $\mu \xrightarrow{\alpha_r}_{\rho_1} \mu_1 \xRightarrow{\tau}_{\rho_1'} \mu_1'$ and $\mu \xrightarrow{\tau}_{\rho_2} \mu_2 \xRightarrow{\alpha_r}_{\rho_2'} \mu_2'$ such that

$$\rho_1 \cdot \rho_1' + \rho_2 \cdot \rho_2' = \rho \text{ and } (\frac{\rho_1 \cdot \rho_1'}{\rho} \cdot \mu_1' + \frac{\rho_2 \cdot \rho_2'}{\rho} \cdot \mu_2') \equiv \mu.$$

Since $\mu \approx^L \nu$, there exists $\nu \stackrel{\alpha_r}{\Longrightarrow}_{\rho_1} \nu_1$ and $\nu \stackrel{\tau}{\Longrightarrow}_{\rho_2} \nu_2$ such that $\mu_1 \approx^L \nu_1$ and $\mu_2 \approx^L \nu_2$. By induction there exists $\nu_1 \stackrel{\alpha_r}{\Longrightarrow}_{\rho_1'} \nu_1'$ and $\nu_2 \stackrel{\tau}{\Longrightarrow}_{\rho_2'} \nu_2'$ such that $\mu_1' \approx^L \nu_1'$ and $\mu_2' \approx^L \nu_2'$, so there exists a

$$\nu \stackrel{\alpha_r}{\Longrightarrow}_{\rho} \nu' \equiv (\frac{\rho_1 \cdot \rho_1'}{\rho} \cdot \nu_1' + \frac{\rho_2 \cdot \rho_2'}{\rho} \cdot \nu_2')$$

such that $\mu' \approx^L \nu'$ i.e. $\mu' \mathcal{R} \nu'$.

The other direction is trivial since the strong transition is a special case of the weak transition. □

The following theorem shows that the weak bisimulation defined in Definition 61 is an equivalence relation, and $\approx^\bullet$ is strictly coarser than $\overset{\bullet}{\approx}$.

Theorem 46. *For any* MLTS L, $\approx^L$ *is an equivalence relation. For any* MA, $\overset{\bullet}{\approx}$, *and* $\approx^\bullet$ *are equivalence relations, moreover* $\overset{\bullet}{\approx} \subset \approx^\bullet$.

Proof. We first prove that $\approx^L$ is an equivalence relation. The symmetry and reflexivity is easy to prove and is omitted here. We only show how to prove the transitivity. Suppose that $\mu_1 \approx^L \mu_2$ and $\mu_2 \approx^L \mu_3$, we need to prove that $\mu_1 \approx^L \mu_3$. By Definition 61, if $\mu_1 \approx^L \mu_2$ and $\mu_2 \approx^L \mu_3$, then there exists two weak bisimulations $\mathcal{R}_1$ and $\mathcal{R}_2$ such that $\mu_1 \mathcal{R}_1 \mu_2$ and $\mu_2 \mathcal{R}_2 \mu_3$. Let

$$\mathcal{R} = \{(\nu_1, \nu_3) \mid \exists \nu_2 . \nu_1 \mathcal{R}_1 \nu_2 \wedge \nu_2 \mathcal{R}_2 \nu_3\}.$$

It is clear that $\mu_1 \mathcal{R} \mu_3$, so once we can prove that $\mathcal{R}$ is a weak bisimulation, we can say that $\mu_1 \approx^L \mu_3$. Suppose that $\mu_1 \stackrel{\alpha_r}{\Longrightarrow}_{\rho} \mu_1'$, then there exists a $\mu_2 \stackrel{\alpha_r}{\Longrightarrow}_{\rho} \mu_2'$ such that $\mu_1' \mathcal{R}_1 \mu_2'$. Since we also have $\mu_2 \mathcal{R}_2 \mu_3$ where $\mathcal{R}_2$ is a weak bisimulation, so there exists a $\mu_3 \stackrel{\alpha_r}{\Longrightarrow}_{\rho} \mu_3'$ such that $\mu_2' \mathcal{R}_2 \mu_3'$. By definition of $\mathcal{R}$, we have $\mu_1' \mathcal{R} \mu_3'$, so $\mathcal{R}$ is a weak bisimulation.

Secondly, we prove that $\overset{\bullet}{\approx} \subset \approx^\bullet$. Suppose that $\overset{\bullet}{\mathcal{M}} = (S, Act_\tau, \overset{\bullet}{\longrightarrow})$ and $\mathcal{M}^\bullet = (S', Act_\tau, \overset{\bullet}{\longrightarrow})$. First we show that $\mu \overset{\bullet}{\approx} \nu$ implies $\mu \approx^\bullet \nu$. Let

$$\mathcal{R} = \{(\mu, \nu) \mid \mu \overset{\bullet}{\approx} \nu\} \cup \mathcal{R}'$$

where $\mathcal{R}'$ is the least relation satisfying:

- $([\![s, \mu]\!], [\![r, \nu]\!]) \in \mathcal{R}'$ with $\delta_s \overset{\bullet}{\approx} \delta_r$ and $\mu \overset{\bullet}{\approx} \nu$,
- $(\mu, \nu) \in \mathcal{R}$ if there exists $\mu_1 \mathcal{R} \nu_1$ and $\mu_2 \mathcal{R} \nu_2$ such that $\mu = \rho \cdot \mu_1 + (1 - \rho) \cdot \mu_2$ and $\nu = \rho \cdot \nu_1 + (1 - \rho) \cdot \nu_2$.

Then according to Definition 62 it is enough to show that $\mathcal{R}$ is a weak bisimulation w.r.t. $\mathcal{M}^{\bullet}$. Let $(\mu,\nu)\in\mathcal{R}$. We need to prove that whenever $\mu \xrightarrow{\alpha_r}\!\!\bullet_\rho\ \mu'$, there exists a $\nu \stackrel{\alpha_r}{\Longrightarrow}\!\!\bullet_\rho\ \nu'$ such that $\mu'\ \mathcal{R}\ \nu'$. First assume that $(\mu,\nu)\notin\mathcal{R}'$, implying that $Supp(\mu), Supp(\nu)\subseteq S$. We then consider the following cases:

1. $\alpha_r=\alpha\in Act$. If $\mu \xrightarrow{\alpha}\!\!\bullet_\rho\ \mu'$, then according to Clause 1 $\mu \bullet\!\!\xrightarrow{\alpha}_\rho\ \mu'$. Since $\mu \overset{\bullet}{\approx}\ \nu$, then there exists a $\nu \bullet\!\!\stackrel{\alpha}{\Longrightarrow}_\rho\ \nu'$ such that $\mu' \overset{\bullet}{\approx}\ \nu'$, therefore there also exists $\nu \stackrel{\alpha}{\Longrightarrow}\!\!\bullet_\rho\ \nu'$ such that $\mu'\ \mathcal{R}\ \nu'$ since $s \bullet\!\!\xrightarrow{\alpha} \mu''$ implies that $s \xrightarrow{\alpha}\!\!\bullet\ \mu''$ for each s.

2. $\alpha_r=\tau$. We prove by induction n i.e. the size of $Supp(\mu)$. If $n=1$ and $\mu=\delta_s$ for some s, then by Definition 59 whenever $\delta_s \xrightarrow{\tau}\!\!\bullet\ \mu'$ for some μ', we know that either

   - $s \bullet\!\!\xrightarrow{\tau} \mu'$, or
   - $s \bullet\!\!\xrightarrow{\lambda}\!\!\bullet\!\!\stackrel{\tau}{\Longrightarrow}_D \mu''$ such that $\mu'=[\![s,\mu'']\!]$.

   For the first case, it is similar as Clause 1, and is omitted here. For the second case, since $\delta_s \overset{\bullet}{\approx}\ \nu$, there exists a $\nu \bullet\!\!\stackrel{\lambda}{\Longrightarrow}_1 \nu''$ such that $\mu'' \overset{\bullet}{\approx}\ \nu''$, that is,

$$\nu \bullet\!\!\stackrel{\tau}{\Longrightarrow} \nu_1 \bullet\!\!\xrightarrow{\lambda}\!\!\bullet\!\!\stackrel{\tau}{\Longrightarrow}_D \nu''$$

   where $\delta_s \overset{\bullet}{\approx}\ \nu_1$. According to Definition 59 $\nu \stackrel{\tau}{\Longrightarrow} [\![\nu_1,\nu'']\!]$ where $[\![\nu_1,\nu'']\!]=[\![r,\nu'']\!]$ for some $r\in Supp(\nu_1)$, obviously $[\![s,\mu'']\!]\ \mathcal{R}\ [\![\nu_1,\nu'']\!]$. As a result there exists a $\nu \stackrel{\tau}{\Longrightarrow}\!\!\bullet\ \nu'=[\![\nu_1,\nu'']\!]$ such that $\mu'\ \mathcal{R}\ \nu'$. When $n>1$, for some $s\in Supp(\mu)$, there exists a $\nu \bullet\!\!\stackrel{\tau}{\Longrightarrow} \nu_1+\nu_2$ such that $\mu(s)=|\nu_1|$ and $\delta_s \overset{\bullet}{\approx}\ (\frac{1}{|\nu_1|}\cdot\nu_1)$. The following proof is straightforward by induction.

3. $\alpha_r=\lambda$. This case is impossible, since according to Definition 59 only states in $[\![S]\!]$ can perform Markovian transitions.

For the case $(\mu,\nu)\in\mathcal{R}'$ we prove that $[\![s,\mu]\!] \overset{\bullet}{\approx} [\![r,\nu]\!]$ provided that $\delta_s \overset{\bullet}{\approx}\ \delta_r$ and $\mu \overset{\bullet}{\approx}\ \nu$. Suppose that $[\![s,\mu]\!] \xrightarrow{\alpha}\!\!\bullet_\rho\ \mu'$, then it must be the case that $\delta_s \bullet\!\!\xrightarrow{\alpha} \mu'$. Since $\delta_s \overset{\bullet}{\approx}\ \delta_r$, there exists a $\delta_r \bullet\!\!\stackrel{\alpha}{\Longrightarrow} \nu'$ such that $\mu' \overset{\bullet}{\approx}\ \nu'$, so we have $[\![r,\nu]\!] \stackrel{\alpha}{\Longrightarrow}\!\!\bullet_\rho\ \nu'$ such that $\mu'\ \mathcal{R}\ \nu'$. If $[\![s,\mu]\!] \xrightarrow{\lambda}\!\!\bullet_\rho\ \mu'$, then $\mu \bullet\!\!\xrightarrow{\tau}_\rho\ \mu'$. Since $\mu \overset{\bullet}{\approx}\ \nu$, there exists a $\nu \bullet\!\!\stackrel{\tau}{\Longrightarrow}_\rho\ \nu'$ such that $\mu' \overset{\bullet}{\approx}\ \nu'$, thus we have $[\![r,\nu]\!] \stackrel{\lambda}{\Longrightarrow}\!\!\bullet_\rho\ \nu'$ such that $\mu'\ \mathcal{R}\ \nu'$. This completes the proof.

For the counterexample of $\overset{\bullet}{\approx}\ =\ \overset{\bullet}{\approx}$, refer to Example 57. □

6.3.3 Compositionality

In this section we show that $\overset{\bullet}{\approx}$ and $\approx^{\bullet}$ are congruence relations for time-convergent MA. First we recall the notion of time-convergent and time-divergent MA.

Definition 63 (Time-convergent)**.** *A state s is* time-convergent *iff there exists $s \stackrel{\tau}{\Longrightarrow} \mu$ such that $\mu\downarrow$, otherwise it is time-divergent. Let $\mathcal{M} = (S, Act_\tau, \rightarrow, \twoheadrightarrow, s_0)$, then $\mathcal{M}$ is time-convergent iff for each $s \in S$, s is time-convergent, otherwise $\mathcal{M}$ is time-divergent.*

The reason to distinguish time-divergent and time-convergent states is because of the maximal progress assumption, that is, the internal action takes no time and can exempt the execution of Markovian transitions, thus for a time-divergent state, it will have infinite τ transitions with positive probability according to Definition 63, as a consequence it will block the execution of Markovian transitions.

Now we recall the parallel composition defined in (5) as follows:

Definition 64 (Parallel Composition)**.** *Let $\mathcal{M}_1 = (S_1, Act_\tau, \rightarrow_1, \twoheadrightarrow_1, s_0')$ and $\mathcal{M}_2 = (S_1, Act_\tau, \rightarrow_2, \twoheadrightarrow_2, s_0'')$ be two* MA*, then $\mathcal{M}_1 \parallel_A \mathcal{M}_2 = (S, Act_\tau, \rightarrow, \twoheadrightarrow, s_0)$ such that*

- $S = \{s_1 \parallel_A s_2 \mid (s_1, s_2) \in S_1 \times S_2\}$,
- $(s_1 \parallel_A s_2, \alpha, \mu_1 \parallel_A \mu_2) \in \rightarrow$ *iff either $\alpha \in A$ and $s_i \xrightarrow{\alpha} \mu_i$ or $\alpha \notin A$, $s_i \xrightarrow{\alpha} \mu_i$, and $\mu_{3-i} = \delta_{s_{3-i}}$ with $i \in \{1, 2\}$*,
- $(s_1 \parallel_A s_2, \lambda, s_1' \parallel_A s_2') \in \twoheadrightarrow$ *iff either*
  - $s_i = s_i'$, $s_i \overset{\lambda_i}{\twoheadrightarrow} s_i'$, *and* $\lambda = \lambda_1 + \lambda_2$, *or*
  - $s_i \overset{\lambda}{\twoheadrightarrow} s_i'$ *and* $s_{3-i}' = s_{3-i}$

  with $i \in \{1, 2\}$.
- $s_0 = s_0' \parallel_A s_0''$,

where $\mu_1 \parallel_A \mu_2$ is a distribution such that $(\mu_1 \parallel_A \mu_2)(s_1 \parallel_A s_2) = \mu_1(s_1) \cdot \mu_2(s_2)$.

The theorem below shows that both $\overset{\bullet}{\approx}$ and $\approx^{\bullet}$ are congruent w.r.t. $\parallel_A$ for time-convergent MA:

Theorem 47. *For time-convergent* MA*, it holds that:*

1. $(\mu \parallel_A \mu_1) \overset{\bullet}{\approx} (\nu \parallel_A \mu_1)$ *for any μ_1 provided that $\mu \overset{\bullet}{\approx} \nu$.*

2. $(\mu \parallel_A \mu_1) \approx^{\bullet} (\nu \parallel_A \mu_1)$ *for any* μ_1 *provided that* $\mu \approx^{\bullet} \nu$.

Proof. We only prove Clause 1 since the proof of Clause 2 is similar, and can be obtained in a straightforward way by considering $\mathcal{M}^{\bullet}$ instead of ${}^{\bullet}\mathcal{M}$. The proof strategy for this result follows the standard way. Let $\mathcal{M}$ be the given MA and ${}^{\bullet}\mathcal{M}$ be the resulting MLTS according to the early semantics in Definition 57. We first define the relation

$$\mathcal{R} = \{(\mu \parallel_A \mu_1, \nu \parallel_A \mu_1) \mid \mu \approx^{{}^{\bullet}\mathcal{M}} \nu \wedge \mu_1 \in Dist(S)\}$$

then, it is sufficient to show that $\mathcal{R}$ is a weak bisimulation. Let $(\mu_0, \nu_0) \in \mathcal{R}$ with $\mu_0 \equiv \mu \parallel_A \mu_1$ and $\nu_0 \equiv \nu \parallel_A \mu_1$. Moreover, let $\mu_0 \stackrel{\alpha_r}{\Longrightarrow}_{\rho} \mu_0'$, We need to prove that there exists a $\nu_0 \stackrel{\alpha_r}{\Longrightarrow}_{\rho} \nu_0'$ such that $\mu_0' \mathcal{R} \nu_0'$.

Suppose that $Supp(\mu) = \{s_i \mid i \in I\}$, $Supp(\nu) = \{s_j' \mid j \in J\}$, and $Supp(\mu_1) = \{t_k \mid k \in K\}$ where I, J, and K are three finite index sets, then

$$Supp(\mu_0) = \{s_i \parallel_A t_k \mid i \in I \wedge k \in K\},$$

$$Supp(\nu_0) = \{s_j' \parallel_A t_k \mid j \in J \wedge k \in K\}.$$

The analysis of the compositional distribution requires some attention, thus we discuss first different cases needed for the weak transition $\mu_0 \stackrel{\alpha_r}{\Longrightarrow}_{\rho} \mu_0'$. Whenever $\mu_0 \stackrel{\alpha_r}{\Longrightarrow}_{\rho} \mu_0'$, then we know there exists a set of states $C \subseteq Supp(\mu_0)$ such that $\mu_0(C) = \rho$ and $r \stackrel{\alpha_r}{\Longrightarrow} \mu_r$ for each $r \in C$ where

$$\mu_0' = \sum_{r \in C} \frac{\mu_0(r)}{\rho} \cdot \mu_r.$$

While the case $\alpha_r \in A$ is more clear, the other case when $\alpha_r \notin A$ is a bit more involved. Let $r \equiv s_i \parallel_A t_k$ for some $i \in I$ and $k \in K$, so if $r \stackrel{\alpha_r}{\Longrightarrow} \mu_r$ with $\alpha_r \notin A$, then either $s_i \stackrel{\alpha_r}{\Longrightarrow} \mu_s$ and $t_k \stackrel{\tau}{\Longrightarrow} \mu_t$, or $s_i \stackrel{\tau}{\Longrightarrow} \mu_s$ and $t_k \stackrel{\alpha_r}{\Longrightarrow} \mu_t$ such that $\mu_s \parallel_A \mu_t = \mu_r$. As a result it is not simple if it is possible to prove only by structural induction, instead we need to prove by induction on structure and on the size of $Supp(\mu)$ simultaneously. There are several cases we need to consider.

1. $\alpha_r \notin A$.
   Suppose that μ is a Dirac distribution, that is, $\mu = \delta_s$ for a s, then there exists a $\mu_1 \stackrel{\tau}{\Longrightarrow} \mu_1^g + \mu_1^s$ such that

   $$\mu_0 = (\delta_s \parallel_A \mu_1^g) + (\delta_s \parallel_A \mu_1^s).$$

   Moreover we also have

   $$\frac{1}{|\mu_1^g|} \cdot (\delta_s \parallel_A \mu_1^g) \stackrel{\alpha_r}{\Longrightarrow}_{\rho_1} \mu_s \parallel_A \mu_2^g$$

where $\delta_s \stackrel{\alpha_r}{\Longrightarrow} \mu_s$ and $\frac{1}{|\mu_1^g|} \cdot \mu_1^g \stackrel{\tau}{\Longrightarrow}_{\rho_2} \mu_2^g$, and

$$\frac{1}{|\mu_1^s|} \cdot (\delta_s \parallel_A \mu_1^s) \stackrel{\alpha_r}{\Longrightarrow}_{\rho_2} (\mu_s' \parallel_A \mu_2^s)$$

where $\delta_s \stackrel{\tau}{\Longrightarrow} \mu_s'$ and $\frac{1}{|\mu_1^s|} \cdot \mu_1^s \stackrel{\alpha_r}{\Longrightarrow}_{\rho_2} \mu_2^s$ such that $\rho = \rho_1 + \rho_2$ and $\frac{\rho_1}{\rho} \cdot (\mu_s \parallel_A \mu_2^g) + \frac{\rho_2}{\rho} \cdot (\mu_s' \parallel_A \mu_2^s) = \mu_0'$. In other words we can divide μ_0 into two parts: $\delta_s \parallel_A \mu_1^g$ and $\delta_s \parallel_A \mu_1^s$ where in $\delta_s \parallel_A \mu_1^g$ the action α_r is performed by δ_s while in $\delta_s \parallel_A \mu_1^s$ it is performed by μ_1^s. Now we can use the structural induction. Since $\mu \approx^{\bullet\mathcal{M}} \nu$, whenever $\mu \stackrel{\alpha_r}{\Longrightarrow} \mu'$ i.e. $\mu \stackrel{\alpha_r}{\Longrightarrow}_1 \mu'$, there exists a $\nu \stackrel{\alpha_r}{\Longrightarrow}_1 \nu'$ such that $\mu' \approx^{\bullet\mathcal{M}} \nu'$, so the following proof is straightforward by structural induction.

Suppose now that the support of μ contains more than one element, then there exists a $\mu \stackrel{\tau}{\Longrightarrow} \mu^g + \mu^s$ such that

$$\mu_0 = (\mu^g \parallel_A \mu_1) + (\mu^s \parallel_A \mu_1).$$

Since $\mu \approx^{\bullet\mathcal{M}} \nu$, then there exists a $\nu \stackrel{\tau}{\Longrightarrow} \nu^g + \nu^s$ such that $\mu^g \approx^{\bullet\mathcal{M}} \nu^g$ and $\mu^s \approx^{\bullet\mathcal{M}} \nu^s$. Also for $\mu_0 \stackrel{\alpha_r}{\Longrightarrow}_\rho \mu_0'$, there must exist

$$\frac{1}{|\mu^g|} \cdot (\mu^g \parallel_A \mu_1) \stackrel{\alpha_r}{\Longrightarrow}_{\rho_1} \mu_0^g \text{ and}$$

$$\frac{1}{|\mu^s|} \cdot (\mu^s \parallel_A \mu_1) \stackrel{\alpha_r}{\Longrightarrow}_{\rho_2} \mu_0^s$$

such that $\rho = \rho_1 + \rho_2$ and

$$\frac{\rho_1}{\rho} \cdot \mu_0^g + \frac{\rho_2}{\rho} \cdot \mu_0^s = \mu_0'.$$

Since μ^g and μ^s contain less elements in their support than μ, we can apply our induction hypothesis on them, and the following proof is trivial and omitted.

2. $\alpha_r \in A$.
   As in the first case we first suppose that μ is Dirac distribution such that $\mu = \delta_s$ for a s. Then there exists a $\mu_1 \stackrel{\tau}{\Longrightarrow} \mu_1^g + \mu_1^s$ such that $\rho = |\mu_1^g|$ and

$$\mu_0 = (\delta_s \parallel_A \mu_1^g) + (\delta_s \parallel_A \mu_1^s).$$

   Moreover $\frac{1}{|\mu_1^g|} \cdot (\delta_s \parallel_A \mu_1^g) \stackrel{\alpha_r}{\Longrightarrow} \mu_0'$ where $\delta_s \stackrel{\alpha_r}{\Longrightarrow} \mu_s'$, $\frac{1}{|\mu_1^g|} \cdot \mu_1^g \stackrel{\alpha_r}{\Longrightarrow} \mu_2^g$, and $\mu_0' = \mu_s' \parallel_A \mu_2^g$. Intuitively, we divide μ_0 into two parts: $\delta_s \parallel_A \mu_1^g$ and $\delta_s \parallel_A \mu_1^s$ where the synchronization only happens between s and $Supp(\mu_1^g)$. Note that we can do such division only because that μ is a Dirac distribution, otherwise we cannot

always divide μ_0 in this way, because each state in $Supp(\mu)$ is not necessary to synchronize with the same set of states in $Supp(\mu_1)$. Since $\mu \approx^{\bullet\mathcal{M}} \nu$, the following proof is straightforward by structural induction.

The case when μ is not a Dirac distribution can be proved similarly as the first case, and is omitted here.

3. $\alpha_r = \lambda$.
Again we first consider the case where $\mu = \delta_s$ for a s. Then there exists a $\mu_1 \stackrel{\tau}{\Longrightarrow} \mu_1^g + \mu_1^s$ such that $\rho = |\mu_1^g|$ and

$$\mu_0 = (\delta_s \parallel_A \mu_1^g) + (\delta_s \parallel_A \mu_1^s).$$

Moreover $\frac{1}{|\mu_1^g|} \cdot (\delta_s \parallel_A \mu_1^g) \stackrel{\lambda}{\Longrightarrow} \mu_0'$ where either

(a) $\delta_s \stackrel{\lambda_1}{\Longrightarrow} \mu_s'$, $\frac{1}{|\mu_1^g|} \cdot \mu_1^g \stackrel{\lambda_2}{\Longrightarrow} \mu_2^g$, and

$$\mu_0' = \frac{\lambda_1}{\lambda} \cdot (\mu_s' \parallel_A (\frac{1}{|\mu_1^g|} \cdot \mu_1^g)) + \frac{\lambda_2}{\lambda} \cdot (\delta_s \parallel \mu_2^g), \text{or}$$

(b) $\delta_s \stackrel{\lambda}{\Longrightarrow} \mu_0'$, $\frac{1}{|\mu_1^g|} \cdot \mu_1^g \stackrel{\lambda'}{\not\Longrightarrow}$, and $\frac{1}{|\mu_1^g|} \cdot \mu_1^g \stackrel{\tau}{\Longrightarrow} \mu_2^g$ such that $\mu_2^g\downarrow$, or

(c) $\frac{1}{|\mu_1^g|} \cdot \mu_1^g \stackrel{\lambda}{\Longrightarrow} \mu_0'$, $\delta_s \stackrel{\lambda'}{\not\Longrightarrow}$, and $\delta_s \stackrel{\tau}{\Longrightarrow} \mu_s'$ such that $\mu_s'\downarrow$.

The following proof is straightforward by structural induction. The case when $Supp(\mu)$ is greater than 1 is similar with the first case and omitted here.

□

The above theorem does not hold for time-divergent MA. A detailed discussion is given in Section 6.6.1.

6.4 Weak Simulations

In this section we introduce the weak simulations w.r.t. early and late semantics respectively. We first give their definitions, and then show their properties.

6.4.1 Early and Late Weak Simulations

Given the definition of weak bisimulation in Definition 61, we can define weak simulation in a straightforward way as follows:

Definition 65 (Weak Simulation)**.** *Let $L = (S, Act_\tau, \rightarrow)$ be an* MLTS*. A relation $\mathcal{R} \subseteq Dist(S) \times Dist(S)$ is a weak simulation over L iff $\mu \ \mathcal{R} \ \nu$ implies that whenever $\mu \xrightarrow{\alpha_r}_\rho \mu'$, there exists a $\nu \stackrel{\alpha_r}{\Longrightarrow}_\rho \nu'$ such that $\mu' \ \mathcal{R} \ \nu'$.*

Let μ and ν be weakly similar, written as $\mu \ \precsim^L \ \nu$, iff there exists a weak simulation $\mathcal{R}$ such that $\mu \ \mathcal{R} \ \nu$. Moreover $s \ \precsim^L \ r$ iff $\delta_s \ \precsim^L \ \delta_r$.

As in Section 6.3, we shall introduce two weak simulations based on early and late semantics of MA respectively.

Definition 66 (Early and Late Weak Simulation)**.** *Two distributions μ, ν over S are*

1. *early weakly similar, written as $\mu \ \precsim^\bullet \ \nu$, iff $\mu \ \precsim^{\bullet\mathcal{M}} \ \nu$,*
2. *late weakly similar, written as $\mu \ \precsim^\bullet \ \nu$, iff $\mu \ \precsim^{\mathcal{M}\bullet} \ \nu$.*

Bellow we give a simple example illustrating the early and late weak simulations.

Example 60. *Let s, t, and r be the three* MA *in Fig. 6.1, moreover let s_0 be the* MA *same as s except that it has an extra transition: $s_0 \xrightarrow{\alpha} s_0'$. Then it is not hard to see that $t \ \precsim^\bullet \ s_0$, $t \ \precsim^\bullet \ s_0$, and $r \ \precsim^\bullet \ s_0$, but $r \ \precsim^\bullet \ s_0$ does not hold. Since r can evolve into ν which cannot be simulated by r under the early semantics.*

If we omit the state s' and its related transition in Fig. 6.1 (a), then s and r can be seen as the resulting MLTS*s by interpreting t according to the early and late semantics respectively. As mentioned in Example 54, we have $s \ \eqsim^\bullet \ r$. Also note that $s \ \precsim^\bullet \ r$, but $r \ \not\precsim^\bullet \ s$ with the same argument as $r \ \not\precsim^\bullet \ s_0$. In other words, by interpreting t according to the late semantics we actually preserve the weak simulation.*

6.4.2 Properties of Early and Late Weak Simulations

In this section we will show several properties of the weak simulations. We first prove that they are preorders. In order to do so, we introduce the following lemma similar to Lemma 36 showing that the weak simulation does not change if we replace the strong transitions by weak transitions.

Lemma 37. *Let $L = (S, Act_\tau, \rightarrow)$ be an* MLTS*. A relation $\mathcal{R} \subseteq Dist(S) \times Dist(S)$ is a weak simulation iff $\mu \ \mathcal{R} \ \nu$ implies that whenever $\mu \stackrel{\alpha_r}{\Longrightarrow}_\rho \mu'$, there exists a $\nu \stackrel{\alpha_r}{\Longrightarrow}_\rho \nu'$ such that $\mu' \ \mathcal{R} \ \nu'$.*

Proof. The proof is similar with the proof of Lemma 36. Let

$$\mathcal{R} = \{(\mu, \nu) \mid \mu \precsim^L \nu\},$$

and suppose that $\mu \mathcal{R} \nu$ and $\mu \stackrel{\alpha_r}{\Longrightarrow}_\rho \mu'$, we are going to show that there exists a $\nu \stackrel{\alpha_r}{\Longrightarrow}_\rho \nu'$ such that $\mu' \sqsubseteq_{\mathcal{R}} \nu'$ by structural induction. According to the definition of $\stackrel{\alpha_r}{\Longrightarrow}_\rho$, there exists $\mu \stackrel{\alpha_r}{\longrightarrow}_{\rho_1} \mu_1 \stackrel{\tau}{\Longrightarrow}_{\rho_1'} \mu_1'$ and $\mu \stackrel{\tau}{\rightarrow}_{\rho_2} \mu_2 \stackrel{\alpha_r}{\Longrightarrow}_{\rho_2'} \mu_2'$ such that $\rho_1 \cdot \rho_1' + \rho_2 \cdot \rho_2' = \rho$ and $(\frac{\rho_1 \cdot \rho_1'}{\rho} \cdot \mu_1' + \frac{\rho_2 \cdot \rho_2'}{\rho} \cdot \mu_2') \equiv \mu$. Since $\mu \precsim^L \nu$, there exists $\nu \stackrel{\alpha_r}{\Longrightarrow}_{\rho_1} \nu_1$ and $\nu \stackrel{\tau}{\Longrightarrow}_{\rho_2} \nu_2$ such that $\mu_1 \precsim^L \nu_1$ and $\mu_2 \precsim^L \nu_2$. By induction there exists $\nu_1 \stackrel{\alpha_r}{\Longrightarrow}_{\rho_1'} \nu_1'$ and $\nu_2 \stackrel{\tau}{\Longrightarrow}_{\rho_2'} \nu_2'$ such that $\mu_1' \precsim^L \nu_1'$ and $\mu_2' \precsim^L \nu_2'$, so there exists a

$$\nu \stackrel{\alpha_r}{\Longrightarrow}_\rho \nu' \equiv (\frac{\rho_1 \cdot \rho_1'}{\rho} \cdot \nu_1' + \frac{\rho_2 \cdot \rho_2'}{\rho} \cdot \nu_2')$$

such that $\mu' \precsim^L \nu'$ i.e. $\mu' \mathcal{R} \nu'$.

The other direction is trivial since the strong transition is a special case of the weak transition. □

The following lemma shows that the weak simulation for MLTSs defined in Definition 65 is a preorder for any L, and as in Section 6.3 $\precsim^\bullet$ is strictly coarser than ${}^\bullet\!\precsim$.

Theorem 48. *For any* MLTS L, $\precsim^L$ *is a preorder. For any* MA, ${}^\bullet\!\precsim$, *and* $\precsim^\bullet$ *are preorders, moreover* ${}^\bullet\!\precsim \subset \precsim^\bullet$.

Proof. We first show that $\precsim^L$ is a preorder. The reflexivity is easy to prove and is omitted here. We only show how to prove the transitivity. Suppose that $\mu_1 \precsim^L \mu_2$ and $\mu_2 \precsim^L \mu_3$, we need to prove that $\mu_1 \precsim^L \mu_3$. By Definition 65, if $\mu_1 \precsim^L \mu_2$ and $\mu_2 \precsim^L \mu_3$, then there exists two weak simulations $\mathcal{R}_1$ and $\mathcal{R}_2$ such that $\mu_1 \mathcal{R}_1 \mu_2$ and $\mu_2 \mathcal{R}_2 \mu_3$. Let

$$\mathcal{R} = \{(\nu_1, \nu_3) \mid \exists \nu_2 . \nu_1 \mathcal{R}_1 \nu_2 \wedge \nu_2 \mathcal{R}_2 \nu_3\}.$$

It is clear that $\mu_1 \mathcal{R} \mu_3$, so once we can prove that $\mathcal{R}$ is a weak simulation, we can say that $\mu_1 \precsim^L \mu_3$. Suppose that $\mu_1 \stackrel{\alpha_r}{\Longrightarrow}_\rho \mu_1'$, then there exists a $\mu_2 \stackrel{\alpha_r}{\Longrightarrow}_\rho \mu_2'$ such that $\mu_1' \mathcal{R}_1 \mu_2'$. Since we also have $\mu_2 \mathcal{R}_2 \mu_3$ where $\mathcal{R}_2$ is a weak simulation, so there exists a $\mu_3 \stackrel{\alpha_r}{\Longrightarrow}_\rho \mu_3'$ such that $\mu_2' \mathcal{R}_2 \mu_3'$. By definition of $\mathcal{R}$, we have $\mu_1' \mathcal{R} \mu_3'$, so $\mathcal{R}$ is a weak simulation. The proof of ${}^\bullet\!\precsim$ and $\precsim^\bullet$ being preorders is straightforward, since both ${}^\bullet\mathcal{M}$ and $\mathcal{M}^\bullet$ are special MLTSs.

The proof of ${}^\bullet\!\precsim \subset \precsim^\bullet$ is similar as Theorem 46 and is omitted here. Intuitively, according to Definition 59 we can defer the execution of all the Markovian transitions,

thus the order of the Markovian transitions and internal transitions does not matter in MLTS. □

Bellows we show that both $\overset{\bullet}{\precsim}$ and $\overset{\bullet}{\succsim}$ are congruences w.r.t. the operator $\|_A$ on time-convergent MA.

Theorem 49. *For time-convergent* MA*, it holds that:*

1. $(\mu \|_A \mu_1) \overset{\bullet}{\precsim} (\nu \|_A \mu_1)$ *for any* μ_1 *provided that* $\mu \overset{\bullet}{\precsim} \nu$.
2. $(\mu \|_A \mu_1) \overset{\bullet}{\succsim} (\nu \|_A \mu_1)$ *for any* μ_1 *provided that* $\mu \overset{\bullet}{\succsim} \nu$.

Proof. The proof is similar with the proof of Theorem 47, we only sketch the proof here. First we assume that μ is a Dirac distribution i.e. its support only contains one element, then we analysis by cases depending on i) whether μ and μ_1 synchronize with each other or not, ii) whether the transition is a Markovian transition or not. Then we can extend the proof to the case where μ is not Dirac, the proof is by induction on the number of elements in $Supp(\mu)$. □

Let $\mathcal{R}^{-1}$ denote the reverse of $\mathcal{R}$, then the weak simulation kernel $\precsim^L \cap (\precsim^L)^{-1}$ is strictly coarser than $\precsim^L$ shown in the following lemma.

Lemma 38. *For any* MLTS L, $\approx^L \subset (\precsim^L \cap (\precsim^L)^{-1})$.

Proof. We omit the parameter L through the proof. The proof of $\approx \subset (\precsim \cap \precsim^{-1})$ is trivial and omitted here. To show that $(\precsim \cap \precsim^{-1})$ is strictly coarser than $\approx$, it is enough to give a counterexample. Suppose we have three states s_1, s_2, and s_3 such that $s_1 \precsim s_2 \precsim s_3$ but $s_3 \not\precsim s_2 \not\precsim s_1$. Let s and r be two states such that $L(s) = L(r)$. In addition s has three transitions: $s \xrightarrow{1} \delta_{s_1}$, $s \xrightarrow{1} \delta_{s_2}$, $s \xrightarrow{1} \delta_{s_3}$, and r only has two transitions: $s \xrightarrow{1} \delta_{s_1}$, $s \xrightarrow{1} \delta_{s_3}$. Then it should be easy to check that $s \precsim r$ and $r \precsim s$, the only non-trivial case is when $s \xrightarrow{1} \delta_{s_2}$. Since $s_2 \precsim s_3$, thus there exists $r \xrightarrow{1} \delta_{s_3}$ such that $\delta_{s_2} \sqsubseteq_{\precsim} \delta_{s_3}$. But obviously $s \not\approx r$, since the transition $s \xrightarrow{1} \delta_{s_2}$ cannot be simulated by any transition of r. □

As a direct consequence of Lemma 38, it also holds that

$$\overset{\bullet}{\approx} \subset (\overset{\bullet}{\precsim} \cap (\overset{\bullet}{\precsim})^{-1}) \text{ and } \overset{\bullet}{\approx} \subset (\overset{\bullet}{\succsim} \cap (\overset{\bullet}{\succsim})^{-1}).$$

6.5 Comparing $\overset{\bullet}{\approx}$, $\overset{\bullet}{\approx}$, $\approx_{ehz}$ and $\approx_{dh}$

In this section we compare our weak bisimulations with the weak bisimulation $\approx_{ehz}$ in (5), and $\approx_{dh}$ in (6) defined upon an MLTS. We show that our early weak bisimulation agrees with both $\approx_{ehz}$ and $\approx_{dh}$, implying that $\approx_{ehz} = \approx_{dh}$. First, we shall recall the definitions of $\approx_{ehz}$ and $\approx_{dh}$ in the following.

6.5.1 Weak Bisimulation à la Eisentraut, Hermanns and Zhang

In this section we recall the definition of weak bisimulation introduced in (5). For simplicity we do not consider combined transitions here, since all the bisimulations defined in this chapter can be changed accordingly by taking combined transitions into account without affecting the theories. According to Lemma 2 in (5) we adopt the following definition of $\approx_{ehz}$ which shall be easier for proving the relationship to our weak bisimulations.

Definition 67 (EHZ-Weak Bisimulation)**.** *Let $L = (S, Act_\tau, \rightarrow)$ be an* MLTS*. A relation $\mathcal{R} \subseteq ADist(S) \times ADist(S)$ is an EHZ-weak bisimulation iff $\mu\ \mathcal{R}\ \nu$ implies that $|\mu| = |\nu|$ and*

- *whenever $\mu \overset{\tau}{\Longrightarrow} \mu^g + \nu^s$, there exists a $\nu \overset{\tau}{\Longrightarrow} \nu^g + \nu^s$ such that*
  - *$\mu^g\ \mathcal{R}\ \nu^g$ and $\mu^s\ \mathcal{R}\ \nu^s$,*
  - *if $\mu^g \overset{\alpha_r}{\Longrightarrow} \mu'$, then there exists a $\nu^g \overset{\alpha_r}{\Longrightarrow} \nu'$ such that $\mu'\ \mathcal{R}\ \nu'$.*
- *symmetrically for ν.*

μ and ν are EHZ-weakly bisimilar, written as $\mu \approx^L_{ehz} \nu$, iff there exists an EHZ-weak bisimulation $\mathcal{R}$ such that $\mu\ \mathcal{R}\ \nu$. Moreover $s \approx^L_{ehz} r$ iff $\delta_s \approx^L_{ehz} \delta_r$.

Intuitively for μ and ν being EHZ-weakly bisimilar, their sizes must coincide. Moreover if μ can split into μ^g and ν^s i.e. $\mu \overset{\tau}{\Longrightarrow} \mu^g + \mu^s$, then μ should also be able to split into two parts i.e. $\nu \overset{\tau}{\Longrightarrow} \nu^g + \nu^s$ such that $\mu^g \approx^L_{ehz} \nu^g$ and $\mu^s \approx^L_{ehz} \nu^s$. Also if μ^g can evolve into μ' via weak α_r transition, in order to simulate it, ν^g is also able to evolve into ν' via weak transition with the same label α_r, and their resulting distributions μ' and ν' are still EHZ-weakly bisimilar.

Even though $\approx^L_{ehz}$ is originally defined on any distributions in (5), we can easily change it to deal only with full distributions due to normalization:

Lemma 39. *Let μ and ν be two distributions. Then $\mu \approx^L_{ehz} \nu$ iff $|\mu| = |\nu|$ and $(\frac{1}{|\mu|} \cdot \mu) \approx^L_{ehz} (\frac{1}{|\nu|} \cdot \nu)$.*

Proof. First we show that $\mu \approx^L_{ehz} \nu$ implies $|\mu| = |\nu|$ and $(\frac{1}{|\mu|} \cdot \mu) \approx^L_{ehz} (\frac{1}{|\nu|} \cdot \nu)$. The fact that $|\mu| = |\nu|$ is trivial from Definition 67. Let

$$\mathcal{R} = \{((\frac{1}{|\mu|} \cdot \mu), (\frac{1}{|\nu|} \cdot \nu)) \mid \mu \approx^L_{ehz} \nu\},$$

we are going to prove that $\mathcal{R}$ is an EHZ-weak bisimulation. It is obvious that $|(\frac{1}{|\mu|} \cdot \mu)| = |(\frac{1}{|\nu|} \cdot \nu)|$, and $Supp(\mu) = Supp((\frac{1}{|\mu|} \cdot \mu))$. For each $t \in Supp((\frac{1}{|\mu|} \cdot \mu))$, we also have $t \in Supp(\mu)$. Since $\mu \approx^L_{ehz} \nu$, there exists a $\nu \stackrel{\tau}{\Longrightarrow} \nu^g + \nu^s$ such that

- $(\mu(t) \cdot \delta_t) \approx^L_{ehz} \nu^g$ and $(\mu - t) \approx^L_{ehz} \nu^s$,
- $(\mu(t) \cdot \delta_t) \xrightarrow{\alpha_r} \mu'$,

then there exists a $\nu^g \stackrel{\alpha_r}{\Longrightarrow} \nu'$ such that $\mu' \approx^L_{ehz} \nu'$. Therefore there exists a

$$(\frac{1}{|\nu|} \cdot \nu) \stackrel{\tau}{\Longrightarrow} ((\frac{1}{|\nu|} \cdot \nu^g)) + ((\frac{1}{|\nu|} \cdot \nu^s))$$

such that

- $(\frac{1}{|\mu|} \cdot \mu(t) \cdot \delta_t)\ \mathcal{R}\ (\frac{1}{|\nu|} \cdot \nu^g)$ and $(\frac{1}{|\mu|} \cdot \mu - t) \approx^L_{ehz} (\frac{1}{|\nu|} \cdot \nu^s)$,
- $(((\frac{1}{|\mu|} \cdot \mu)(t)) \cdot \delta_t) \xrightarrow{\alpha_r} (\frac{1}{|\mu|} \cdot \mu')$,

then there exists a $(\frac{1}{|\nu|} \cdot \nu^g) \stackrel{\alpha_r}{\Longrightarrow} (\frac{1}{|\nu|} \cdot \nu')$ such that

$$(\frac{1}{|\mu|} \cdot \mu')\ \mathcal{R}\ (\frac{1}{|\nu|} \cdot \nu'),$$

so $\mathcal{R}$ is an EHZ-weak bisimulation.

The proof of the other direction is similar and omitted here. □

According to the lemma above, we shall restrict the discussions to full distributions while discussing the relationships between various weak bisimulation relations in the following sections.

6.5.2 Weak Bisimulation à la Deng and Hennesy

In (6) another definition of weak bisimulation is proposed but with the definition of MLTSs being slightly different. By lifting their weak bisimulation to the MLTSs defined in Definition 56, we obtain the following definition.

Definition 68 (DH-Weak Bisimulation)**.** *Let $L = (S, Act_\tau, \rightarrow)$ be an* MLTS*. A relation $\mathcal{R} \subseteq Dist(S) \times Dist(S)$ is a DH-weak bisimulation if $\mu \ \mathcal{R} \ \nu$ implies that*

1. *whenever $\mu \stackrel{\alpha_r}{\Longrightarrow} \sum_{i\in I} p_i \cdot \mu_i$, there exists a $\nu \stackrel{\alpha_r}{\Longrightarrow} \sum_{i\in I} p_i \cdot \nu_i$ such that $\mu_i \ \mathcal{R} \ \nu_i$ for each $i \in I$,*

2. *whenever $\nu \stackrel{\alpha_r}{\Longrightarrow} \sum_{i\in I} p_i \cdot \nu_i$, there exists a $\mu \stackrel{\alpha_r}{\Longrightarrow} \sum_{i\in I} p_i \cdot \mu_i$ such that $\mu_i \ \mathcal{R} \ \nu_i$ for each $i \in I$.*

where I is a finite set of indexes and $\sum_{i\in I} p_i = 1$. Let μ and ν be DH-weakly bisimilar, written as $\mu \ \approx^L_{dh} \ \nu$, iff there exists a DH-weak bisimulation $\mathcal{R}$ such that $\mu \ \mathcal{R} \ \nu$. Moreover $s \ \approx^L_{dh} \ r$ iff $\delta_s \ \approx^L_{dh} \ \delta_r$.

Definition 67 and 68 are defined upon a given MLTS, similar as in Definition 62 we can lift them to an MA in a straightforward way. In both (5) and (6), only the early semantics is considered, thus we have the following definition.

Definition 69. *Given an* MA *$\mathcal{M} = (S, Act_\tau, \rightarrow, \twoheadrightarrow, s_0)$ and distributions μ and ν over S, $\mu \ \approx_{ehz} \ \nu$ iff $\mu \ \approx^{\bullet\mathcal{M}}_{ehz} \ \nu$, similarly $\mu \ \approx_{dh} \ \nu$ iff $\mu \ \approx^{\bullet\mathcal{M}}_{dh} \ \nu$.*

Example 61. *Given an* MA *where s, t, and r are depicted as Fig. 6.1, by the early semantics, t has a similar transition as s, and can evolve into distribution μ via a Markovian transition labeled with 2λ, i.e. $t \stackrel{2\lambda}{\bullet\!\!\longrightarrow} \mu = \{\frac{1}{2} : s_1, \frac{1}{2} : s_2\}$. Let*

$$\mathcal{R} = \{(\delta_s, \delta_t), (\delta'_s, \mu)\} \cup ID$$

where ID is the identity relation, it is not hard to see that $\mathcal{R}$ is both an EHZ-weak bisimulation and a DH-weak bisimulation by Definition 67 and 68, thus $s \ \approx_{ehz} \ t$ and $s \ \approx_{dh} \ t$. But for r there is no way for s and t to simulate it, for instance r_1 can evolve into t_1 directly via a Markovian transition labeled with 2λ, while no state or distribution in s and t can do so, thus neither $t \ \approx_{ehz} \ r$ nor $t \ \approx_{dh} \ r$.

6.5.3 $\approx_{ehz}$ and $\approx_{dh}$ are Equivalent

In this section we show that $\overset{\bullet}{\approx}$ agrees with both $\approx_{ehz}$ and $\approx_{dh}$. To be clear it is worthwhile to emphasize that the definition of $\approx^{\bullet}$ is upon the late semantics of the given MA, while all the others are defined upon the early semantics, therefore we first consider the relations of $\overset{\bullet}{\approx}$, $\approx_{ehz}$ and $\approx_{dh}$. The following theorem shows that $\overset{\bullet}{\approx}$ coincides with both $\approx_{ehz}$ and $\approx_{dh}$:

Theorem 50. $\overset{\bullet}{\approx} = \approx_{ehz} = \approx_{dh}$.

Proof. We first prove that $\overset{\bullet}{\approx} = \approx_{ehz}$, it is enough to show that $\approx^L = \approx^L_{ehz}$ according to Definition 62 and 69 for any MLTS L. First we prove $\approx^L_{ehz} \subseteq \approx^L$. Let

$$\mathcal{R} = \{(\mu, \nu) \mid \mu \ \approx^L_{ehz} \ \nu\},$$

then it is sufficient to show that $\mathcal{R}$ is a weak bisimulation according to Definition 61. For each $\mu \overset{\alpha_r}{\Longrightarrow}_\rho \mu'$, we need to prove that there exists a $\nu \overset{\alpha_r}{\Longrightarrow}_\rho \nu'$ such that $\mu' \ \mathcal{R} \ \nu'$. By definition of $\Longrightarrow_\rho$, there exists a $\mu \overset{\tau}{\Longrightarrow} \mu^g + \mu^s$ such that $|\mu^g| = \rho$ and $(\frac{1}{|\mu^g|} \cdot \mu^g) \overset{\alpha_r}{\Longrightarrow} \mu'$. Since $\mu \ \approx^L_{ehz} \ \nu$, then $\nu \overset{\tau}{\Longrightarrow} \nu^g + \nu^s$ such that

$$(\frac{1}{|\mu^g|} \cdot \mu^g) \ \approx^L_{ehz} \ (\frac{1}{|\nu^g|} \cdot \nu^g) \text{ and}$$

$$(\frac{1}{|\mu^s|} \cdot \mu^s) \ \approx^L_{ehz} \ (\frac{1}{|\nu^s|} \cdot \nu^s)$$

by Definition 67 and Lemma 39. In addition $(\frac{1}{|\nu^g|} \cdot \nu^g) \overset{\alpha_r}{\Longrightarrow} \nu'$ such that $\mu' \ \approx^L_{ehz} \ \nu'$, thus $\mu' \ \mathcal{R} \ \nu'$. As a result there exists a $\nu \overset{\alpha_r}{\Longrightarrow}_\rho \nu'$ such that $\mu' \ \mathcal{R} \ \nu'$, so $\mathcal{R}$ is indeed a weak bisimulation.

For the other direction we prove $\approx^L \subseteq \approx^L_{ehz}$. Similarly we need to prove that

$$\mathcal{R} = \{(\mu, \nu) \mid \mu \ \approx^L \ \nu\}$$

is an EHZ-weak bisimulation. Suppose that $\mu \ \mathcal{R} \ \nu$ and $\mu \overset{\tau}{\Longrightarrow} \mu^g + \mu^s$, then we first prove that there exists $\nu \overset{\tau}{\Longrightarrow} \nu^g + \nu^s$ such that

1. $(\frac{1}{|\mu^g|} \cdot \mu^g) \ \mathcal{R} \ (\frac{1}{|\nu^g|} \cdot \nu^g)$ and $(\frac{1}{|\mu^s|} \cdot \mu^s) \ \mathcal{R} \ (\frac{1}{|\nu^s|} \cdot \nu^s)$,
2. whenever $(\frac{1}{|\mu^g|} \cdot \mu^g) \overset{\alpha_r}{\Longrightarrow} \mu'^g$, there exists a $(\frac{1}{|\nu^g|} \cdot \nu^g) \overset{\alpha_r}{\Longrightarrow} \nu'^g$ such that $\mu'^g \ \mathcal{R} \ \nu'^g$.

If $\mu \overset{\tau}{\Longrightarrow} \mu^g + \mu^s$, then $\mu \overset{\tau}{\Longrightarrow}_\rho (\frac{1}{|\mu^g|} \cdot \mu^g)$ with $\rho = |\mu^g|$. Since $\mu \ \approx^L \ \nu$, then there exists a weak transition $\nu \overset{\tau}{\Longrightarrow}_\rho (\frac{1}{|\nu^g|} \cdot \nu^g)$ such that $(\frac{1}{|\mu^g|} \cdot \mu^g) \ \approx^L \ (\frac{1}{|\nu^g|} \cdot \nu^g)$, thus

$(\frac{1}{|\mu^g|} \cdot \mu^g)\ \mathcal{R}\ (\frac{1}{|\mu^g|} \cdot \nu^g)$, then the second clause is easy to verify. It only remains to prove that $(\frac{1}{|\mu^s|} \cdot \mu^s)\ \mathcal{R}\ (\frac{1}{|\nu^s|} \cdot \nu^s)$. Suppose it holds that $(\frac{1}{|\mu^s|} \cdot \mu^s)\ \not\approx^L\ (\frac{1}{|\nu^s|} \cdot \nu^s)$, there must exist $(\frac{1}{|\mu^s|} \cdot \mu^s) \stackrel{\alpha_r}{\Longrightarrow}_\rho \mu'^s$ such that there does not exist $(\frac{1}{|\nu^s|} \cdot \nu^s) \stackrel{\alpha_r}{\Longrightarrow}_\rho \nu'^s$ with $\mu'^s\ \approx^L\ \nu'^s$. By definition of $\stackrel{\alpha_r}{\Longrightarrow}_\rho$, we have $\mu \stackrel{\alpha_r}{\Longrightarrow}_{\rho'} \mu'$ where $\rho' = |\mu^s|\ \cdot \rho$ and $\mu' = \mu'^s$, so there exists a $\nu \stackrel{\alpha_r}{\Longrightarrow}_{\rho'} \nu'$ such that $\mu'\ \approx^L\ \nu'$ but $\nu' \neq \nu'^s$. As a result it must holds that $(\frac{1}{|\nu^g|} \cdot \nu^g) \stackrel{\alpha_r}{\Longrightarrow}_{\rho_1} \nu_1$ and $(\frac{1}{|\nu^s|} \cdot \nu^s) \stackrel{\alpha_r}{\Longrightarrow}_{\rho_2} \nu_2$ such that $\rho_1 \cdot |\nu^g|\ + \rho_2 \cdot |\nu^s|\ = \rho'$ and $(\frac{\rho_1 \cdot |\nu^g|}{\rho'} \cdot \nu_1 + \frac{\rho_2 \cdot |\nu^s|}{\rho'} \cdot \nu_2) = \nu'$. Since $(\frac{1}{|\mu^g|} \cdot \mu^g)\ \approx^L\ (\frac{1}{|\nu^g|} \cdot \nu^g)$, there exists a weak transition $(\frac{1}{|\mu^g|} \cdot \mu^g) \stackrel{\alpha_r}{\Longrightarrow}_{\rho_1} \mu_1$ such that $\mu_1\ \approx^L\ \nu_1$, so we have

$$\mu \stackrel{\alpha_r}{\Longrightarrow}_{(|\mu^g|\ \cdot \rho_1 + |\mu^s|\ \cdot \rho)} (\frac{|\mu^g|\ \cdot \rho_1}{|\mu^g|\ \cdot \rho_1 + |\mu^s|\ \cdot \rho} \cdot \mu'^g + \frac{|\mu^s|\ \cdot \rho}{|\mu^g|\ \cdot \rho_1 + |\mu^s|\ \cdot \rho} \cdot \mu'^s)$$

which cannot be simulated by ν, and this contradicts with the assumption that $\mu\ \approx^L\ \nu$, thus

$$(\frac{1}{|\mu^s|} \cdot \mu^s)\ \mathcal{R}\ (\frac{1}{|\nu^s|} \cdot \nu^s).$$

By Lemma 39, $\mathcal{R}$ is an EHZ-weak bisimulation.

Secondly, we show that $\overset{\bullet}{\approx} = \approx_{dh}$. As in the proof of $\overset{\bullet}{\approx} = \approx_{ehz}$, it is enough to prove that $\approx^L = \approx^L_{dh}$ for any MLTS L. We first show that $\mu\ \approx^L_{dh}\ \nu$ implies that $\mu\ \approx^L\ \nu$. We need to prove that

$$\mathcal{R} = \{(\mu, \nu) \mid \mu\ \approx^L_{dh}\ \nu\}$$

is a weak bisimulation. Suppose that $\mu\ \mathcal{R}\ \nu$ and $\mu \stackrel{\alpha_r}{\Longrightarrow}_\rho \mu'$, there exists a $\nu \stackrel{\alpha_r}{\Longrightarrow}_\rho \nu'$ such that $\mu'\ \mathcal{R}\ \nu'$. By definition of $\stackrel{\alpha_r}{\Longrightarrow}_\rho$, there exists

$$\mu \stackrel{\tau}{\Longrightarrow} \mu^g + \mu^s = (|\mu^g|\ \cdot \frac{1}{|\mu^g|} \cdot \mu^g + |\mu^s|\ \cdot \frac{1}{|\mu^s|} \cdot \mu^s)$$

such that $\rho = |\mu^g|$ and $\frac{1}{\rho} \cdot \mu^g \stackrel{\alpha_r}{\Longrightarrow} \mu'$. Since $\mu\ \approx^L_{dh}\ \nu$, there exists a

$$\nu \stackrel{\tau}{\Longrightarrow} (|\nu^g|\ \cdot \frac{1}{|\nu^g|} \cdot \nu^g + |\nu^s|\ \cdot \frac{1}{|\nu^s|} \cdot \nu^s) = \nu^g + \nu^s$$

such that $|\mu^g|\ = |\nu^g|$, $\frac{1}{|\mu^g|} \cdot \mu^g\ \approx^L_{dh}\ \frac{1}{|\nu^g|} \cdot \nu^g$ and $\frac{1}{|\mu^s|} \cdot \mu^s\ \approx^L_{dh}\ \frac{1}{|\nu^s|} \cdot \nu^s$, so there exists a $\frac{1}{|\nu^g|} \cdot \nu^g \stackrel{\alpha_r}{\Longrightarrow} \nu'$ such that $\mu'\ \approx^L_{dh}\ \nu'$. Therefore there exists a $\nu \stackrel{\alpha_r}{\Longrightarrow}_\rho \nu'$ such that $\mu'\ \mathcal{R}\ \nu'$.

Secondly we show that $\mu\ \approx^L\ \nu$ implies that $\mu\ \approx^L_{dh}\ \nu$ by proving that

$$\mathcal{R} = \{(\mu, \nu) \mid \mu\ \approx^L\ \nu\}$$

is a DH-weak bisimulation. Suppose that $\mu\ \mathcal{R}\ \nu$ and $\mu \stackrel{\alpha_r}{\Longrightarrow} \sum_{i \in I} p_i \cdot \mu_i$, then we need to show that there exists a $\nu \stackrel{\alpha_r}{\Longrightarrow} \sum_{i \in I} p_i \cdot \nu_i$ such that $\mu_i\ \mathcal{R}\ \nu_i$ for each $i \in I$. We prove

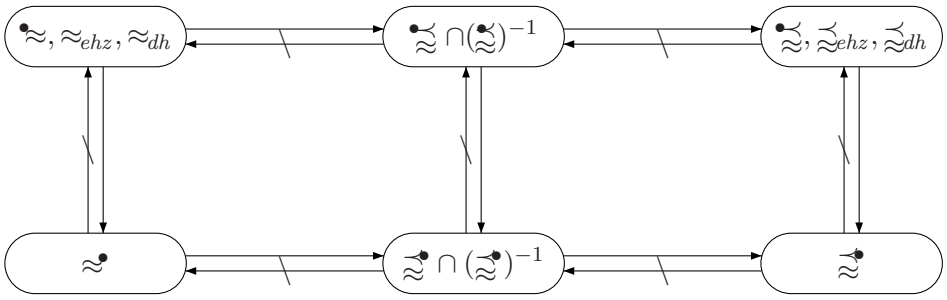

Figure 6.5: Summary.

by induction on the size of I. The case when $|I| = 1$ is simple and we assume that $|I| > 1$. Since $\mu \overset{\alpha_r}{\Longrightarrow} \sum_{i \in I} p_i \cdot \mu_i$, there exists a $\mu \overset{\tau}{\Longrightarrow} \mu^g + \mu^s$ such that $|\mu^g| = p_1$ and $|\mu^s| = \sum_{i \neq 1 \wedge i \in I} p_i$. In addition $\frac{1}{p_1} \cdot \mu^g \overset{\alpha_r}{\Longrightarrow} \mu_1$ and

$$\frac{1}{1-p_1} \cdot \mu^s \overset{\alpha_r}{\Longrightarrow} \frac{1}{1-p_1} \cdot \sum_{i \neq 1 \wedge i \in I} p_i \cdot \mu_i.$$

Therefore by the similar argument as in the proof of $\overset{\bullet}{\approx} = \approx_{ehz}$, there exists a $\nu \overset{\tau}{\Longrightarrow} \nu^g + \nu^s$ such that $|\mu^g| = |\nu^g|$, $\frac{1}{|\mu^g|} \cdot \mu^g \approx^L \frac{1}{|\nu^g|} \cdot \nu^g$, and $\frac{1}{|\mu^s|} \cdot \mu^s \approx^L \frac{1}{|\nu^s|} \cdot \nu^s$. By induction there exists $\frac{1}{p_1} \cdot \nu^g \overset{\alpha_r}{\Longrightarrow} \nu_1$ and

$$\frac{1}{1-p_1} \cdot \nu^s \overset{\alpha_r}{\Longrightarrow} \frac{1}{1-p_1} \cdot \sum_{i \neq 1 \wedge i \in I} p_i \cdot \nu_i$$

such that $\mu_i \approx^L \nu_i$ for each $i \in I$, so there exists a $\nu \overset{\alpha_r}{\Longrightarrow} \sum_{i \in I} p_i \cdot \nu_i$ such that $\mu_i \; \mathcal{R} \; \nu_i$ for each $i \in I$. This completes the proof. □

6.5.4 Summary

Let $\precsim_{ehz}$ and $\precsim_{dh}$ denote EHZ-weak simulation (109) and DH-weak simulation, whose definitions can be obtained by omitting Clause 2 in Definition 67 and 68 respectively. With a similar proof as Theorem 50, we can show that $\overset{\bullet}{\precsim} = \precsim_{ehz} = \precsim_{dh}$. We summarize all the relations in Fig. 6.5 where $\rightarrow$ denotes "implication" while $\nrightarrow$ denotes that the implication does not hold. Moreover $\overset{\bullet}{\approx}, \approx_{ehz}$, and $\approx_{dh}$ are in the same node meaning that they are equivalent, similarly for $\overset{\bullet}{\precsim}, \precsim_{ehz}$, and $\precsim_{dh}$.

6.6 Related Work

Weak bisimulations have been studied for various stochastic models, for instance for Markov chains (24, 54), interactive Markov chains (32), probabilistic automata (53, 78), and alternating automata (56). MA arise as a combination of probabilistic automata and interactive Markov chains. Two – seemingly – different weak bisimulation semantics have been proposed in (5, 6) for MA. They have been shown to be equivalent in this chapter, moreover, we have proposed a weaker version – the late weak bisimulation – in this chapter. Another interesting related work is (98), where Rabe and Schewe have shown that finite optimal control exists w.r.t. reachability probability for MA.

Below we discuss how the compositionality result for late weak bisimulation (early as well) generalizes to time-divergent systems, and that it is a reduction barbed congruence.

6.6.1 Compositionality for Time-Divergent MA

We have shown that $\overset{\bullet}{\approx}$ agrees with both $\approx_{ehz}$ and $\approx_{dh}$. The latter two relations have been shown to be congruences w.r.t. parallel compositions, but only for time-convergent MA. The reason why Theorem 47 does not apply for general MA can be understood by the following example considered in chapter (6).

Example 62. *Assume that we have two states s, r with s having no transition available while r only has a self loop labeled with τ. It easy to check that s and r are weakly bisimilar according to all the three weak bisimulation definitions. Now consider another state t with only a self loop labeled with λ. After parallel composition with s and r, $(s \parallel_A t)$ and $(r \parallel_A t)$ are no longer weakly bisimilar, as the λ loop has no effect for state $r \parallel_A t$ because of the maximal progress assumption.*

This problem was elegantly solved in (32) by adding a third condition for defining a divergence sensitive weak bisimulation, that is, two weakly bisimilar states either both are divergent or none of them diverges. We could also modify our notion of weak bisimulations along this line, then Theorem 47 could also be shown to be true for all MA. In this case states s and t would not be weakly bisimilar anymore.

Recently, Deng and Hennesy (6) have proposed another nice solution to deal with compositionality for time-divergent MA, by giving a new semantics for the parallel oper-

ator[1], using the notion of *indefinite delays* associated with transition. These transitions are also referred to as *passive transitions*. For $s \parallel_A t$ being able to perform a Markovian transition $\xrightarrow{\lambda}$, s needs be able to perform $\xrightarrow{\lambda}$ and t needs to perform a passive transition, or vice versa. Thus the Markovian transition will be blocked by participating component without Markovian or passive transitions. Under this new semantics, $\approx_{dh}$ is shown to be congruent w.r.t. all MA. In our previous example we have then $s \approx_{dh} r$, and moreover $s \parallel_A t \approx_{dh} r \parallel_A t$, as $s \parallel_A t$ cannot perform Markovian transitions due to the fact that s cannot perform any Markovian transition even with indefinite rate.

More importantly, in (6) Deng and Hennesy have shown that $\approx_{dh}$ enjoys the nice properties of being barb-preserving, reduction-closed, and compositional i.e. $\approx_{dh}$ is the largest *reduction barbed congruence* relation. In the following section, we shall argue that our late weak bisimulation also enjoys these properties even though our relation is strictly coarser than $\approx_{dh}$.

6.6.2 Late Weak Bisimulation is Reduction Barbed Congruence

In (6) Deng and Hennesy have proved that $\approx_{dh}$ is the coarsest relation which is a reduction barbed congruence, i.e., it is barb-preserving, reduction-closed, and compositional w.r.t. a process language (mCCS) with underlying semantics as a MLTS – with extension of passive transitions[2]. In Theorem 46 we have shown that $\approx^{\bullet}$ is strictly coarser than $\approx_{dh}$, therefore it seems that $\approx^{\bullet}$ should not be a reduction barbed congruence. Interestingly, $\approx^{\bullet}$ is indeed such a congruence. The reason that $\approx^{\bullet}$ is coarser than $\approx_{dh}$ is because that they are defined upon different semantics: $\approx^{\bullet}$ is based on the late semantics while $\approx_{dh}$ is upon the early semantics. Moreover, both semantics are in terms of MLTSs. In the proof of Theorem 50 we have proved that $\approx^{L}$ coincides with $\approx^{L}_{dh}$ for any MLTS L. Therefore if we define $\approx_{dh}$ upon the late semantics of a given MA $\mathcal{M}$, it will be equivalent to $\approx^{\bullet}$ due to $\approx^{\mathcal{M}^{\bullet}}_{dh} = \approx^{\mathcal{M}^{\bullet}}$. Since $\mathcal{M}^{\bullet}$ is an MLTS, thus as a direct consequence of (6), $\approx^{\bullet}$ is also the coarsest relation which is bard-preserving, reduction-closed, and compositional w.r.t. mCCS.

[1] A slight difference is that in (6) $\parallel$ is considered instead of $\parallel_A$.
[2] Our discussion here holds directly for the extension with passive transitions.

Chapter 7

Conclusion and Future Work

We conclude this thesis in this section. First we summary our contributions in Section 7.1, and then in Section 7.2 we point out some possible directions for future work.

7.1 Conclusion

In this thesis we mainly work on two things: i) probabilistic process calculi for MANETs, and ii) (bi)simulations and their characterizations on different probabilistic models. We first propose a discrete process calculus with which we can model unreliable wireless connections, and moreover the network topology changes can also be modeled by a probabilistic mobility function. We then define several variants of bisimulations and simulations for both networks and PMFs. We then propose a continuous-time process calculus for MANETs by extending the discrete process calculus in several ways. First of all we allow a mobility step to change part of a network topology not just a single connection. This is inspired by the fact that the movement of a node may affect a large part of the network topology, not just a connection with one of its neighbors. Secondly, we introduce stochastic time behavior for processes running at certain locations. Due to the introduction of the group broadcast and flooding avoidance operators, we also present a novel broadcast abstraction enabling that a broadcast action can be simulated by several broadcast actions in a sequence.

The semantics of the two process calculi gives rise to two different widely used probabilistic models i.e. probabilistic automata and Markov automata respectively, therefore in this thesis we also investigate some related problems for these two models.

For PA we discuss a variant of (bi)simulations and their logic characterizations w.r.t. PCTL* and its sublogics. We propose a sequence of strong i-depth bisimulations which can be characterized by a sequence of sublogics of PCTL*. This sequence of bisimulations will converge to PCTL* equivalence finally, similarly for weak bisimulations and simulations. Since CTMDP can be seen as a continuous-time counterpart of PA, thus we can extend the work to CTMDP in a natural way. Differently, we show that for a subclass of CTMDP i.e. 2-step recurrent CTMDP, the weak bisimulation can be characterized by CSL equivalence without the next operator.

An MA is a compositional behavior model with both probabilistic transitions and exponentially distributed random delays, and is a combination of PA and IMC. Previously, two different weak bisimulations, denoted as $\approx_{ehz}$ and $\approx_{dh}$ respectively, have been proposed by different authors, and the relation between $\approx_{ehz}$ and $\approx_{dh}$ is unclear. In this thesis, we propose two different semantics for MAs, early and late semantics respectively. Based on the semantics, we can define two variants of weak bisimulation for MAs: early and late weak bisimulation correspondingly. We also show that late weak bisimulation is strictly coarser than early weak bisimulation, while the early weak bisimulation coincides both $\approx_{ehz}$ and $\approx_{dh}$, thus as a side contribution we prove that $\approx_{ehz}$ and $\approx_{dh}$ are equivalent essentially. Early and late weak simulations are also defined.

7.2 Future Work

A number of directions for future work are possible. Since time is important for wireless networks, one extension is to consider a timed version of our calculus like in (110), which enables us to model behaviors like "each node will wait for at most 2 seconds before it sends acknowledgement to the parent."

Even though there always exists n such that $\sim_n^b$ can be characterized by PCTL equivalence, it turns out that it is expensive to compute the $\sim_n^b$, actually it has been shown in (91) that it is NP-complete to compute the $\sim_1^b$. But we also observe that in practice the worst case when computing $\sim_n^b$ can hardly happen. As we mentioned before the sequence of $\sim_i^b$ will converge to PCTL equivalence eventually. Suppose that $\sim_n^b = \sim_{\mathsf{PCTL}}$, then each $\sim_i^b$ such that $i < n$ can be seen as an approximation of $\sim_{\mathsf{PCTL}}$. Similar as in (111, 112, 113, 114), we can build an abstract system of a given PA based on $\sim_1^b$ (or even coarser relations) initially in order to verify certain properties, and we

keep refining the abstract system until a real counterexample of the verified property is found, or the property is proved to be true. This technique will work for other variants of (bi)simulations as well as for the continuous case.

As we have extended the work in Chapter 4 to countable state space, therefore another future work will be the extension of the work in Chapter 5 to countable state space. Since we have shown in Section 5.7.3 that the weak simulation for CTMC proposed in (54) is only sound but not complete w.r.t. $\mathsf{CSL}^0_{s\setminus \mathsf{X}}$ (safe fragment of CSL without next operator and all the time bounds are in the form of $[0,t)$), so a natural question is that can we adopt the original definition of weak simulation in (54) such that it is both sound and complete w.r.t. $\mathsf{CSL}^0_{s\setminus \mathsf{X}}$.

Markov automata have been introduced as a compositional behavioral model supporting both probabilistic transitions and exponentially distributed random delays. To the best of our knowledge, no logic has been proposed which enables us to describe the properties of MA, so another future work would be to consider a proper logic for MA as well as its model checking algorithm. In Chapter 6 we proposed different variants of weak (bi)simulations for MA, we could also study their logic characterizations.

References

[1] Roberto Segala and Nancy Lynch. **Probabilistic simulations for probabilistic processes**. *Nordic J. of Computing*, **2**:250–273, June 1995. ii, 4, 7, 15, 34, 47, 51, 75, 84, 86, 115, 119, 123, 124, 135, 137, 138, 144, 145, 151, 164, 175

[2] Hans Hansson and Bengt Jonsson. **A logic for reasoning about time and reliability**. *Formal Aspects of Computing*, **6**:512–535, 1994. 10.1007/BF01211866. ii, 7, 115, 121

[3] Andrea Bianco and Luca de Alfaro. **Model checking of probabilistic and nondeterministic systems**. In P. Thiagarajan, editor, *Foundations of Software Technology and Theoretical Computer Science*, **1026** of *Lecture Notes in Computer Science*, pages 499–513. Springer Berlin / Heidelberg, 1995. 10.1007/3-540-60692-0_70. iii, 7, 115, 121

[4] C. Baier and J.-P. Katoen. *Principles of model checking*. MIT Press, 2008. iii, 115, 120

[5] Christian Eisentraut, Holger Hermanns, and Lijun Zhang. **On Probabilistic Automata in Continuous Time**. In *Proceedings of the 2010 25th Annual IEEE Symposium on Logic in Computer Science*, LICS '10, pages 342–351, Washington, DC, USA, 2010. IEEE Computer Society. iii, 5, 9, 10, 77, 84, 95, 209, 210, 212, 213, 225, 232, 234, 238

[6] Yuxin Deng and Matthew Hennessy. **On the semantics of Markov automata**. In *Proceedings of the 38th international conference on Automata, languages and programming - Volume Part II*, ICALP'11, pages 307–318, Berlin, Heidelberg, 2011. Springer-Verlag. iii, 9, 10, 209, 212, 213, 232, 234, 238, 239

[7] R. Milner. *A Calculus of Communicating Systems*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 1982. 3, 6

[8] R. Milner. *Communication and Concurrency*. Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 1989. 3, 6, 51, 127, 144

[9] C. A. R. Hoare. **Communicating sequential processes**. *Commun. ACM*, **21**(8):666–677, August 1978. 3

[10] J.A. Bergstra and J.W. Klop. **Process algebra for synchronous communication**. 1984. 3

[11] J.A. Bergstra and J.W. Klop. **Algebra of communicating processes with abstraction**. *Theoretical Computer Science*, **37**(0):77 – 121, 1985. 3

[12] J. C. M. Baeten and W. P. Weijland. *Process Algebra*. Cambridge University Press, 1990. 3

[13] Robin Milner, Joachim Parrow, and David Walker. **A calculus of mobile processes, I**. *Inf. Comput.*, **100**:1–40, September 1992. 3

[14] Robin Milner, Joachim Parrow, and David Walker. **A calculus of mobile processes, II**. *Inf. Comput.*, **100**:41–77, September 1992. 3

[15] Davide Sangiorgi and David Walker. *π-Calculus: A Theory of Mobile Processes*. Cambridge University Press, New York, NY, USA, 2001. 3

[16] Gordon D. Plotkin. **A structural approach to operational semantics**. *J. Log. Algebr. Program.*, **60-61**:17–139, 2004. 3

[17] Alessandro Giacalone, Chi chang Jou, and Scott A. Smolka. **Algebraic Reasoning for Probabilistic Concurrent Systems**. In *Proceedings IFIP TC2 Working Conference on Programming Concepts and Methods*, pages 443–458. North-Holland, 1990. 3

[18] Gavin Lowe. **Probabilistic and prioritized models of timed CSP**. In *Selected papers of the meeting on Mathematical foundations of programming semantics*, pages 315–352, Amsterdam, The Netherlands, The Netherlands, 1995. Elsevier Science Publishers B. V. 3

[19] Manuel Núñez, David de Frutos-Escrig, and Luis Fernando Llana Díaz. **Acceptance Trees for Probabilistic Processes**. In *Proceedings of the 6th International Conference on Concurrency Theory*, CONCUR '95, pages 249–263, London, UK, 1995. Springer-Verlag. 3

[20] D. Cazorla, F. Cuartero, V. Valero, and F. L. Pelayo. **A process algebra for probabilistic and nondeterministic processes**. *Inf. Process. Lett.*, **80**:15–23, October 2001. 3

[21] Diego Cazorla, Fernando Cuartero, Valentín Valero Ruiz, Fernando L. Pelayo, and Juan José Pardo. **Algebraic theory of probabilistic and nondeterministic processes**. *J. Log. Algebr. Program.*, **55**(1C2):57 – 103, 2003. 3

[22] Suzana Andova and Jos C. M. Baeten. **Abstraction in Probabilistic Process Algebra**. In *Proceedings of the 7th International Conference on Tools and Algorithms for the Construction and Analysis of Systems*, TACAS 2001, pages 204–219, London, UK, 2001. Springer-Verlag. 3

[23] Rance Cleaveland, Scott Smolka, and Amy Zwarico. **Testing preorders for probabilistic processes**. In W. Kuich, editor, *Automata, Languages and Programming*, **623** of *Lecture Notes in Computer Science*, pages 708–719. Springer Berlin / Heidelberg, 1992. 10.1007/3-540-55719-9_116. 3

[24] Christel Baier and Holger Hermanns. **Weak Bisimulation for Fully Probabilistic Processes**. In *Proceedings of the 9th International Conference on Computer Aided Verification*, CAV '97, pages 119–130, London, UK, 1997. Springer-Verlag. 3, 7, 33, 34, 238

REFERENCES

[25] Rob J. van Glabbeek, Scott A. Smolka, and Bernhard Steffen. **Reactive, generative, and stratified models of probabilistic processes**. *Inf. Comput.*, **121**:59–80, August 1995. 4, 7

[26] Hans Hansson and Bengt Jonsson. **A Framework for Reasoning about Time and Reliability**. In *IEEE Real-Time Systems Symposium*, pages 102–111, 1989. 4

[27] Wang Yi and Kim Guldstrand Larsen. **Testing Probabilistic and Nondeterministic Processes**. In *Proceedings of the IFIP TC6/WG6.1 Twelth International Symposium on Protocol Specification, Testing and Verification XII*, pages 47–61, Amsterdam, The Netherlands, The Netherlands, 1992. North-Holland Publishing Co. 4

[28] Norbert Götz, Ulrich Herzog, and Michael Rettelbach. **Multiprocessor and Distributed System Design: The Integration of Functional Specification and Performance Analysis Using Stochastic Process Algebras**. In *Performance Evaluation of Computer and Communication Systems, Joint Tutorial Papers of Performance '93 and Sigmetrics '93*, pages 121–146, London, UK, 1993. Springer-Verlag. 4

[29] Jane Hillston. *A compositional approach to performance modelling*. Cambridge University Press, New York, NY, USA, 1996. 4, 7, 84, 113

[30] Marco Bernardo and Roberto Gorrieri. **A tutorial on EMPA: a theory of concurrent processes with nondeterminism, priorities, probabilities and time**. *Theor. Comput. Sci.*, **202**:1–54, July 1998. 4

[31] C. Priami. **Stochastic π-calculus**. *The Computer Journal*, **38**(7):578, 1995. 4

[32] Holger Hermanns. *Interactive Markov chains: and the quest for quantified quality*. Springer-Verlag, Berlin, Heidelberg, 2002. 4, 7, 76, 84, 89, 113, 173, 175, 209, 210, 213, 238

[33] Rocco De Nicola, Joost-Pieter Katoen, Diego Latella, Michele Loreti, and Mieke Massink. **Model checking mobile stochastic logic**. *Theor. Comput. Sci.*, **382**:42–70, August 2007. 4

[34] Maria G. Vigliotti and Peter G. Harrison. **Stochastic Ambient Calculus**. *Electronic Notes in Theoretical Computer Science*, **164**(3):169 – 186, 2006. 4

[35] G. Chiola, M. A. Marsan, G. Balbo, and G. Conte. **Generalized Stochastic Petri Nets: A Definition at the Net Level and its Implications**. *IEEE Trans. Softw. Eng.*, **19**:89–107, February 1993. 4

[36] Martin L. Puterman. *Markov Decision Processes: Discrete Stochastic Dynamic Programming*. John Wiley & Sons, Inc., New York, NY, USA, 1st edition, 1994. 4

[37] Martin R. Neuhäusser and Joost-Pieter Katoen. **Bisimulation and Logical Preservation for Continuous–Time Markov Decision Processes.** In Luís Caires and Vasco Thudichum Vasconcelos, editors, *CONCUR '07*, **4703** of *Lecture Notes in Computer Science*, pages 412–427. Springer, 2007. 4, 7, 167, 168, 171, 172, 175, 186, 208

[38] Eugene A. Feinberg. **Continuous Time Discounted Jump Markov Decision Processes: A Discrete-Event Approach**. *Math. Oper. Res.*, **29**:492–524, August 2004. 4

[39] Yasmina Abdeddaïm, Eugene Asarin, and Oded Maler. **On optimal scheduling under uncertainty**. In *Proceedings of the 9th international conference on Tools and algorithms for the construction and analysis of systems*, TACAS'03, pages 240–253, Berlin, Heidelberg, 2003. Springer-Verlag. 4

[40] Qinru Qiu and Massoud Pedram. **Dynamic power management based on continuous-time Markov decision processes**. In *Proceedings of the 36th annual ACM/IEEE Design Automation Conference*, DAC'99, pages 555–561, New York, NY, USA, 1999. ACM. 4

[41] David Park. **Concurrency and Automata on Infinite Sequences**. In *Proceedings of the 5th GI-Conference on Theoretical Computer Science*, pages 167–183, London, UK, 1981. Springer-Verlag. 6

[42] R.J. van Glabbeek. **The Linear Time - Branching Time Spectrum I**. In J.A. Bergstra, A. Ponse, and S.A. Smolka, editors, *Handbook of Process Algebra*, pages 3–99. Elsevier, 2001. 6, 168

[43] Rob J. van Glabbeek. **The Linear Time - Branching Time Spectrum II**. In *Proceedings of the 4th International Conference on Concurrency Theory*, CONCUR '93, pages 66–81, London, UK, 1993. Springer-Verlag. 6, 168

[44] Edmund M. Clarke and E. Allen Emerson. **Design and Synthesis of Synchronization Skeletons Using Branching-Time Temporal Logic**. In *Logic of Programs, Workshop*, pages 52–71, London, UK, 1982. Springer-Verlag. 6

[45] M. C. Browne, E. M. Clarke, and O. Grümberg. **Characterizing finite Kripke structures in propositional temporal logic**. *Theor. Comput. Sci.*, **59**:115–131, July 1988. 6

[46] Edmund M. Clarke, Orna Grumberg, and David E. Long. **Model checking and abstraction**. *ACM Trans. Program. Lang. Syst.*, **16**:1512–1542, September 1994. 7

[47] Chi-Chang Jou and Scott A. Smolka. **Equivalences, Congruences, and Complete Axiomatizations for Probabilistic Processes**. In *Proceedings of the Theories of Concurrency: Unification and Extension*, CONCUR '90, pages 367–383, London, UK, 1990. Springer-Verlag. 7

[48] Bengt Jonsson and Kim Guldstrand Larsen. **Specification and Refinement of Probabilistic Processes**. In *LICS*, pages 266–277, 1991. 7, 51

[49] Kim G. Larsen and Arne Skou. **Bisimulation through probabilistic testing**. *Inf. Comput.*, **94**:1–28, September 1991. 7, 164

[50] Adnan Aziz, Vigyan Singhal, and Felice Balarin. **It Usually Works: The Temporal Logic of Stochastic Systems**. In *Proceedings of the 7th International Conference on Computer Aided Verification*, pages 155–165, London, UK, 1995. Springer-Verlag. 7

[51] Luca de Alfaro. **Temporal Logics for the Specification of Performance and Reliability**. In *Proceedings of the 14th Annual Symposium on Theoretical Aspects of Computer Science*, STACS '97, pages 165–176, London, UK, 1997. Springer-Verlag. 7

[52] J. Desharnais, A. Edalat, and P. Panangaden. **A Logical Characterization of Bisimulation for Labeled Markov Processes**. In *Proceedings of the 13th Annual IEEE Symposium on Logic in Computer Science*, LICS '98, pages 478–, Washington, DC, USA, 1998. IEEE Computer Society. 7

[53] Anna Philippou, Insup Lee, and Oleg Sokolsky. **Weak Bisimulation for Probabilistic Systems**. In *Proceedings of the 11th International Conference on Concurrency Theory*, CONCUR '00, pages 334–349, London, UK, 2000. Springer-Verlag. 7, 164, 210, 238

[54] Christel Baier, Joost-Pieter Katoen, Holger Hermanns, and Verena Wolf. **Comparative branching-time semantics for Markov chains**. *Inf. Comput.*, **200**:149–214, August 2005. 7, 51, 116, 135, 143, 144, 148, 164, 167, 168, 178, 192, 202, 204, 205, 208, 238, 243

[55] Pedro R. D'Argenio, Nicolás Wolovick, Pedro Sánchez Terraf, and Pablo Celayes. **Nondeterministic Labeled Markov Processes: Bisimulations and Logical Characterization**. In *Proceedings of the 2009 Sixth International Conference on the Quantitative Evaluation of Systems*, QEST '09, pages 11–20, Washington, DC, USA, 2009. IEEE Computer Society. 7, 208

[56] Josee Desharnais, Vineet Gupta, Radha Jagadeesan, and Prakash Panangaden. **Weak Bisimulation is Sound and Complete for pCTL***. In *Proceedings of the 13th International Conference on Concurrency Theory*, CONCUR '02, pages 355–370, London, UK, 2002. Springer-Verlag. 7, 15, 155, 156, 157, 158, 159, 164, 208, 215, 238

[57] Holger Hermanns, Augusto Parma, Roberto Segala, Björn Wachter, and Lijun Zhang. **Probabilistic Logical Characterization**. *Inf. Comput.*, **209**:154–172, February 2011. 7, 160, 164, 208

[58] Marco Bernardo and Roberto Gorrieri. **Extended Markovian Process Algebra**. In *Proceedings of the 7th International Conference on Concurrency Theory*, CONCUR '96, pages 315–330, London, UK, 1996. Springer-Verlag. 7

[59] Christel Baier, Joost-Pieter Katoen, and Holger Hermanns. **Approximate Symbolic Model Checking of Continuous-Time Markov Chains**. In *Proceedings of the 10th International Conference on Concurrency Theory*, CONCUR '99, pages 146–161, London, UK, 1999. Springer-Verlag. 7

[60] Adnan Aziz, Kumud Sanwal, Vigyan Singhal, and Robert Brayton. **Model-checking continuous-time Markov chains**. *ACM Trans. Comput. Logic*, **1**:162–170, July 2000. 7

[61] J. Desharnais and P. Panangaden. **Continuous Stochastic Logic characterizes Bisimulation of Continuous-time Markov Processes**. *J. Log. Algebr. Program.*, **56**(1-2):99–115, 2003. 7, 208

[62] Augusto Parma and Roberto Segala. **Logical characterizations of bisimulations for discrete probabilistic systems**. In *Proceedings of the 10th international conference on Foundations of software science and computational structures*, FOSSACS'07, pages 287–301, Berlin, Heidelberg, 2007. Springer-Verlag. 7

[63] Sebastian Nanz and Chris Hankin. **A framework for security analysis of mobile wireless networks**. *Theor. Comput. Sci.*, **367**:203–227, November 2006. 13, 71, 72

[64] Anu Singh, C. R. Ramakrishnan, and Scott A. Smolka. **A process calculus for mobile ad hoc networks**. In *Proceedings of the 10th international conference on Coordination models and languages*, COORDINATION'08, pages 296–314, Berlin, Heidelberg, 2008. Springer-Verlag. 13, 72

[65] Massimo Merro. **An Observational Theory for Mobile Ad Hoc Networks**. *Electron. Notes Theor. Comput. Sci.*, **173**:275–293, April 2007. 13, 26, 72

[66] Fatemeh Ghassemi, Wan Fokkink, and Ali Movaghar. **Restricted Broadcast Process Theory**. In *Proceedings of the 2008 Sixth IEEE International Conference on Software Engineering and Formal Methods*, pages 345–354, Washington, DC, USA, 2008. IEEE Computer Society. 13, 72, 113

[67] Jens Chr. Godskesen. **A calculus for mobile ad hoc networks**. In *Proceedings of the 9th international conference on Coordination models and languages*, COORDINATION'07, pages 132–150, Berlin, Heidelberg, 2007. Springer-Verlag. 13, 26, 72

[68] Jens Chr. Godskesen. **A Calculus for Mobile Ad-hoc Networks with Static Location Binding**. *Electron. Notes Theor. Comput. Sci.*, **242**:161–183, July 2009. 13, 26

[69] Davide Sangiorgi and David Walker. *PI-Calculus: A Theory of Mobile Processes*. Cambridge University Press, New York, NY, USA, 2001. 23, 30

[70] Bengt Jonsson. **Simulations Between Specifications of Distributed Systems**. In *Proceedings of the 2nd International Conference on Concurrency Theory*, CONCUR '91, pages 346–360, London, UK, 1991. Springer-Verlag. 51, 144

[71] M. R. Henzinger, T. A. Henzinger, and P. W. Kopke. **Computing simulations on finite and infinite graphs**. In *Proceedings of the 36th Annual Symposium on Foundations of Computer Science*, FOCS '95, pages 453–462, Washington, DC, USA, 1995. IEEE Computer Society. 51, 144

[72] Fatemeh Ghassemi, Wan Fokkink, and Ali Movaghar. **Equational Reasoning on Mobile Ad Hoc Networks**. *Fundam. Inf.*, **105**:375–415, December 2010. 73

[73] Lei Song and Jens Chr. Godskesen. **Probabilistic Mobility Models for Mobile and Wireless Networks**. In Cristian Calude and Vladimiro Sassone, editors, *Theoretical Computer Science*, **323** of *IFIP Advances in Information and Communication Technology*, pages 86–100. Springer Boston, 2010. 10.1007/978-3-642-15240-5_7. 79

REFERENCES

[74] Xavier Nicollin and Joseph Sifakis. **An Overview and Synthesis on Timed Process Algebras**. In *Proceedings of the 3rd International Workshop on Computer Aided Verification*, CAV '91, pages 376–398, London, UK, 1992. Springer-Verlag. 89

[75] Wang Yi. **CCS + Time = An Interleaving Model for Real Time Systems**. In *Proceedings of the 18th International Colloquium on Automata, Languages and Programming*, pages 217–228, London, UK, 1991. Springer-Verlag. 89

[76] Sudarshan Vasudevan, Jim Kurose, and Don Towsley. **Design and Analysis of a Leader Election Algorithm for Mobile Ad Hoc Networks**. In *Proceedings of the 12th IEEE International Conference on Network Protocols*, pages 350–360, Washington, DC, USA, 2004. IEEE Computer Society. 109, 110

[77] Fatemeh Ghassemi, Mahmoud Talebi, Ali Movaghar, and Wan Fokkink. **Stochastic Restricted Broadcast Process Theory**. In *EPEW*, pages 72–86, 2011. 113

[78] Roberto Segala. *Modeling and verification of randomized distributed real-time systems*. PhD thesis, Cambridge, MA, USA, 1995. 115, 118, 173, 209, 210, 213, 215, 238

[79] Hichem Boudali, Pepijn Crouzen, and Marielle Stoelinga. **A Rigorous, Compositional, and Extensible Framework for Dynamic Fault Tree Analysis**. *IEEE Trans. Dependable Secur. Comput.*, **7**:128–143, April 2010. 116

[80] Stefano Cattani and Roberto Segala. **Decision Algorithms for Probabilistic Bisimulation**. In *Proceedings of the 13th International Conference on Concurrency Theory*, CONCUR '02, pages 371–385, London, UK, 2002. Springer-Verlag. 116, 215, 217

[81] Christel Baier, Bettina Engelen, and Mila Majster-Cederbaum. **Deciding bisimilarity and similarity for probabilistic processes**. *J. Comput. Syst. Sci.*, **60**:187–231, February 2000. 116

[82] Joost-Pieter Katoen, Tim Kemna, Ivan Zapreev, and David N. Jansen. **Bisimulation minimisation mostly speeds up probabilistic model checking**. In *Proceedings of the 13th international conference on Tools and algorithms for the construction and analysis of systems*, TACAS'07, pages 87–101, Berlin, Heidelberg, 2007. Springer-Verlag. 116

[83] Moshe Y. Vardi. **Automatic verification of probabilistic concurrent finite state programs**. In *Proceedings of the 26th Annual Symposium on Foundations of Computer Science*, pages 327–338, Washington, DC, USA, 1985. IEEE Computer Society. 119

[84] Hans A. Hansson. *Time and Probability in Formal Design of Distributed Systems*. Elsevier Science Inc., New York, NY, USA, 1994. 119

[85] Rob J. van Glabbeek and W. Peter Weijland. **Branching time and abstraction in bisimulation semantics**. *J. ACM*, **43**:555–600, May 1996. 128

[86] H.H. Schaefer, M.P.H. Wolff, and M. Wolff. *Topological vector spaces*, **3**. Springer Verlag, 1999. 157

[87] Hans Hansson and Bengt Jonsson. **A Calculus for Communicating Systems with Time and Probabilities**. In *IEEE Real-Time Systems Symposium*, pages 278–287, 1990. 164

[88] Matthew Hennessy and Robin Milner. **Algebraic laws for nondeterminism and concurrency**. *J. ACM*, **32**:137–161, January 1985. 164

[89] B. Jonsson, K. Larsen, and W. Yi. **Probabilistic extensions of process algebras**. In *Handbook of Process Algebra*, Elsevier, pages 685–710, 2001. 164, 208

[90] Roberto Segala and Andrea Turrini. **Comparative Analysis of Bisimulation Relations on Alternating and Non-Alternating Probabilistic Models**. In *QEST*, pages 44–53, 2005. 164, 175

[91] Mathieu Tracol, Josée Desharnais, and Abir Zhioua. **Computing Distances between Probabilistic Automata**. In *QAPL*, pages 148–162, 2011. 165, 242

[92] Luca de Alfaro, Rupak Majumdar, Vishwanath Raman, and Marielle Stoelinga. **Game Relations and Metrics**. In *Proceedings of the 22nd Annual IEEE Symposium on Logic in Computer Science*, pages 99–108, Washington, DC, USA, 2007. IEEE Computer Society. 165

[93] John Fearnley, Markus Rabe, Sven Schewe, and Lijun Zhang. **Efficient Approximation of Optimal Control for Continuous-Time Markov Games**. In *FSTTCS*, pages 399–410, 2011. 167

[94] Tomás Brázdil, Vojtech Forejt, Jan Krcál, Jan Kretínský, and Antonín Kucera. **Continuous-Time Stochastic Games with Time-Bounded Reachability**. In *FSTTCS*, pages 61–72, 2009. 167

[95] Martin R. Neuhäusser, Mariëlle Stoelinga, and Joost-Pieter Katoen. **Delayed Nondeterminism in Continuous-Time Markov Decision Processes**. In *Proceedings of the 12th International Conference on Foundations of Software Science and Computational Structures: Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2009*, FOSSACS '09, pages 364–379, Berlin, Heidelberg, 2009. Springer-Verlag. 167, 170

[96] Martin R. Neuhausser and Lijun Zhang. **Time-Bounded Reachability Probabilities in Continuous-Time Markov Decision Processes**. In *Proceedings of the 2010 Seventh International Conference on the Quantitative Evaluation of Systems*, QEST '10, pages 209–218, Washington, DC, USA, 2010. IEEE Computer Society. 167, 175, 177

[97] Peter Buchholz, Ernst Moritz Hahn, Holger Hermanns, and Lijun Zhang. **Model checking algorithms for CTMDPs**. In *Proceedings of the 23rd international conference on Computer aided verification*, CAV'11, pages 225–242, Berlin, Heidelberg, 2011. Springer-Verlag. 167

[98] Markus N. Rabe and Sven Schewe. **Finite optimal control for time-bounded reachability in CTMDPs and continuous-time Markov games.** *Acta Inf.*, **48**(5-6):291–315, 2011. 167, 175, 177, 238

[99] Lei Song, Lijun Zhang, and Jens Chr. Godskesen. **Bisimulations meet PCTL equivalences for probabilistic automata**. In *Proceedings of the 22nd international conference on Concurrency theory*, CONCUR'11, pages 108–123, Berlin, Heidelberg, 2011. Springer-Verlag. 168, 185, 208

[100] Peter Buchholz and Ingo Schulz. **Numerical analysis of continuous time Markov decision processes over finite horizons**. *Comput. Oper. Res.*, **38**:651–659, March 2011. 170, 177

[101] Nicols Wolovick and Sven Johr. **A Characterization of Meaningful Schedulers for Continuous–Time Markov Decision Processes.** In Eugene Asarin and Patricia Bouyer, editors, *FORMATS '06*, **4202** of *Lecture Notes in Computer Science*, pages 352–367. Springer, 2006. 171

[102] Christel Baier, Boudewijn Haverkort, Holger Hermanns, and Joost-Pieter Katoen. **Model-Checking Algorithms for Continuous-Time Markov Chains**. *IEEE Trans. Softw. Eng.*, **29**:524–541, June 2003. 172, 186

[103] Yuxin Deng, Rob van Glabbeek, Matthew Hennessy, Carroll Morgan, and Chenyi Zhang. **Characterising Testing Preorders for Finite Probabilistic Processes**. In *Proceedings of the 22nd Annual IEEE Symposium on Logic in Computer Science*, pages 313–325, Washington, DC, USA, 2007. IEEE Computer Society. 173

[104] Christian Eisentraut, Holger Hermanns, and Lijun Zhang. **On Probabilistic Automata in Continuous Time**. In *Proceedings of the 2010 25th Annual IEEE Symposium on Logic in Computer Science*, LICS '10, pages 342–351, Washington, DC, USA, 2010. IEEE Computer Society. 173, 175

[105] Holger Hermanns and Sven Johr. **Uniformity by Construction in the Analysis of Nondeterministic Stochastic Systems**. In *Proceedings of the 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, DSN '07, pages 718–728, Washington, DC, USA, 2007. IEEE Computer Society. 175

[106] Lijun Zhang, Holger Hermanns, Friedrich Eisenbrand, and David N. Jansen. **Flow faster: efficient decision algorithms for probabilistic simulations**. In *Proceedings of the 13th international conference on Tools and algorithms for the construction and analysis of systems*, TACAS'07, pages 155–169, Berlin, Heidelberg, 2007. Springer-Verlag. 185

[107] Kohei Honda and Mario Tokoro. **On Asynchronous Communication Semantics**. In *Proceedings of the Workshop on Object-Based Concurrent Computing*, pages 21–51, London, UK, 1992. Springer-Verlag. 212

[108] Yuxin Deng, Rob Glabbeek, Matthew Hennessy, and Carroll Morgan. **Testing Finitary Probabilistic Processes**. In *Proceedings of the 20th International Conference on Concurrency Theory*, CONCUR 2009, pages 274–288, Berlin, Heidelberg, 2009. Springer-Verlag. 215

[109] Christian Eisentraut, Holger Hermanns, and Lijun Zhang. **Concurrency and composition in a stochastic world**. In *Proceedings of the 21st international conference on Concurrency theory*, CONCUR'10, pages 21–39, Berlin, Heidelberg, 2010. Springer-Verlag. 237

[110] Massimo Merro, Francesco Ballardin, and Eleonora Sibilio. **A timed calculus for wireless systems**. *Theor. Comput. Sci.*, **412**:6585–6611, November 2011. 242

[111] Holger Hermanns, Björn Wachter, and Lijun Zhang. **Probabilistic CEGAR**. In *Proceedings of the 20th international conference on Computer Aided Verification*, CAV '08, pages 162–175, Berlin, Heidelberg, 2008. Springer-Verlag. 242

[112] Björn Wachter and Lijun Zhang. **Best probabilistic transformers**. In *Proceedings of the 11th international conference on Verification, Model Checking, and Abstract Interpretation*, VMCAI'10, pages 362–379, Berlin, Heidelberg, 2010. Springer-Verlag. 242

[113] Mark Kattenbelt, Marta Kwiatkowska, Gethin Norman, and David Parker. **A game-based abstraction-refinement framework for Markov decision processes**. *Form. Methods Syst. Des.*, **36**(3):246–280, September 2010. 242

[114] Rohit Chadha and Mahesh Viswanathan. **A counterexample-guided abstraction-refinement framework for markov decision processes**. *ACM Trans. Comput. Logic*, **12**(1):1:1–1:49, November 2010. 242