METRIC SEMANTICS FOR REACTIVE PROBABILISTIC PROCESSES

by

GETHIN JOSIAH NORMAN

A thesis submitted to the Faculty of Science
of The University of Birmingham
for the Degree of
DOCTOR OF PHILOSOPHY

School of Computer Science
Faculty of Science
University of Birmingham
November 1997

Abstract

In this thesis we present three mathematical frameworks for the modelling of reactive probabilistic communicating processes. We first introduce generalised labelled transition systems as a model of such processes and introduce an equivalence, coarser than probabilistic bisimulation, over these systems. Two processes are identified with respect to this equivalence if, for all experiments, the probabilities of the respective processes passing a given experiment are equal. We next consider a probabilistic process calculus including external choice, internal choice, action-guarded probabilistic choice, synchronous parallel and recursion. We give operational semantics for this calculus be means of our generalised labelled transition systems and show that our equivalence is a congruence for this language.

Following the methodology introduced by de Bakker & Zucker, we then give denotational semantics to the calculus by means of a complete metric space of probabilistic processes. The derived metric, although not an ultra-metric, satisfies the intuitive property that the distance between two processes tends to 0 if a measure of the differences of their observable behaviour also tends to 0. We show that the denotational model is fully abstract with respect to our equivalence.

We also provide a logical characterisation of the process equivalence by means of a variant of the quantitative Hennessy-Milner Logic (HML), where each HML formula is interpreted as the probability of it being satisfied by the process instead of the usual truth value. Two processes are then shown equivalent if, and only if, they agree on the quantities assigned to all HML formulae.

Acknowledgements

I would like to thank my supervisor, Marta Kwiatkowska, for her advice, guidance and useful suggestions throughout my time as a PhD student. I would also like to thank Michael Huth for taking the time to read and comment on an early draft of this thesis, Peter Hancox, Achim Jung, Gavin Lowe and Mark Ryan for their many helpful comments and advice.

Finally I would like to thank Sam and my parents for their understanding and continued support.

This research was made possible by a grant from the School of Computer Science, at the University of Birmingham.

Contents

Chapter 1

Introduction

Formulating suitable models for the formal description, specification and analysis of concurrent systems is an important topic of study in theoretical computer science. A *concurrent* system is one where programs communicate among themselves by some well-defined mechanism. A designer or verifier will need a way to assign a consistent meaning to the program or language under consideration. This meaning is the *semantics* of the language or program.

There are three main approaches to giving semantics to programming languages: operational, denotational and logical. The different semantics offer alternative views. The *operational* model is closely related to the actual implementation of the language, and is defined by means of some abstract machine. This machine will then describe the steps taken to execute the program. The *denotational* semantics is given in terms of some mathematical structure where programs are considered as elements of this structure. This then yields a *compositional* model: the semantics of a complex program is defined in terms of its components by means of operators on the mathematical structure. The *logical* model enables the investigation of properties and satisfaction conditions of programs. As the different semantic approaches offer different "views" of the same system, understanding the relationships between them can prove useful. The correspondence often sought between the operational and denotational models is one of *full abstraction*, which means that two program phrases have the same denotation if and only if the operational meaning of every program is unchanged when one phrase is replaced by the other in any context. A similar correspondence regarding the logical and operational approaches is also useful, where instead of program phrases having the same denotation we consider program phrases which have the same interpretations under all formulae of the logical model.

Depending on the application required, one of the three approaches will prove more useful. For example, a programmer is likely to prefer the denotational approach because the model will be compositional; an implementer will choose an operational semantics since this approach is most closely linked to an actual implementation, whereas, if we wish to reason about properties of programs, a logical semantics is the natural choice since we can express the desired properties as formulae of the logic and then investigate whether they are true for a particular program.

In recent times, randomisation has proved to be a very useful tool in the construction of certain algorithms for concurrent systems which, unlike their deterministic counterparts, can be programmed efficiently: they have relatively simple structures, use less memory and can achieve results that deterministic algorithms cannot be proved to meet. The algorithms include: a symmetric distributed solution to the dining philosopher's problem [LR81] and solutions to: consensus protocols [Sei92], load balancing [Pug90] and self-stabilisation [Her90].

Traditionally, the modelling of concurrent systems has abstracted away from quantitative aspects. As a result, there is no information about how frequently or with what chance certain behaviour of a system will occur, whereas, at a practical level, there need to be distinctions relating to this, since many aspects of concurrent systems are probabilistic in nature, or at least can be modelled adequately by assuming random behaviour. Thus, adding randomisation allows us to use a more realistic model of such systems. For example, it is often infeasible to construct a system that is error-free and some measure of the frequency of erroneous behaviour could be useful, as illustrated by modelling communication media, see for example [PS87], where it is often necessary to allow for processes to lose messages with a certain probability. Using probabilities will also offer a method of telling how good or bad certain systems are: if the probabilities of errors occurring are very low the system can be deemed useful, whereas if the probabilities of errors are very high, then clearly the system will have no practical applications.

Furthermore, allowing randomised behaviour can be seen as a way of modelling fairness, since a fair choice can be considered as a choice, where the probability of either action occurring is greater than zero or some assigned lower bound.

The modelling of concurrent systems is already made complex by the phenomenon of *non-determinism*. Non-determinism presents a powerful tool to model situations where there exist two or more possible choices for how a system will behave, but it is unknown which choice is going to be taken; we call such a choice an internal (or non-deterministic) choice. This, therefore, offers us a way to under-specify systems, that is, we can allow certain areas of a system's behaviour to be partially defined. Then adding randomisation will increase the complexity of the model since this adds a different kind of non-determinism: the choice is made as a result of some random draw, or more simply from the result of the toss of a coin.

The usual approach to adding randomisation to concurrent systems has been to replace non-deterministic behaviour by probabilistic behaviour, that is, substitute the unspecified choice by a probability distribution over the possible choices. However, although, as indicated above, these two phenomena are similar, they are in fact used to model very distinct situations: as discussed above, non-determinism allows us to under-specify the behaviour of system, whereas randomisation fully specifies the behaviour of systems, as we will know the exact frequency (probability) of the choices of a system. To illustrate this, consider a choice between picking any number from 1 to 6, then if this choice is internal (non-deterministic) we will be unable to say which number is picked or how often each number is picked. However, if this choice arises through randomisation, one example would be to consider the choice being made according to the throw of a die and, in this case, over any long series of trials the frequency of any one of the numbers occurring is one sixth, assuming the die is fair.

Also, non-determinism arises in systems through other forms of behaviour, for example, if we are in a situation where the environment in which the system is placed decides how the system behaves. If the system can offer two distinct choices which the environment cannot distinguish, this type of choice will then degenerate to an internal choice.

Following this discussion we feel it is important to model both non-determinism and randomisation and treat them as distinct entities. The main objective of this thesis is, therefore, to investigate the different semantic views and relationships between the alternative modelling approaches for concurrent systems which exhibit both non-determinism and randomisation and distinguish clearly between them, or, in other words, to construct operational, denotational and logical semantics for such systems.

1.1 Outline

The next chapter gives an overview of related work, concentrating on the classical operational models for non-probabilistic systems and extensions to allow for probabilities. Chapter 3 introduces most of the notation used and the background material needed for this thesis.

Chapter 4 introduces reactive probabilistic transition systems, a model of processes that exhibit (action-guarded) probabilistic, deterministic and non-deterministic behaviour. This chapter, furthermore, introduces an observational order and equivalence over elements of such systems.

Chapter 5 presents the syntax and semantics of our calculus for reactive processes RP, where the difference between RP and standard (non-probabilistic) process calculi is that prefixing is replaced by action-guarded probabilistic choice of which the former is a special case. Moreover, we investigate the properties of our operational ordering over this semantics.

Chapter 6 gives a denotational semantics for our process calculus based on the work of de Bakker and Zucker [BZ82], which we show is fully abstract with respect to our operational semantics.

Chapter 7 investigates a logical approach based on the re-interpretation of the modal μ-calculus for probabilistic processes introduced by Huth and Kwiatkowska [HK97], and we show a strong connection between this interpretation and our operational semantics.

Finally, in Chapter 8 we conclude with an evaluation of the presented work and a discussion of possible future research directions.

Chapter 2

Related Work

Models of concurrency containing probabilistic behaviour can be classified according to two main criteria: which process calculus theory the probabilistic work is based on and the kind of probabilistic behaviour modelled. There are two main process calculi that serve as the basis for probabilistic extensions, namely Milner's Calculus of Communicating Systems (CCS) [Mil89] and Hoare's Communicating Sequential Processes (CSP) [BHR84]. The difference between the theories of CCS and CSP arises from the types of equivalences and the approach used in modelling systems, and in particular the process constructors.

CCS is modelled using *labelled transition systems* [Plo81]: a tuple $(T, \mathcal{A}ct, \longrightarrow)$, where T is a set of processes (or states), $\mathcal{A}ct$ is a set of actions (or labels), and $\longrightarrow \subseteq T \times \mathcal{A}ct \times T$ is a transition relation, where for any $(P, a, Q) \in \longrightarrow$ we write $P \xrightarrow{a} Q$, denoting the process P performing the action a and then behaving as the process Q. Equivalences for these transition systems are based on *bisimulation* [Par81] and [Mil83]. A (strong) bisimulation is a relation $\sim$ such that for any $P, Q \in T$, $P \sim Q$ if and only if for all $a \in \mathcal{A}ct$:

$$\begin{array}{ll} (i) & \text{if } P \xrightarrow{a} P' \text{ then } \exists\, Q' \in T :\ Q \xrightarrow{a} Q' \text{ and } P' \sim Q' \\ (ii) & \text{if } Q \xrightarrow{a} Q' \text{ then } \exists\, P' \in T :\ P \xrightarrow{a} P' \text{ and } P' \sim Q'. \end{array}$$

Two processes P and Q are said to be *bisimilar* if there exists a bisimulation relation $\sim$ such that $P \sim Q$. An alternative and weaker equivalence for CCS results from considering *simulations* (see [Par81]), where a simulation relation corresponds to only the first clause in the definition of bisimulation above. The classical denotational models for CCS are then based on Milner's synchronization trees [Mil89] and can be divided into domain-theoretic and metric-space approaches, for example see [Abr91a] and [BZ82] respectively.

In contrast, the models and equivalences for CSP are based on *traces* [Hoa85] and *failures* [BHR84]. The traces of a process are the possible sequences of actions that the process can perform, and failures are represented by pairs (σ, X) where σ is a trace and X is a set of actions. Each process is represented by the set of all failures, where each failure (σ, X) means that the process can perform the trace σ and then refuse to perform all the actions in the set X (failure sets are closed with respect to certain axioms). Processes are then trace or failure equivalent when their traces or failure sets are equal (for the formal definition see Section 3.4). Both models form an algebraic inductive partial order, a structure used to give denotational models for CSP (see Mislove [Mis91]).

The above models can be constructed for both CCS and CSP; for example, Brookes [Bro83] constructs a model for CSP based on synchronization trees. However, the general tendency is to use synchronisation trees for CCS and traces or failures for CSP. The equivalences mentioned above differ substantially in how well they discriminate branching: trace equivalence is the prime example of a *linear-time* equivalence, bisimulation is the prime example of a *branching-time* equivalence and failure equivalence can be considered as linear-time equivalence enriched with "local branching information". Intuitively, linear time equivalences are completely determined by the observable contents of processes' possible runs, whereas branching-time equivalences also use the information as to when the processes make choices. For these reasons, the equivalences form a hierarchy, with bisimulation being the finest equivalence and the coarsest being trace equivalence (see [BKO88] and [Gla90]). To illustrate the differences between these equivalences consider the example given below:

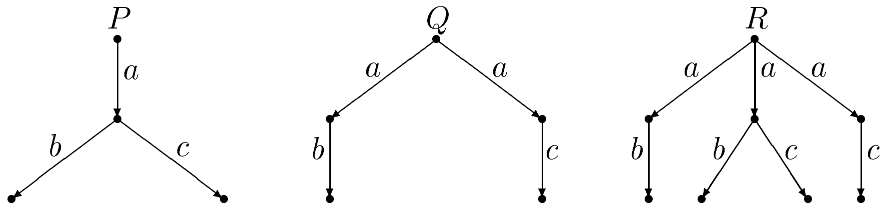


Figure 2.1: Linear versus Branching-time equivalences

In Figure 2.1 all processes can only perform the traces ab and ac, and hence are linear-time (trace) equivalent. However, whenever P performs an a transition it then offers a choice between performing the actions b and c, which is not the case for either Q and R, and thus P is not branching-time equivalent (bisimilar) to either Q or R. Furthermore, since R can perform an a transition such that there exists a choice between performing the actions b and c and Q cannot perform such a transition, Q and R are also not branching-time equivalent. As mentioned before, failure equivalence is an extended linear-time equivalence, and to illustrate this fact failures can distinguish between the processes P and Q but cannot distinguish between the processes P and R.

There are arguments for and against which type of equivalence is more appropriate, depending on how strict the notion of observable behaviour is and what is considered a realistic testing scenario. In van Glabbeek [Gla90, Gla93] a detailed description of the different options available is provided.

The choice of whether a metric or a domain-theoretic approach is used to give denotational semantics is to some degree a matter of taste. Denotational semantics was first introduced by Scott and Strachey using ordered sets (domains) as the mathematical framework [Sto77] and since then Nivat [Niv79] followed by de Bakker and Zucker [BZ82] introduced metric spaces as an alternative framework. In both settings, to deal with recursive programs, for example while statements, a solution of a recursive domain equation is used to give denotational semantics, and general techniques for such constructions, for example [Plo81] and [AJ94] for domains and [AR89] for metric spaces, are offered.

However, in certain cases one approach can have advantages over the other. For example, when considering fixed points for metric spaces we have *unique* fixed points from Banach's theorem, whereas in domain-theoretic approaches typically we use *least* fixed points according to the Knaster-Tarski theorem. As a result, proofs of statements relating to fixed points are often simpler in the metric space approach. On the other hand, one of the main arguments against a metric approach arises from the question of whether we need to know the actual distance between processes given by a metric, or whether it is enough to know that one process approximates another as given by an ordering. In fact, the primary role of metric denotational semantics appears to be concerned with limit point arguments, as opposed to the quantitative role that the numerical distance between processes offers.

Although not yet applied to the field of concurrency, there has been some recent work establishing connections between the theory of metric spaces and domain theory. Research in this area includes Edalat and Heckmann [EH], where metric spaces can be represented as the set of maximal elements of suitably constructed domains.

2.1 Probabilistic and Other Choice Operators

If we now consider the different options available to model probabilistic choice, we see there are two approaches to defining the type of probabilistic choice. The first, introduced by Lowe [Low93], is based on the choice operators of CSP, namely internal (or non-deterministic) choice and external (or deterministic) choice, denoted $\sqcap$ and

$\Box$ respectively. The difference between these operators is that, for any processes P and Q, $P \sqcap Q$ represents the process that will behave as either P or Q, whereas the behaviour of $P \Box Q$ depends on the actions offered by the environment: if only one of the processes P and Q can perform the actions offered by the environment then $P \Box Q$ will behave as that process, but if both P and Q can perform the actions offered by the environment, then $P \Box Q$ will choose between P and Q non-deterministically, that is, $\Box$ degenerates to $\sqcap$ in this case. Hence, the environment only has control over the choices with respect to the external choice operator.

Extending this to the probabilistic setting, we arrive at two probabilistic choice operators, internal and external probabilistic choice, which we will denote ${}_p\sqcap_q$ and ${}_p\Box_q$ respectively (where $p+q=1$). $E\,{}_p\sqcap_q\,F$ will act as the process E with probability p and F with probability q. If the environment offers actions which only E or F can perform then $E\,{}_p\Box_q\,F$ will act as E or F respectively, and if the environment offers actions which both E and F can perform then $E\,{}_p\Box_q\,F$ will act as E with probability p and F with probability q. Lowe [Low93], furthermore, considers the two extreme cases of the external probabilistic choice, that is, when $p=1$ and $q=0$ and when $p=0$ and $q=1$, named *prioritised* choice: for example, if the environment offers actions that both E and F can perform then $E\,{}_1\Box_0\,F$ will act as E, since the probability of acting as E is 1 and the probability of acting as F is 0, but if the environment offers only actions that F can perform then $E\,{}_1\Box_0\,F$ will act as F.

An alternative approach has been introduced by van Glabbeek et al. [GSST90] where three different models for probabilistic choice are presented, namely *reactive*, *generative* and *stratified*. In the reactive model, the model selected for consideration in this thesis, the environment is only allowed to offer processes one action at a time, and if a process can perform this action a probabilistic choice is made between the transitions associated with this action. The result is that, for any action a process can perform, the total probability of the process performing transitions associated with this action is required to be 1. Moreover, we can consider this model as having both external and internal probabilistic choice: an external (deterministic) choice made by the environment as to which action a process is allowed to perform, and an internal probabilistic choice as to which transition associated with this action the process subsequently performs.

On the other hand, the generative model allows the environment to offer more than one action and processes then make probabilistic choices between transitions associated with these actions. Hence, this model represents a type of external probabilistic choice and allows no other form of choice.

To illustrate the difference between these models consider the following example (where + denotes probabilistic choice):

$$\frac{1}{4}a.E_1 + \frac{3}{4}a.F_1 + \frac{2}{3}b.E_2 + \frac{1}{3}b.F_2 \quad \text{and} \quad \frac{1}{8}a.E + \frac{1}{2}b.F + \frac{3}{8}c.G.$$

First, if we consider the behaviour of the reactive process on the left, we note that if the environment offers the action a then the process will perform an a transition and behave as E_1 with probability $\frac{1}{4}$ and F_1 with probability $\frac{3}{4}$. Similarly, if the process is offered a b, it will perform a b transition and then behave as E_2 with probability $\frac{2}{3}$ and F_2 with probability $\frac{1}{3}$. Now, the generative process on the right (recall that in the generative model the environment is allowed to offer more than one action at a time), when offered the actions a, b and c, it will choose the a transition with probability $\frac{1}{8}$, the b transition with probability $\frac{1}{2}$ and the c transition with probability $\frac{3}{8}$. If, however, the environment offers the actions a and b, then the process will perform the a transition with probability $\frac{1}{5}$ and the b transition with probability $\frac{4}{5}$. Note that these values are reached by normalising the probabilities over the possible choices allowed, that is over $\frac{1}{8} + \frac{1}{2}$. Similar calculations can be made for other actions being performed; in particular, if only one of a, b and c is offered, the process will choose the associated transition with probability 1.

The stratified model captures the probabilistic branching of processes in a more satisfactory way, by allowing probabilistic choice to be separate from action transitions. This model contains an external probabilistic choice operator and, as for the generative model, the only type of choice is probabilistic. To illustrate this consider the following example of a stratified process:

$$\frac{1}{2}a.E' + \frac{1}{2}\left(\frac{1}{4}b.F' + \frac{3}{4}c.G'\right).$$

It first makes a probabilistic choice between performing an a transition and a b or c transition, and only after this choice is made does the process make a probabilistic choice between a b and c transition.

2.2 Probabilistic Versions of CCS

Probabilistic extensions to CCS are based on probabilistic labelled transition systems and probabilistic bisimulation introduced by Larsen and Skou [LS91]. Probabilistic transition systems are essentially labelled transition systems with probabilities attached to each transition, such that transitions are now of the form $E \xrightarrow{a}_{\mu} F$, which stands for E performing an a transition and then behaving as the process F with probability μ. To model reactive and generative processes we require:

$$\sum\{\mu \mid \exists F \in T.\ E \xrightarrow{a}_{\mu} F\} = 1 \quad \text{and} \quad \sum\{\mu \mid \exists F \in T,\ \exists a \in \mathcal{A}ct.\ E \xrightarrow{a}_{\mu} F\} = 1$$

for each process E and action a that E can perform, and (active) process E respectively. Modelling stratified processes becomes more difficult, but if we introduce a distinct action to represent probabilistic choice and we require that all transitions of other action types occur with probability 1, a transition system for stratified processes can be formulated.

Probabilistic bisimulation [LS91] is an extension of bisimulation to allow for probabilities. Formally, we can define a probabilistic bisimulation relation $\sim_p$ over the set of processes of a probabilistic transition system, $\mathcal{P}$ say, as follows. A probabilistic bisimulation $\sim_p$ is an equivalence on $\mathcal{P}$ such that whenever $E \sim_p F$ the following holds:

$$\forall a \in \mathcal{A}ct.\ \forall S \in \mathcal{P}/\!\sim_p.\ E \xrightarrow{a}_{\mu} S \ \Leftrightarrow\ F \xrightarrow{a}_{\mu} S$$

where $\mathcal{P}/\!\sim_p$ denotes the set of equivalence classes of $\mathcal{P}$ under $\sim_p$ and $E \xrightarrow{a}_{\mu} S$ if and only if $\mu = \sum\{\mu' \,|\, E' \in S \text{ and } E \xrightarrow{a}_{\mu'} E'\}$. Then two probabilistic processes E and F are said to be *probabilistic bisimilar* in the case that (E, F) is contained in some probabilistic bisimulation. Although the definition of probabilistic bisimulation appears very different from the definition of bisimulation given above, we note its similarity to ordinary bisimulation by instead considering the following equivalent formulation of bisimulation given in [LS91]. A bisimulation $\sim$ is an equivalence on T (the set of processes of a labelled transition system) such that whenever $P \sim Q$ the following holds:

$$\forall a \in \mathcal{A}ct.\ \forall S \in T/\!\sim.\ P \xrightarrow{a} S \ \Leftrightarrow\ Q \xrightarrow{a} S.$$

Formally, a connection between bisimulation and probabilistic bisimulation has been shown by Bloom and Meyer [BM89] in that, for any two finitely branching bisimilar non-deterministic processes, there exists an assignment of probabilities such that the resultant probabilistic processes are probabilistic bisimilar. The close relationship between bisimulation and probabilistic bisimulation implies that probabilistic bisimulation is also a branching time equivalence. Therefore, the time at which probabilistic choices occur will influence the equivalence of processes.

Larsen and Skou [LS91] have introduced a notion of testing such that if two processes are probabilistic bisimilar then there exists a testing algorithm that with probability $1 - \varepsilon$, for ε arbitrarily small, will distinguish the processes.

Also, Jonsson and Larsen [JL91] generalize probabilistic bisimulation by means of a specification formalism, which extends specifications for non-probabilistic processes (for example see [Lam89]). Specifications are represented by probabilistic transition systems where each transition is labelled with a set of probabilities. Using this they define a satisfaction relation between processes and specifications. A process and specification are in such a relation if the probabilities of the process performing transitions lie within the set of probabilities of the corresponding transition of the specification. They then show that, if processes are turned into specifications by considering singleton sets, then two processes are probabilistic bisimilar if and only if they are in a satisfaction relation. Moreover, Jonsson and Larsen define a relation between specifications which leads to a probabilistic simulation relation over probabilistic processes.

Based on this work, Segala and Lynch [SL94] extend both probabilistic bisimulation and simulation to a generalized reactive model of probabilistic processes. Processes of the model can be interpreted as allowing an internal choice between behaving as reactive processes which can perform only one action type. Their notion of probabilistic simulation is shown to coincide with the usual definition of simulations if the processes are restricted to non-probabilistic processes by letting all transitions occur with probability 1.

Of approaches related to probabilistic bisimulation we mention Giacalone, Jou and Smolka [GJS90], where a probabilistic version of Milner's synchronous version of CCS (SCCS [Mil83]), called PCCS is considered. The difference from SCCS arises from the choice operator being replaced by a probabilistic choice operator. Formally, any SCCS expression of the form $\sum_{i\in I} E_i$, denoting the process that can make an internal choice between behaving as E_i for any $i \in I$, is replaced by an expression of the form $\sum_{i\in I}[p_i]E_i$, where $p_i \in (0,1]$ and $\sum_{i\in I} p_i = 1$, which denotes the process which can behave as the process E_i with probability p_i. Adapting Larsen and Skou's probabilistic transition systems and probabilistic bisimulation to the reactive, generative and stratified models, van Glabbeek et al. [GSST90] have given operational semantics for PCCS for each of the three models, where in each case probabilistic bisimulation is a congruence over all the usual operators of SCCS. For the generative model, Jou and Smolka [JS90] have given a complete axiomatisation of probabilistic bisimulation. Similarly, Larsen and Skou [LS92] have constructed a Calculus for Probabilistic Processes (CPP), also based on SCCS, which can be considered as a subset of PCCS, and given a sound and complete axiomatisation of probabilistic bisimulation for reactive processes.

In [JS90] a weaker form of probabilistic bisimulation is introduced, namely ε-bisimulation. Two processes are considered ε-bisimilar if their transitions differ by at most ε. Using this weaker form the authors have investigated a possible metric over generative probabilistic processes. However, the "metric" fails to satisfy the triangle inequality except in the restricted case where processes can perform at most one transition of any action type.

Alternative equivalences for generative PCCS [GJS90] have been introduced by Jou and Smolka [JS90] extending the classical CSP equivalences of traces [Hoa85], failures

[BHR84] and readies [BKO88] (see Section 3.4 for the definition of ready equivalence over non-probabilistic processes). They show that the equivalences based on failures and readies coincide, and all fail to be congruences over PCCS.

Tofts [Tof90] presents a version of SCCS extended with weights as opposed to probabilities. The operational model is based on a labelled transition system in which there exist two types of transitions: weighted and action. Hence, his model can be regarded as a stratified model. He furthermore extends probabilistic bisimulation to this setting and shows it to be a congruence over his calculus. Also, Hansson [Han94] considers an extension of CCS with respect to the alternating model of [HJ90], an extension of the reactive model so named because states alternate between having an internal probabilistic choice or an internal choice between actions. Probabilistic bisimulation is then extended to this setting. The resulting equivalence is shown to be a congruence and a complete axiomatisation of the equivalence is given. It should be noted that time is also present in his model.

Although not based on CCS, Baeten, Bergsta and Smolka [BBS92] have considered probabilistic bisimulation over an extended version of Bergstra and Klop's Algebra for Communicating Processes (ACP) [BK84] to allow generative probabilistic choice. Probabilistic bisimulation is shown to be a congruence over this calculus and also a sound and complete axiomatisation of this equivalence is given.

As for denotational models, Baier and Kwiatkowska [BK97] have used the model of [SL94] to give denotational semantics to the (full) calculus of CCS enriched with action-guarded probabilistic choice. Two semantic frameworks are provided: a domain-theoretic model which is shown to be fully abstract with respect to probabilistic simulation [SL94] and an ultra-metric semantic model which they show to be fully abstract with respect to probabilistic bisimulation. Both semantics are based on classical results for the non-probabilistic case, for example see [Abr87] and [AJ94] for the domain-theoretic and [BZ82] and [AR89] for the metric space construction and framework respectively.

2.3 Probabilistic Versions of CSP

Relating to CSP, Lowe [Low93] considers a probabilistic version of CSP, where internal choice is replaced by internal probabilistic choice and external choice by prioritised choice. The result is a rather complex semantic model in which all forms of choice are probabilistic in nature.

Lowe [Low] has since considered a model which includes internal probabilistic choice, external choice and internal choice. The model is constructed by first considering processes as Non-deterministic-Probabilistic-Action (NPA) graphs, where NPA graphs are graphs with three different nodes: non-deterministic, action and probabilistic, and hence the three sorts of transitions processes can perform can be modelled separately. Next Probabilistic-Action (PA) graphs are introduced and using these the non-deterministic behaviour is factored out by considering a NPA graph as a set of PA graphs, with each graph representing the result of the possible internal choices made. Using these sets of PA graphs different possible equivalences over processes were considered, based on, for example, traces, failures and readies. However, each equivalence arrived at turned out *not* to be a congruence over certain operators of CSP including relabelling, and, as such, the resulting denotational model would not be compositional (the main property sought in denotational models).

Similarly to [Low], Morgan et al. [MMSS96] also add probabilistic choice to CSP by adding an extra operator, and therefore the original external and internal choice remain part of their model. They give denotational semantics to this calculus by applying the probabilistic powerdomain construction of Jones and Plotkin [JP89, Jon90] (which is possible over any directed complete partial order) to an extended failures model for CSP. Intuitively, they consider probabilistic processes as probability distributions over the non-probabilistic processes of CSP, where for any probabilistic process E, the value corresponding to any process P of CSP is the probability that E is the process P. A problem that occurs in their model when considering certain operators is with processes which "appear twice". To give an example, consider the asynchronous parallel operator of CSP, then for actions $a \neq b$ according to the theory of CSP the "unravelling" law for $|||$ is:

$$(a \to P) \,|||\, (b \to Q) = \big(a \to P \,|||\, (b \to Q)\big) \,\Box\, \big(b \to (a \to P) \,|||\, Q\big)$$

and we see that the processes P and Q appear only once on the left-hand side of the equation and twice on the right. When we add probabilistic choice to the model, probabilities of the form p on the left-hand side may become p^2 on the right-hand side, and thus the equality (or law) is lost. We note that a similar problem is encountered in this thesis (see Section 5.7), although for different reasons. Solutions to this problem, in their model, have been investigated in [MMSS95].

Seidel [Sei92] has constructed two probabilistic models of CSP. The difference from the standard CSP is that an internal probabilistic choice operator replaces the internal choice operator. In the first model the (denotational) semantics for processes is in terms of probability measures on the space of infinite traces. For any process E and set of traces A, $[\![E]\!]A$ denotes the probability of E performing a trace from the set A.

To illustrate this construction, the prefix operator is defined as follows:

$$[\![a \to E]\!]A = [\![E]\!](\mathit{prefix}_a^{-1}(A))$$

where $\mathit{prefix}_a^{-1}(A)$ denotes the set of traces u such that $au \in A$. Furthermore, the probabilistic choice operator is defined as:

$$[\![E\ {}_p\sqcap_q F]\!]A = p \cdot [\![E]\!]A + q \cdot [\![F]\!]A.$$

However, Seidel is unable to define external (deterministic) choice in her model, since the probability of deterministic processes performing traces depends upon the environment. To overcome this, *conditional probability measures* are introduced, where if y is a trace, $(\![E]\!)(A, y)$ is the probability that E will perform a trace in the set A under the condition that the environment is willing to perform the trace y and nothing else. Using this model an external choice operator ${}_S\Box$, where S is a set of traces, is introduced. Intuitively, this operator will act as its left argument if offered a trace from S and as its right argument otherwise. This, therefore, leads to a fully *deterministic* model, since even if E and F can perform the same traces $E\,{}_S\Box\,F$ will act as E or F depending on whether the trace is in S. Also, hiding cannot be defined in this extended model.

2.4 Equivalences of Probabilistic Processes

In this section we discuss the properties of the equivalences mentioned above and other equivalences over probabilistic processes. We will restrict our attention to models containing internal probabilistic choice (for example, any model of reactive probabilistic processes), as this is the model considered in this thesis. First, we believe that probabilistic bisimulation of Larsen and Skou [LS91] is too fine for any model where the type of probabilistic choice is internal, in the sense that it will distinguish processes which are indistinguishable in a reasonable testing scenario. This arises from, as already mentioned above, probabilistic bisimulation being influenced by the time at which probabilistic choices occur, which we feel is unimportant, since, unlike other forms of choice, internal probabilistic choice is made neither by the process nor by the environment, but instead by some prescribed probability distribution. To illustrate this, consider the simple reactive probabilistic processes given in Figure 2.2 below.

Intuitively, the process E behaves as follows: it flips a coin and then performs the trace *abc* if the coin lands on heads, or the trace *abd* if the coin lands on tails. On

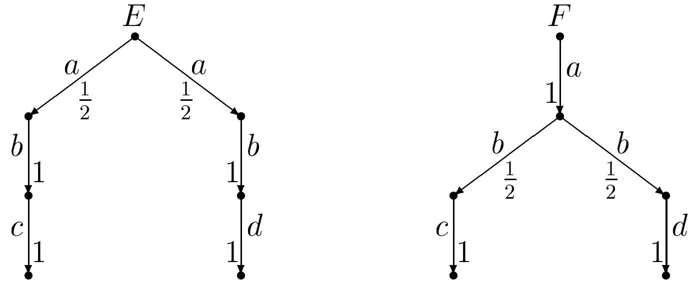


Figure 2.2: Probabilistic bisimulation is too fine.

the other hand, the process F first performs an a transition, and then flips a coin and performs the trace bc if the coin lands on heads, or the trace bd if the coin lands on tails. Then, since performing an a transition before or after flipping a coin has no effect on whether the coin lands on heads or tails, that is, the time at which the probabilistic choice is made is unimportant, the processes should be observationally equivalent: both perform the traces abc and abd with probability $\frac{1}{2}$. However, it is straightforward to show that probabilistic bisimulation will distinguish between these processes; this is due to the difference in their probabilistic branching behaviour, that is, when the probabilistic choice actually occurs.

A further example illustrating the unimportance of the time at which probabilistic choices occur is given by Morgan et al. [MMSS96], where "scratch cards" are considered. Each card comprises of a number of windows, one of which may be rubbed out by a customer to either reveal a prize or not. There are two possible ways to implement such cards. The first is by placing prizes with a certain distribution on every card, and thus the probabilistic choice is made by the customer when he or she chooses which window to rub out. Alternatively, two types of cards can be printed: one kind with no prizes at all and the other with prizes under all the windows, and therefore in this case the probabilistic choice is made before the customer buys the card, as it will depend on how the cards are arranged in the factory. Although the probabilistic choices are made at different times, to the customer – if he or she is only allowed to rub out one window – the two approaches would appear the same, and therefore the time at which the probabilistic choice is made has no effect, and hence can be considered unimportant.

Other equivalences that distinguish the processes given in Figure 2.2 and which we therefore view as too fine include: Segala and Lynch's probabilistic simulation [SL94] and Wang Yi and Larsen's testing equivalence [YL92], based on de Nicola and Hennessy [NH84] testing equivalences for non-deterministic processes and defined over Hansson and Jonsson's [HJ90] *alternating* model. In Yi and Larsen's model tests are represented by non-deterministic (and non-probabilistic) processes, and processes can pass tests with a set of probabilities corresponding to different internal choices made.

They use these sets to deal with two different testing scenarios: *must-testing*, where processes pass tests if the minimum probability of the process passing the test is 1, and *may-testing*, where a process passes a test if the maximum probability of the process passing the test is greater than 0.

Nevertheless, when considering models with external probabilistic choice (not considered in this thesis), the probabilistic branching structure may become important, since the probabilistic choices the processes make depend on the choices made by the environment.

Of equivalences that will identify the processes in Figure 2.2 there are several based on extending traces, failures and readies by incorporating the probabilities of processes performing traces and then refusing or accepting to then perform a certain set of actions. Seidel [Sei92] and Lowe [Low] define equivalences for models including an internal probabilistic choice operator based on traces and both failures and readies respectively. Also, Jou and Smolka [JS90] have introduced equivalences for generative process based on traces, failures and readies. We have considered these equivalences over our reactive setting. However, we feel the resulting equivalences are too coarse: although they do capture the probabilistic behaviour of processes (and hence do not distinguish between the processes of Figure 2.2), they are linear-time based equivalences, and therefore do not capture the branching behaviour associated with choices other than probabilistic, such as external choice which is contained in reactive systems. We illustrate this point by the example given in Figure 2.3 below. Observe that

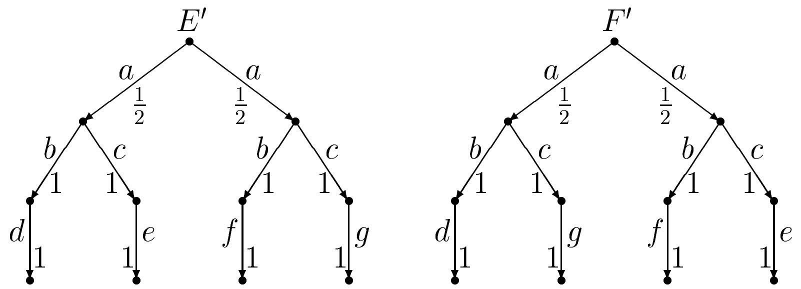


Figure 2.3: Trace, failure and ready equivalence are too coarse.

E' can reach an intermediate state (after performing the action a with probability $\frac{1}{2}$) where there is an *external choice* between performing a b transition followed by a d transition, and performing a c transition followed by an e transition. In contrast, F' cannot reach such a state.

On the other hand, if we now consider the traces of E' and F' endowed with the probabilities of the occurring traces, it is straightforward to show that these processes are equivalent, and hence the equivalence of Seidel [Sei92] cannot distinguish between them. Similarly, if we extend ready sets [BKO88] with probabilities, where (σ, Y, p) is a ready set of a probabilistic process if the process can perform the trace σ and is then able only to perform the actions in Y with probability p, we observe that the ready sets of E' and F' are equal to

$$\left\{(a, \{b, c\}, 1)\,,\ \left(ab, \{d\}, \frac{1}{2}\right),\ \left(ab, \{f\}, \frac{1}{2}\right),\ \left(ac, \{e\}, \frac{1}{2}\right),\ \left(ac, \{g\}, \frac{1}{2}\right),\right.$$
$$\left.\left(abd, \emptyset, \frac{1}{2}\right),\ \left(abf, \emptyset, \frac{1}{2}\right),\ \left(ace, \emptyset, \frac{1}{2}\right),\ \left(acg, \emptyset, \frac{1}{2}\right)\right\}$$

and hence these processes are also ready equivalent. Likewise, they will be equivalent with respect to Jou and Smolka's and Lowe's versions of failures equivalence.

A different approach is introduced by Morgan et al. [MMSS96] where, similarly to [Low], the model is based on the failures model of CSP, but instead of basing the equivalence on how processes "make decisions", that is, the behaviour of processes, the authors base their equivalence on what the process "is" by intuitively considering the probability that probabilistic processes are standard CSP processes. The equivalence of [MMSS96] will not distinguish between the processes given in Figure 2.2. However, we still feel that their equivalence is too fine in certain cases, which we illustrate by the following example in which τ is used to represent internal choice. First, observe that

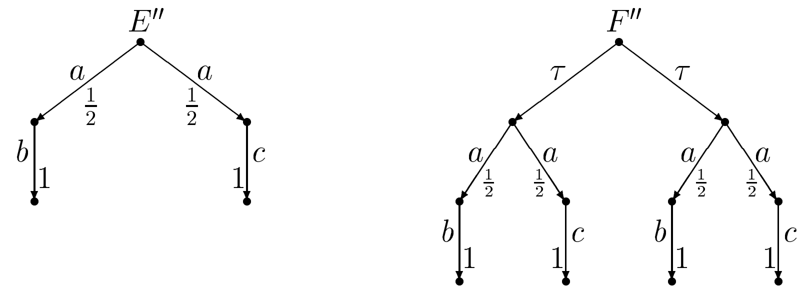


Figure 2.4: Morgan et al.'s equivalence is too fine.

E'' can either perform the trace ab or the trace ac, both with probability $\frac{1}{2}$. Moreover, no matter which internal choice F'' can make, the outcome will match the behaviour of E''. Therefore, these processes should be observationally equivalent. However, in the approach of Morgan et al. [MMSS96], the processes are distinguished: for example, the probability that E'' is the CSP process $a \to (b \to \mathbf{0})$ is $\frac{1}{2}$, whereas the probability that F'' is the process $a \to (b \to \mathbf{0})$ is $\frac{1}{4}$ since F'' only becomes the process $a \to (b \to \mathbf{0})$ when both instances of E'' in F'' choose to perform the trace ab.

If we return to any of the equivalences mentioned previously, it is straightforward to show that these processes will not be distinguished, even considering probabilistic bisimulation.

In addition, Christoff [Chr90], Cleaveland, Smolka and Zwarico [CSZ92] and Yen et al. [YCDS94] have adapted de Nicola and Hennessy's testing equivalences [NH84] to generative processes. However, as this work depends heavily on the generative nature of processes, and hence on external probabilistic choices, they cannot be compared with our setting in which probabilistic choices are internal.

As for results relating to probabilistic process calculi and equivalences on probabilistic processes, the conclusions we reach are as follows. If one works with a fine (or strong) equivalence over probabilistic processes, then almost all operators of CCS and CSP can be adapted to the probabilistic setting and the equivalence will be a congruence for the resulting calculus. For example, van Glabbeek et al. [GSST90] show that probabilistic bisimulation is a congruence over their calculus PCCS (which contains all the usual SCCS operators) and Baier and Kwiatkowska [BK97] show congruence properties of full CCS extended with action-guarded probabilistic choice. However, as discussed in the previous chapter, this equivalence will discriminate between processes that have equivalent operational behaviour under a realistic testing scenario.

One alternative is to work with a weaker (or coarser) equivalence, which can be considered more satisfactory as it will only distinguish processes that can be distinguished by external observations. In this case the difficulty is that only a subset of operators can be considered if we wish to ensure our equivalence is a congruence; the latter is an important property, since without it any resulting denotational model will not be compositional. Examples of these difficulties are mentioned above and include Jou and Smolka [JS90], where even restriction forces both trace and failure equivalence to fail to be congruences, and also in [Sei92] and [Low] where hiding cannot be defined.

2.5 Logics for Probabilistic Processes

Modal and temporal logics offer a framework for reasoning about the truth of properties of systems over time. This is achieved by the introduction of modal/temporal operators which typically express: *invariance* (properties will always hold), *eventuality* (properties will hold at some time in the future) and *precedence* (one property must hold before another one becomes true).

Temporal logics were first introduced to reason about concurrent systems by Pnueli [Pnu77]. Since then a variety of logics have been introduced. For example, Hennessy and Milner define a modal logic known as the Hennessy-Milner Logic (`HML`) [HM85] for expressing properties of labelled transition systems. `HML` extends classical propositional logic by the inclusion of the basic modal operator $\langle a \rangle \phi$ which holds true for a process if it can perform an a transition such that the formula ϕ then holds for the resulting process. Hennessy and Milner have then shown that two processes are bisimilar if and only if they satisfy the same `HML` formulae. Another example is Emerson, Clarke and Sistla's Computational Tree Logic (`CTL`) [CES83] which includes the temporal operators: $AX\phi$ (ϕ is true in all immediately succeeding states), $A[\phi U\psi]$ (always ϕ holds until ψ holds), $EX\phi$ there exists an immediate successor state such that ϕ holds) and $E[\phi U\psi]$ (there exists a path such that ϕ holds until ψ holds).

Modal and temporal logics have been extended to the setting of probabilistic concurrent systems. The work in this area falls into two categories. The first is a *qualitative* approach, where processes either satisfy a formula or they do not, that is, the formulae are assigned truth values. This is achieved by either keeping the standard syntax and requiring that formulae hold "with probability 1" (see [SPH84]), or extending the syntax by including explicit probabilities: the formulae are of the form ϕ_p for some $p \in [0,1]$, and are satisfied if the (non-probabilistic) formula ϕ holds with probability *at least* p (see [Chr93, HJ94, LS91, SL94]). The alternative approach is *quantitative*, where the logic is re-interpreted in the sense that instead of formulae either being true or false they are assigned (estimates of) probabilities as their meaning (see [HK97] and [MM]).

To illustrate the difference between the two approaches given above, we consider Larsen and Skou's [LS91] qualitative extension to `HML` and Huth and Kwiatkowska's [HK97] quantitative re-interpretation of the modal $\mu-$calculus [Koz83a]. Recall that a process satisfies the formula $\langle a\rangle\phi$ of `HML` (and of the modal $\mu-$calculus) if it can perform an a transition and the state reached satisfies the formula ϕ. Formally:

$$[\![\langle a\rangle\phi]\!]P = \begin{cases} \texttt{true} & \text{if } \exists\, Q \text{ such that } P \xrightarrow{a} Q \text{ and } [\![\phi]\!]Q = \texttt{true} \\ \texttt{false} & \text{otherwise.} \end{cases}$$

Then Larsen and Skou formulate Probabilistic Modal Logic (PML) by replacing the formula $\langle a\rangle\phi$ with $\langle a\rangle_\mu\phi$, where $\mu \in [0,1]$. Furthermore, a probabilistic process satisfies this formula if it can perform an a transition with probability greater than or equal to μ and reach a state satisfying the formula ϕ. Formally:

$$[\![\langle a\rangle_\mu\phi]\!]E = \begin{cases} \texttt{true} & \text{if } \exists\, S \text{ such that } E \xrightarrow{a}_{\mu'} S,\ \mu \leq \mu' \text{ and } [\![\phi]\!]F = \texttt{true}\ \forall F \in S \\ \texttt{false} & \text{otherwise.} \end{cases}$$

On the other hand, Huth and Kwiatkowska's re-interpretation assigns to $\langle a\rangle\phi$ the weighted sum over the values assigned to ϕ in the states reached by the process performing an a transition. Formally:

$$[\![\langle a\rangle\phi]\!]E = \sum_{E \xrightarrow{a}_\lambda F} \lambda \cdot [\![\phi]\!]F.$$

If we return to the processes given in Figure 2.2, then under Larsen and Skou's interpretation the formula

$$\phi = \langle a \rangle_1 \langle b \rangle_{0\cdot 5} \langle c \rangle_1 \mathtt{true}$$

yields $[\![\phi]\!]E = \mathtt{false}$ and $[\![\phi]\!]F = \mathtt{true}$. On the other hand, for the formula

$$\psi = \langle a \rangle \langle b \rangle \langle c \rangle \mathtt{true}$$

we have $[\![\psi]\!]E = [\![\psi]\!]F = \frac{1}{2}$ in Huth and Kwiatkowska's re-interpretation. In fact, Larsen and Skou show that the equivalence induced from PML is the same as probabilistic bisimulation, and Huth and Kwiatkowska show their induced equivalence is strictly weaker. On the other hand, the induced equivalence of Huth and Kwiatkowska is strictly finer than the equivalences for probabilistic processes based on trace, failure or ready equivalence, for example those of Jou and Smolka [JS90]. To illustrate this, their induced equivalence will distinguish between the processes of Figure 2.3 by means of the formula:

$$\langle a \rangle \Big(\langle b \rangle \langle d \rangle \mathtt{true} \wedge \langle c \rangle \langle e \rangle \mathtt{true} \Big)$$

whereas, as already stated, the equivalences based on trace, failure or ready equivalence will not.

Christoff [Chr93] defines an extension of `HML` similar to [LS91] where, instead of single probabilities, intervals of probabilities are considered. Other logics extended to a probabilistic setting include `CTL` [CES83] with qualitative extensions [BCHKR97, HJ94, Han94, Sei92] and propositional dynamic logic (`PDL`) [Har79] with quantitative extensions [FH82, Koz83a, FL79].

2.6 Other Related Research

Other research into probabilistic behaviour includes Kozen [Koz81] where semantics for a probabilistic `while`-language is given in terms of linear continuous operators on partially ordered Banach spaces. Also, Jones and Plotkin [Jon90, JP89] construct a general framework for giving domain-theoretic semantics for probabilistic programming languages in terms of the so called probabilistic powerdomain. They furthermore give semantics to a simple language containing probabilistic choice, sequential composition and while statements, but no form of external choice.

Chapter 3

Preliminary Material

This chapter will introduce the notation used and the material required to understand the rest of the thesis. It divides into four main sections: traces, probability theory, metric spaces and trace, failure and ready equivalences.

3.1 Traces

In this section we give a summary of the notation we use for traces and operations on traces; for more formal definitions see for example [Hoa85].

Definition 3.1.1 (Traces) *For any set A, A^* is the set of all finite traces (= sequences) made up of elements of A. Furthermore, we have the following notation for any $u, v \in A^*$, $a \in A$, $n \in \mathbb{N}$ and $B \subseteq A$:*

$\langle\rangle$	*the empty trace*
au	*the concatenation of a with the trace u*
A^n	*the set of traces with length at most n*
$u\restriction n$	*restriction of u to its first n symbols*
$u \leq v$	*u is a prefix of v*
$u\restriction B$	*the largest prefix of u such that all its elements are in the set B*
$u \cap v$	*the largest common prefix of u and v.*

3.2 Probability Theory

In this section we introduce the basic concepts and definitions of probability theory we shall need throughout this thesis. A more detailed introduction can be found in [GW86] or any good textbook on probability theory.

3.2.1 Random Experiments and Events

Games of chance such as tossing a coin or rolling a die are examples of "random experiments". If we pick a ball from a bag containing a number of different coloured balls and look for the colour of this ball, this is another random experiment.

More formally, a random experiment is an experiment which has the following properties:

- it is performed according to a set of rules that determine for each the outcome completely
- it can be repeated arbitrarily often
- the result of each experiment depends upon "chance", that is, the outcome or event is beyond our control, and thus the outcome cannot be uniquely determined.

Experience has shown that most random experiments exhibit *statistical regularity*, that is, the relative frequency of an outcome of an experiment in a long series of trials is the same if we perform several of such trials. For example, classical results confirm this for the experiment of flipping a coin, in that a head will be the outcome for half of the experiments in any long series of trials. The relative frequency of an event for any random experiment is called the *probability* of the event.

3.2.2 Conditional Probabilities and Independence

In certain cases, we may require to find the probability of an event B occurring under the condition that an event A occurs. Formally, this is the *conditional probability* that B will occur given A has occurred.

Conditional probabilities lead us to the definition of *independent* events: two events A and B are independent if the probability of B occurring under the condition that A has occurred is equal to the probability that B occurs. Furthermore, classical results have shown that when A and B are independent, the probability that both A and B occur is the multiplication of the probability of A occurring and the probability of B occurring, and thus the formal definition of independence turns out to be symmetric.

3.2.3 Probability Distributions

In this thesis we need only consider *discrete* probability distributions which we now define.

Definition 3.2.1 *Let D be a set. A (discrete)* probability distribution *on D is a function $f : D \to [0, 1]$ such that $\sum_{d \in D} f(d) = 1$. Furthermore, let $\mu(D)$ denote the set of discrete probability distributions on D.*

We note that as we are considering discrete probability distributions, for any set D and $f \in \mu(D)$, the set $\mathsf{s}(f) = \{d \in D \mid f(d) > 0\}$ called the *support* of f is countable.

Definition 3.2.2 *For any set D and $f \in \mu(D)$, f is called a* point distribution *if there exists $p \in D$ such that for any $q \in D$:*

$$f(q) = \begin{cases} 1 & \textit{if } p = q \\ 0 & \textit{otherwise} \end{cases}$$

and in this case we denote f by η_p (the point distribution at p).

3.3 Metric Spaces

In this section, we include some definitions and results relating to metric spaces required for the construction of our denotational semantics. For a more detailed introduction to metric spaces see [Sut77] or any good textbook on metric space theory.

Definition 3.3.1 (Metric Space) *Let M be a set. A map $d : M \times M \to \mathbb{R}$ is called a* metric *and (M, d) is called a* metric space *if the following conditions are satisfied for all $x, y, z \in M$:*

$$\begin{array}{ll} \text{(M1)} & d(x, y) \geq 0 \ \textit{ and } \ d(x, y) = 0 \Leftrightarrow x = y \\ \text{(M2)} & d(x, y) = d(y, x) \\ \text{(M3)} & d(x, y) + d(y, z) \geq d(x, z). \end{array}$$

Furthermore, if (M1) *is weakened to:*

$$\text{(M1}') \quad d(x, y) \geq 0 \ \textit{ and } \ d(x, x) = 0$$

then d is called a pseudo-metric *and (M, d) a* pseudo-metric space*. On the other hand, if* (M3) *is strengthened to:*

$$\text{(M3}') \quad d(x, z) \leq \max\{d(x, y),\ d(y, z)\}$$

then d is called an ultra-metric *and (M, d) an* ultra-metric space.

Definition 3.3.2 *Let (M_1, d_1) and (M_2, d_2) be metric spaces. We say that (M_1, d_1) and (M_2, d_2) are* isometric *if there exists a bijection $\phi : M_1 \to M_2$ such that for all $x, y \in M_1$:*

$$d_2(\phi(x), \phi(y)) = d_1(x, y).$$

We then write $M_1 \cong M_2$. When f is not a bijection, but only an injection, we call f an isometric embedding.

Definition 3.3.3 *A sequence $\langle x_n \rangle_{n \in \mathbb{N}}$ in a metric space (M, d)* converges to x, *denoted $\lim_{n\to\infty} x_n = x$, if for any $\varepsilon > 0$, there exists $N \in \mathbb{N}$ such that $d(x_n, x) < \varepsilon$ for all $n \geq N$. Furthermore, a sequence is called* convergent *if the sequence converges to some point.*

Definition 3.3.4 (Cauchy Sequence) *A sequence $\langle x_n \rangle_{n \in \mathbb{N}}$ in a metric space (M, d) is a* Cauchy sequence *if, for any $\varepsilon > 0$, there exists $N \in \mathbb{N}$ such that $d(x_n, x_m) < \varepsilon$ for all $m, n \geq N$.*

Lemma 3.3.5 *Every convergent sequence in a metric space is Cauchy.*

Definition 3.3.6 *A metric space (M, d) is called* complete *if every Cauchy sequence in M converges to some element of M.*

Theorem 3.3.7 (Metric Completion) *Let (M, d) be an arbitrary (pseudo-)metric space. Then there exists a metric space $(\hat{M}, \hat{d})$, called the* completion *of (M, d), together with an isometric embedding $\imath : M \to \hat{M}$ such that:*

(i) $(\hat{M}, \hat{d})$ is complete

(ii) for every complete metric space (M', d') and isometric embedding $\jmath : M \to M'$, there exists a unique isometric embedding $\hat{\jmath} : \hat{M} \to M'$ such that $\hat{\jmath} \circ \imath = \jmath$.

Proof. The space $(\hat{M}, \hat{d})$ is constructed as the set of equivalence classes under the equivalence relation $\sim$ on the set of Cauchy sequences in M is defined by:

$$\langle x_n \rangle_{n \in \mathbb{N}} \sim \langle y_n \rangle_{n \in \mathbb{N}} \quad \text{if and only if} \quad \lim_{n\to\infty} d(x_n, y_n) = 0$$

endowed with the metric:

$$\hat{d}([\langle x_n \rangle_{n \in \mathbb{N}}]_\sim, [\langle y_n \rangle_{n \in \mathbb{N}}]_\sim) = \lim_{n\to\infty} d(x_n, y_n).$$

Furthermore, the isometric embedding $\imath$ maps every $x \in M$ to the equivalence class of the Cauchy sequence of which all elements are equal to x:

$$\imath(x) = [(x)_{n \in \mathbb{N}}]_\sim.$$

It is easy to show that $(\hat{M}, \hat{d})$ and $\imath$ satisfy the above properties. $\square$

Definition 3.3.8 (Closed Set) *Let (M, d) be a metric space. A subset $X \subseteq M$ is called* closed *if every convergent sequence in X converges to a point in X.*

Definition 3.3.9 (Hausdorff Distance) *Let (M, d) be a metric space and let X, Y be subsets of M. We define the* Hausdorff distance *between X and Y as follows:*

$$\begin{array}{ll} (a) & d(x,Y) = inf_{y \in Y} d(x,y) \\ (b) & d(X,Y) = \max\left\{sup_{x \in X} d(x,Y),\, sup_{y \in Y} d(y,X)\right\} \end{array}$$

where $inf\,\emptyset = 1$ and $\sup \emptyset = 0$.

Lemma 3.3.10 *Let (M, d) be a metric space, and let $\mathcal{P}_c(M)$ be the collection of all non-empty closed subsets of M. Then, if d is the Hausdorff distance $(\mathcal{P}_c(M), d)$ is a metric space.*

Definition 3.3.11 (Intervals) *Let $\mathcal{I} = \{[a,b] \mid 0 \leq a \leq b \leq 1\}$. We now define addition, multiplication, union and scalar multiplication on $\mathcal{I}$ as follows. For all $[a,b], [c,d] \in \mathcal{I}$ and $e \in [0,1]$:*

$$\begin{array}{rcl} [a,b] + [c,d] & = & [a+c, b+d] \\ [a,b] \cdot [c,d] & = & [a \cdot c, b \cdot d] \\ [a,b] \sqcup [c,d] & = & [\min\{a,c\}, \max\{b,d\}] \\ e \cdot [a,b] & = & [e \cdot a, e \cdot b]. \end{array}$$

Furthermore, we introduce the orderings $\leq_{left}$ and $\leq_{right}$ and induced equivalences $=_{left}$ and $=_{right}$ over $\mathcal{I}$ as follows. For all $[a,b], [c,d] \in \mathcal{I}$:

$$[a,b] \leq_{left} [c,d] \;\; if \;\; a \leq c \quad and \quad [a,b] \leq_{right} [c,d] \;\; if \;\; b \leq d.$$

Proposition 3.3.12 *For all finite $I_1, I_2 \subseteq \mathcal{I}$: $\sqcup_{[a,b] \in I_1}[a,b] = \sqcup_{[c,d] \in I_2}[c,d]$ if and only if*

$$\min_{[a,b] \in I_1} [a,b] =_{left} \min_{[c,d] \in I_2} [c,d] \quad and \quad \max_{[a,b] \in I_1} [a,b] =_{right} \max_{[c,d] \in I_2} [c,d]$$

where the minimum and maximum are taken with respect to the orderings $\leq_{left}$ and $\leq_{right}$ respectively.

Proof. The proof follows by Definition 3.3.11. □

Definition 3.3.13 *Let $d_{\mathcal{I}} : \mathcal{I} \times \mathcal{I} \to [0,1]$ be the map defined as follows. For all $[a_1, b_1], [a_2, b_2] \in \mathcal{I}$ put:*

$$d_{\mathcal{I}}([a_1,b_1],[a_2,b_2]) = \max\{|a_1 - a_2|, |b_1 - b_2|\}.$$

Proposition 3.3.14 *The mapping $d_{\mathcal{I}}$ is a metric on $\mathcal{I}$.*

Proof. (M1) If $[a,b],[c,d] \in \mathcal{I}$, then by definition of $d_{\mathcal{I}}$:

$$\begin{array}{rcll} d_{\mathcal{I}}([a,b],[c,d]) = 0 & \Leftrightarrow & \max\{|a-c|,|b-d|\} = 0 & \\ & \Leftrightarrow & |a-c| = 0 \text{ and } |b-d| = 0 & \text{rearranging} \\ & \Leftrightarrow & a = c \text{ and } b = d & \text{by definition} \\ & \Leftrightarrow & [a,b] = [a,c]. & \end{array}$$

(M2) If $[a,b],[c,d] \in \mathcal{I}$, then by definition of $d_{\mathcal{I}}$:

$$\begin{array}{rcll} d_{\mathcal{I}}([a,b],[c,d]) & = & \max\{|a-c|,|b-d|\} & \\ & = & \max\{|c-a|,|d-b|\} & \text{by properties of the Euclidean metric} \\ & = & d_{\mathcal{I}}([c,d],[a,b]) & \text{by definition of } d_{\mathcal{I}}. \end{array}$$

(M3) If $[a,b],[c,d],[e,f] \in \mathcal{I}$, then by definition of $d_{\mathcal{I}}$:

$$\begin{array}{cll} \multicolumn{3}{l}{d_{\mathcal{I}}([a,b],[c,d]) + d_{\mathcal{I}}([c,d],[e,f])} \\ = & \max\{|a-c|,|b-d|\} + \max\{|c-e|,|d-f|\} & \\ \geq & \max\{|a-c|+|c-e|,|b-d|+|d-f|\} & \\ \geq & \max\{|a-e|,|b-f|\} & \text{by properties of the Euclidean metric} \\ = & d_{\mathcal{I}}([a,b],[e,f]) & \text{by definition of } d_{\mathcal{I}}. \end{array}$$

□

Lemma 3.3.15 *For all $[a,b],[c,d] \in \mathcal{I}$, $0 \leq d_{\mathcal{I}}([a,b],[c,d]) \leq 1$.*

Proof. The proof follows by definition of $d_{\mathcal{I}}$. □

Proposition 3.3.16 *For all $[a_1,b_1]$, $[a_2,b_2]$ and $[c,d]$ $\in \mathcal{I}$:*

$$\begin{array}{rl} (i) & d_{\mathcal{I}}([a_1,b_1]\cdot[c,d],[a_2,b_2]\cdot[c,d]) \leq d_{\mathcal{I}}([a_1,b_1],[a_2,b_2]) \\ (ii) & d_{\mathcal{I}}([a_1,b_1]\sqcup[c,d],[a_2,b_2]\sqcup[c,d]) \leq d_{\mathcal{I}}([a_1,b_1],[a_2,b_2]). \end{array}$$

Proof. If $[a_1,b_1]$, $[a_2,b_2]$ and $[c,d]$ $\in \mathcal{I}$, then by Definition 3.3.11:

$$\begin{array}{cll} \multicolumn{3}{l}{d_{\mathcal{I}}([a_1,b_1]\cdot[c,d],[a_2,b_2]\cdot[c,d])} \\ = & d_{\mathcal{I}}([a_1\cdot c, b_1\cdot d],[a_2\cdot c, b_2\cdot d]) & \\ = & \max\{|a_1\cdot c - a_2\cdot c|,|b_1\cdot d - b_2\cdot d|\} & \text{by definition of } d_{\mathcal{I}} \\ = & \max\{|a_1-a_2|\cdot c,|b_1-b_2|\cdot d\} & \text{rearranging} \\ \leq & \max\{|a_1-a_2|,|b_1-b_2|\} & \text{since } c,d \in [0,1] \\ = & d_{\mathcal{I}}([a_1,b_1],[a_2,b_2]) & \text{by definition} \end{array}$$

and thus the first part of the proposition holds. For the second part, by Definition 3.3.11 and the definition of $d_{\mathcal{I}}$ we have:

$$\begin{aligned}
&d_{\mathcal{I}}([a_1,b_1]\sqcup[c,d],[a_2,b_2]\sqcup[c,d])\\
&\quad= d_{\mathcal{I}}([\min\{a_1,c\},\max\{b_1,d\}],[\min\{a_2,c\},\max\{b_2,d\}])\\
&\quad= \max\{|\min\{a_1,c\}-\min\{a_2,c\}|,|\max\{b_1,d\}-\max\{b_2,d\}|\}. \qquad (3.1)
\end{aligned}$$

Then, considering the values of a_1, a_2 and c, we have the following four cases:

1. If $a_1, a_2 \leq c$, then $|\min\{a_1,c\}-\min\{a_2,c\}| = |a_1-a_2|$.
2. If $c \leq a_1, a_2$, then $|\min\{a_1,c\}-\min\{a_2,c\}| = |c-c| = 0 \leq |a_1-a_2|$.
3. If $a_1 \leq c \leq a_2$, then

$$\begin{aligned}
|\min\{a_1,c\}-\min\{a_2,c\}| &= |a_1-c|\\
&= c-a_1 && \text{since } a_1\leq c\\
&\leq a_2-a_1 && \text{since } c\leq a_2\\
&= |a_1-a_2| && \text{since } a_1\leq a_2.
\end{aligned}$$

4. If $a_2 \leq c \leq a_1$, then by symmetry on item 3 we have

$$|\min\{a_1,c\}-\min\{a_2,c\}| \leq |a_1-a_2|.$$

Since these are all the possible cases:

$$|\min\{a_1,c\}-\min\{a_2,c\}| \leq |a_1-a_2|.$$

Furthermore, using the dual of the above, we have:

$$|\max\{b_1,d\}-\max\{b_2,d\}| \leq |b_1-b_2|$$

and substituting these facts into (3.1) we have:

$$\begin{aligned}
d_{\mathcal{I}}([a_1,b_1]\sqcup[c,d],[a_2,b_2]\sqcup[c,d]) &\leq \max\{|a_1-a_2|,|b_1-b_2|\}\\
&= d_{\mathcal{I}}([a_1,b_1],[a_2,b_2]) && \text{by definition of } d_{\mathcal{I}}
\end{aligned}$$

as required. □

Proposition 3.3.17 *If $n \geq 1$ and $\{[a_i,b_i] \mid i \in \{1,\ldots,n\}\}$ and $\{[c_i,d_i] \mid i \in \{1,\ldots,n\}\}$ are subsets of $\mathcal{I}$, then there exists $j \in \{1,\ldots,n\}$ such that:*

$$d_{\mathcal{I}}(\sqcup_{i=1}^n[a_i,b_i],\sqcup_{i=1}^n[c_i,d_i]) \leq d_{\mathcal{I}}([a_j,b_j],[c_j,d_j]).$$

Proof. If $n \geq 1$ and $\{[a_i, b_i] \mid i \in \{1, \ldots, n\}\}$ and $\{[c_i, d_i] \mid i \in \{1, \ldots, n\}\}$ are subsets of $\mathcal{I}$, then by Definition 3.3.11:

$$\sqcup_{i=1}^{n}[a_i, b_i] = \left[\min_{i\in\{1,\ldots,n\}} a_i, \max_{i\in\{1,\ldots,n\}} b_i\right] \quad \text{and} \quad \sqcup_{i=1}^{n}[c_i, d_i] = \left[\min_{i\in\{1,\ldots,n\}} c_i, \max_{i\in\{1,\ldots,n\}} d_i\right]$$

and hence:

$$\begin{aligned} & d_{\mathcal{I}}(\sqcup_{i=1}^{n}[a_i, b_i], \sqcup_{i=1}^{n}[c_i, d_i]) \\ & \quad = \max\left\{\left|\min_{i\in\{1,\ldots,n\}} a_i - \min_{i\in\{1,\ldots,n\}} c_i\right|, \left|\max_{i\in\{1,\ldots,n\}} b_i - \max_{i\in\{1,\ldots,n\}} d_i\right|\right\} \end{aligned} \tag{3.2}$$

by definition of $d_{\mathcal{I}}$. Next, we show there exists $k \in \{1, \ldots, n\}$ such that:

$$\left|\min_{i\in\{1,\ldots,n\}} a_i - \min_{i\in\{1,\ldots,n\}} c_i\right| \leq d_{\mathcal{I}}([a_k, b_k], [c_k, d_k]). \tag{3.3}$$

If $\min_{i\in\{1,\ldots,n\}} a_i \leq \min_{i\in\{1,\ldots,n\}} c_i$, then setting k such that $a_k = \min_{i\in\{1,\ldots,n\}} a_i$:

$$\begin{array}{rcll} \left|\min_{i\in\{1,\ldots,n\}} a_i - \min_{i\in\{1,\ldots,n\}} c_i\right| & = & \min_{i\in\{1,\ldots,n\}} c_i - \min_{i\in\{1,\ldots,n\}} a_i & \\ & = & \min_{i\in\{1,\ldots,n\}} c_i - a_k & \text{by definition of } k \\ & \leq & c_k - a_k & \text{since } \min_{i\in\{1,\ldots,n\}} c_i \leq c_k \\ & = & |a_k - c_k| & \text{since } a_k \leq c_k \\ & \leq & \max\{|a_k - c_k|, |b_k - d_k|\} & \text{rearranging} \\ & = & d_{\mathcal{I}}([a_k, b_k], [c_k, d_k]) & \text{by definition of } d_{\mathcal{I}}. \end{array}$$

On the other hand, if $\min_{i\in\{1,\ldots,n\}} a_i \geq \min_{i\in\{1,\ldots,n\}} c_i$, then setting k such that $c_k = \min_{i\in\{1,\ldots,n\}} c_i$ the result follows by symmetry on the case above. Dually, we show there exists $m \in \{1, \ldots, n\}$ such that:

$$\left|\max_{i\in\{1,\ldots,n\}} b_i - \max_{i\in\{1,\ldots,n\}} d_i\right| \leq d_{\mathcal{I}}([a_m, b_m], [c_m, d_m]) \tag{3.4}$$

by setting m such that $b_m = \max_{i\in\{1,\ldots,n\}} b_i$ if $\max_{i\in\{1,\ldots,n\}} b_i \geq \max_{i\in\{1,\ldots,n\}} d_i$ and m such that $d_m = \max_{i\in\{1,\ldots,n\}} d_i$ otherwise. Now substituting (3.3) and (3.4) into (3.2) we have:

$$\begin{array}{rcl} d_{\mathcal{I}}(\sqcup_{i=1}^{n}[a_i, b_i], \sqcup_{i=1}^{n}[c_i, d_i]) & \leq & \max\{d_{\mathcal{I}}([a_k, b_k], [c_k, d_k]), d_{\mathcal{I}}([a_m, b_m], [c_m, d_m])\} \\ & = & d_{\mathcal{I}}([a_j, b_j], [c_j, d_j]) \quad \text{for some } j \in \{1, \ldots, n\} \end{array}$$

as required. □

3.4 Trace, Failure and Ready Equivalences

Recall the definition of a labelled transition system $(T, \mathcal{A}ct, \longrightarrow)$ given in Chapter 2. In order to define trace, failure and ready equivalences over such a system, we first need to introduce the following two auxiliary definitions of initial actions of processes and the generalised action relations.

Definition 3.4.1 *The set of* initial actions *of any* $P \in T$ *is defined by:*

$$\mathrm{i}nitials(P) = \{a \in \mathcal{A}ct \mid \exists\, Q \textit{ such that } P \overset{a}{\longrightarrow} Q\}.$$

Definition 3.4.2 *The* generalized action relations $\overset{\sigma}{\longrightarrow}$ *for* $\sigma \in \mathcal{A}ct^*$ *are defined inductively by:*

1. $P \overset{\langle\rangle}{\longrightarrow} P$ *for all* $P \in T$
2. $P \overset{a}{\longrightarrow} Q$ *with* $a \in \mathcal{A}ct$ *implies* $P \overset{a}{\longrightarrow} Q$ *with* $a \in \mathcal{A}ct^*$
3. $P \overset{\sigma}{\longrightarrow} Q \overset{\rho}{\longrightarrow} R$ *implies* $P \overset{\sigma\rho}{\longrightarrow} R$.

We are now in a position to introduce the following equivalences over the set of processes T of any labelled transition system $(T, \mathcal{A}ct, \longrightarrow)$.

Definition 3.4.3 *For any* $P \in T$*, the set of traces* $\mathrm{t}races(P)$ *of* P *is given by:*

$$\mathrm{t}races(P) = \{\sigma \mid \exists\, Q \textit{ such that } P \overset{\sigma}{\longrightarrow} Q\}.$$

Definition 3.4.4 (Trace Equivalence) *Let* $P, Q \in T$*, then* P *and* Q *are* trace equivalent *if* $\mathrm{t}races(P) = \mathrm{t}races(Q)$.

Definition 3.4.5 *Let* $(\sigma, X) \in \mathcal{A}ct^* \times \mathcal{P}(\mathcal{A}ct)$ *and* $P \in T$*, then* (σ, X) *is a* failure *of the process* P *if there exists* $Q \in T$ *such that* $P \overset{\sigma}{\longrightarrow} Q$ *and* $\mathrm{i}nitials(Q) \cap X = \emptyset$. *Furthermore, let* $\mathrm{f}ailures(P)$ *denote the set of failures of* P.

Definition 3.4.6 (Failure Equivalence) *Let* $P, Q \in T$*, then* P *and* Q *are* failure equivalent *if* $\mathrm{f}ailures(P) = \mathrm{f}ailures(Q)$.

Definition 3.4.7 *Let* $(\sigma, X) \in \mathcal{A}ct^* \times \mathcal{P}(\mathcal{A}ct)$ *and* $P \in T$*, then* (σ, X) *is a* ready set *of the process* P *if there exists* $Q \in T$ *such that* $P \overset{\sigma}{\longrightarrow} Q$ *and* $\mathrm{i}nitials(Q) = X$. *Furthermore, let* $\mathrm{r}eadies(P)$ *denote the set of readies of* P.

Definition 3.4.8 (Ready Equivalence) *Let* $P, Q \in T$*, then* P *and* Q *are* ready equivalent *if* $\mathrm{r}eadies(P) = \mathrm{r}eadies(Q)$.

Chapter 4

Reactive Probabilistic Transition Systems

In this chapter we introduce a model for reactive probabilistic systems based on labelled transition systems and define appropriate operational equivalence notions.

4.1 Introduction

We begin by recalling the definition of Larsen and Skou's probabilistic transition systems introduced in [LS91]. A *probabilistic transition system* is a tuple:

$$S = (P, Act, Can, \mu)$$

where P is a set of processes (states), Act is a set of observable actions, Can is an Act-indexed family of sets of processes where Can_a is the set of processes capable of performing the action a as their initial move, and μ is a family of probabilistic distributions, $\mu_{p,a} : P \to [0,1]$, for $a \in Act$, with $p \in Can_a$ indicating the possible next states and their probabilities after p has performed a, that is, $\mu_{p,a}(q) = \lambda$ means that the probability that p becomes q after performing a is λ.

If we consider any $p \in P$ and $a \in Act$ such that $p \in Can_a$ then, since $\mu_{p,a}$ is a probability distribution, the total probability of p performing the action a is 1, and hence in the terminology of van Glabbeek et al. [GSST90], p is a *reactive* process. Furthermore, since for any $a \in Act$ there is at most one probability distribution associated with p performing a, the choice between which action p performs is *external*.

Therefore, since we wish to model reactive processes with probabilistic, external and *internal* choices we will need to extend the above model to allow for internal choice. Formally, we generalise Larsen and Skou's transition systems as follows. First, we introduce the following definitions.

Definition 4.1.1 (Reactiveness Condition) *Let A and S be sets. Then if $X \subseteq A \times S$, X is said to satisfy the* reactiveness condition *if, for any $(a_1, s_1), (a_2, s_2) \in X$, either $a_1 \neq a_2$ or $(a_1, s_1) = (a_2, s_2)$. In other words, the set X is a partial function from A to S.*

Definition 4.1.2 (Powerset Operators) *Let $\mathcal{P}_f(\cdot)$ and $\mathcal{P}_{fn}(\cdot)$ denote the powerset operators restricted to only finite and finite non-empty subsets respectively. Furthermore, let $\mathcal{P}_{fr}(\cdot \times \cdot)$ and $\mathcal{P}_{fnr}(\cdot \times \cdot)$ denote the powerset operators restricted to only finite and finite non-empty subsets of cartesian products satisfying the reactiveness condition respectively.*

We are now ready to introduce our generalised model. The main difference from ordinary transition systems is that the transition relation is between states and certain *sets*, with each such set representing a probabilistic processes *deterministic* on the first step of its behaviour (that is, a set consisting of action-probability distribution pairs).

Definition 4.1.3 *A* Reactive Probabilistic Transition System *is a tuple $(\mathcal{R}, \mathcal{A}ct, \rightarrow)$, where $\mathcal{R}$ is a set of states, $\mathcal{A}ct$ is a finite set of actions and $\rightarrow$ a transition relation*

$$\rightarrow \;\subseteq\; \mathcal{R} \times \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathcal{R}))$$

satisfying: for all $E \in \mathcal{R}$ there exists $S \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathcal{R}))$ such that $(E, S) \in \rightarrow$. We write $E \rightarrow S$ instead of $(E, S) \in \rightarrow$. Furthermore, $(\mathcal{R}, \mathcal{A}ct, \rightarrow)$ is called:

purely probabilistic *if for each $E \in \mathcal{R}$ there is a unique transition $E \rightarrow S$ and either $S = \emptyset$ or $S = \{(a, \pi)\}$ for some $a \in \mathcal{A}ct$ and $\pi \in \mu(\mathcal{R})$.*

deterministic *if for each $E \in \mathcal{R}$ there is a unique transition $E \rightarrow S$.*

non-deterministic *if for each $E \in \mathcal{R}$ and $S \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathcal{R}))$ such that $E \rightarrow S$, either $S = \emptyset$ or $S = \{(a, \pi)\}$ for some $a \in \mathcal{A}ct$ and $\pi \in \mu(\mathcal{R})$.*

Unless it is clear from the context, if $\mathcal{R}$ is the set of processes or states of a purely probabilistic transition system, deterministic probabilistic transition system or non-deterministic probabilistic transition system, we shall refer to $\mathcal{R}$ as $\mathcal{R}^{\mathrm{p}}$, $\mathcal{R}^{\mathrm{d}}$ and $\mathcal{R}^{\mathrm{nd}}$ respectively.

Intuitively, any $S \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathcal{R}))$ should be thought of as a reactive probabilistic process which is *deterministic* on the first step of its behaviour: either $S =$

$\{(a_1, \pi_1), \ldots, (a_m, \pi_m)\}$, the process which makes an external choice between the actions $\{a_1, \ldots, a_m\}$ and for any $1 \leq i \leq m$ and $F \in \mathcal{R}$ the probability of S performing the action a_i and then behaving as F is given by $\pi_i(F)$, or $S = \emptyset$, the inactive process. We can relate this to Larsen and Skou's probabilistic transition systems by considering any process $p \in P$ as such a set S_p where:

$$S_p = \{(a, \mu_{a,p}) \mid a \in Act \text{ and } p \in Can_a\}.$$

Non-determinism is introduced by allowing a choice between "deterministic" processes: for any $E \in \mathcal{R}$ and distinct $S_1, S_2 \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathcal{R}))$, if $E \to S_1$ and $E \to S_2$, then E makes an *internal* choice between continuing as the process S_1 or S_2. The class of all reactive systems allows (reactive) probabilistic, external and internal choice.

We now illustrate how the states of such reactive probabilistic transition systems can be represented graphically by means of the following examples, recall that η_E is the point distribution at E (see Definition 3.2.2). Consider the states $\hat{E}, \hat{F}, \hat{G}, \hat{H}$ of a reactive probabilistic transition system $(\mathcal{R}, \mathcal{A}ct, \to)$ with the following possible transitions:

$$\begin{array}{lll}
\hat{E} \to S & \text{if and only if} & S = \{(a, \frac{1}{4} \cdot \eta_{\hat{G}} + \frac{3}{4} \cdot \eta_{\hat{H}})\} \\
\hat{F} \to S & \text{if and only if} & S = \{(b, \eta_{\hat{H}}), (c, \eta_{\hat{H}})\} \text{ or } S = \{(b, \eta_{\hat{H}}), (d, \eta_{\hat{H}})\} \\
\hat{G} \to S & \text{if and only if} & S = \{(b, \eta_{\hat{H}})\} \text{ or } S = \{(c, \eta_{\hat{H}})\} \\
\hat{H} \to S & \text{if and only if} & S = \emptyset.
\end{array}$$

Then $\hat{E}$ and $\hat{F}$ can be represented by the graphs given in Figure 4.1 below (note that τ is used to represent internal choices).

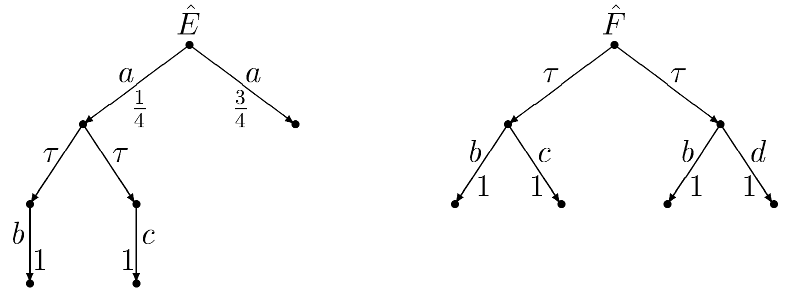


Figure 4.1: Example of the states of a reactive probabilistic transition system.

4.2 Purely Probabilistic Transition Systems

Our goal is to define an operational ordering on reactive probabilistic transition systems based on testing, such that two processes will only be distinguished by the ordering if they have observably different behaviour. In this section we only consider an operational ordering over purely probabilistic transition systems. In the next sections the ordering is respectively extended to deterministic and non-deterministic probabilistic transition systems. Finally, the latter two orderings are combined to yield an order on all reactive probabilistic transition systems.

To begin with, we introduce the set of tests referred to as $\mathtt{T}^{\mathrm{p}}$ for purely probabilistic systems. Following Milner [Mil89], we motivate the tests by means of *button pushing experiments* on transition systems: we suppose we have a series of buttons, one for every action ($a \in \mathcal{A}ct$), which act as an interface between an experimenter and processes of the transition system as follows. For any process E of the system, if no buttons are pressed the process E will remain in rest. However, if an *experiment* is performed, that is, the a-button is pressed for some action a, the process E can react in one of two ways:

- by performing an a action, in which case the button will go down and the experiment *succeeds*. We are then in a position to perform an experiment on the process reached by E performing the a action (by pressing another button).
- by not performing an a action, in which case the button will not go down and the experiment *fails*.

If we consider these experiments over processes of a reactive probabilistic transition system, they are in fact *random experiments*, since for any process the success of the experiment will depend on the probabilistic choices the process performs. We can, therefore, consider the relative frequency of experiments succeeding, that is, the *probability* of the experiment succeeding. Before we investigate the probabilities associated with experiments on processes we formally define the set of tests as follows.

Definition 4.2.1 *Let $\mathtt{T}^{\mathrm{p}}$, be the testing language defined inductively as follows:*

$$t ::= \perp \mid a.t$$

where $a \in \mathcal{A}ct$.

In terms of button pushing experiments, $\perp$ is the experiment where no buttons are pressed and $a.t$ is the experiment where we first press the a-button and, if the experiment succeeds, the experiment t is then performed. One can think of elements of $\mathtt{T}^{\mathrm{p}}$ as tests for the occurrence of paths: $\perp$ is the empty test, that is, any path can pass the test $\perp$, and $a.t$ tests for the occurrence of paths which begin with the action a and then pass the test t. We note that any $t \in \mathtt{T}^{\mathrm{p}}$ is of the form $a_1 \dots a_n.\perp$ for some $n \in \mathbb{N}$ with $a_i \in \mathcal{A}ct$ for all $1 \leq i \leq n$, and so intuitively t is a test for paths beginning with the sequence of actions $a_1 \dots a_n$.

If we now consider a purely probabilistic transition system $(\mathcal{R}^{\mathrm{p}}, \mathcal{A}ct, \rightarrow)$ and $E \in \mathcal{R}^{\mathrm{p}}$, by definition there exists a unique $S \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathcal{R}^{\mathrm{p}}))$ such that $E \rightarrow S$ and either $S = \emptyset$ or $S = \{(a, \pi)\}$ for some $a \in \mathcal{A}ct$ and $\pi \in \mu(\mathcal{R}^{\mathrm{p}})$. Therefore, we use E as an abbreviation for the unique element of $(\mathcal{A}ct \times \mu(\mathcal{R}^{\mathrm{p}})) \cup \{\emptyset\}$ into which it can evolve. We can now define a map P from $\mathcal{R}^{\mathrm{p}}$ and $\mathtt{T}^{\mathrm{p}}$ to the unit interval which, for any process $E \in \mathcal{R}^{\mathrm{p}}$ and test $t \in \mathtt{T}^{\mathrm{p}}$, yields *the probability* $\mathsf{P}(E)(t)$ *of* E *passing the test* t, that is, the probability of E performing the paths that t tests for.

Definition 4.2.2 *Let* $\mathsf{P} : \mathcal{R}^{\mathrm{p}} \rightarrow (\mathtt{T}^{\mathrm{p}} \rightarrow [0,1])$ *be the map defined inductively on* $t \in \mathtt{T}^{\mathrm{p}}$ *as follows. For any* $E \in \mathcal{R}^{\mathrm{p}}$ *put:* $\mathsf{P}(E)(\perp) = 1$ *and*

$$\mathsf{P}(E)(a.t) = \begin{cases} \sum_{F \in \mathcal{R}^{\mathrm{p}}} \pi(F) \cdot \mathsf{P}(F)(t) & \text{if } E \rightarrow \{(a,\pi)\} \text{ for some } \pi \in \mu(\mathcal{R}^{\mathrm{p}}) \\ 0 & \text{otherwise.} \end{cases}$$

The intuition behind the map P is as follows. Firstly, $\mathsf{P}(E)(\perp)$ calculates the probability of E passing the test $\perp$, and since any process can pass $\perp$ we set this value to 1. Secondly, $\mathsf{P}(E)(a.t)$ calculates the probability of E performing paths which have the initial action a and then pass the test t. If E cannot perform the action a, that is $E \not\rightarrow \{(a, \pi)\}$ for any $\pi \in \mu(\mathcal{R}^{\mathrm{p}})$, then clearly E cannot perform any paths which have the initial action a and thus we set $\mathsf{P}(E)(a.t) = 0$. On the other hand, if E can perform the action a, that is $E \rightarrow \{(a, \pi)\}$ for some $\pi \in \mu(\mathcal{R}^{\mathrm{p}})$, then for any $F \in \mathcal{R}^{\mathrm{p}}$ the probability of E performing the action a and behaving as the process F is given by $\pi(F)$. So supposing we have calculated the probability of F passing the test t, that is, the value of $\mathsf{P}(F)(t)$, if this was the only a transition E can perform $\mathsf{P}(E)(a.t)$ would be given by $\pi(F) \cdot \mathsf{P}(F)(t)$; however, since there may be other a transitions E can perform, we take the *weighted sum* of $\pi(F) \cdot \mathsf{P}(F)(t)$ over all $F \in \mathcal{R}^{\mathrm{p}}$ giving the value of $\mathsf{P}(E)(a.t)$ in the definition of P.

Using the map P we formulate the following ordering and resultant equivalence on processes.

Definition 4.2.3 *For any* $E, F \in \mathcal{R}^{\mathrm{p}}$, $E \sqsubseteq^{\mathsf{p}} F$ *if* $\mathsf{P}(E)(t) \leq \mathsf{P}(F)(t)$ *for all* $t \in \mathtt{T}^{\mathrm{p}}$. *Moreover, for any* $E, F \in \mathcal{R}^{\mathrm{p}}$, $E \overset{\mathsf{p}}{\sim} F$ *if* $E \sqsubseteq^{\mathsf{p}} F$ *and* $F \sqsubseteq^{\mathsf{p}} E$.

The order $\sqsubseteq^{\mathsf{p}}$ can be understood as follows: if $E \sqsubseteq^{\mathsf{p}} F$ then any path that E performs F can perform with a *higher or equal* probability, or any experiment that E can pass F can pass with a higher or equal probability.

Lemma 4.2.4 $\sqsubseteq^{\mathsf{p}}$ *is a pre-ordering over* $\mathcal{R}^{\mathrm{p}}$.

Proof. (i) (*Reflexivity*) $E \sqsubseteq^{\mathsf{p}} E$ for all $E \in \mathcal{R}^{\mathsf{p}}$ follows by definition of $\sqsubseteq^{\mathsf{p}}$.
(ii) (*Transitivity*) If $E \sqsubseteq^{\mathsf{p}} F$ and $F \sqsubseteq^{\mathsf{p}} G$, then by definition for any $t \in \mathtt{T}^{\mathsf{p}}$: $\mathsf{P}(E)(t) \leq \mathsf{P}(F)(t)$ and $\mathsf{P}(F)(t) \leq \mathsf{P}(G)(t)$, and hence $\mathsf{P}(E)(t) \leq \mathsf{P}(G)(t)$. Since this was for arbitrary $t \in \mathtt{T}^{\mathsf{p}}$, $E \sqsubseteq^{\mathsf{p}} G$ as required. $\square$

We now give some examples of purely probabilistic processes to illustrate the ordering $\sqsubseteq^{\mathsf{p}}$. First, consider the processes given in Figure 4.2 below.

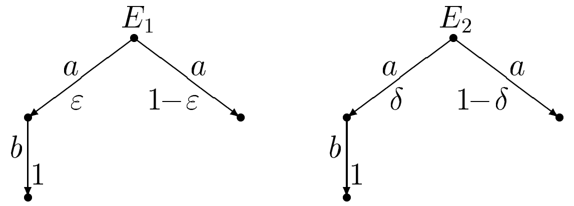


Figure 4.2: Example of the ordering $\sqsubseteq^{\mathsf{p}}$.

We will often summarise the results of tests on processes in tables, omitting the zero values and the trivial case of the empty test ($\perp$). The table for $\mathsf{P}(E_1)$ and $\mathsf{P}(E_2)$ on $\mathtt{T}^{\mathsf{p}}$ is:

t	$a.\perp$	$a.b.\perp$
$\mathsf{P}(E_1)$	1	ε
$\mathsf{P}(E_2)$	1	δ

and hence if $\varepsilon \leq \delta$ we have $E_1 \sqsubseteq^{\mathsf{p}} E_2$ and if $\varepsilon \geq \delta$, $E_2 \sqsubseteq^{\mathsf{p}} E_1$. Next consider the processes given in Figure 4.3.

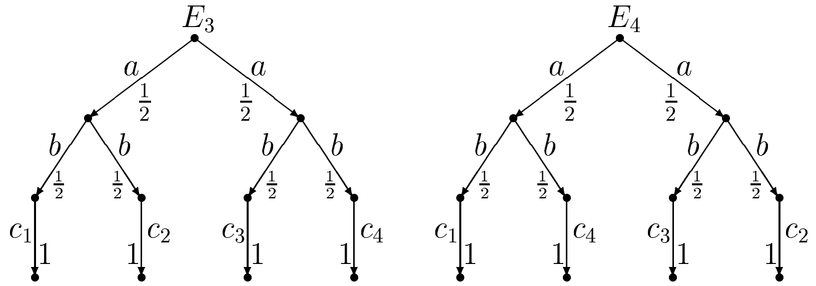


Figure 4.3: Example of equivalent purely probabilistic processes.

Observe that for any $i \in \{1, 2, 3, 4\}$, both E_3 and E_4 can perform the actions a, then b followed by the action c_i, with probability $\frac{1}{4}$, and therefore to any observer they would appear equivalent. The table summarising test results for the processes in Figure 4.3, where $i \in \{1, 2, 3, 4\}$, is:

t	$a.\perp$	$a.b.\perp$	$a.b.c_i.\perp$
$\mathsf{P}(E_3)$	1	1	1/4
$\mathsf{P}(E_4)$	1	1	1/4

and hence we have $E_3 \overset{\mathsf{p}}{\precsim} E_4$, which corresponds to the processes being equivalent under any observation. Finally, consider the processes in Figure 4.4.

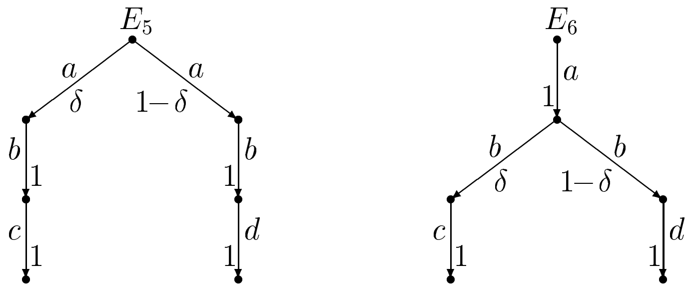


Figure 4.4: Example of equivalent purely probabilistic processes.

Then, both E_5 and E_6 can perform the action a, then b followed by c with probability δ, and otherwise perform the action a, then b followed by d with probability $1-\delta$. For E_5 and E_6 the table of test results is:

t	$a.\bot$	$a.b.\bot$	$a.b.c.\bot$	$a.b.d.\bot$
$\mathsf{P}(E_5)$	1	1	δ	$1-\delta$
$\mathsf{P}(E_6)$	1	1	δ	$1-\delta$

and so $E_5 \overset{\mathsf{p}}{\precsim} E_6$, which corresponds to the fact that we cannot distinguish between the behaviour of E_5 and E_6 by any observation made with the help of our testing language. The reader should note that both E_3 and E_4, and E_5 and E_6, will be distinguished by probabilistic bisimulation which opposes our view that the processes cannot be distinguished by any observation.

4.3 Deterministic Probabilistic Transition Systems

We now consider an ordering over any deterministic probabilistic transition system. Adding external choice adds an extra level of complexity to our model and, as a result, we need to extend our definitions of $\mathtt{T}^{\mathsf{p}}$ and P since otherwise the resultant ordering will not distinguish processes that have observably different behaviour. We demonstrate this by means of the example given in Figure 4.5.
The table for H_1 and H_2 and tests $t \in \mathtt{T}^{\mathsf{p}}$ is:

t	$a.\bot$	$a.b.\bot$	$a.c.\bot$
$\mathsf{P}(H_1)$	1	1/2	1/2
$\mathsf{P}(H_2)$	1	1/2	1/2

and thus $H_1 \overset{\mathsf{p}}{\precsim} H_2$ under $\mathtt{T}^{\mathsf{p}}$ tests. However, if we consider the behaviour of H_1 and H_2, we note that H_1 can perform the action a with probability $\frac{1}{2}$ and then either perform

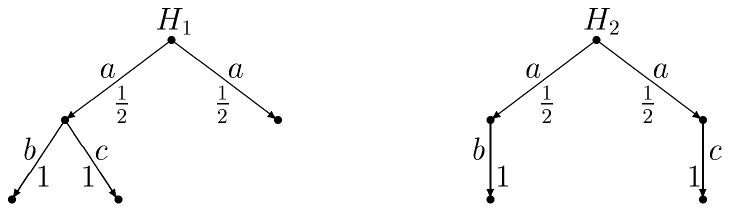


Figure 4.5: $\sqsubseteq^{\mathrm{p}}$ is too coarse over deterministic probabilistic processes.

the action b with probability 1 or perform the action c with probability 1 (where the choice between these is external). In contrast, H_2 cannot exhibit this behaviour.

We therefore extend $\mathtt{T}^{\mathrm{p}}$ by allowing tests of the form $(a_1.t_1, \ldots, a_m.t_m)$ which corresponds to the experiment involving making m copies of a process and pushing the a_i-button followed by the experiment t_i on one copy of the process for each $1 \leq i \leq m$. We impose the restriction on these tests that $a_i \neq a_j$ for all $1 \leq i \neq j \leq m$, which follows from the earlier discussion concerning button pushing experiments, in that we wish to press different buttons on the different copies made of processes. This also ensures that the tests are *independent*, since, for any action a process can perform, there is a distinct probability distribution associated with the process performing this action. Although we can add dependent tests, by removing this condition, in terms of probability theory our testing scenario becomes unrealistic: for certain dependent events, the probability of *both* events occurring in the same run will always be zero, and therefore if we perform dependent tests realistically one of them will always fail. For example, if we consider the random experiment of tossing a coin, the events of heads and tails are dependent, and testing for both heads and tails will always fail, that is, occur with probability 0.

Following this, to ease notation, we say any tests t and t' are *independent* if and only if the first step of their corresponding experiments are associated with pressing different buttons (which is indeed the case). Furthermore, in any construction of tests of the form $(t_1, \ldots, t_m)$, we require that t_i and t_j are independent for all $1 \leq i \neq j \leq m$. We now formally extend the definition of $\mathtt{T}^{\mathrm{p}}$ as follows.

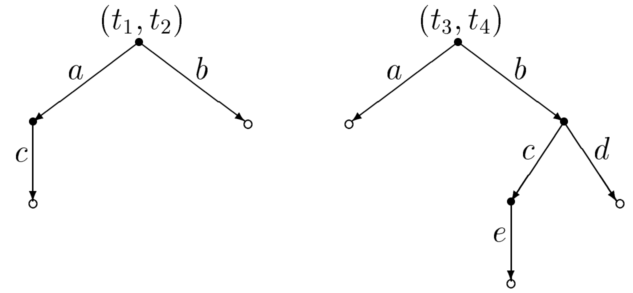
Definition 4.3.1 *Let $\mathtt{T}^{\mathrm{d}}$ and $\mathtt{T}^{\mathrm{d}}_{\omega}$ be the testing languages, with elements t and T respectively, defined inductively as follows:*

$$\begin{array}{rcl} t & ::= & \perp \mid a.T \\ T & ::= & (t, \ldots, t) \end{array}$$

where $a \in \mathcal{A}ct$.

As in the case of $\mathtt{T}^{\mathrm{p}}$, we can consider any $T \in \mathtt{T}^{\mathrm{d}}_{\omega}$ as a test for the occurrence of certain paths, with the addition that (t_1, t_2) is a test for the occurrence of the paths that t_1 *and* t_2 test for. For example, for the tests $t_1 = a.c.\bot$ and $t_2 = b.\bot$, (t_1, t_2) tests for the paths which have the initial actions ac and those which have the initial action b.

Alternatively, the following examples demonstrate how $\mathtt{T}^{\mathrm{d}}_{\omega}$ can be thought of graphically: letting t_1 and t_2 be the tests given above, and $t_3 = a.\bot$ and $t_4 = b.(c.e.\bot, d.\bot)$, then (t_1, t_2) and (t_3, t_4) can be represented as follows (note that $\bot$ is represented by an open circle):



Now for any deterministic probabilistic transition system $(\mathcal{R}^{\mathrm{d}}, \mathcal{A}ct, \rightarrow)$ and $E \in \mathcal{R}^{\mathrm{d}}$, by definition there exists a unique $S \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathcal{R}^{\mathrm{d}}))$ such that $E \rightarrow S$, and therefore any $E \in \mathcal{R}^{\mathrm{d}}$ can be used as an abbreviation of the set $S \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathcal{R}^{\mathrm{d}}))$ such that $E \rightarrow S$. We now extend P to the set of states $\mathcal{R}^{\mathrm{d}}$ of any deterministic probabilistic transition system and the set of tests $\mathtt{T}^{\mathrm{d}}_{\omega}$, with the resulting map called D for clarity.

Definition 4.3.2 *Let $\mathsf{D} : \mathcal{R}^{\mathrm{d}} \rightarrow (\mathtt{T}^{\mathrm{d}}_{\omega} \rightarrow [0,1])$ be the map defined inductively on $\mathtt{T}^{\mathrm{d}}_{\omega}$ as follows. For any $E \in \mathcal{R}^{\mathrm{d}}$ put: $\mathsf{D}(E)(\bot) = 1$,*

$$\mathsf{D}(E)(a.T) = \begin{cases} \sum_{F \in \mathcal{R}^{\mathrm{d}}} \pi(F) \cdot \mathsf{D}(F)(T) & \textit{if } (a, \pi) \in E \textit{ for some } \pi \in \mu(\mathcal{R}^{\mathrm{d}}) \\ 0 & \textit{otherwise} \end{cases}$$

$$\textit{and} \quad \mathsf{D}(E)((t_1, \ldots, t_m)) = \prod_{i=1}^{m} \mathsf{D}(E)(t_i).$$

As in the case of P, the value of $\mathsf{D}(E)(t)$ denotes the probability of E passing the test t and is calculated as follows. For any test $(t_1, \ldots, t_m)$, we first calculate the probability of E passing the tests t_i, that is $\mathsf{D}(E)(t_i)$, for all $1 \leq i \leq m$, and then since $\mathsf{D}(E)((t_1, \ldots, t_m))$ calculates the probabilities of E passing *all* the tests $t_1, \ldots, t_m$ we multiply these probabilities to give the probability of E passing the composite test $(t_1, \ldots, t_m)$. Multiplication can be used since by construction the probabilities of E passing the tests t_i and t_j are *independent* for all $1 \leq i \neq j \leq m$.

If we now return to Figure 4.5, we see that for $T = (a.(b.\bot, c.\bot)) \in \mathtt{T}^{\mathrm{d}}_{\omega}$:

$$\mathsf{D}(H_1)(T) = \frac{1}{2} \text{ and } \mathsf{D}(H_2)(T) = 0$$

and hence with the help of the tests $\mathtt{T}^{\mathrm{d}}_{\omega}$ we can distinguish between the processes H_1 and H_2.

The pre-order and equivalence on purely probabilistic transition systems lift to the following pre-order and equivalence on deterministic probabilistic transition systems.

Definition 4.3.3 *For any $E, F \in \mathcal{R}^{\mathrm{d}}$, $E \sqsubseteq^{\mathsf{d}} F$ if $\mathsf{D}(E)(T) \leq \mathsf{D}(F)(T)$ for all $T \in \mathtt{T}^{\mathrm{d}}_{\omega}$. Moreover, for any $E, F \in \mathcal{R}^{\mathrm{d}}$, $E \overset{\mathsf{d}}{\sim} F$ if $E \sqsubseteq^{\mathsf{d}} F$ and $F \sqsubseteq^{\mathsf{d}} E$.*

As in the purely probabilistic case, the order $\sqsubseteq^{\mathsf{d}}$ can be understood as follows: for any $E, F \in \mathcal{R}^{\mathrm{d}}$, $E \sqsubseteq^{\mathsf{d}} F$ just in the case any test that E can pass, F can pass with a higher or equal probability.

Lemma 4.3.4 *For all $E, F \in \mathcal{R}^{\mathrm{d}}$, $E \sqsubseteq^{\mathsf{d}} F$ if and only if $\mathsf{D}(E)(t) \leq \mathsf{D}(F)(t)$ for all $t \in \mathtt{T}^{\mathrm{d}}$.*

Proof. For the "if" direction consider any $E, F \in \mathcal{R}^{\mathrm{d}}$ such that $\mathsf{D}(E)(t) \leq \mathsf{D}(F)(t)$ for all $t \in \mathtt{T}^{\mathrm{d}}$. Then for any $T \in \mathtt{T}^{\mathrm{d}}_{\omega}$, $T = (t_1, \ldots, t_m)$ for some independent $t_1, \ldots, t_m$ and by definition of D:

$$\begin{array}{rcll} \mathsf{D}(E)(T) & = & \prod_{i=1}^{m} \mathsf{D}(E)(t_i) & \\ & \leq & \prod_{i=1}^{m} \mathsf{D}(F)(t_i) & \text{since } t_i \in \mathtt{T}^{\mathrm{d}} \text{ for all } 1 \leq i \leq m \text{ and the hypothesis} \\ & = & \mathsf{D}(F)(T) & \text{by definition of } \mathsf{D} \end{array}$$

and since this was for arbitrary $T \in \mathtt{T}^{\mathrm{d}}_{\omega}$, $E \sqsubseteq^{\mathsf{d}} F$ as required. The "only if" direction follows by definition of D and since $(t) \in \mathtt{T}^{\mathrm{d}}_{\omega}$ for all $t \in \mathtt{T}^{\mathrm{d}}$. $\square$

The lemma above implies that we need only consider the set of tests $\mathtt{T}^{\mathrm{d}}$ to investigate properties of our ordering $\sqsubseteq^{\mathsf{d}}$, as opposed to the larger set of tests $\mathtt{T}^{\mathrm{d}}_{\omega}$.

In later work we will need to consider the composition of certain tests of $\mathtt{T}^{\mathrm{d}}_{\omega}$ which we now define. We also introduce an important property of this composition by means of the lemma below.

Definition 4.3.5 *If $T_1 = (t_1, \ldots, t_m) \in \mathtt{T}^{\mathrm{d}}_{\omega}$ and $T_2 = (t'_1, \ldots, t'_{m'}) \in \mathtt{T}^{\mathrm{d}}_{\omega}$ such that T_1 and T_2 are independent, put $T_1 \,\|\, T_2 = (t_1, \ldots, t_m, t'_1, \ldots, t'_{m'})$.*

Lemma 4.3.6 *If $T_1, T_2 \in \mathtt{T}^{\mathrm{d}}_{\omega}$ and $T_1 \,\|\, T_2$ is defined, then $T_1 \,\|\, T_2 \in \mathtt{T}^{\mathrm{d}}_{\omega}$, and for all $E \in \mathcal{R}^{\mathrm{d}}$: $\mathsf{D}(E)(T_1 \,\|\, T_2) = \mathsf{D}(E)(T_1) \cdot \mathsf{D}(E)(T_2)$.*

4.3.1 Comparisons with Larsen and Skou's Testing Scenario

Since, as indicated above, deterministic probabilistic transition systems are equivalent to Larsen and Skou's probabilistic transition systems, we are now in a position to compare our testing scenario with that of Larsen and Skou [LS91]. To do this we first modify their definition of tests over probabilistic transition systems as given in the introduction to this chapter to the case of deterministic probabilistic transition systems $(\mathcal{R}^{\mathrm{d}}, \mathcal{A}ct, \rightarrow)$. Note that they do not impose any conditions on the construct $(t, \ldots, t)$.

Definition 4.3.7 *The testing language of Larsen and Skou [LS91] is constructed from the following syntax:*

$$t ::= \ \omega \mid a.t \mid (t, \ldots, t)$$

where $a \in \mathcal{A}ct$. The tests induce the following observation sets:

$$O_\omega = \{1_\omega\}, \ \ O_{a.t} = \{O_a\} \cup \{\, 1_a : e \mid e \in O_t\} \ \ \textit{and} \ \ O_{(t_1,\ldots,t_n)} = O_{t_1} \times \cdots \times O_{t_n}.$$

Then for any $E \in \mathcal{R}^{\mathrm{d}}$ and test t, $P_{t,E} : O_t \rightarrow [0,1]$ is the probability distribution defined structurally on the possible tests t as follows:

1. $P_{\omega,E}(1_\omega) = 1$
2. $P_{a.t,E}(O_a) = \begin{cases} 0 & \textit{if } (a,\pi) \in E \textit{ for some } \pi \in \mu(\mathcal{R}^{\mathrm{d}}) \\ 1 & \textit{otherwise} \end{cases}$

   $P_{a.t,E}(1_a : e) = \begin{cases} \sum_{F \in \mathcal{R}^{\mathrm{d}}} \pi(F) \cdot P_{t,F}(e) & \textit{if } (a,\pi) \in E \textit{ for some } \pi \in \mu(\mathcal{R}^{\mathrm{d}}) \\ 0 & \textit{otherwise} \end{cases}$
3. $P_{(t_1,\ldots,t_n),E}((e_1, \ldots, e_n)) = \prod_{i=1}^{n} P_{t_i,E}(e_i).$

There is a clear similarity between the above definition and the definitions of $\mathtt{T}^{\mathrm{d}}$ and D (Definition 4.3.1 and Definition 4.3.2 respectively). Formally, we have the following proposition.

Proposition 4.3.8 *For all $t \in \mathtt{T}^{\mathrm{d}}$ there exists (t'_t, e_t) such that $\mathsf{D}(E)(t) = P_{t'_t,E}(e_t)$ for all $E \in \mathcal{R}^{\mathrm{d}}$.*

Proof. The proof is by induction on $t \in \mathtt{T}^{\mathrm{d}}$. If $t = \perp$, then setting $(t'_\perp, e_\perp) = (\omega, 1_\omega)$ we have: $\mathsf{D}(E)(\perp) = P_{t'_\perp,E}(e_\perp) = 1$ for all $E \in \mathcal{R}^{\mathrm{d}}$ by definition of D and Definition 4.3.7.

If $t = a.T$ for some $a \in \mathcal{A}ct$, then $T = (t_1, \ldots, t_m)$ for some $m \geq 1$ such that $\{t_1, \ldots, t_m\} \subseteq \mathtt{T}^{\mathrm{d}}$. If we set $(t'_T, e_T) = (t'_{t_1}, \ldots, t'_{t_m}, e_{t_1} \times \cdots \times e_{t_m})$ and $(t'_t, e_t) =$

$(a.t'_T, 1_a : e_T)$ then showing that $\mathsf{D}(E)(t) = P_{t'_t,E}(e_t)$ for all $E \in \mathcal{R}^{\mathrm{d}}$ follows by definition of D and Definition 4.3.7, by first showing $\mathsf{D}(E)(T) = P_{t'_T,E}(e_T)$ for all $E \in \mathcal{R}^{\mathrm{d}}$. □

Intuitively, since both constructions allow tests of the form $(t, \ldots, t)$, both induce branching time equivalences. However, there is a clear difference, in that Larsen and Skou's testing scenario removes the syntactic restriction of independence we impose on our testing language. As a result, the two approaches attach a different meaning to the phrase "the probability of a process passing a test". In our approach, the probability of a process passing a test corresponds to the probability of *one run* (or execution) of the process passing a test, with the addition that we allow the value to correspond to the probability of one run of a process passing a test under different conditions, for example due to changes in the behaviour of the environment: in our setting the probability of a process passing the test $(a.T, b.T)$ is the probability of some run of the process passing the test $a.T$ when the environment offers the action a, and the *same* run passing the test $b.T$ when the action b is offered. On the other hand, the probability of a process passing a test in Larsen and Skou's scenario may correspond to more than one run of a process. To see this consider the process that flips a fair coin (denoted by the action "flip") and then performs the action a if the coin lands on heads and the action b otherwise; then under Definition 4.3.7, the probability of FLIP passing the test $(\mathrm{f}lip.a.\omega, \mathrm{f}lip.b.\omega)$ and observation set $(1_{flip} : 1_a : 1_\omega) \times (1_{flip} : 1_b : 1_\omega)$ is $\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$, which is the probability of tossing a coin *twice* and the coin landing on heads one time and tails the other, and not the probability of tossing a coin once and it landing on heads and tails (which is zero). Hence, the outcome of a test corresponds to more than one run of the process.

The impact of this difference is that, unlike our testing equivalences, Larsen and Skou's will be influenced by the time at which probabilistic choices are made. Intuitively, this results from allowing different experiments on the same probabilistic choice in the same test, which we do not allow. Furthermore, using this fact and Proposition 4.3.8, our induced equivalence is in fact coarser than Larsen and Skou's. Moreover, since Larsen and Skou have shown that their testing equivalence corresponds to probabilistic bisimulation, our induced equivalence is also coarser than probabilistic bisimulation . For example, Larsen and Skou's testing scenario (and probabilistic bisimulation) will distinguish the processes E_3 and E_4 in Figure 4.3, and the processes E_5 and E_6 in Figure 4.4, whereas our testing scenario will not.

4.4 Non-deterministic Probabilistic Transition Systems

If we now consider any non-deterministic probabilistic transition system $(\mathcal{R}^{\mathrm{n}d}, \mathcal{A}ct, \rightarrow)$ and $E \in \mathcal{R}^{\mathrm{nd}}$, then by definition we have that if $E \rightarrow S$ then $S = \{(a, \pi)\}$ (a singleton set) for some $a \in A$ and $\pi \in \mu(\mathcal{R}^{\mathrm{n}d})$, which to ease notation we will abbreviate to (a, π), or $S = \emptyset$. Then, for any $E \in \mathcal{R}^{\mathrm{nd}}$, since the processes are *non-deterministic* in nature, the decision as to which transition E will perform, that is, which $s \in (\mathcal{A}ct \times \mu(\mathcal{R}^{\mathrm{n}d})) \cup \{\emptyset\}$ such that $E \rightarrow s$ will be selected, and the probability of the transitions occurring cannot be determined. Thus, if we perform any button pushing experiment of the form $a.T$ on E, the outcome of the experiment will depend on the internal choice that E makes. Hence, we will lose any information about the discarded choices of E.

To overcome this, we extend our tests of the form $a.T$ to tests $(\!|a.T|\!)$, where, in terms of button pushing experiments, $(\!|a.T|\!)$ is the experiment in which we make sufficiently (finitely) many copies of a process, such that each internal choice that the process can perform will occur in at least one of the copies made, and then we perform the experiment $a.T$ on each copy, that is, we press the a-button and then perform the experiment T. We note that the above imposes a condition on the *demons* that influence the internal choices processes make: any internal choice a process can make will become possible within a finite period. Formally, we extend our testing language to $\mathtt{T}^{\mathrm{nd}}$ as follows.

Definition 4.4.1 *Let $\mathtt{T}^{\mathrm{nd}}$ and $\mathtt{T}^{\mathrm{nd}}_{\omega}$ be the testing languages, with elements t and T respectively, defined inductively as follows:*

$$\begin{array}{rcl} r & ::= & \perp \mid a.T \\ t & ::= & (\!|r|\!) \\ T & ::= & (t, \ldots, t) \end{array}$$

where $a \in \mathcal{A}ct$.

We note that, in any construction of tests of the form $(t_1, \ldots, t_m)$, we still impose the restriction that t_i and t_j are independent for all $1 \leq i \neq j \leq m$, that is, the first step of their corresponding button pushing experiments are with pressing different buttons. The reason behind including tests of the form $(t, \ldots, t)$ in $\mathtt{T}^{\mathrm{nd}}_{\omega}$ will be illustrated once we have investigated extending the map P to the non-deterministic setting, which now follows.

Recall that, for any process E and test t, $\mathsf{P}(E)(t)$ calculates the probability of the process E passing the test t. For any $E \in \mathcal{R}^{\mathrm{nd}}$ and test $(\!|a.T|\!)$, by means of the definition of P over purely probabilistic transition systems, we can calculate the probability of any $s \in (\mathcal{A}ct \times \mu(\mathcal{R}^{\mathrm{nd}})) \cup \{\emptyset\}$ passing the test $a.T$ where $E \to s$. However, since the transitions that E can perform may pass the test $a.T$ with different probabilities, we are unable to calculate the *exact* probability of E passing the test $a.T$. Given the test $(\!|a.T|\!)$ note that we will, in fact, have a set of values corresponding to the probability of each $s \in (\mathcal{A}ct \times \mu(\mathcal{R}^{nd})) \cup \{\emptyset\}$, where $E \to s$, passing the test $a.T$. This leads to two possible extensions of P to non-deterministic processes: one calculating the *greatest lower bound* on the probability of processes passing the tests and the other calculating the *least upper bound* on the probability of processes passing the tests; we will denote these extensions $\mathsf{N}_{\mathbf{glb}}$ and $\mathsf{N}_{\mathbf{lub}}$ respectively.

We note that these are the only realistic options since we are unable to take any kind of meaningful average, since the choice is internal and so we are unable to calculate the frequency of each choice being made; in fact, all we know is that each choice will be made within finitely many steps. Furthermore, if we wanted to model *demonic* or *angelic* non-determinism then we would only need to consider $\mathsf{N}_{\mathbf{glb}}$ or $\mathsf{N}_{\mathbf{lub}}$ respectively.

To put this another way, for any process E and test $(\!|r|\!)$: E will always pass the test r with a probability that is *greater than or equal to* $\mathsf{N}_{\mathbf{glb}}(E)((\!|r|\!))$ and *less than or equal to* $\mathsf{N}_{\mathbf{lub}}(E)((\!|r|\!))$, that is, the probability of E passing the test r always falls inside the *interval*

$$[\mathsf{N}_{\mathbf{glb}}(E)((\!|r|\!)), \mathsf{N}_{\mathbf{lub}}(E)((\!|r|\!))].$$

Formally, we define $\mathsf{N}_{\mathbf{lub}}$ and $\mathsf{N}_{\mathbf{glb}}$ as follows over the set of tests $\mathtt{T}_{\omega}^{\mathrm{nd}}$.

Definition 4.4.2 *Let* $\mathsf{N}_{\mathbf{glb}}, \mathsf{N}_{\mathbf{lub}} : \mathcal{R}^{nd} \to (\mathtt{T}_{\omega}^{\mathrm{nd}} \to [0,1])$ *be the maps defined inductively on* $\mathtt{T}_{\omega}^{\mathrm{nd}}$ *as follows, where we use* N_* *to denote either* $\mathsf{N}_{\mathbf{lub}}$ *or* $\mathsf{N}_{\mathbf{glb}}$. *For any* $E \in \mathcal{R}^{\mathrm{nd}}$ *put:*

$$\mathsf{N}_{\mathbf{glb}}(E)((\!|r|\!)) = \min_{E \to s} \mathsf{N}_{\mathbf{glb}}(s)(r), \quad \mathsf{N}_{\mathbf{lub}}(E)((\!|r|\!)) = \max_{E \to s} \mathsf{N}_{\mathbf{lub}}(s)(r)$$

$$\textit{and} \quad \mathsf{N}_*(E)((t_1, \ldots, t_m)) = \prod_{i=1}^{m} \mathsf{N}_*(E)(t_i)$$

where for any $s \in (\mathcal{A}ct \times \mu(\mathcal{R}^{\mathrm{nd}})) \cup \{\emptyset\}$ *we put:* $\mathsf{N}_*(s)(\perp) = 1$ *and*

$$\mathsf{N}_*(s)(a.T) = \begin{cases} \sum\limits_{F \in \mathcal{R}^{\mathrm{nd}}} \pi(F) \cdot \mathsf{N}_*(F)(T) & \textit{if } s = (a, \pi) \textit{ for some } \pi \in \mu(\mathcal{R}^{\mathrm{nd}}) \\ 0 & \textit{otherwise.} \end{cases}$$

The intuitive explanation behind the definition above follows from our discussion above except when considering tests of the form $(t_1, \ldots, t_m)$. In this case, similarly to the deterministic case, we can use multiplication, since for any test $(t_1, \ldots, t_m)$ by the restriction we have imposed the corresponding button pushing experiments of t_i and t_j for any $1 \leq i \leq j \leq m$ are associated with pressing different buttons at their first step, and so the (bounds on the) probabilities of any process passing the tests t_i and t_j are associated with different probability distributions (or zero) for all $1 \leq i \leq m$, and hence these values are independent.

To ease notation, since by definition $\mathsf{N}_{\mathbf{glb}}(E)((\!|\perp|\!)) = \mathsf{N}_{\mathbf{lub}}(E)((\!|\perp|\!)) = 1$ for all non-deterministic probabilistic transition systems $(\mathcal{R}^{nd}, \mathcal{A}ct, \rightarrow)$ and $E \in \mathcal{R}^{nd}$, we denote any occurrence of the test $(\!|\perp|\!)$ by $\perp$ in our tables.

We now illustrate the reasoning behind including the $(t_1, \ldots, t_m)$ construct in our definition of $\mathsf{T}^{\mathrm{nd}}_{\omega}$ by means of the example given in Figure 4.6 below, where τ is used to denote internal choice.

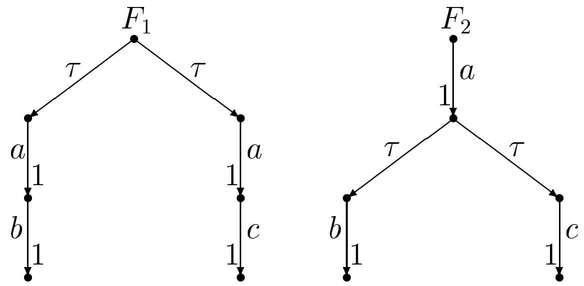


Figure 4.6: Example of non-deterministic probabilistic processes.

Consider the behaviour of F_1 and F_2. When F_1 has performed a, either b or c are possible, but not both. In contrast, when F_2 has performed a, both b and c remain possible. Hence, these processes have different behaviour, if we allow copies of processes to be made during any stage of their executions, and therefore we would wish to distinguish them under testing. However, if we calculate the nonzero values of the maps $\mathsf{N}_{\mathbf{lub}}$ and $\mathsf{N}_{\mathbf{glb}}$ with respect to the processes F_1 and F_2, and the subset of $\mathsf{T}^{\mathrm{nd}}_{\omega}$ where each test is of the form $(\!|a_1.(\!|a_2 \ldots (\!|a_m.\perp|\!) \ldots |\!)|\!)$, for some $\{a_1, \ldots, a_m\} \subseteq \mathcal{A}ct$ we have:

T	$(\!\vert a.\perp\vert\!)$
$\mathsf{N}_{\mathbf{glb}}(F_1)$	1
$\mathsf{N}_{\mathbf{glb}}(F_2)$	1

T	$(\!\vert a.\perp\vert\!)$	$(\!\vert a.(\!\vert b.\perp\vert\!)\vert\!)$	$(\!\vert a.(\!\vert c.\perp\vert\!)\vert\!)$
$\mathsf{N}_{\mathbf{lub}}(F_1)$	1	1	1
$\mathsf{N}_{\mathbf{lub}}(F_2)$	1	1	1

and hence the orderings induced from $\mathsf{N}_{\mathbf{glb}}$ and $\mathsf{N}_{\mathbf{lub}}$ with respect to the restricted set of tests cannot distinguish between F_1 and F_2. However, if instead we consider all the tests $\mathsf{T}^{\mathrm{nd}}_{\omega}$, letting $T = ((\!|a.((\!|b.\perp|\!), (\!|c.\perp|\!))|\!))\in \mathsf{T}^{\mathrm{nd}}_{\omega}$ and calculating the values of $\mathsf{N}_{\mathbf{lub}}$

with respect to t and the processes F_1 and F_2 allows us to obtain:

$$\mathsf{N}_{\mathbf{lub}}(F_1)(T) = 0 \neq 1 = \mathsf{N}_{\mathbf{lub}}(F_2)(T).$$

Therefore, $\mathsf{N}_{\mathbf{lub}}$ can distinguish between the processes F_1 and F_2 when we use the tests $\mathsf{T}^{\mathrm{nd}}_{\omega}$. On the other hand, even with the set of tests $\mathsf{T}^{\mathrm{nd}}_{\omega}$, $\mathsf{N}_{\mathbf{glb}}$ cannot distinguish between F_1 and F_2. This may lead us to conclude that the ordering induced from $\mathsf{N}_{\mathbf{lub}}$ is the best candidate for the ordering over non-deterministic processes.

However, if we now consider the processes given in Figure 4.7 below:

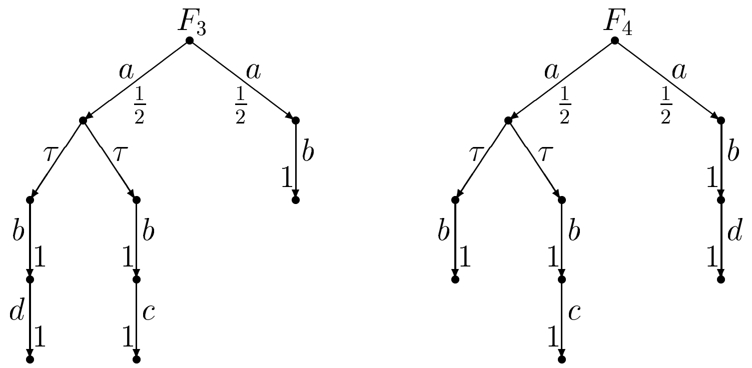


Figure 4.7: Example of non-deterministic probabilistic processes.

we see that the process F_3 can perform an action a with probability $\frac{1}{2}$, and then always perform an action b and terminate with probability 1. However, F_4 cannot behave in this way, and so we would wish to distinguish these processes through testing. Calculating the non-zero values of $\mathsf{N}_{\mathbf{lub}}$ and $\mathsf{N}_{\mathbf{glb}}$ with respect to the processes F_3 and F_4 we have:

T	$((\!|a.\bot|\!))$	$((\!|a.((\!|b.\bot|\!))|\!))$	$((\!|a.((\!|b.((\!|c.\bot|\!))|\!))|\!))$	$((\!|a.((\!|b.((\!|d.\bot|\!))|\!))|\!))$
$\mathsf{N}_{\mathbf{glb}}(F_3)$	1	1	0	0
$\mathsf{N}_{\mathbf{glb}}(F_4)$	1	1	0	1/2
$\mathsf{N}_{\mathbf{lub}}(F_3)$	1	1	1/2	1/2
$\mathsf{N}_{\mathbf{lub}}(F_4)$	1	1	1/2	1/2

and thus $\mathsf{N}_{\mathbf{glb}}$ can distinguish F_3 and F_4, whereas $\mathsf{N}_{\mathbf{lub}}$ cannot.

Taking the above two examples into account, we observe that in certain cases there will exist non-deterministic processes with differing observable behaviour which only one of the maps $\mathsf{N}_{\mathbf{glb}}$ and $\mathsf{N}_{\mathbf{lub}}$ can distinguish. Therefore, to incorporate the advantages of both, we take the *intersection* of the orderings induced from $\mathsf{N}_{\mathbf{glb}}$ and $\mathsf{N}_{\mathbf{lub}}$ as our operational ordering over non-deterministic processes. Formally, we define the following pre-order and equivalence on non-deterministic probabilistic transition systems.

Definition 4.4.3 *For any $E, F \in \mathcal{R}^{\mathrm{nd}}$, $E \sqsubseteq^{\mathsf{nd}} F$ if $\mathsf{N}_*(E)(T) \leq \mathsf{N}_*(F)(T)$ for $\mathsf{N}_* = \mathsf{N}_{\mathbf{glb}}$, $\mathsf{N}_* = \mathsf{N}_{\mathbf{lub}}$ and for all tests $T \in \mathtt{T}^{\mathrm{nd}}_{\omega}$. Moreover, for any $E, F \in \mathcal{R}^{\mathrm{nd}}$, $E \stackrel{\mathsf{nd}}{\eqsim} F$ if $E \sqsubseteq^{\mathsf{nd}} F$ and $F \sqsubseteq^{\mathsf{nd}} E$.*

Similar to the deterministic case, the following lemma demonstrates why we need only consider the set of tests $\mathtt{T}^{\mathrm{nd}}$, as opposed to the (larger) set of tests $\mathtt{T}^{\mathrm{nd}}_{\omega}$, when investigating properties of the ordering $\sqsubseteq^{\mathsf{nd}}$.

Lemma 4.4.4 *For all $E, F \in \mathcal{R}^{\mathrm{nd}}$, $E \sqsubseteq^{\mathsf{nd}} F$ if and only if $\mathsf{N}_{\mathbf{glb}}(E)(t) \leq \mathsf{N}_{\mathbf{glb}}(F)(t)$ and $\mathsf{N}_{\mathbf{lub}}(E)(t) \leq \mathsf{N}_{\mathbf{lub}}(F)(t)$ for all $t \in \mathtt{T}^{\mathrm{nd}}$.*

Proof. The proof is similar to that of Lemma 4.3.4. □

We now give some examples of non-deterministic probabilistic processes to illustrate the ordering $\sqsubseteq^{\mathsf{nd}}$. To begin with, consider the processes in Figure 4.8.

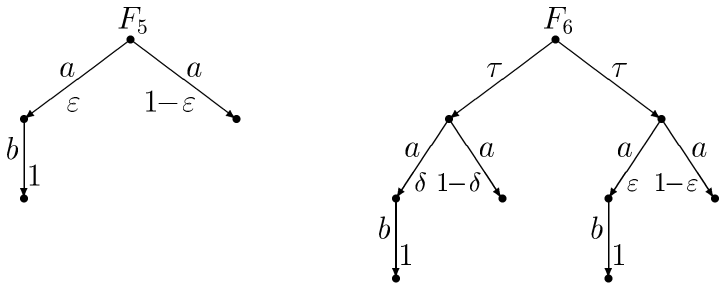


Figure 4.8: Example of the ordering $\sqsubseteq^{\mathsf{nd}}$.

The table for $\mathsf{N}_{\mathbf{glb}}$ and $\mathsf{N}_{\mathbf{lub}}$ with respect to the processes F_5 and F_6 and $\mathtt{T}^{\mathrm{nd}}$ is:

t	$(\!\|a.\bot\|\!)$	$(\!\|a.(\!\|b.\bot\|\!)\|\!)$
$\mathsf{N}_{\mathbf{glb}}(F_5)$	1	ε
$\mathsf{N}_{\mathbf{glb}}(F_6)$	1	$\min\{\varepsilon, \delta\}$

t	$(\!\|a.\bot\|\!)$	$(\!\|a.(\!\|b.\bot\|\!)\|\!)$
$\mathsf{N}_{\mathbf{lub}}(F_5)$	1	ε
$\mathsf{N}_{\mathbf{lub}}(F_6)$	1	$\max\{\varepsilon, \delta\}$

and therefore if $\varepsilon = \delta$, $\varepsilon > \delta$ or $\varepsilon < \delta$, then $F_5 \stackrel{\mathsf{nd}}{\eqsim} F_6$, $F_6 \sqsubseteq^{\mathsf{nd}} F_5$ and $F_5 \sqsubseteq^{\mathsf{nd}} F_6$ respectively. In particular, the outcome of the experiment $(\!|a.(\!|b.\bot|\!)|\!)$ on F_6 can be considered as any probability in the closed interval $[\min\{\varepsilon, \delta\}, \max\{\varepsilon, \delta\}]$.

Finally, we give an example of the induced equivalence $\stackrel{\mathsf{nd}}{\eqsim}$ by means of the processes given in Figure 4.9.

Both processes can perform an internal choice and reach a state, where for any $i \in \{1, 2, 3, 4\}$ the probability of performing the trace ab_i is either one half or zero. Moreover, the probability of either process performing the traces ab_i and ab_j for any $i \neq j \in \{1, 2, 3, 4\}$ is zero, since either the processes reach a state which is unable to

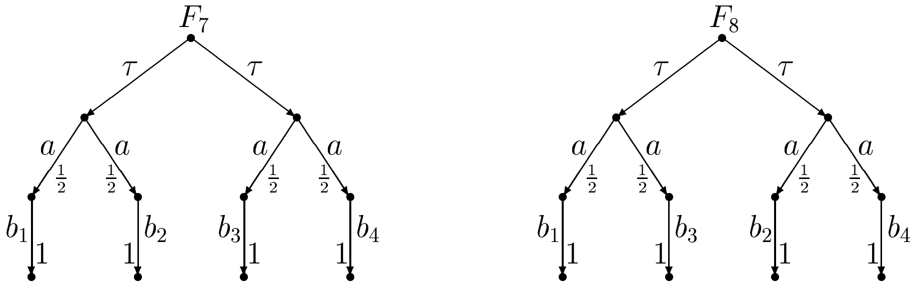


Figure 4.9: Example of equivalent non-deterministic probabilistic processes.

perform one of the traces, or the probabilities of performing the traces are *dependent* (for example, the probability of tossing a coin and the coin landing on heads and tails is zero). Summarising, this yields the tables below for $\mathsf{N}_{\mathbf{glb}}$ and $\mathsf{N}_{\mathbf{lub}}$ with respect to the processes F_7 and F_8 and $\mathtt{T}^{\mathrm{nd}}$, where $i \in \{1, 2, 3, 4\}$:

t	$(\!| a.\bot |\!)$
$\mathsf{N}_{\mathbf{glb}}(F_7)$	1
$\mathsf{N}_{\mathbf{glb}}(F_8)$	1

t	$(\!| a.\bot |\!)$	$(\!| a.(\!| b_i.\bot |\!) |\!)$
$\mathsf{N}_{\mathbf{lub}}(F_7)$	1	1/2
$\mathsf{N}_{\mathbf{lub}}(F_8)$	1	1/2

and thus $F_7 \overset{\mathsf{n}d}{\approx} F_8$, which corresponds with their observable behaviour being equivalent. Recall that F_7 and F_8 will be distinguished by probabilistic bisimulation.

Before we consider arbitrary reactive probabilistic transition systems, as for the deterministic case we introduce the definition of the composition for certain tests of $\mathtt{T}^{\mathrm{nd}}_\omega$ and an important property of this composition.

Definition 4.4.5 *If $T_1 = (t_1, \ldots, t_m) \in \mathtt{T}^{\mathrm{nd}}_\omega$ and $T_2 = (t'_1, \ldots, t'_{m'}) \in \mathtt{T}^{\mathrm{nd}}_\omega$ such that T_1 and T_2 are independent, put: $T_1 \,\|\, T_2 = (t_1, \ldots, t_m, t'_1, \ldots, t'_{m'})$.*

Lemma 4.4.6 *If $T_1, T_2 \in \mathtt{T}^{\mathrm{nd}}_\omega$ and $T_1 \,\|\, T_2$ is defined, then $T_1 \,\|\, T_2 \in \mathtt{T}^{\mathrm{nd}}_\omega$ and for all $E \in \mathcal{R}^{nd}$: $\mathsf{N}_*(E)(T_1 \,\|\, T_2) = \mathsf{N}_*(E)(T_1) \cdot \mathsf{N}_*(E)(T_2)$.*

4.5 Reactive Probabilistic Transition Systems

In this section we wish to extend the orderings $\sqsubseteq^{\mathsf{p}}$, $\sqsubseteq^{\mathsf{d}}$ and $\sqsubseteq^{\mathsf{n}d}$ to an ordering over arbitrary reactive probabilistic transition systems $(\mathcal{R}, \mathcal{A}ct, \to)$. As processes of reactive probabilistic transition systems may exhibit non-deterministic behaviour, the first step is to introduce extensions of the maps $\mathsf{N}_{\mathbf{glb}}$ and $\mathsf{N}_{\mathbf{lub}}$ to this setting.

The first approach we consider is simply applying the maps $\mathsf{N}_{\mathbf{glb}}$ and $\mathsf{N}_{\mathbf{lub}}$ defined for non-deterministic probabilistic transition systems to reactive probabilistic transition systems. Note that $\mathsf{N}_{\mathbf{glb}}$ and $\mathsf{N}_{\mathbf{lub}}$ were already constructed over transition systems where processes exhibit non-deterministic behaviour. However, since reactive probabilistic processes exhibit external choices, as well as internal, the ordering induced from the maps $\mathsf{N}_{\mathsf{glb}}$ and $\mathsf{N}_{\mathsf{lub}}$ will not distinguish certain reactive probabilistic processes with different observable behaviour. We demonstrate this by means of an example. Consider the processes given in Figure 4.10.

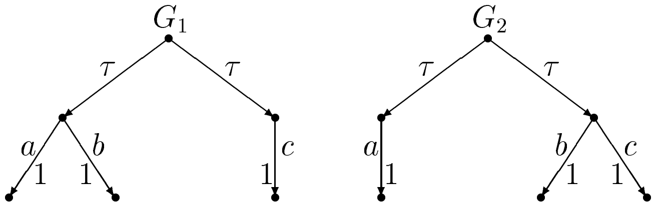


Figure 4.10: Example of reactive probabilistic processes.

Observe that G_1 can perform a transition which offers an external choice between the actions a and b, a behaviour that G_2 cannot match. Therefore, we would wish to distinguish these processes through testing. Calculating the values of $\mathsf{N}_{\mathsf{glb}}$ and $\mathsf{N}_{\mathsf{lub}}$ we have:

$$\mathsf{N}_{\mathsf{glb}}(G_1)(t) = \mathsf{N}_{\mathsf{glb}}(G_2)(t) = \begin{cases} 1 & \text{if } t = \bot \\ 0 & \text{otherwise} \end{cases} \qquad \text{and}$$

$$\mathsf{N}_{\mathsf{lub}}(G_1)(t) = \mathsf{N}_{\mathsf{lub}}(G_2)(t) = \begin{cases} 1 & \text{if } t \in \{\bot, (\!|a.\bot|\!), (\!|b.\bot|\!), (\!|c.\bot|\!)\} \\ 0 & \text{otherwise} \end{cases}$$

and thus we cannot distinguish these processes with the ordering induced from $\mathsf{N}_{\mathsf{glb}}$ and $\mathsf{N}_{\mathsf{lub}}$.

We, therefore, need to find alternatives to $\mathsf{N}_{\mathsf{glb}}$ and $\mathsf{N}_{\mathsf{lub}}$, and since in the example above the difference between the observable behaviour of processes G_1 and G_2 results from differences in their external choices, we base our definition to a greater degree on the construction of the tests $\mathtt{T}^{\mathrm{d}}_{\omega}$ and the map D for deterministic processes, as opposed to $\mathsf{N}_{\mathsf{glb}}$ and $\mathsf{N}_{\mathsf{lub}}$. To accomplish this, we form the testing language $\mathtt{T}^{\mathrm{d}\,\prime}_{\omega}$ by replacing any test of the form $(t_1, \ldots, t_n)$ in $\mathtt{T}^{\mathrm{d}}_{\omega}$ by the test $(\!|(t_1, \ldots, t_n)|\!)$. Then using this testing language we now introduce the maps $\mathsf{D}_{\mathsf{glb}}$ and $\mathsf{D}_{\mathsf{lub}}$ as follows.

Definition 4.5.1 *Let* $\mathsf{D}_{\mathsf{glb}}, \mathsf{D}_{\mathsf{lub}} : \mathcal{R} \to (\mathtt{T}^{\mathrm{d}\,\prime}_{\omega} \to [0,1])$ *be the maps defined inductively on* $\mathtt{T}^{\mathrm{d}\,\prime}_{\omega}$ *as follows where* D_* *denotes either* $\mathsf{D}_{\mathsf{glb}}$ *or* $\mathsf{D}_{\mathsf{lub}}$. *For any* $E \in \mathcal{R}$ *put:*

$$\mathsf{D}_{\mathsf{glb}}(E)((\!|(t_1, \ldots, t_n)|\!)) = \min_{E \to S} \mathsf{D}_{\mathsf{glb}}(S)((t_1, \ldots, t_n)) \quad \textit{and}$$

$$\mathsf{D}_{\mathsf{lub}}(E)((\!|(t_1, \ldots, t_n)|\!)) = \max_{E \to S} \mathsf{D}_{\mathsf{lub}}(S)((t_1, \ldots, t_n))$$

where for any $S \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathcal{R}))$ *put:* $\mathsf{D}_*(S)(\bot) = 1$,

$$\mathsf{D}_*(S)((t_1, \ldots, t_n)) = \prod_{i=1}^{m} \mathsf{D}_*(S)(t_i) \quad \textit{and}$$

$$\mathsf{D}_*(S)(a.T) = \begin{cases} \sum\limits_{F \in \mathcal{R}} \pi(F) \cdot \mathsf{D}_*(F)(T) & \textit{if } (a, \pi) \in S \textit{ for some } \pi \in \mu(\mathcal{R}) \\ 0 & \textit{otherwise.} \end{cases}$$

Note that, the difference between the definition of $\mathsf{D}_{\mathbf{glb}}$ and $\mathsf{D}_{\mathbf{lub}}$ and the definition of $\mathsf{N}_{\mathbf{glb}}$ and $\mathsf{N}_{\mathbf{lub}}$ (see Definition 4.4.2), results from the difference between when the tests of $\mathsf{T}_\omega^{\mathrm{d}\,\prime}$ and $\mathsf{T}_\omega^{\mathrm{nd}}$ make copies of processes in order to perform different tests on each copy: in $\mathsf{T}_\omega^{\mathrm{d}\,\prime}$ these copies are made *after* processes perform internal choices, whereas in $\mathsf{T}_\omega^{\mathrm{nd}}$ these copies are made *before* the internal choices.

If we return to Figure 4.10 above and consider the test $T = (\!|(a.\bot, b.\bot)|\!) \in \mathsf{T}_\omega^{\mathrm{d}\,\prime}$ then using the definition above we have:

$$\mathsf{D}_{\mathbf{lub}}(G_1)(T) = 1 \neq 0 = \mathsf{D}_{\mathbf{lub}}(G_2)(T)$$

and thus the ordering induced from $\mathsf{D}_{\mathbf{glb}}$ and $\mathsf{D}_{\mathbf{lub}}$ will distinguish the processes G_1 and G_2.

However, this is still unsatisfactory as we will not correctly discriminate internal behaviour. As an example, let us return to the processes F_1 and F_2 given in Figure 4.6 and calculate the values of $\mathsf{D}_{\mathbf{glb}}$ and $\mathsf{D}_{\mathbf{lub}}$ with respect to these processes:

$$\mathsf{D}_{\mathbf{glb}}(F_1)(t) = \mathsf{D}_{\mathbf{glb}}(F_2)(t) = \begin{cases} 1 & \text{if } t \in \{\bot, (\!|(a.\bot)|\!)\} \\ 0 & \text{otherwise} \end{cases} \qquad \text{and}$$

$$\mathsf{D}_{\mathbf{lub}}(F_1)(t) = \mathsf{D}_{\mathbf{lub}}(F_2)(t) = \begin{cases} 1 & \text{if } t \in \{\bot, (\!|(a.\bot)|\!), (\!|(a.(\!|(b.\bot)|\!))|\!), (\!|(a.(\!|(c.\bot)|\!))|\!)\} \\ 0 & \text{otherwise} \end{cases}$$

and thus $\mathsf{D}_{\mathbf{glb}}$ and $\mathsf{D}_{\mathbf{lub}}$ cannot distinguish between these processes.

The reason for the failure of the above two approaches is that reactive probabilistic processes can make *three* types of choices: probabilistic, external and internal, whereas in the tests of $\mathsf{T}_\omega^{\mathrm{d}}$ and $\mathsf{T}_\omega^{\mathrm{nd}}$ we only have two levels of complexity, namely $a.T$ and $(t, \ldots, t)$. As a result, when testing reactive processes we can only capture the behaviour associated with two of the choices processes make: $a.T$ is a test relating to the probabilistic behaviour of processes (since probabilistic choice is action-guarded) and $(t, \ldots, t)$ relates to either the external or internal choices between actions that processes make. The difference between whether $(t, \ldots, t)$ tests for external choice or internal choice results from where $(\!|.|\!)$ appears in the test, for example, in the first attempt (N_*) the construct was of the form $((\!|r|\!), \ldots, (\!|r|\!))$ and the internal choices were captured, whereas in the second (D_*) the construct was of the form $(\!|t, \ldots, t|\!)$ and the external choices were captured.

Following on from this argument, we need to combine the definition of $\mathsf{T}_\omega^{\mathrm{d}}$ and $\mathsf{T}_\omega^{\mathrm{nd}}$ to allow for both constructions in order to form a set of tests that will capture probabilistic, external and internal choices, which we will denote by $\mathtt{T}_\omega$. Formally, we combine the definitions of $\mathtt{T}^{\mathrm{d}}_\omega$ and $\mathtt{T}^{\mathrm{nd}}_\omega$ to the set of tests $\mathtt{T}_\omega$ as follows. We note that we still impose the restriction on any construct of the form $(t_1, \ldots, t_m)$ in that for any $1 \leq i \neq j \leq m$ the first steps of their corresponding experiments are associated with pressing different buttons. Furthermore, we introduce a separate construct $[t, \ldots, t]$ to the syntax of our testing language $\mathtt{T}_\omega$ to distinguish the different types of tests and apply the same restriction to it.

Definition 4.5.2 *Let* $\mathtt{T}$ *and* $\mathtt{T}_\omega$*, with elements* t *and* T *respectively, be the testing languages defined inductively as follows:*

$$\begin{array}{rcl} r & ::= & \bot \,|\, [a.T, \ldots, a.T] \\ t & ::= & (\!| r |\!) \\ T & ::= & (t, \ldots, t) \end{array}$$

where $a \in \mathcal{A}ct$*.*

Combining the definition of D over deterministic probabilistic processes, and the definitions of $\mathsf{N}_{\mathbf{glb}}$ and $\mathsf{N}_{\mathbf{lub}}$ over non-deterministic probabilistic processes, we define the maps $\mathsf{R}_{\mathbf{glb}}$ and $\mathsf{R}_{\mathbf{lub}}$ over reactive probabilistic transition systems. Similar to the non-deterministic case, $\mathsf{R}_{\mathbf{glb}}$ calculates the greatest lower bound on the probability of the process passing the test and $\mathsf{R}_{\mathbf{lub}}$ calculates the least upper bound on the probability of the process passing the test. Formally, we define $\mathsf{R}_{\mathbf{glb}}$ and $\mathsf{R}_{\mathbf{lub}}$ as follows.

Definition 4.5.3 *Let* $\mathsf{R}_{\mathbf{glb}}, \mathsf{R}_{\mathbf{lub}} : \mathcal{R} \to (\mathtt{T}_\omega \to [0,1])$ *be the maps defined inductively on* $\mathtt{T}_\omega$ *where* R_* *stands for either* $\mathsf{R}_{\mathbf{glb}}$ *or* $\mathsf{R}_{\mathbf{lub}}$*. For any* $E \in \mathcal{R}$ *put:*

$$\mathsf{R}_{\mathbf{glb}}(E)((\!| r |\!)) = \min_{E \to S} \mathsf{R}_{\mathbf{glb}}(S)(r), \quad \mathsf{R}_{\mathbf{lub}}(E)((\!| r |\!)) = \max_{E \to S} \mathsf{R}_{\mathbf{lub}}(S)(r)$$

$$\textit{and} \quad \mathsf{R}_*(E)((t_1, \ldots, t_m)) = \prod_{j=1}^{m} \mathsf{R}_*(E)(t_j)$$

where for any $S \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathcal{R}))$ *and* $1 \leq i \leq m$ *put:*

$$\mathsf{R}_*(S)(\bot) = 1, \quad \mathsf{R}_*(S)([a_1.T_1, \ldots, a_m.T_m]) = \prod_{i=1}^{m} \mathsf{R}_*(S)(a_i.T_i) \quad \textit{and}$$

$$\mathsf{R}_*(S)(a.T) = \begin{cases} \sum_{F \in \mathcal{R}} \pi(F) \cdot \mathsf{R}_*(F)(T) & \textit{if } (a, \pi) \in S \textit{ for some } \pi \in \mu(\mathcal{R}) \\ 0 & \textit{otherwise.} \end{cases}$$

The intuition behind the above calculations is similar to those for D, $\mathsf{N}_{\mathbf{glb}}$ and $\mathsf{N}_{\mathbf{lub}}$, where we note that, as a result of our restriction on the construct $(t, \ldots, t)$ and $[a.T, \ldots, a.T]$, multiplication can be used since the tests will be independent. We note that as in the non-deterministic case and to ease notation we replace all occurrences of the test $(\!|\bot|\!)$ by $\bot$.

The pre-order and equivalence on all reactive probabilistic transition systems is defined as follows, where for similar reasons to the non-deterministic case we take the intersection of the orderings induced from $\mathsf{R}_{\mathbf{glb}}$ and $\mathsf{R}_{\mathbf{lub}}$.

Definition 4.5.4 *For any $E, F \in \mathcal{R}$, $E \sqsubseteq^{\mathbf{glb}} F$ if $\mathsf{R}_{\mathbf{glb}}(E)(T) \leq \mathsf{R}_{\mathbf{glb}}(F)(T)$ and $E \sqsubseteq^{\mathbf{lub}} F$ if $\mathsf{R}_{\mathbf{lub}}(E)(T) \leq \mathsf{R}_{\mathbf{lub}}(F)(T)$ for all $T \in \mathtt{T}_\omega$ respectively. Moreover, for any $E, F \in \mathcal{R}$, $E \sqsubseteq^{\mathsf{r}} F$ if $E \sqsubseteq^{\mathbf{glb}} F$ and $E \sqsubseteq^{\mathbf{lub}} F$, and $E \overset{\mathsf{r}}{\sim} F$ if $E \sqsubseteq^{\mathsf{r}} F$ and $F \sqsubseteq^{\mathsf{r}} E$.*

As before, we need only consider the set of tests $\mathtt{T}$ since the following lemma holds similarly to Lemma 4.3.4.

Lemma 4.5.5 *For all $E, F \in \mathcal{R}$, $E \sqsubseteq^{\mathsf{r}} F$ if and only if $\mathsf{R}_{\mathbf{glb}}(E)(t) \leq \mathsf{R}_{\mathbf{glb}}(F)(t)$ and $\mathsf{R}_{\mathbf{lub}}(E)(t) \leq \mathsf{R}_{\mathbf{lub}}(F)(t)$ for all $t \in \mathtt{T}$.*

If we now return to Figure 4.6 for $\mathsf{R}_{\mathbf{glb}}$ and $\mathsf{R}_{\mathbf{lub}}$ with respect to the processes F_1 and F_2 and tests $\mathtt{T}$:

t	$(\!|[a.\bot]|\!)$	$(\!|[a.(\!|[b.\bot]|\!)]|\!)$	$(\!|[a.(\!|[c.\bot]|\!)]|\!)$	$(\!|[a.((\!|[b.\bot]|\!),(\!|[c.\bot]|\!))]|\!)$
$\mathsf{R}_{\mathbf{glb}}(F_1)$	1	0	0	0
$\mathsf{R}_{\mathbf{glb}}(F_2)$	1	0	0	0
$\mathsf{R}_{\mathbf{lub}}(F_1)$	1	1	1	0
$\mathsf{R}_{\mathbf{lub}}(F_2)$	1	1	1	1

Similarly, returning to Figure 4.10 we have:

t	$(\!|[a.\bot]|\!)$	$(\!|[b.\bot]|\!)$	$(\!|[c.\bot]|\!)$	$(\!|[a.\bot, b.\bot]|\!)$	$(\!|[b.\bot, c.\bot]|\!)$
$\mathsf{R}_{\mathbf{lub}}(G_1)$	1	1	1	1	0
$\mathsf{R}_{\mathbf{lub}}(G_2)$	1	1	1	0	1

and $\mathsf{R}_{\mathbf{glb}}(G_1)$ and $\mathsf{R}_{\mathbf{glb}}(G_2)$ are zero for all tests not equal to $(\!|\bot|\!)$. Therefore, using the testing language $\mathtt{T}$, we can now distinguish between the processes F_1 and F_2 and the processes G_1 and G_2.

Moreover, as the definition of the maps $\mathsf{R}_{\mathbf{glb}}$ and $\mathsf{R}_{\mathbf{lub}}$ are based on those of P, D, $\mathsf{N}_{\mathbf{glb}}$ and $\mathsf{N}_{\mathbf{lub}}$, by construction the ordering $\sqsubseteq^{\mathsf{r}}$ is based on the orderings $\sqsubseteq^{\mathsf{p}}$, $\sqsubseteq^{\mathsf{d}}$ and $\sqsubseteq^{nd}$. As a result it is straightforward to show that each of the following propositions hold for any purely probabilistic transition system $(\mathcal{R}^{\mathrm{p}}, \mathcal{A}ct, \rightarrow)$, deterministic probabilistic transition system $(\mathcal{R}^{\mathrm{d}}, \mathcal{A}ct, \rightarrow)$ and non-deterministic probabilistic transition system $(\mathcal{R}^{\mathrm{nd}}, \mathcal{A}ct, \rightarrow)$.

Proposition 4.5.6 *For all* $E, F \in \mathcal{R}^{\mathrm{p}}$, $E \sqsubseteq^{\mathsf{p}} F$ *if and only if* $E \sqsubseteq^{\mathsf{r}} F$.

Proposition 4.5.7 *For all* $E, F \in \mathcal{R}^{\mathrm{d}}$, $E \sqsubseteq^{\mathsf{d}} F$ *if and only if* $E \sqsubseteq^{\mathsf{r}} F$.

Proposition 4.5.8 *For all* $E, F \in \mathcal{R}^{\mathrm{n}d}$, $E \sqsubseteq^{\mathsf{nd}} F$ *if and only if* $E \sqsubseteq^{\mathsf{r}} F$.

Consequently, all the examples considered so far will remain valid if $\sqsubseteq^{\mathsf{r}}$ replaces the relevant equivalence or ordering. In particular, $\sqsubseteq^{\mathsf{r}}$ will distinguish between the processes of Figure 4.6, and hence we have overcome the problems associated with the first two attempts at extending our orderings to reactive probabilistic transition systems.

We now illustrate the ordering $\sqsubseteq^{\mathsf{r}}$ over reactive probabilistic processes by means of the example given in Figure 4.11 below, where we have removed the probabilities associated with transitions since all occur with probability 1.

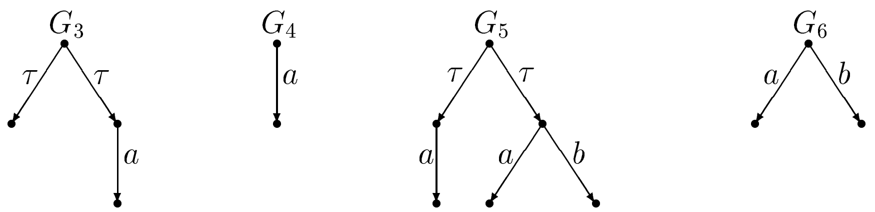


Figure 4.11: Example of the ordering $\sqsubseteq^{\mathsf{r}}$.

Summarising $\mathsf{R_{glb}}$ and $\mathsf{R_{lub}}$ with respect to the processes G_1, G_2 and G_3 and tests $\mathtt{T}$ we have the tables:

t	$(\![a.\bot]\!)$	$(\![b.\bot]\!)$	$(\![a.\bot, b.\bot]\!)$
$\mathsf{R_{glb}}(G_3)$	0	0	0
$\mathsf{R_{glb}}(G_4)$	1	0	0
$\mathsf{R_{glb}}(G_5)$	1	0	0
$\mathsf{R_{glb}}(G_6)$	1	1	1

t	$(\![a.\bot]\!)$	$(\![b.\bot]\!)$	$(\![a\bot, b.\bot]\!)$
$\mathsf{R_{lub}}(G_3)$	1	0	0
$\mathsf{R_{lub}}(G_4)$	1	0	0
$\mathsf{R_{lub}}(G_5)$	1	1	1
$\mathsf{R_{lub}}(G_6)$	1	1	1

and therefore $G_3 \sqsubseteq^{\mathsf{glb}} G_4 \overset{\mathrm{glb}}{\eqsim} G_5 \sqsubseteq^{\mathsf{glb}} G_6$ and $G_3 \overset{\mathrm{lub}}{\eqsim} G_4 \sqsubseteq^{\mathsf{lub}} G_5 \overset{\mathrm{lub}}{\eqsim} G_6$. This gives $G_3 \sqsubseteq^{\mathsf{r}} G_4 \sqsubseteq^{\mathsf{r}} G_5 \sqsubseteq^{\mathsf{r}} G_6$, and so "more deterministic" processes are further up the ordering.

To further illustrate this point, consider the reactive processes given in Figure 4.12, where again we remove the probabilities since all transitions occur with probability 1.

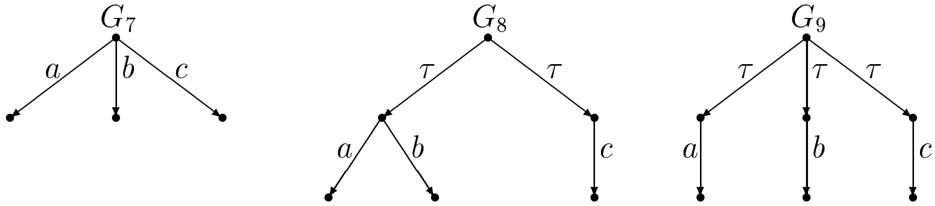


Figure 4.12: Example of the ordering $\sqsubseteq^{\mathsf{r}}$.

Then for the processes G_7, G_8 and G_9 we have:

t	$(\!|[a.\bot]|\!)$	$(\!|[b.\bot]|\!)$	$(\!|[c.\bot]|\!)$	$(\!|[a.\bot, b.\bot]|\!)$	$(\!|[a.\bot, c.\bot]|\!)$	$(\!|[b.\bot, c.\bot]|\!)$	$(\!|[a.\bot, b.\bot, c.\bot]|\!)$
$\mathsf{R}_{\mathbf{glb}}(G_7)$	1	1	1	1	1	1	1
$\mathsf{R}_{\mathbf{glb}}(G_8)$	0	0	0	0	0	0	0
$\mathsf{R}_{\mathbf{glb}}(G_9)$	0	0	0	0	0	0	0
$\mathsf{R}_{\mathbf{lub}}(G_7)$	1	1	1	1	1	1	1
$\mathsf{R}_{\mathbf{lub}}(G_8)$	1	1	1	1	0	0	0
$\mathsf{R}_{\mathbf{lub}}(G_9)$	1	1	1	0	0	0	0

and hence $G_9 \sqsubseteq^{\mathsf{r}} G_8 \sqsubseteq^{\mathsf{r}} G_7$.

As for the deterministic and non-deterministic case, we now introduce the composition of tests, which we do for both $\mathtt{T}$ and $\mathtt{T}_\omega$.

Definition 4.5.9 *If $(\!|r|\!) \in \mathtt{T}$, put $r \,\|\, \bot = \bot \,\|\, r = r$, and if $(\!|r_1|\!), (\!|r_2|\!) \in \mathtt{T}$ are such that $r_1 = [a_1.T_1, \ldots, a_m.T_m]$, $r_2 = [a'_1.T'_1, \ldots, a'_m.T'_{m'}]$, and r_1 and r_2 are independent, put*

$$r_1 \,\|\, r_2 = [a_1.T_1, \ldots, a_m.T_m, a'_1.T'_1, \ldots, a'_m.T'_{m'}].$$

Furthermore, if $T_1 = (t_1, \ldots, t_m) \in \mathtt{T}_\omega$ and $T_2 = (t'_1, \ldots, t'_{m'}) \in \mathtt{T}_\omega$ such that T_1 and T_2 are independent, put:

$$T_1 \,\|\, T_2 = (t_1, \ldots, t_m, t'_1, \ldots, t'_{m'}).$$

Lemma 4.5.10 *If $(\!|r_1|\!), (\!|r_2|\!) \in \mathtt{T}$ and $r_1 \,\|\, r_2$ is defined, then $(\!|r_1 \,\|\, r_2|\!) \in \mathtt{T}$ and for all $S \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathcal{R}))$: $\mathsf{R}_*(S)(r_1 \,\|\, r_2) = \mathsf{R}_*(S)(r_1) \cdot \mathsf{R}_*(S)(r_2)$.*

Lemma 4.5.11 *If $T_1, T_2 \in \mathtt{T}_\omega$ and $T_1 \,\|\, T_2$ is defined, then $T_1 \,\|\, T_2 \in \mathtt{T}_\omega$ and for all $E \in \mathcal{R}$: $\mathsf{R}_*(E)(T_1 \,\|\, T_2) = \mathsf{R}_*(E)(T_1) \cdot \mathsf{R}_*(E)(T_2)$.*

4.6 Comparisons with Alternative Equivalences

We first relate our ordering to the classical equivalences over labelled transition systems, that is, non-probabilistic processes. We accomplish this by restricting any reactive probabilistic transition system $(\mathcal{R}, \mathcal{A}ct, \rightarrow)$ so that all transitions occur with probability one, that is in the definition of our transition relation $\rightarrow$ we restrict the set of probability distributions $\mu(\mathcal{R})$ to the set of point distributions over $\mathcal{R}$ (see Definition 3.2.2): that is the set $\{\eta_E \mid E \in \mathcal{R}\}$. This then yields a transition system equivalent to a labelled transition system of the form $(S, \mathcal{A}ct \cup \{\tau\}, \longrightarrow)$ where τ denotes internal choice, with the following restrictions on all $P \in S$:

$$\begin{array}{ll} (i) & P \xrightarrow{\tau} \text{ if and only if } P \not\xrightarrow{a} \text{ for all } a \in \mathcal{A}ct \\ (ii) & \text{if } P \xrightarrow{a} P' \text{ and } P \xrightarrow{a} P'' \text{ then } P' = P''. \end{array}$$

Considering our maps $\mathsf{R}_{\mathbf{glb}}$ and $\mathsf{R}_{\mathbf{lub}}$ under the above restriction, it is straightforward to show that their type is now $\mathsf{R}_{\mathbf{glb}}, \mathsf{R}_{\mathbf{lub}} : S \rightarrow (\mathtt{T}_\omega \rightarrow \{0,1\})$ (the two-valued set).

As usual, since such a labelled transition system $(S, \mathcal{A}ct \cup \{\tau\}, \longrightarrow)$ allows τ moves, we generalise transition relation as follows:

Definition 4.6.1 *For any $P, Q \in S$ and $a \in \mathcal{A}ct$, $P \stackrel{a}{\Longrightarrow} Q$, if $P(\xrightarrow{\tau})^* \xrightarrow{a} (\xrightarrow{\tau})^* Q$.*

Using this new transition relation we reach the following proposition.

Proposition 4.6.2 *For all $P \in S$, $\sigma = a_1 \ldots a_n \in A^*$ and $X = \{b_1, \ldots, b_m\} \subseteq \mathcal{A}ct$, if $r = [a_1.(\!| \ldots (\!|[a_n.\bot]|\!) \ldots |\!)]$, $r' = [a_1.(\!| \ldots (\!|[a_n.((\!|[b_1.\bot, \ldots, b_m.\bot]|\!))]|\!) \ldots |\!)]$ and $r'' = [a_1.(\!| \ldots (\!|[a_n.((\!|[b_1.\bot]|\!), \ldots, (\!|[b_m.\bot]|\!))]|\!) \ldots |\!)]$, then:*

1. *$\sigma \in traces(P)$ if and only if $\mathsf{R}_{\mathbf{lub}}(P)((\!|r|\!)) = 1$.*

2. *there exists $Q \in S$ such that $P \stackrel{\sigma}{\Longrightarrow} Q$ and $X \setminus initials(Q) \neq \emptyset$ if and only if $\mathsf{R}_{\mathbf{lub}}(P)((\!|r|\!)) = 1$ and $\min\{\mathsf{R}_{\mathbf{lub}}(P)((\!|r'|\!)), \mathsf{R}_{\mathbf{lub}}(P)((\!|r''|\!))\} = 0$.*

3. *there exists $Q \in S$ such that $P \stackrel{\sigma}{\Longrightarrow} Q$ and $X \subseteq initials(Q)$ if and only if $\max\{\mathsf{R}_{\mathbf{lub}}(P)((\!|r'|\!)), \mathsf{R}_{\mathbf{lub}}(P)((\!|r''|\!))\} = 1$.*

Proof. The proof follows by induction on $\sigma \in A^*$. □

Now comparing the third part of Proposition 4.6.2 with Hennessy's *acceptance sets* [Hen85], for any $P \in S$ (using the notation from Proposition 4.6.2) the set:

$$\{(\sigma, X) \mid (\sigma, X) \in \mathcal{A}ct^* \times \mathcal{P}_f(\mathcal{A}ct) \text{ and } \max\{\mathsf{R}_{\mathbf{lub}}(P)((\!|r'|\!)) = 1, \mathsf{R}_{\mathbf{lub}}(P)((\!|r''|\!))\} = 1\}$$

corresponds to the acceptance sets of P.

Next, we compare our equivalence with the classical equivalences of CSP, namely trace, failure and ready equivalences (see Section 3.4) over such labelled transition systems. However, we must first define these equivalences for transition systems allowing τ moves, which we accomplish by replacing the usual transition relation $\longrightarrow$ with the transition relation $\Longrightarrow$ (see Definition 4.6.1) throughout the definitions in Section 3.4.

Now, using Proposition 4.6.2, the definition of $\stackrel{r}{\sim}$ and of trace equivalence, it follows that for any $P, Q \in S$, if $P \stackrel{r}{\sim} Q$ then P and Q are trace equivalent. Furthermore, when restricted to only *deterministic* processes it is straightforward to show, using Proposition 4.6.2, that for any $P, Q \in S$ if $P \stackrel{r}{\sim} Q$, then P and Q are also failure and ready equivalent. However, in general this result does not hold, to illustrate this consider the processes given in Figure 4.13 below.

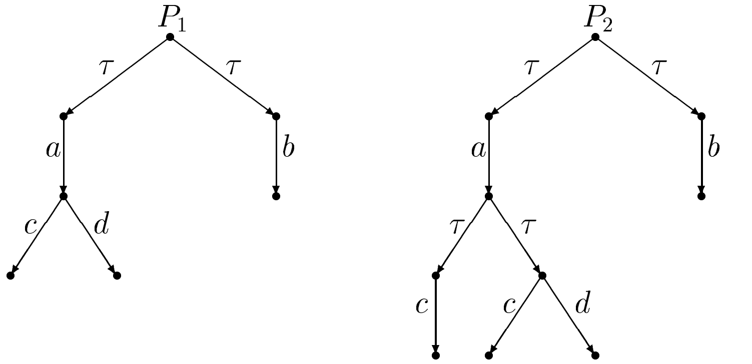


Figure 4.13: Example of processes that our equivalence cannot distinguish.

Then calculating the tables for P_1 and P_2 we have:

t	$\llparenthesis[a.\bot]\rrparenthesis$	$\llparenthesis[b.\bot]\rrparenthesis$	$\llparenthesis[a.\llparenthesis[c.\bot]\rrparenthesis]\rrparenthesis$	$\llparenthesis[a.\llparenthesis[d.\bot]\rrparenthesis]\rrparenthesis$	$\llparenthesis[a.\llparenthesis[c.\bot, d.\bot]\rrparenthesis]\rrparenthesis$
$\mathsf{R_{lub}}(P_1)$	1	1	1	1	1
$\mathsf{R_{lub}}(P_2)$	1	1	1	1	1

and $\mathsf{R_{glb}}(P_2)(t) = \mathsf{R_{glb}}(P_2)(t) = 0$ for all $t \neq \bot$, and hence $P_1 \stackrel{r}{\sim} P_2$. However, P_1 and P_2 are neither failure nor ready equivalent, since for example:

$$(a, \{c\}) \in readies(P_2) \setminus readies(P_1) \quad \text{and} \quad (a, \{d\}) \in failures(P_1) \setminus failures(P_2).$$

Furthermore, if we consider the processes Q_1 and Q_2 given in Figure 4.14 below.

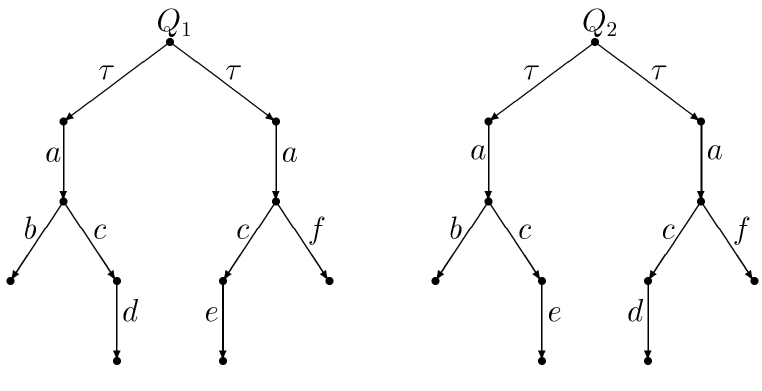


Figure 4.14: Example of processes that failures and readies cannot distinguish.

It is straight forward to show that these processes are failure and ready equivalent, for example, the set of readies of Q_1 and of Q_2 is:

$$\{(\langle\rangle, \{a\}), (a, \{b, c\}), (a, \{c, f\}), (ab, \emptyset), (ac, \{d\}), (ac, \{e\}), (af, \emptyset), (acd, \emptyset), (ace, \emptyset)\}.$$

However, if we consider the test $t = (\![[a.(\![[b.\bot, c.(\![[d.\bot]]\!)]]\!)]]\!)$, then $\mathsf{R}_{\mathsf{lub}}(Q_1)(t) = 1 \neq 0 = \mathsf{R}_{\mathsf{lub}}(Q_2)(t)$, and hence $\overset{\mathsf{r}}{\sim}$ distinguishes between the processes. Putting these results together, clearly our equivalence is distinct from both failure and ready equivalence defined over non-probabilistic processes.

On the other hand, for CCS type equivalences it is straightforward to show that our equivalence is weaker than bisimulation ($\overset{\mathsf{b}}{\sim}$) and distinct from simulation ($\overset{\mathsf{s}}{\sim}$). Intuitively, our equivalence $\overset{\mathsf{r}}{\sim}$ is coarser than both bisimulation and simulation equivalences, as $\overset{\mathsf{r}}{\sim}$ is based on the behaviour of *one run* of a processes, possibly under different conditions (that is, changes in the environment), whereas both bisimulation and simulation equivalences are based on the the *total* behaviour of processes. This is accomplished by an inductive definition, for example see the definition of bisimulation given in Chapter 2. To illustrate this fact consider the processes given in Figure 4.15 below, where all choices are internal.

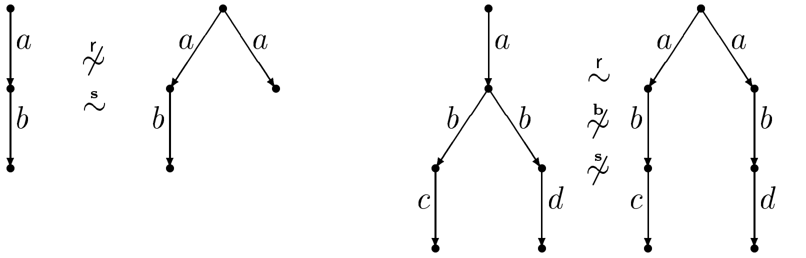


Figure 4.15: Example of non-probabilistic processes.

As for other equivalences on probabilistic processes, it is straight forward to show $\stackrel{\mathsf{r}}{\sim}$ is finer than the equivalences of Seidel [Sei92], Lowe [Low] and Jou and Smolka [JS90] for probabilistic processes, all of which are based on these classical equivalences. To illustrate this, if we recall the processes in Figure 2.3, which we have shown not to be distinguishable by the equivalences of [Sei92, Low] and [JS90], it can be shown that for the test $\llparenthesis a.(\llparenthesis b.\llparenthesis d.\bot\rrparenthesis\rrparenthesis, \llparenthesis c.\llparenthesis e.\bot\rrparenthesis\rrparenthesis)\rrparenthesis$ our equivalence $\stackrel{\mathsf{r}}{\sim}$ distinguishes these processes.

Also, as mentioned in Subsection 4.3.1, probabilistic bisimulation is finer than $\stackrel{\mathsf{d}}{\sim}$ (on deterministic reactive systems) and it follows that the same holds true for $\stackrel{\mathsf{r}}{\sim}$. Furthermore, it is straightforward to show $\stackrel{\mathsf{r}}{\sim}$ is coarser than Segala and Lynch's probabilistic simulation [SL94] and Yi and Larsen's testing equivalence [YL92].

The last equivalence we compare $\stackrel{\mathsf{r}}{\sim}$ with is Morgan et al.'s equivalence over probabilistic processes [MMSS96], using as an example the processes of Figure 2.4 which are distinguished by the equivalence of [MMSS96]. It is easy to show that $\stackrel{\mathsf{r}}{\sim}$ does not distinguish these processes. However, since their equivalence is based on failure equivalence, which we have shown is distinct from $\stackrel{\mathsf{r}}{\sim}$ in the non-probabilistic setting, there will exist probabilistic processes which their equivalence will not distinguish but $\stackrel{\mathsf{r}}{\sim}$ will. Therefore, $\stackrel{\mathsf{r}}{\sim}$ is incomparable with the equivalence of [MMSS96].

Finally, we mention two other results relating to our testing scenario. First, when we restrict our model to only deterministic probabilistic transition systems and enrich our tests by allowing to test for termination and for the set of initial actions of a process, the resulting equivalence will correspond with our equivalence $\stackrel{\mathsf{d}}{\sim}$ over deterministic transition systems. This result appears interesting since, although in a different setting, both Lowe [Low] and Jou and Smolka [JS90] also define different equivalences which they then show to coincide.

Also, if we consider the equivalence derived from the map $\mathsf{R}_{\mathsf{lub}}$ and allow dependent tests in the construction of $\mathtt{T}$, the equivalence will coincide with branching simulation [Gla93] on non-probabilistic systems.

Chapter 5

The Process Calculus

In this chapter, we present a process calculus for reactive probabilistic processes, which we call RP, following the construction of the operational ordering $\sqsubseteq^{\mathsf{r}}$ over reactive probabilistic transition systems. We do this in the following four steps.

1. First we define the syntax of a purely probabilistic calculus $\mathrm{RP_p}$, that is, a calculus where the only form of choice is (action-guarded) probabilistic choice. We then present an operational semantics for $\mathrm{RP_p}$ in terms of a purely probabilistic transition system, and then investigate the properties of the ordering $\sqsubseteq^{\mathsf{p}}$ over this calculus.

2. We then extend $\mathrm{RP_p}$ by including an external choice operator to form the calculus $\mathrm{RP_d}$, and give this calculus an operational semantics by means of a deterministic probabilistic transition system and investigate the properties of the ordering $\sqsubseteq^{\mathsf{d}}$ over $\mathrm{RP_d}$.

3. Similarly to the above, we extend $\mathrm{RP_p}$ to form the calculus $\mathrm{RP_{nd}}$, where instead of allowing external choice we allow internal choice.

4. We then combine the above to obtain the calculus for arbitrary reactive probabilistic processes RP and give an operational semantics to this calculus by means of a reactive probabilistic transition system, and investigate the ordering $\sqsubseteq^{\mathsf{r}}$ over this calculus.

Intuitively, we can consider the above calculi as forming the following hierarchy:

$$\begin{tikzcd} & \mathrm{RP} & \\ \mathrm{RP_d} \arrow[ur] & & \mathrm{RP_{nd}} \arrow[ul] \\ & \mathrm{RP_p} \arrow[ul] \arrow[ur] & \end{tikzcd}$$

5.1 Preliminaries

In this section we introduce notation that we will use in the construction of our calculus and for investigating properties of our operational orderings over the calculus.

Definition 5.1.1 (Process Calculus Notation)

- *$\mathcal{A}ct$ is a (finite) set of actions (or labels) that processes can perform (ranged over by $a, b \ldots$) and, furthermore, we let B be any subset of $\mathcal{A}ct$.*
- *$\sum_{i \in I} \mu_i$ is a summation over a countable index set I, where $\mu_i \in (0,1]$ for all $i \in I$ and $\sum_{i \in I} \mu_i = 1$.*
- *$\mathcal{X}$ is the set of process variables (ranged over by $x, y \ldots$).*
- *λ is a relabelling function, that is, a function from $\mathcal{A}ct$ to $\mathcal{A}ct$; we also require that λ is bijective.*

When discussing to our operational orderings we will require the notion of an action a being in a test t, written $a \in t$. Intuitively, a is in the test t if t's corresponding button pushing experiment involves, at some stage, pressing the a–button. More formally, we can define this by induction on tests, for example, for the set of tests $\mathtt{T}^{\mathrm{d}}$ (see Definition 4.3.1) and for any $a \in \mathcal{A}ct$: $a \notin \perp$ and $a \in a'.(t_1, \ldots, t_m)$ if $a = a'$, or $a \in t_i$ for some $1 \leq i \leq m$.

Furthermore, we will need to extend any relabelling function $\lambda : \mathcal{A}ct \to \mathcal{A}ct$ to a function on our testing languages. Again, this can be done easily by induction on tests, where for the testing language $\mathtt{T}^{\mathrm{d}}$ we define the extended map $\lambda : \mathtt{T}^{\mathrm{d}} \to \mathtt{T}^{\mathrm{d}}$ by putting: $\lambda(\perp) \stackrel{def}{=} \perp$ and $\lambda(a.(t_1, \ldots, t_m)) \stackrel{def}{=} \lambda(a).(\lambda(t_1), \ldots, \lambda(t_m))$.

5.2 Purely Probabilistic Processes

As described above, in this section we consider a purely probabilistic process calculus called $\mathrm{RP_p}$, where the only form of choice is action-guarded probabilistic choice. The syntax, however, also includes (full synchronous) parallel composition and recursion.

Definition 5.2.1 *The set of* $\mathrm{RP_p}$ *expressions is given by the syntax:*

$$F ::= \; x \mid \mathbf{0} \mid a.\textstyle\sum_{i \in I} \mu_i.F_i \mid F_1 \parallel F_2 \mid F \upharpoonright B \mid F\,[\lambda] \mid \mathit{fix}_x.F.$$

As usual, "$\mathbf{0}$" denotes the inactive process, "$F_1 \,\|\, F_2$" denotes parallel composition, "$F \lceil B$" denotes restriction, "$F\,[\lambda]$" denotes relabelling and "$\mathit{fix}_x.F$" denotes recursion. Furthermore, "$a.\sum_{i\in I}\mu_i.F_i$" denotes action-guarded probabilistic choice. Observe that prefixing is a special case of probabilistic choice: $a \to F$ and $a.F$ (prefixing in CSP and CCS notation respectively) are equivalent to $a.1.F$, meaning after a is performed the process becomes F with probability 1.

The above syntax allows variables to occur freely in expressions. However, as usual, we will only consider guarded and closed expressions as terms of our calculus. Formally, we have the following definitions.

Definition 5.2.2 *A variable $x \in \mathcal{X}$ is* bound *in any expression $F \in \mathrm{RP_p}$ if and only if every occurrence of x in F occurs within the scope of a subexpression of F of the form $\mathit{fix}_x.F'$. If x is not bound in F then we say x is* free *in F.*

Definition 5.2.3 *A variable $x \in \mathcal{X}$ is* guarded *in an expression $F \in \mathrm{RP_p}$ if any occurrence of the variable x in G lies within a subexpression of the form $\sum_{i\in I} a_{\mu_i}.G_i$. Furthermore, we denote the set of guarded expressions of $\mathrm{RP_p}$ by $\mathcal{G}^{\mathrm{p}}$, that is, the set expressions without unguarded variables.*

Definition 5.2.4 *A* closed *expression or* process *is a term without free or unguarded variables. We denote the set of processes of $\mathrm{RP_p}$ by $\mathrm{Pr^p}$.*

5.2.1 Operational Semantics

We now give operational semantics for the set of processes of $\mathrm{RP_p}$, based on reactive probabilistic transition systems. Since the states of a purely probabilistic transition system $(\mathcal{R}^{\mathrm{p}}, \mathcal{A}ct, \to)$ can be considered as elements of $(\mathcal{A}ct \times \mu(\mathcal{R}^{\mathrm{p}})) \cup \{\emptyset\}$, we map an element of $\mathrm{Pr^p}$ into an element of $(\mathcal{A}ct \times \mu(\mathrm{Pr^p})) \cup \{\emptyset\}$ as follows.

1. $\mathcal{O}[\![\mathbf{0}]\!] = \emptyset$.
2. $\mathcal{O}[\![a.\sum_{i\in I}\mu_i.F_i]\!] = (a, \pi)$ such that $\pi(F) \overset{def}{=} \sum\limits_{\substack{i\in I\,\&\\ F_i = F}} \mu_i$ for any $F \in \mathrm{Pr^p}$.
3. $\mathcal{O}[\![E_1 \,\|\, E_2]\!] = (a, \pi)$, if $\mathcal{O}[\![E_1]\!] = (a, \pi_1)$ and $\mathcal{O}[\![E_2]\!] = (a, \pi_2)$ for some $\pi_1, \pi_2 \in \mu(\mathrm{Pr^p})$ such that for any $F \in \mathrm{Pr^p}$:
$$\pi(F) \overset{def}{=} \begin{cases} \pi_1(F_1)\cdot\pi_2(F_2) & \text{if } F = F_1 \,\|\, F_2 \\ 0 & \text{otherwise} \end{cases}$$
and $\mathcal{O}[\![E_1 \,\|\, E_2]\!] = \emptyset$ otherwise.

4. $\mathcal{O}[\![E \upharpoonright B]\!] = (a, \pi)$, if $\mathcal{O}[\![E]\!] = (a, \pi')$ for some $\pi' \in \mu(\mathrm{Pr}^{\mathrm{p}})$ such that $a \in B$ and for any $F \in \mathrm{Pr}^{\mathrm{p}}$:
$$\pi(F) \stackrel{def}{=} \begin{cases} \pi'(F') & \text{if } F = F' \upharpoonright B \\ 0 & \text{otherwise} \end{cases}$$
and $\mathcal{O}[\![E \upharpoonright B]\!] = \emptyset$ otherwise.

5. $\mathcal{O}[\![E\,[\lambda]]\!] = (a, \pi)$, if $\mathcal{O}[\![E]\!] = (b, \pi')$ for some $\pi' \in \mu(\mathrm{Pr}^{\mathrm{p}})$ such that $\lambda(b) = a$ and for any $F \in \mathrm{Pr}^{\mathrm{p}}$:
$$\pi(F) \stackrel{def}{=} \begin{cases} \pi'(F') & \text{if } F = F'\,[\lambda] \\ 0 & \text{otherwise.} \end{cases}$$
and $\mathcal{O}[\![E\,[\lambda]]\!] = \emptyset$ otherwise.

6. $\mathcal{O}[\![\mathit{fix}_x.E]\!] = \mathcal{O}[\![E\{\mathit{fix}_x.E/x\}]\!]$ where $E\{F/x\}$ denotes the result of changing all free occurrences of x in E by F, with change of bound variables to avoid clashes.

The following proposition shows the semantics to be well defined.

Proposition 5.2.5 *For all $E \in \mathrm{Pr}^{\mathrm{p}}$, either $\mathcal{O}[\![E]\!] = \emptyset$ or $\mathcal{O}[\![E]\!] = (a, \pi)$ for some $a \in \mathcal{A}ct$ and $\pi \in \mu(\mathrm{Pr}^{\mathrm{p}})$, that is, π is a probability distribution on the set of processes of* $\mathrm{RP_p}$.

Proof. The proof is by induction on the structure of $E \in \mathrm{Pr}^{\mathrm{p}}$.

1. If $E = \mathbf{0}$, then $\mathcal{O}[\![E]\!] = \emptyset$.

2. If $E = a.\sum_{i \in I} \mu_i.F_i$, then $\mathcal{O}[\![E]\!] = (a, \pi)$ where by definition of the transition rules:
$$\begin{aligned} \sum_{F \in \mathrm{Pr}^{\mathrm{p}}} \pi(F) &= \sum_{F \in \mathrm{Pr}^{\mathrm{p}}} \left(\sum_{\substack{i \in I \,\&\\ F_i = F}} \mu_i \right) \\ &= \sum_{i \in I} \mu_i && \text{since } F_i \in \mathrm{Pr}^{\mathrm{p}} \text{ for all } i \in I \\ &= 1 && \text{by Definition 5.1.1} \end{aligned}$$
and thus $\pi \in \mu(\mathrm{Pr}^{\mathrm{p}})$.

3. If $E = E_1 \parallel E_2$, then either $\mathcal{O}[\![E]\!] = \emptyset$, or $\mathcal{O}[\![E]\!] = (a, \pi)$ for some $a \in \mathcal{A}ct$ such that $\mathcal{O}[\![E_1]\!] = (a, \pi_1)$ and $\mathcal{O}[\![E_2]\!] = (a, \pi_2)$, and by induction $\pi_i \in \mu(\mathrm{Pr}^{\mathrm{p}})$ for

$i \in \{1, 2\}$. In the second case by definition of the transition rules:

$$\begin{aligned}
\sum_{F \in \mathrm{Pr}^{\mathrm{p}}} \pi(F) &= \sum_{F_1 \,\|\, F_2 \in \mathrm{Pr}^{\mathrm{p}}} \pi_1(F_1) \cdot \pi_2(F_2) \\
&= \left(\sum_{F_1 \in \mathrm{Pr}^{\mathrm{p}}} \pi_1(F_1) \right) \cdot \left(\sum_{F_2 \in \mathrm{Pr}^{\mathrm{p}}} \pi_2(F_2) \right) && \text{rearranging} \\
&= 1 && \text{by induction}
\end{aligned}$$

and hence $\pi \in \mu(\mathrm{Pr}^{\mathrm{p}})$.

4. If $E = E' \lceil B$ or $E = E'\,[\lambda]$, the result follows by induction on E' and the transition rules.

5. If $E = \mathit{fix}_x.E'$, then $\mathcal{O}[\![E]\!] = \mathcal{O}[\![E'\{\mathit{fix}_x.E'/x\}]\!]$ and the result follows by induction on $E' \in \mathcal{G}^{\mathrm{p}}$.

□

5.2.2 RP_{p} and the ordering $\sqsubseteq^{\mathsf{P}}$

Using the operational semantics defined above, we now relate the ordering $\sqsubseteq^{\mathsf{P}}$ to RP_{p}. We first investigate the properties of the map P with respect to the processes Pr^{p} and semantic operators of RP_{p}. Since it follows from Proposition 5.2.5 that, for all $E \in \mathrm{Pr}^{\mathrm{p}}$ and $t \in \mathtt{T}^{\mathrm{p}}$, we can calculate $\mathsf{P}(\mathcal{O}[\![E]\!])(t)$, the ordering $\sqsubseteq^{\mathsf{P}}$ will be well defined on the set $\{\mathcal{O}[\![E]\!] \mid E \in \mathrm{Pr}^{\mathrm{p}}\}$. As usual we extend the ordering $\sqsubseteq^{\mathsf{P}}$ to all guarded expressions by means of the following definition.

Definition 5.2.6 *For all $F, G \in \mathcal{G}^{\mathrm{p}}$, $\mathcal{O}[\![F]\!] \sqsubseteq^{\mathsf{P}} \mathcal{O}[\![G]\!]$ if and only if $\mathcal{O}[\![F\{\tilde{E}/\tilde{x}\}]\!] \sqsubseteq^{\mathsf{P}} \mathcal{O}[\![G\{\tilde{E}/\tilde{x}\}]\!]$ for all $\tilde{E} \subseteq \mathrm{Pr}^{\mathrm{p}}$, where the free variables of F and G are contained in the vector of variables $\tilde{x}$.*

With the help of the above definition, all results for the set of processes of RP_{p} will also hold for the guarded terms of RP_{p}, and hence for the remainder of this chapter we will only prove results with respect to processes. Moreover, to simplify notation, we will denote expressions of the form $\mathsf{P}(\mathcal{O}[\![E]\!])$ by $\mathsf{P}(E)$ for any $E \in \mathrm{Pr}^{\mathrm{p}}$, and repeat this notation when we extend the calculus RP_{p} and consider the maps D, N_* and R_*.

Lemma 5.2.7 *For all $E_1, E_2 \in \mathrm{Pr}^{\mathrm{p}}$ and $t \in \mathtt{T}^{\mathrm{p}}$: $\mathsf{P}(E_1 \,\|\, E_2)(t) = \mathsf{P}(E_1)(t) \cdot \mathsf{P}(E_2)(t)$.*

Proof. The proof is by induction on $t \in \mathtt{T}^{\mathrm{p}}$. If $t = \bot$, then by definition of P for all $E_1, E_2 \in \mathrm{Pr}^{\mathrm{p}}$: $\mathsf{P}(E_1 \,\|\, E_2)(\bot) = 1 = 1 \cdot 1 = \mathsf{P}(E_1)(\bot) \cdot \mathsf{P}(E_2)(\bot)$.

If $t = a.t'$ for some $a \in \mathcal{A}ct$, then for any $E_1 \,\|\, E_2 \in \mathrm{Pr}^{\mathrm{p}}$ we have the following two cases to consider.

1. $\mathcal{O}[\![E_1 \,\|\, E_2]\!] = (a, \pi)$ for some $\pi \in \mu(\mathrm{Pr}^{\mathrm{p}})$, and hence by definition of the transition rules, $\mathcal{O}[\![E_1]\!] = (a, \pi_1)$ and $\mathcal{O}[\![E_2]\!] = (a, \pi_2)$ for some $\pi_1, \pi_2 \in \mu(\mathrm{Pr}^{\mathrm{p}})$, and by definition of P and the transition rules:

$$\begin{aligned}
&\mathsf{P}(E_1 \,\|\, E_2)(a.t') = \sum_{F_1 \,\|\, F_2 \in \mathrm{Pr}^{\mathrm{p}}} \Big(\pi_1(F_1) \cdot \pi_2(F_2)\Big) \cdot \mathsf{P}(F_1 \,\|\, F_2)(t') \\
&= \sum_{F_1 \,\|\, F_2 \in \mathrm{Pr}^{\mathrm{p}}} \Big(\pi_1(F_1) \cdot \pi_2(F_2)\Big) \cdot \Big(\mathsf{P}(F_1)(t') \cdot \mathsf{P}(F_2)(t')\Big) && \text{by induction} \\
&= \left(\sum_{F_1 \in \mathrm{Pr}^{\mathrm{p}}} \pi_1(F_1) \cdot \mathsf{P}(F_1)(t')\right) \cdot \left(\sum_{F_2 \in \mathrm{Pr}^{\mathrm{p}}} \pi_2(F_2) \cdot \mathsf{P}(F_2)(t')\right) && \text{rearranging} \\
&= \mathsf{P}(E_1)(a.t') \cdot \mathsf{P}(E_2)(a.t') && \text{by definition of } \mathsf{P}.
\end{aligned}$$

2. $\mathcal{O}[\![E_1 \,\|\, E_2]\!] \neq (a, \pi)$ for any $\pi \in \mu(\mathrm{Pr}^{\mathrm{p}})$, then without loss of generality we can suppose $\mathcal{O}[\![E_1]\!] \neq (a, \pi)$ for any $\pi \in \mu(\mathrm{Pr}^{\mathrm{p}})$, and therefore by definition of P:

$$\mathsf{P}(E_1 \,\|\, E_2)(t) = 0 = 0 \cdot \mathsf{P}(E_2)(t) = \mathsf{P}(E_1)(t) \cdot \mathsf{P}(E_2)(t).$$

Since these are the only possible cases, the lemma is proved by induction on $t \in \mathtt{T}^{\mathrm{p}}$. □

Lemma 5.2.8 *For all $E \in \mathrm{Pr}^{\mathrm{p}}$, $t \in \mathtt{T}^{\mathrm{p}}$ and $B \subseteq \mathcal{A}ct$:*

$$\mathsf{P}(E \upharpoonright B)(t) = \begin{cases} 0 & \textit{if } a \in t \textit{ for any } a \in \mathcal{A}ct \setminus B \\ \mathsf{P}(E)(t) & \textit{otherwise.} \end{cases}$$

Proof. We prove the lemma by induction on $t \in \mathtt{T}^{\mathrm{p}}$. If $t = \bot$, the lemma holds by definition of P and since $a \notin \bot$ for any $a \in \mathcal{A}ct$.

If $E \upharpoonright B \in \mathrm{Pr}^{\mathrm{p}}$ and $t = a.t'$ for some $a \in \mathcal{A}ct$, then if $a' \notin t$ for all $a' \in \mathcal{A}ct \setminus B$ by definition of P and the transition rules:

$$\mathsf{P}(E \upharpoonright B)(a.t') = \begin{cases} \sum_{F \in \mathrm{Pr}^{\mathrm{p}}} \pi(F) \cdot \mathsf{P}(F \upharpoonright B)(t') & \text{if } \mathcal{O}[\![E]\!] = (a, \pi) \text{ for some } \pi \in \mu(\mathrm{Pr}^{\mathrm{p}}) \\ 0 & \text{otherwise} \end{cases}$$

$$= \begin{cases} \sum_{F \restriction B \in \mathrm{Pr}^{\mathrm{p}}} \pi(F) \cdot \mathsf{P}(F)(t') & \text{if } \mathcal{O}[\![E]\!] = (a, \pi) \text{ for some } \pi \in \mu(\mathrm{Pr}^{\mathrm{p}}) \\ 0 & \text{otherwise} \end{cases} \qquad \text{by induction}$$

$$= \begin{cases} \sum_{F \in \mathrm{Pr}^{\mathrm{p}}} \pi(F) \cdot \mathsf{P}(F)(t') & \text{if } \mathcal{O}[\![E]\!] = (a, \pi) \text{ for some } \pi \in \mu(\mathrm{Pr}^{\mathrm{p}}) \\ 0 & \text{otherwise} \end{cases} \qquad \text{rearranging}$$

$$= \mathsf{P}(E)(a.t') \qquad \text{by definition of } \mathsf{P}.$$

On the other hand, if $a' \in a.t'$ for some $a' \in \mathcal{A}ct \setminus B$, we have the following two cases to consider.

1. $a = a'$, then by definition of the transition rules, $\mathcal{O}[\![E \restriction B]\!] \neq (a, \pi)$ for any $\pi \in \mu(\mathrm{Pr}^{\mathrm{p}})$ and therefore by definition of P: $\mathsf{P}(E \restriction B)(a.t') = 0$.
2. $a \neq a'$ and $a' \in t'$, then by definition of P and the transition rules:

$$\mathsf{P}(E \restriction B)(a.t') = \begin{cases} \sum_{F \in \mathrm{Pr}^{\mathrm{p}}} \pi(F) \cdot \mathsf{P}(F \restriction B)(t') & \text{if } \mathcal{O}[\![E]\!] = (a, \pi) \text{ for some } \pi \in \mu(\mathrm{Pr}^{\mathrm{p}}) \\ 0 & \text{otherwise} \end{cases}$$

$$= \begin{cases} \sum_{F \in \mathrm{Pr}^{\mathrm{p}}} \pi(F) \cdot 0 & \text{if } \mathcal{O}[\![E]\!] = (a, \pi) \text{ for some } \pi \in \mu(\mathrm{Pr}^{\mathrm{p}}) \\ 0 & \text{otherwise} \end{cases} \qquad \text{by induction}$$

$$= 0.$$

Since these are all the possible cases the lemma holds by induction. $\square$

Lemma 5.2.9 *For all $E \in \mathrm{Pr}^{\mathrm{p}}$, λ and $t \in \mathtt{T}^{\mathrm{p}}$: $\mathsf{P}(E\,[\lambda])(t) = \mathsf{P}(E)(\lambda^{-1}(t))$.*

Proof. The proof is by induction on $t \in \mathtt{T}^{\mathrm{p}}$. The case when $t = \perp$ is trivial as $\lambda^{-1}(\perp) = \perp$.

If $t = a.t'$ for some $a \in \mathcal{A}ct$ and $E\,[\lambda] \in \mathrm{Pr}^{\mathrm{p}}$, then by definition of P and the transition rules $\mathsf{P}(E\,[\lambda])(a.t')$ equals:

$$= \begin{cases} \sum_{F \in \mathrm{Pr}^{\mathrm{p}}} \pi(F) \cdot \mathsf{P}(F\,[\lambda])(t') & \text{if } \mathcal{O}[\![E]\!] = (\lambda^{-1}(a), \pi) \text{ for some } \pi \in \mu(\mathrm{Pr}^{\mathrm{p}}) \\ 0 & \text{otherwise} \end{cases}$$

$$= \begin{cases} \sum_{F \in \mathrm{Pr}^{\mathrm{p}}} \pi(F) \cdot \mathsf{P}(F)(\lambda^{-1}(t')) & \text{if } \mathcal{O}[\![E]\!] = (\lambda^{-1}(a), \pi) \text{ for some } \pi \in \mu(\mathrm{Pr}^{\mathrm{p}}) \\ 0 & \text{otherwise} \end{cases}$$

by induction

$$= \mathsf{P}(E)(\lambda^{-1}(a).\lambda^{-1}(t')) \quad \text{by definition of } \mathsf{P}$$
$$= \mathsf{P}(E)(\lambda^{-1}(a.t')) \quad \text{by definition of } \lambda \text{ on } \mathtt{T}^{\mathrm{p}}$$

and thus the lemma holds by induction on $n \in \mathbb{N}$. □

Lemma 5.2.10 *If $G \in \mathcal{G}^{\mathrm{p}}$ such that $G\{E/x\} \in \mathrm{Pr}^{\mathrm{p}}$ for all $E \in \mathrm{Pr}^{\mathrm{p}}$, then either $\mathcal{O}[\![G\{E/x\}]\!] = \emptyset$ for all $E \in \mathrm{Pr}^{\mathrm{p}}$, or there exists $a \in \mathcal{A}ct$ and $\pi_G \in \mu(\mathrm{RP_p})$ such that for any $E \in \mathrm{Pr}^{\mathrm{p}}$, $\mathcal{O}[\![G\{E/x\}]\!] = (a, \pi)$ where for any $F \in \mathrm{Pr}^{\mathrm{p}}$:*

$$\pi(F) = \begin{cases} \pi_G(F') & \textit{if } F = F'\{E/x\} \textit{ for some } F' \in \mathrm{RP_p} \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. The proof follows by induction on the structure of $E \in \mathcal{G}^{\mathrm{p}}$ and the transition rules. □

Lemma 5.2.11 *For any $E \in \mathrm{RP_p}$ and $F, F' \in \mathrm{Pr}^{\mathrm{p}}$ such that $E\{F/x\}, E\{F'/x\} \in \mathrm{Pr}^{\mathrm{p}}$ and $\mathsf{P}(F)(t) \leq \mathsf{P}(F')(t)$ for all $t \in \mathtt{T}^{\mathrm{p}}$ then: $\mathsf{P}(E\{F/x\})(t) \leq \mathsf{P}(E\{F'/x\})(t)$ for all $t \in \mathtt{T}^{\mathrm{p}}$.*

Proof. Consider any $E \in \mathrm{RP_p}$ and $F, F' \in \mathrm{Pr}^{\mathrm{p}}$ such that $E\{F/x\}, E\{F'/x\} \in \mathrm{Pr}^{\mathrm{p}}$ and $\mathsf{P}(F)(t) \leq \mathsf{P}(F')(t)$ for all $t \in \mathtt{T}^{\mathrm{p}}$. We prove the lemma by induction on the structure of $E \in \mathcal{E}^{\mathrm{p}}$.

1. If $E \in \mathcal{X}$, then $E = x$ since $E\{F/x\} \in \mathrm{Pr}^{\mathrm{p}}$, and hence for any $t \in \mathtt{T}^{\mathrm{p}}$:

   $$\mathsf{P}(E\{F/x\})(t) = \mathsf{P}(F)(t) \leq \mathsf{P}(F')(t) = \mathsf{P}(E\{F'/x\})(t)$$

   by hypothesis.

2. If $E = a.\sum_{i \in I} \mu_i.E_i$ and $t \in \mathtt{T}^{\mathrm{p}}$, then

   $$E\{F/x\} = a.\sum_{i \in I} \mu_i.(E_i\{F/x\}) \quad \text{and} \quad E\{F'/x\} = a.\sum_{i \in I} \mu_i.(E_i\{F'/x\})$$

   and we have the following three cases to consider:

   (a) $t = \bot$, then by definition of P: $\mathsf{P}(E\{F/x\})(t) = 1 = \mathsf{P}(E\{F'/x\})(t)$.

   (b) $t = b.t'$ and $b \neq a$, then $\mathsf{P}(E\{F/x\})(t) = 0 = \mathsf{P}(E\{F'/x\})(t)$ by definition of the transition rules and P.

(c) $t = a.t'$, then by definition of P and the transition rules:

$$\begin{array}{rcll} \mathsf{P}(E\{F/x\})(a.t') & = & \sum_{i\in I} \mu_i \cdot \mathsf{P}(E_i\{F/x\})(t') & \\ & \leq & \sum_{i\in I} \mu_i \cdot \mathsf{P}(E_i\{F'/x\})(t') & \text{by induction} \\ & = & \mathsf{P}(E\{F'/x\})(a.t') & \text{by definition of } \mathsf{P} \text{ and} \\ & & & \text{the transition rules.} \end{array}$$

3. If $E = E_1 \parallel E_2$, $E = E' \upharpoonright B$ or $E = E'\,[\lambda]$, the result follows using induction, the above lemmas concerning these operators and P. For example if $E = E_1 \parallel E_2$, then for any $t \in \mathtt{T}^{\mathrm{p}}$, by definition:

$$\begin{array}{rcll} \mathsf{P}((E_1 \parallel E_2)\{F/x\})(t) & = & \mathsf{P}((E_1\{F/x\}) \parallel (E_2\{F/x\}))(t) & \\ & = & \mathsf{P}(E_1\{F/x\})(t) \cdot \mathsf{P}(E_2\{F/x\})(t) & \text{by Lemma 5.2.7} \\ & \leq & \mathsf{P}(E_1\{F'/x\})(t) \cdot \mathsf{P}(E_2\{F'/x\})(t) & \text{by induction} \\ & = & \mathsf{P}((E_1\{F'/x\}) \parallel (E_2\{F'/x\}))(t) & \text{by Lemma 5.2.7} \\ & = & \mathsf{P}((E_1 \parallel E_2)\{F'/x\})(t). & \end{array}$$

4. If $E = \mathit{fix}_y.E'$, then either $x = y$ in which case x is not free in E, therefore $E\{F/x\} = E\{F'/x\} = E$, and hence the lemma holds in this case, or $y \neq x$ in which case for any $t \in \mathtt{T}^{\mathrm{p}}$, since $x \neq y$ we have $\mathsf{P}(E\{F/x\})(t)$ is equal to:

$$\begin{array}{cll} = & \mathsf{P}(\mathit{fix}_y.(E'\{F/x\}))(t) & \\ = & \mathsf{P}(E'\{F/x\}\{\mathit{fix}_y.E'\{F/x\}/y\})(t) & \text{by the transition rules} \\ = & \mathsf{P}(E'\{F/x\}\{E\{F/x\}/y\})(t) & \text{by definition of } E \\ = & \mathsf{P}(E'\{E/y\}\{F/x\})(t) & \text{rearranging since } x \neq y \\ \leq & \mathsf{P}(E'\{E/y\}\{F'/x\})(t) & \text{by induction on } E'\{E/y\} \\ = & \mathsf{P}(E'\{F'/x\}\{E\{F'/x\}/y\})(t) & \text{rearranging since } x \neq y \\ = & \mathsf{P}(E'\{F'/x\}\{\mathit{fix}_y.E'\{F'/x\}/y\})(t) & \text{by definition of } E \\ = & \mathsf{P}(\mathit{fix}_y.(E'\{F'/x\}))(t) & \text{by the transition rules} \\ = & \mathsf{P}(E\{F'/x\})(t) & \text{since } x \neq y, \end{array}$$

as required.

□

Using the above lemmas we can now show that $\sqsubseteq^{\mathsf{p}}$ is a congruence over Pr^{p} by means of the following proposition.

Proposition 5.2.12 *The pre-order $\sqsubseteq^{\mathsf{p}}$ is preserved by all contexts in the language*

$\mathrm{RP_p}$. *Formally, if we have that* $\mathcal{O}[\![E_i]\!] \sqsubseteq^{\mathsf{p}} \mathcal{O}[\![F_i]\!]$ *for all* $i \in I$ *and* $\mathcal{O}[\![E]\!] \sqsubseteq^{\mathsf{p}} \mathcal{O}[\![F]\!]$, *then:*

$$\begin{array}{rcl}
\mathcal{O}[\![a.\sum_{i\in I}\mu_i.E_i]\!] & \sqsubseteq^{\mathsf{p}} & \mathcal{O}[\![a.\sum_{i\in I}\mu_i.F_i]\!] \\
\mathcal{O}[\![E \,\|\, G]\!] & \sqsubseteq^{\mathsf{p}} & \mathcal{O}[\![F \,\|\, G]\!] \\
\mathcal{O}[\![E \upharpoonright B]\!] & \sqsubseteq^{\mathsf{p}} & \mathcal{O}[\![F \upharpoonright B]\!] \\
\mathcal{O}[\![E\,[\lambda]]\!] & \sqsubseteq^{\mathsf{p}} & \mathcal{O}[\![F\,[\lambda]]\!] \\
\mathcal{O}[\![\mathit{fix}_x.E]\!] & \sqsubseteq^{\mathsf{p}} & \mathcal{O}[\![\mathit{fix}_x.F]\!].
\end{array}$$

Proof.

1. If $E' = a.\sum_{i\in I}\mu_i.E_i$ and $F' = a.\sum_{i\in I}\mu_i.F_i$, then $E' = (a,\pi)$ and $F' = (a,\pi')$ such that for any $G \in \mathrm{Pr}^{\mathrm{p}}$:

$$\pi(G) = \sum_{\substack{i\in I\,\&\\ G=E_i}} \mu_i \quad \text{and} \quad \pi'(G) = \sum_{\substack{i\in I\,\&\\ G=F_i}} \mu_i. \tag{5.1}$$

Considering any $t \in \mathtt{T}^{\mathrm{p}}$, either $t = \perp$ and by definition of P: $\mathsf{P}(E')(\perp) = \mathsf{P}(F')(\perp) = 1$, or $t = a'.t'$ for some $a' \in \mathcal{A}ct$ and $t' \in \mathtt{T}^{\mathrm{p}}$, in which case by definition of P:

$$\begin{array}{rcll}
\mathsf{P}(E')(a'.t') & = & \begin{cases} \sum_{G\in\mathrm{Pr}^{\mathrm{p}}} \pi(G)\cdot\mathsf{P}(G)(t') & \text{if } a' = a \\ 0 & \text{otherwise.} \end{cases} & \\
& = & \begin{cases} \sum_{i\in I} \mu_i\cdot\mathsf{P}(E_i)(t') & \text{if } a' = a \\ 0 & \text{otherwise.} \end{cases} & \text{by (5.1)} \\
& \leq & \begin{cases} \sum_{i\in I} \mu_i\cdot\mathsf{P}(F_i)(t') & \text{if } a' = a \\ 0 & \text{otherwise.} \end{cases} & \text{by the hypothesis} \\
& = & \begin{cases} \sum_{G\in\mathrm{Pr}^{\mathrm{p}}} \pi'(G)\cdot\mathsf{P}(G)(t') & \text{if } a' = a \\ 0 & \text{otherwise.} \end{cases} & \text{by (5.1)} \\
& = & \mathsf{P}(F')(a'.t') & \text{by definition of } \mathsf{P}.
\end{array}$$

Putting the above together we have $\mathcal{O}[\![E']\!] \sqsubseteq^{\mathsf{p}} \mathcal{O}[\![F']\!]$.

2. If $E' = E \,\|\, G$ and $F' = F \,\|\, G$, then for any $t \in \mathtt{T}^{\mathrm{p}}$,

$$\begin{array}{rcll}
\mathsf{P}(E')(t) & = & \mathsf{P}(E)(t)\cdot\mathsf{P}(G)(t) & \text{by Lemma 5.2.7} \\
& \leq & \mathsf{P}(F)(t)\cdot\mathsf{P}(G)(t) & \text{since } E \sqsubseteq^{\mathsf{p}} F \\
& = & \mathsf{P}(F')(t) & \text{by Lemma 5.2.7}
\end{array}$$

and since this was for any $t \in \mathtt{T}^{\mathrm{p}}$, $\mathcal{O}[\![E']\!] \sqsubseteq^{\mathsf{p}} \mathcal{O}[\![F']\!]$.

3. If $E' = E \lceil B$ and $F' = F \lceil B$, then for any $t \in \mathtt{T}^{\mathrm{p}}$ either $a \in t$ for some $a \in \mathcal{A}ct \backslash B$ and by Lemma 5.2.8: $\mathsf{P}(E')(t) = \mathsf{P}(F')(t) = 0$, or $a \notin t$ for all $a \in \mathcal{A}ct \setminus B$ and in this case:
$$\begin{array}{rcll} \mathsf{P}(E')(t) & = & \mathsf{P}(E)(t) & \text{by Lemma 5.2.8} \\ & \leq & \mathsf{P}(F)(t) & \text{since } E \sqsubseteq^{\mathsf{p}} F \\ & = & \mathsf{P}(F')(t) & \text{by Lemma 5.2.8.} \end{array}$$
Then since this was for any $t \in \mathtt{T}^{\mathrm{p}}$, $\mathcal{O}[\![E']\!] \sqsubseteq^{\mathsf{p}} \mathcal{O}[\![F']\!]$.

4. If $E' = E\,[\lambda]$ and $F' = F\,[\lambda]$, then for any $t \in \mathtt{T}^{\mathrm{p}}$,
$$\begin{array}{rcll} \mathsf{P}(E')(t) & = & \mathsf{P}(E)(\lambda^{-1}(t)) & \text{by Lemma 5.2.9} \\ & \leq & \mathsf{P}(F))(\lambda^{-1}(t)) & \text{since } E \sqsubseteq^{\mathsf{p}} F \\ & = & \mathsf{P}(F')(t) & \text{by Lemma 5.2.9} \end{array}$$
giving $\mathcal{O}[\![E']\!] \sqsubseteq^{\mathsf{p}} \mathcal{O}[\![F']\!]$.

5. If $E' = \mathit{fix}_x.E$ and $F' = \mathit{fix}_x.F$, to simplify the proof we assume that E and F have at most x as a free variable, in which case by definition $E', F' \in \mathrm{Pr}^{\mathrm{p}}$ and $E\{G'/x\}, F\{G'/x\} \in \mathrm{Pr}^{\mathrm{p}}$ for all $G' \in \mathrm{Pr}^{\mathrm{p}}$. Furthermore, since $E \sqsubseteq^{\mathsf{p}} F$ we have $\mathcal{O}[\![E\{G'/x\}]\!] \sqsubseteq^{\mathsf{p}} \mathcal{O}[\![F\{G'/x\}]\!]$ for all $G' \in \mathrm{Pr}^{\mathrm{p}}$ by Definition 5.2.6, that is:
$$\mathsf{P}(E\{G'/x\})(t) \leq \mathsf{P}(F\{G'/x\})(t) \text{ for all } G' \in \mathrm{Pr}^{\mathrm{p}} \text{ and } t \in \mathtt{T}^{\mathrm{p}}. \tag{5.2}$$
Now, by definition of $\sqsubseteq^{\mathsf{p}}$, to prove $\mathcal{O}[\![E']\!] \sqsubseteq^{\mathsf{p}} \mathcal{O}[\![F']\!]$ it is sufficient to show that: $\mathsf{P}(E')(t) \leq \mathsf{P}(F')(t)$ for all $t \in \mathtt{T}^{\mathrm{p}}$, which we prove by induction on $t \in \mathtt{T}^{\mathrm{p}}$. If $t = \perp$ the result follows by definition of P.

   If $t = a.t'$, then by definition of the transition rules:
$$\begin{array}{ll} \multicolumn{2}{l}{\mathsf{P}(E')(a.t') = \mathsf{P}(E\{E'/x\})(a.t')} \\ = & \mathsf{P}(E\{E'/x\})(a.t') \\ \leq & \mathsf{P}(F\{E'/x\})(a.t') \qquad\qquad\qquad \text{by (5.2)} \\ = & \begin{cases} \sum_{G \in \mathrm{Pr}^{\mathrm{p}}} \pi(G) \cdot \mathsf{P}(G)(t') & \text{if } F\{E'/x\} = (a, \pi) \text{ for some } \pi \in \mu(\mathrm{Pr}^{\mathrm{p}}) \\ 0 & \text{otherwise} \end{cases} \\ & \qquad\qquad\qquad\qquad\qquad\qquad \text{by definition of } \mathsf{P} \end{array}$$

$$= \begin{cases} \sum_{G \in \mathrm{RP}^{\mathrm{p}}} \pi_F(G) \cdot \mathsf{P}(G\{E'/x\})(t') & \text{if } F\{E'/x\} = (a, \pi) \text{ for some } \pi \in \mu(\mathrm{Pr}^{\mathrm{p}}) \\ 0 & \text{otherwise} \end{cases}$$

by Lemma 5.2.10

$$\leq \begin{cases} \sum_{G \in \mathrm{RP}^{\mathrm{p}}} \pi_F(G) \cdot \mathsf{P}(G\{F'/x\})(t') & \text{if } F\{E'/x\} = (a, \pi) \text{ for some } \pi \in \mu(\mathrm{Pr}^{\mathrm{p}}) \\ 0 & \text{otherwise} \end{cases}$$

by induction and Lemma 5.2.11

$$\leq \begin{cases} \sum_{G \in \mathrm{Pr}^{\mathrm{p}}} \pi(G) \cdot \mathsf{P}(G)(t') & \text{if } F\{F'/x\} = (a, \pi) \text{ for some } \pi \in \mu(\mathrm{Pr}^{\mathrm{p}}) \\ 0 & \text{otherwise} \end{cases}$$

by Lemma 5.2.10

$$\begin{aligned} &= \mathsf{P}(F\{F'/x\})(a.t') && \text{by definition of } \mathsf{P} \\ &= \mathsf{P}(F')(a.t') && \text{by the transition rules} \end{aligned}$$

and hence $\mathsf{P}(E')(t) \leq \mathsf{P}(F')(t)$ for all $t \in \mathtt{T}^{\mathrm{p}}$, as required.

□

5.3 Deterministic Probabilistic Processes

In this section we extend the process calculus $\mathrm{RP_p}$ by allowing *external choice*, denoted $\Box$, to form the process calculus $\mathrm{RP_d}$.

Definition 5.3.1 *The set of* $\mathrm{RP_d}$ *expressions is given by the syntax:*

$$F ::= x \mid \mathbf{0} \mid a.\sum_{i \in I} \mu_i.F_i \mid F_1 \Box F_2 \mid F_1 \parallel F_2 \mid F \upharpoonright B \mid F\,[\lambda] \mid \mathit{fix}_x.F.$$

Again, we only consider the guarded and closed expressions of $\mathrm{RP_d}$, denoted $\mathcal{G}^{\mathrm{d}}$ and Pr^{d} respectively. As is customary, we require that the set of initial actions of E_1 and E_2 are disjoint in the construct $E_1 \Box E_2$, that is, $\mathrm{init}(E_1) \cap \mathrm{init}(E_2) = \emptyset$, where, for any $E \in \mathcal{G}^{\mathrm{d}}$, $\mathrm{init}(E)$ is the set of initial actions of E. Intuitively, this restriction is needed since if we considered an external choice between two process, each having the same action as one of its initial moves, then such a choice must degenerate to an internal choice which we must exclude since there is no operator for internal choice in the syntax of $\mathrm{RP_d}$. Formally, we have the following definition of the set of initial actions of a process.

Definition 5.3.2 *Let* init : $\mathcal{G}^{\mathrm{d}} \to \mathcal{P}_f(\mathcal{A}ct)$ *be the map defined inductively on the syntax of* $\mathrm{RP_d}$ *as follows:*

$$\begin{array}{rcl}
\mathrm{init}(\mathbf{0}) & = & \emptyset \\
\mathrm{init}\left(a.\sum_{i\in I}\mu_i.F_i\right) & = & \{a\} \\
\mathrm{init}(E_1 \,\square\, E_2) & = & \mathrm{init}(E_1) \cup \mathrm{init}(E_2) \\
\mathrm{init}(E_1 \,\|\, E_2) & = & \mathrm{init}(E_1) \cap \mathrm{init}(E_2) \\
\mathrm{init}(E \restriction B) & = & \mathrm{init}(E) \cap B \\
\mathrm{init}(E\,[\lambda]) & = & \{\lambda(a) \mid a \in \mathrm{init}(E)\} \\
\mathrm{init}(\mathit{fix}_x.E) & = & \mathrm{init}(E).
\end{array}$$

5.3.1 Operational Semantics

We give operational semantics for the processes of $\mathrm{RP_d}$ in terms of reactive probabilistic transition systems by mapping elements of $\mathrm{Pr^d}$ into $\mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathrm{Pr^d}))$ as follows:

1. $\mathcal{O}[\![\mathbf{0}]\!] = \emptyset$.

2. $\mathcal{O}[\![a.\sum_{i\in I}\mu_i.F_i]\!] = \{(a,\pi)\}$ such that for any $F \in \mathrm{Pr^d}$: $\pi(E) \stackrel{def}{=} \sum_{\substack{i\in I\ \& \\ F=F_i}} \mu_i$.

3. $\mathcal{O}[\![E_1 \,\square\, E_2]\!] = \mathcal{O}[\![E_1]\!] \cup \mathcal{O}[\![E_2]\!]$.

4. $\mathcal{O}[\![E_1 \,\|\, E_2]\!] = S$, if $\mathcal{O}[\![E_1]\!] = S_1$ and $\mathcal{O}[\![E_2]\!] = S_2$ such that $(a,\pi) \in S$ if and only if there exists $(a,\pi_i) \in S_i$ for $i \in \{1,2\}$ and for any $F \in \mathrm{Pr^d}$:
$$\pi(F) \stackrel{def}{=} \begin{cases} \pi_1(F_1)\cdot\pi_2(F_2) & \text{if } F = F_1 \,\|\, F_2 \\ 0 & \text{otherwise.} \end{cases}$$

5. $\mathcal{O}[\![E \restriction B]\!] = S$, if $\mathcal{O}[\![E]\!] = S'$ such that $(a,\pi) \in S$ if and only if $(a,\pi') \in S'$, $a \in B$, and for any $F \in \mathrm{Pr^d}$:
$$\pi(F) \stackrel{def}{=} \begin{cases} \pi'(F') & \text{if } F = F' \restriction B \\ 0 & \text{otherwise.} \end{cases}$$

6. $\mathcal{O}[\![E\,[\lambda]]\!] = S$, if $\mathcal{O}[\![E]\!] = S'$ such that $(a,\pi) \in S$ if and only if $(\lambda^{-1}(a),\pi') \in S'$ and for any $F \in \mathrm{Pr^d}$:
$$\pi(F) \stackrel{def}{=} \begin{cases} \pi'(F') & \text{if } F = F'\,[\lambda] \\ 0 & \text{otherwise} \end{cases}$$

7. $\mathcal{O}[\![\mathit{fix}_x.E]\!] = \mathcal{O}[\![E\{\mathit{fix}_x.E/x\}]\!]$.

The well-definedness of the above semantics can be demonstrated by the following proposition.

Proposition 5.3.3 *For all* $E \in \mathrm{Pr}^{\mathrm{d}}$: $\mathcal{O}[\![E]\!] \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathrm{Pr}^{\mathrm{d}}))$.

Proof. The proof follows similarly to Proposition 5.2.5 by induction on the structure of $E \in \mathrm{Pr}^{\mathrm{d}}$, with the following additional case for external choice. If $E = E_1 \,\Box\, E_2$ then, by the restriction we have imposed on $\mathrm{RP_d}$, the transition rules and induction, we know that $\mathrm{init}(E_1) \cap \mathrm{init}(E_2) = \emptyset$, $\mathcal{O}[\![E]\!] = \mathcal{O}[\![E_1]\!] \cup \mathcal{O}[\![E_2]\!]$ and $\mathcal{O}[\![E_1]\!], \mathcal{O}[\![E_2]\!] \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathrm{Pr}^{\mathrm{d}}))$ respectively. Combining these facts and using Proposition 5.3.4, it follows that $\mathcal{O}[\![E]\!] \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathrm{Pr}^{\mathrm{d}}))$ as required. $\Box$

Furthermore, the above semantics gives the following characterisation of the mapping init.

Proposition 5.3.4 *For all* $E \in \mathrm{Pr}^{\mathrm{d}}$: $a \in \mathrm{init}(E)$ *if and only if* $(a, \pi) \in \mathcal{O}[\![E]\!]$ *for some* $\pi \in \mu(\mathrm{Pr}^{\mathrm{d}})$.

Proof. The proof follows by induction on the structure of $E \in \mathrm{Pr}^{\mathrm{d}}$. $\Box$

5.3.2 $\mathrm{RP_d}$ and the ordering $\sqsubseteq^{\mathsf{d}}$

As for the calculus $\mathrm{RP_p}$, we now investigate the properties of the ordering $\sqsubseteq^{\mathsf{d}}$ over the operators of $\mathrm{RP_d}$. Using the lemmas below we show that $\sqsubseteq^{\mathsf{d}}$ is a congruence over the calculus $\mathrm{RP_d}$. We note that many of the proofs are simple extensions of similar lemmas for $\mathrm{RP_p}$, and have therefore been omitted.

Lemma 5.3.5 *For all* $E_1, E_2 \in \mathrm{Pr}^{\mathrm{d}}$ *and* $t \in \mathtt{T}^{\mathrm{d}}$: $\mathsf{D}(E_1 \,\|\, E_2)(t) = \mathsf{D}(E_1)(t) \cdot \mathsf{D}(E_2)(t)$. *Furthermore, for all* $E \in \mathrm{Pr}^{\mathrm{d}}$, $t \in \mathtt{T}^{\mathrm{d}}$, $B \subseteq \mathcal{A}ct$ *and relabelling function* λ:

$$\mathsf{D}(E \restriction B)(t) = \begin{cases} 0 & \text{if } a \in t \text{ for any } a \in \mathcal{A}ct \setminus B \\ \mathsf{D}(E)(t) & \text{otherwise} \end{cases}$$

and $\mathsf{D}(E\,[\lambda])(t) = \mathsf{D}(E)(\lambda^{-1}(t))$.

Lemma 5.3.6 *For all* $E, F \in \mathrm{Pr}^{\mathrm{d}}$ *such that* $E \,\Box\, F \in \mathrm{Pr}^{\mathrm{d}}$ *and* $t \in \mathtt{T}^{\mathrm{d}}$:

$$\mathsf{D}(E \,\Box\, F)(t) = \max\{\mathsf{D}(E)(t),\ \mathsf{D}(F)(t)\}.$$

Proof. Consider any $E, F \in \mathrm{Pr}^{\mathrm{d}}$ such that $E \,\Box\, F \in \mathrm{Pr}^{\mathrm{d}}$ and $t \in \mathtt{T}^{\mathrm{d}}$, then either $t = \bot$ and the lemma holds by definition of D, or t is of the form $a.T$ for some $a \in \mathcal{A}ct$. In the second case, depending on whether a is a member of $\mathrm{init}(E)$ or $\mathrm{init}(F)$, since by the definition of $\mathrm{RP_d}$, $\mathrm{init}(E) \cap \mathrm{init}(F) = \emptyset$, we have the following three cases to consider:

1. $a \notin \mathrm{init}(E) \cup \mathrm{init}(F)$, then using Proposition 5.3.4, $(a, \pi) \notin \mathcal{O}[\![E]\!]$ and $(a, \pi) \notin \mathcal{O}[\![F]\!]$ for any $\pi \in \mu(\mathrm{Pr}^{\mathrm{d}})$, and since $\mathcal{O}[\![E \,\Box\, F]\!] = \mathcal{O}[\![E]\!] \cup \mathcal{O}[\![F]\!]$ by definition of D: $\mathsf{D}(E \,\Box\, F)(t) = \max\{\mathsf{D}(E)(t),\ \mathsf{D}(F)(t)\} = 0$.

2. $a \in \mathrm{init}(E)$ and $a \notin \mathrm{init}(F)$, then similarly to the above, $\mathsf{D}(F)(t) = 0$. Furthermore, since $a \in \mathrm{init}(E)$, using Proposition 5.3.4 there exists $(a, \pi) \in \mathcal{O}[\![E]\!]$ for some $\pi \in \mu(\mathrm{Pr}^{\mathrm{p}})$, and since $\mathcal{O}[\![E \,\Box\, F]\!] = \mathcal{O}[\![E]\!] \cup \mathcal{O}[\![F]\!]$ by definition of D:
$$\mathsf{D}(E \,\Box\, F)(t) = \mathsf{D}(E)(t) = \max\{\mathsf{D}(E)(t),\ 0\} = \max\{\mathsf{D}(E)(t),\ \mathsf{D}(F)(t)\}.$$

3. $a \in \mathrm{init}(F)$ and $a \notin \mathrm{init}(E)$, then by symmetry on item 2:
$$\mathsf{D}(E \,\Box\, F)(t) = \max\{\mathsf{D}(E)(t),\ \mathsf{D}(F)(t)\}.$$

Then since these are the only possible cases the proof is complete. □

Lemma 5.3.7 *If $G \in \mathcal{G}^{\mathrm{d}}$ such that $G\{E/x\} \in \mathrm{Pr}^{\mathrm{d}}$ for all $E \in \mathrm{Pr}^{\mathrm{d}}$, then there exists $S_G \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathrm{RP_d}))$ such that for any $E \in \mathrm{Pr}^{\mathrm{p}}$, $\mathcal{O}[\![G\{E/x\}]\!] = \emptyset$ if and only if $S_G = \emptyset$ and $\mathcal{O}[\![G\{E/x\}]\!] = \{(a_1, \pi_1), \ldots, (a_m, \pi_m)\}$ if and only if $S_G = \{(a_1, \pi_G^1), \ldots, (a_m, \pi_G^m)\}$ where for any $F \in \mathrm{Pr}^{\mathrm{d}}$ and $i \in \{1, \ldots, m\}$:*
$$\pi_i(F) = \begin{cases} \pi_G^i(F') & \text{if } F = F'\{E/x\} \text{ for some } F' \in \mathrm{RP_d} \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 5.3.8 *For any $E \in \mathrm{RP_d}$ and $F, F' \in \mathrm{Pr}^{\mathrm{d}}$ such that $E\{F/x\}, E\{F'/x\} \in \mathrm{Pr}^{\mathrm{d}}$ and $\mathsf{D}(F)(t) \leq \mathsf{D}(F')(t)$ for all $t \in \mathsf{T}^{\mathrm{d}}$ then: $\mathsf{D}(E\{F/x\})(t) \leq \mathsf{D}(E\{F'/x\})(t)$ for all $t \in \mathsf{T}^{\mathrm{d}}$.*

Proposition 5.3.9 *The pre-order $\sqsubseteq^{\mathsf{d}}$ is preserved by all contexts in the language $\mathrm{RP_d}$. Formally, if we have that $E_i \sqsubseteq^{\mathsf{d}} F_i$ for all $i \in I$ and $E \sqsubseteq^{\mathsf{d}} F$, then:*
$$\begin{array}{rcl} \mathcal{O}[\![a.\sum_{i\in I}\mu_i.E_i]\!] & \sqsubseteq^{\mathsf{d}} & \mathcal{O}[\![a.\sum_{i\in I}\mu_i.F_i]\!] \\ \mathcal{O}[\![E \,\Box\, G]\!] & \sqsubseteq^{\mathsf{d}} & \mathcal{O}[\![F \,\Box\, G]\!] \\ \mathcal{O}[\![E \,\|\, G]\!] & \sqsubseteq^{\mathsf{d}} & \mathcal{O}[\![F \,\|\, G]\!] \\ \mathcal{O}[\![E \upharpoonright B]\!] & \sqsubseteq^{\mathsf{d}} & \mathcal{O}[\![F \upharpoonright B]\!] \\ \mathcal{O}[\![E\,[\lambda]]\!] & \sqsubseteq^{\mathsf{d}} & \mathcal{O}[\![F\,[\lambda]]\!] \\ \mathcal{O}[\![\mathit{fix}_x.E]\!] & \sqsubseteq^{\mathsf{d}} & \mathcal{O}[\![\mathit{fix}_x.F]\!]. \end{array}$$

Proof. The proof follows the same arguments as that of Proposition 5.2.12, with the additional clause for external choice, which we now prove. If $E' = E \Box G$ and $F' = F \Box G$, then for any $t \in \mathtt{T}^{\mathrm{d}}$:

$$\begin{array}{rcll} \mathsf{D}(E')(t) & = & \max\{\mathsf{D}(E)(t),\ \mathsf{D}(G)(t)\} & \text{by Lemma 5.3.6} \\ & \leq & \max\{\mathsf{D}(F)(t),\ \mathsf{D}(G)(t)\} & \text{since } E \sqsubseteq^{\mathsf{d}} F \\ & = & \mathsf{D}(F')(t) & \text{by Lemma 5.3.6} \end{array}$$

and since this was for any $t \in \mathtt{T}^{\mathrm{d}}$, $\mathcal{O}[\![E']\!] \sqsubseteq^{\mathsf{d}} \mathcal{O}[\![F']\!]$ as required. $\square$

5.4 Non-deterministic Probabilistic Processes

In this section, we extend the syntax of the process calculus $\mathrm{RP_p}$ to $\mathrm{RP_{nd}}$ by allowing *internal choice* (denoted $\sqcap$) as follows.

Definition 5.4.1 *The set of* $\mathrm{RP_{nd}}$ *expressions is given by the syntax:*

$$F ::= x \mid \mathbf{0} \mid a.\sum_{i \in I} \mu_i.F_i \mid F_1 \sqcap F_2 \mid F_1 \parallel F_2 \mid F \upharpoonright B \mid F\,[\lambda] \mid \mathit{fix}_x.F.$$

As before, we only consider the set of guarded expressions and processes of $\mathrm{RP_{nd}}$, denoted $\mathcal{G}^{\mathrm{nd}}$ and Pr^{nd} respectively.

5.4.1 Operational Semantics

We give operational semantics for $\mathrm{RP_{nd}}$ in terms of reactive probabilistic transition systems. We take Pr^{nd} as the set of states and define the transition relation $\rightarrow\, \subseteq \mathrm{Pr}^{nd} \times (\mathcal{A}ct \times \mu(\mathrm{Pr}^{\mathrm{nd}})) \cup \{\emptyset\}$ as the smallest relation satisfying the following conditions:

1. $\mathcal{O}[\![\mathbf{0}]\!] \rightarrow \emptyset$.

2. $\mathcal{O}[\![a.\sum_{i \in I} \mu_i.F_i]\!] \rightarrow (a, \pi)$ such that for any $F \in \mathrm{Pr}^{nd}$: $\pi(F) \stackrel{\mathit{def}}{=} \sum_{\substack{i \in I\,\& \\ F = F_i}} \mu_i$.

3. $\mathcal{O}[\![E_1 \sqcap E_2]\!] \rightarrow s$, if $\mathcal{O}[\![E_1]\!] \rightarrow s$ or $\mathcal{O}[\![E_2]\!] \rightarrow s$.

4. $\mathcal{O}[\![E_1 \parallel E_2]\!] \rightarrow \emptyset$, if $\mathcal{O}[\![E_1]\!] \rightarrow (a_1, \pi_1)$ and $\mathcal{O}[\![E_2]\!] \rightarrow (a_2, \pi_2)$ such that $a_1 \neq a_2$, or either $\mathcal{O}[\![E_1]\!] \rightarrow \emptyset$ or $\mathcal{O}[\![E_2]\!] \rightarrow \emptyset$.

5. $\mathcal{O}[\![E_1 \parallel E_2]\!] \rightarrow (a, \pi)$, if $\mathcal{O}[\![E_1]\!] \rightarrow (a, \pi_1)$ and $\mathcal{O}[\![E_2]\!] \rightarrow (a, \pi_2)$ such that for any $F \in \mathrm{Pr}^{nd}$:
$$\pi(F) \stackrel{\mathit{def}}{=} \begin{cases} \pi_1(F_1) \cdot \pi_2(F_2) & \text{if } F = F_1 \parallel F_2 \\ 0 & \text{otherwise.} \end{cases}$$

6. $\mathcal{O}[\![E \upharpoonright B]\!] \to \emptyset$, if $\mathcal{O}[\![E]\!] \to (a, \pi)$ such that $b \in \mathcal{A}ct \setminus B$, or $\mathcal{O}[\![E]\!] \to \emptyset$.

7. $\mathcal{O}[\![E \upharpoonright B]\!] \to (a, \pi)$, if $\mathcal{O}[\![E]\!] \to (a, \pi')$ such that $a \in B$ and for any $F \in \mathrm{Pr}^{\mathrm{nd}}$:

$$\pi(F) \stackrel{def}{=} \begin{cases} \pi'(F') & \text{if } F = F' \upharpoonright B \\ 0 & \text{otherwise.} \end{cases}$$

8. $\mathcal{O}[\![E\,[\lambda]]\!] \to \emptyset$, if $\mathcal{O}[\![E]\!] \to \emptyset$.

9. $\mathcal{O}[\![E\,[\lambda]]\!] \to (a, \pi)$, if $\mathcal{O}[\![E]\!] \to (\lambda^{-1}(a), \pi')$ such that for any $F \in \mathrm{Pr}^{\mathrm{nd}}$:

$$\pi(F) \stackrel{def}{=} \begin{cases} \pi'(F') & \text{if } F = F'\,[\lambda] \\ 0 & \text{otherwise} \end{cases}$$

10. $\mathcal{O}[\![\mathit{fix}_x.E]\!] \to s$, if $\mathcal{O}[\![E\{\mathit{fix}_x.E/x\}]\!] \to s$.

Proposition 5.4.2 *If $E \in \mathrm{Pr}^{\mathrm{nd}}$ and $\mathcal{O}[\![E]\!] \to s$, then $s \in (\mathcal{A}ct \times \mu(\mathrm{Pr}^{\mathrm{nd}})) \cup \{\emptyset\}$.*

5.4.2 $\mathrm{RP}_{\mathrm{nd}}$ and the ordering $\sqsubseteq^{\mathsf{nd}}$

Recall that the ordering $\sqsubseteq^{\mathsf{nd}}$ on non-deterministic probabilistic processes is based on the mappings $\mathsf{N}_{\mathbf{lub}}$ and $\mathsf{N}_{\mathbf{glb}}$. We now investigate the properties of $\mathsf{N}_{\mathbf{lub}}$ and $\mathsf{N}_{\mathbf{glb}}$ with respect to the operators of $\mathrm{RP}_{\mathrm{nd}}$. In the lemmas below we suppose N_* denotes both $\mathsf{N}_{\mathbf{glb}}$ and $\mathsf{N}_{\mathbf{lub}}$ and, similarly to the case for D, when the proofs are simple extensions of those relating P and RP_{p} they are omitted.

Lemma 5.4.3 *For all $E_1, E_2 \in \mathrm{Pr}^{\mathrm{nd}}$, $t \in \mathtt{T}^{\mathrm{nd}}$:*

$$\begin{array}{rl} (i) & \mathsf{N}_{\mathbf{glb}}(E_1 \,\|\, E_2)(t) = \mathsf{N}_{\mathbf{glb}}(E_1)(t) \cdot \mathsf{N}_{\mathbf{glb}}(E_2)(t) \\ (ii) & \mathsf{N}_{\mathbf{lub}}(E_1 \,\|\, E_2)(t) = \mathsf{N}_{\mathbf{lub}}(E_1)(t) \cdot \mathsf{N}_{\mathbf{lub}}(E_2)(t). \end{array}$$

Proof. We only consider the case for $\mathsf{N}_{\mathbf{glb}}$; the case for $\mathsf{N}_{\mathbf{lub}}$ follows similarly. The lemma is proved by induction on $t \in \mathtt{T}^{\mathrm{nd}}$. If $t \in \mathtt{T}^{\mathrm{nd}}$, then t is of the form $(\!|r|\!)$. First, if we consider any $s_1, s_2 \in (\mathcal{A}ct \times \mu(\mathrm{Pr}^{\mathrm{nd}})) \cup \{\emptyset\}$, then returning to the operational semantics of the operator $\|$ for RP_{p} and replacing $\mu(\mathrm{Pr}^{\mathrm{p}})$ by $\mu(\mathrm{Pr}^{\mathrm{nd}})$, we reach a definition of $s_1 || s_2$. Using this we obtain:

$$\mathsf{N}_{\mathbf{glb}}(s_1 \,\|\, s_2)(r) = \mathsf{N}_{\mathbf{glb}}(s_1)(r) \cdot \mathsf{N}_{\mathbf{glb}}(s_2)(r) \tag{5.3}$$

following the arguments in the inductive step of Lemma 5.2.7. Next, consider any $E_1, E_2 \in \mathrm{Pr}^{\mathrm{nd}}$, then by comparing the definition of $s_1 || s_2$ for any $s_1, s_2 \in (\mathcal{A}ct \times \mu(\mathrm{Pr}^{\mathrm{nd}}))$ with the operational semantics for $\|$ in $\mathrm{RP}_{\mathrm{nd}}$ we have:

$$\mathcal{O}[\![E_1 \,\|\, E_2]\!] \to s \;\Leftrightarrow\; \mathcal{O}[\![E_1]\!] \to s_1 \text{ and } \mathcal{O}[\![E_2]\!] \to s_2 \text{ such that } s = s_1 || s_2. \tag{5.4}$$

Now, by definition of $\mathsf{N}_{\mathbf{glb}}$ we have $\mathsf{N}_{\mathbf{glb}}(E_1 \,\|\, E_2)(\llparenthesis r \rrparenthesis)$ is equal to:

$$\begin{array}{lll}
= & \min\{\mathsf{N}_{\mathbf{glb}}(s)(r) \mid \mathcal{O}[\![E_1 \,\|\, E_2]\!] \rightarrow s\} & \\
= & \min\{\mathsf{N}_{\mathbf{glb}}(s_1 \,\|\, s_2)(r) \mid \mathcal{O}[\![E_1]\!] \rightarrow s_1 \;\&\; \mathcal{O}[\![E_2]\!] \rightarrow s_2\} & \text{by (5.4)} \\
= & \min\{\mathsf{N}_{\mathbf{glb}}(s_1)(r) \cdot \mathsf{N}_{\mathbf{glb}}(s_2)(r) \mid \mathcal{O}[\![E_1]\!] \rightarrow s_1 \;\&\; \mathcal{O}[\![E_2]\!] \rightarrow s_2\} & \text{by (5.3)} \\
= & (\min\{\mathsf{N}_{\mathbf{glb}}(s_1)(r) \mid \mathcal{O}[\![E_1]\!] \rightarrow s_1\}) \cdot (\min\{\mathsf{N}_{\mathbf{glb}}(s_2)(r) \mid \mathcal{O}[\![E_2]\!] \rightarrow s_2\}) & \\
& & \text{rearranging} \\
= & \mathsf{N}_{\mathbf{glb}}(E_1)(\llparenthesis r \rrparenthesis) \cdot \mathsf{N}_{\mathbf{glb}}(E_2)(\llparenthesis r \rrparenthesis) & \text{by definition of } \mathsf{N}_{\mathbf{glb}}
\end{array}$$

and hence the lemma holds for $\mathsf{N}_{\mathbf{glb}}$ by induction. □

Lemma 5.4.4 *For all $E \in \mathrm{Pr}^{nd}$, $t \in \mathtt{T}^{\mathrm{nd}}$, $B \subseteq \mathcal{A}ct$ and λ:*

$$\mathsf{N}_*(E \upharpoonright B)(t) = \begin{cases} 0 & \text{if } a \in t \text{ for any } a \in \mathcal{A}ct \setminus B \\ \mathsf{N}_*(E)(t) & \text{otherwise} \end{cases}$$

and $\mathsf{N}_*(E\,[\lambda])(t) = \mathsf{N}_*(E)(\lambda^{-1}(t))$.

Lemma 5.4.5 *For all $E, F \in \mathrm{Pr}^{nd}$ and $t \in \mathtt{T}^{\mathrm{nd}}$:*

$$\begin{array}{rl}
(i) & \mathsf{N}_{\mathbf{glb}}(E \sqcap F)(t) = \min\{\mathsf{N}_{\mathbf{glb}}(E)(t),\ \mathsf{N}_{\mathbf{glb}}(F)(t)\} \\
(ii) & \mathsf{N}_{\mathbf{lub}}(E \sqcap F)(t) = \max\{\mathsf{N}_{\mathbf{lub}}(E)(t),\ \mathsf{N}_{\mathbf{lub}}(F)(t)\}.
\end{array}$$

Proof. We only prove the case for $\mathsf{N}_{\mathbf{glb}}$ as the case for $\mathsf{N}_{\mathbf{lub}}$ follows similarly. Consider any $E, F \in \mathrm{Pr}^{nd}$ and $t \in \mathtt{T}^{\mathrm{nd}}$, then by definition of $\mathtt{T}^{\mathrm{nd}}$, t is of the form $\llparenthesis r \rrparenthesis$, and hence by definition of $\mathsf{N}_{\mathbf{glb}}$:

$$\begin{array}{lll}
\multicolumn{3}{l}{\mathsf{N}_{\mathbf{glb}}(E \sqcap F)(t) = \min\{\mathsf{N}_{\mathbf{glb}}(s)(r) \mid \mathcal{O}[\![E \sqcap F]\!] \rightarrow s\}} \\
= & \min\{\mathsf{N}_{\mathbf{glb}}(s)(r) \mid \mathcal{O}[\![E]\!] \rightarrow s \text{ and } \mathcal{O}[\![F]\!] \rightarrow s\} & \text{by the transition rules} \\
= & \min\{\min\{\mathsf{N}_{\mathbf{glb}}(s)(r) \mid \mathcal{O}[\![E]\!] \rightarrow s\},\ \min\{\mathsf{N}_{\mathbf{glb}}(s)(r) \mid \mathcal{O}[\![F]\!] \rightarrow s\} & \\
& & \text{rearranging} \\
= & \min\{\mathsf{N}_{\mathbf{glb}}(E)(t),\ \mathsf{N}_{\mathbf{glb}}(F)(t)\} & \text{by definition of } \mathsf{N}_{\mathbf{glb}}.
\end{array}$$

□

Lemma 5.4.6 *If $G \in \mathcal{G}^{\mathrm{nd}}$ such that $G\{E/x\} \in \mathrm{Pr}^{nd}$ for all $E \in \mathrm{Pr}^{nd}$, then there exists a set $S_G \subseteq (\mathcal{A}ct \times \mu(\mathrm{RP}_{\mathrm{nd}})) \cup \{\emptyset\}$ such that for any $E \in \mathrm{Pr}^{nd}$, $\mathcal{O}[\![G\{E/x\}]\!] \rightarrow \emptyset$ if and only if $\emptyset \in S_G$ and $\mathcal{O}[\![G\{E/x\}]\!] \rightarrow (a, \pi)$ if and only if $(a, \pi_G) \in S_G$ where for any $F \in \mathrm{Pr}^{nd}$:*

$$\pi(F) = \begin{cases} \pi_G(F') & \text{if } F = F'\{E/x\} \text{ for some } F' \in \mathrm{RP}_{\mathrm{nd}} \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 5.4.7 *For any $E \in \mathrm{RP}_{\mathrm{nd}}$ and $F, F' \in \mathrm{Pr}^{nd}$ such that $E\{F/x\}, E\{F'/x\} \in \mathrm{Pr}^{nd}$ and $\mathsf{N}_{\mathsf{lub}}(F)(t) \leq \mathsf{N}_{\mathsf{lub}}(F')(t)$ for all $t \in \mathtt{T}^{\mathrm{nd}}$ then:*

$$\mathsf{N}_{\mathsf{lub}}(E\{F/x\})(t) \leq \mathsf{N}_{\mathsf{lub}}(E\{F'/x\})(t) \text{ for all } t \in \mathtt{T}^{\mathrm{nd}}.$$

Proposition 5.4.8 *The pre-order $\sqsubseteq^{\mathsf{nd}}$ is preserved by all contexts in the language $\mathrm{RP}_{\mathrm{nd}}$. Formally, if we have that $E_i \sqsubseteq^{\mathsf{nd}} F_i$ for all $i \in I$ and $E \sqsubseteq^{\mathsf{nd}} F$, then:*

$$\begin{array}{rcl}
\mathcal{O}[\![a.\sum_{i\in I}\mu_i.E_i]\!] & \sqsubseteq^{\mathsf{nd}} & \mathcal{O}[\![a.\sum_{i\in I}\mu_i.F_i]\!] \\
\mathcal{O}[\![E \sqcap G]\!] & \sqsubseteq^{\mathsf{nd}} & \mathcal{O}[\![F \sqcap G]\!] \\
\mathcal{O}[\![E \,\|\, G]\!] & \sqsubseteq^{\mathsf{nd}} & \mathcal{O}[\![F \,\|\, G]\!] \\
\mathcal{O}[\![E \upharpoonright B]\!] & \sqsubseteq^{\mathsf{nd}} & \mathcal{O}[\![F \upharpoonright B]\!] \\
\mathcal{O}[\![E\,[\lambda]]\!] & \sqsubseteq^{\mathsf{nd}} & \mathcal{O}[\![F\,[\lambda]]\!] \\
\mathcal{O}[\![\mathit{fix}_x.E]\!] & \sqsubseteq^{\mathsf{nd}} & \mathcal{O}[\![\mathit{fix}_x.F]\!].
\end{array}$$

Proof. The proof follows similarly to the cases for RP_{p} and RP_{d}. □

5.5 Reactive Probabilistic Processes

We now give the syntax of the calculus RP, combining RP_{d} and $\mathrm{RP}_{\mathrm{nd}}$ as follows.

Definition 5.5.1 *The set of* RP *expressions is given by the syntax:*

$$F ::= x \mid \mathbf{0} \mid a.\sum_{i\in I}\mu_i.F_i \mid F_1 \,\Box\, F_2 \mid F_1 \sqcap F_2 \mid F_1 \,\|\, F_2 \mid F \upharpoonright B \mid F\,[\lambda] \mid \mathit{fix}_x.F.$$

Again we only consider the guarded expressions and processes (closed terms) of RP, which we denote $\mathcal{G}$ and Pr respectively. Note that we do not restrict when the construct $E_1 \,\Box\, E_2$ appears in RP since, unlike RP_{d}, RP also contains internal choice.

5.5.1 Operational Semantics

We give operational semantics for RP based on reactive probabilistic transition systems, where the states are Pr and $\rightarrow \subseteq \mathrm{Pr} \times \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ is the smallest relation satisfying the following conditions:

1. $\mathcal{O}[\![\mathbf{0}]\!] \rightarrow \emptyset$.
2. $\mathcal{O}[\![a.\sum_{i\in I}\mu_i.F_i]\!] \rightarrow \{(a,\pi)\}$ such that for any $F \in \mathrm{Pr}$: $\pi(F) \stackrel{\text{def}}{=} \sum_{\substack{i\in I\\ F_i=F}} \mu_i$.
3. $\mathcal{O}[\![E_1 \,\Box\, E_2]\!] \rightarrow S$, if $\mathcal{O}[\![E_1]\!] \rightarrow S_1$ and $\mathcal{O}[\![E_2]\!] \rightarrow S_2$ such that S is a maximal reactive subset of $S_1 \cup S_2$.

4. $\mathcal{O}[\![E_1 \sqcap E_2]\!] \rightarrow S$, if $\mathcal{O}[\![E_1]\!] \rightarrow S$ or $\mathcal{O}[\![E_2]\!] \rightarrow S$.

5. $\mathcal{O}[\![E_1 \parallel E_2]\!] \rightarrow S$, if $\mathcal{O}[\![E_1]\!] \rightarrow S_1$ and $\mathcal{O}[\![E_2]\!] \rightarrow S_2$ such that $(a, \pi) \in S$ if and only if $(a, \pi_i) \in S_i$ for $i \in \{1, 2\}$, and for any $F \in \mathrm{Pr}$:

$$\pi(F) \stackrel{def}{=} \begin{cases} \pi_1(F_1) \cdot \pi_2(F_2) & \text{if } F = F_1 \parallel F_2 \\ 0 & \text{otherwise.} \end{cases}$$

6. $\mathcal{O}[\![E \upharpoonright B]\!] \rightarrow S$, if $\mathcal{O}[\![E]\!] \rightarrow S'$ such that $(a, \pi) \in S$ if and only if $(a, \pi') \in S'$, $a \in B$ and for any $F \in \mathrm{Pr}$:

$$\pi(F) \stackrel{def}{=} \begin{cases} \pi'(F') & \text{if } F = F' \upharpoonright B \\ 0 & \text{otherwise.} \end{cases}$$

7. $\mathcal{O}[\![E\,[\lambda]]\!] \rightarrow S$, if $\mathcal{O}[\![E]\!] \rightarrow S'$ such that $(a, \pi) \in S$ if and only if $(\lambda^{-1}(a), \pi') \in S'$ and for any $F \in \mathrm{Pr}$:

$$\pi(F) \stackrel{def}{=} \begin{cases} \pi'(F') & \text{if } F = F'\,[\lambda] \\ 0 & \text{otherwise.} \end{cases}$$

8. $\mathcal{O}[\![\mathit{fix}_x.E]\!] \rightarrow S$, if $\mathcal{O}[\![E\{\mathit{fix}_x.E/x\}]\!] \rightarrow S$.

With the exception of the rule for $\Box$, all the above transition rules are in agreement with those given in the subcalculi discussed earlier. We illustrate the rule for $\Box$ by means of the following examples. First, if $\mathcal{O}[\![E_1]\!] \rightarrow \{(a, \pi)\}$ and $\mathcal{O}[\![E_2]\!] \rightarrow \{(b, \pi')\}$ and $a \neq b$, then from the transition rules above $\mathcal{O}[\![E_1 \Box E_2]\!] \rightarrow \{(a, \pi), (b, \pi')\}$, and hence $\mathcal{O}[\![E_1 \Box E_2]\!]$ makes an external choice between the actions a and b. As a second example, suppose $\mathcal{O}[\![E_1]\!] \rightarrow \{(a, \pi), (c, \pi_1)\}$ and $\mathcal{O}[\![E_2]\!] \rightarrow \{(b, \pi'), (c, \pi_2)\}$ for some distinct actions a, b and c, then $\mathcal{O}[\![E_1 \Box E_2]\!] \rightarrow \{(a, \pi), (b, \pi'), (c, \pi_i)\}$ for $i \in \{1, 2\}$, and thus $\mathcal{O}[\![E_1 \Box E_2]\!]$ makes an external choice between the actions a, b and c, but there is an *internal* choice between the distributions π_1 and π_2 when performing the action c, that is, external choice degenerates to internal choice when processes can perform the same action as their initial move.

We show that the above semantics is well-defined by means of the following proposition.

Proposition 5.5.2 *If $E \in \mathrm{Pr}$ and $\mathcal{O}[\![E]\!] \rightarrow S$, then $S \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$.*

5.5.2 RP and the ordering $\sqsubseteq^{\mathsf{r}}$

As for the case of $\mathrm{RP_{nd}}$, to relate the ordering $\sqsubseteq^{\mathsf{r}}$ to the operational semantics of RP, we first consider the mappings $\mathsf{R_{lub}}$ and $\mathsf{R_{glb}}$. We arrive at the following lemmas with proofs similar to the cases for $\mathrm{RP_p}$, $\mathrm{RP_d}$ and $\mathrm{RP_{nd}}$, where R_* denotes both $\mathsf{R_{glb}}$ and $\mathsf{R_{lub}}$.

Lemma 5.5.3 *For all $E_1, E_2 \in \mathrm{Pr}$ and $t \in \mathtt{T}$:*

$$\begin{array}{rl} (i) & \mathsf{R_{glb}}(E_1 \sqcap E_2)(t) = \min\{\mathsf{R_{glb}}(E_1)(t),\ \mathsf{R_{glb}}(E_2)(t)\} \\ (ii) & \mathsf{R_{lub}}(E_1 \sqcap E_2)(t) = \max\{\mathsf{R_{lub}}(E_1)(t),\ \mathsf{R_{lub}}(E_2)(t)\} \\ (iii) & \mathsf{R_{glb}}(E_1 \,\|\, E_2)(t) = \mathsf{R_{glb}}(E_1)(t) \cdot \mathsf{R_{glb}}(E_2)(t) \\ (vi) & \mathsf{R_{lub}}(E_1 \,\|\, E_2)(t) = \mathsf{R_{lub}}(E_1)(t) \cdot \mathsf{R_{lub}}(E_2)(t). \end{array}$$

Furthermore, for any $E \in \mathrm{Pr}$, $t \in \mathtt{T}$, $B \subseteq \mathcal{A}ct$ and relabelling function λ:

$$\mathsf{R}_*(E \upharpoonright B)(t) = \begin{cases} 0 & \text{if } a \in t \text{ for any } a \in \mathcal{A}ct \setminus B \\ \mathsf{R}_*(E)(t) & \text{otherwise.} \end{cases}$$

and $\mathsf{R}_*(E\,[\lambda])(t) = \mathsf{R}_*(E)(\lambda^{-1}(t))$.

Lemma 5.5.4 *If $G \in \mathcal{G}$ such that $G\{E/x\} \in \mathrm{Pr}$ for all $E \in \mathrm{Pr}$, then there exists a set $\mathbf{S}_G \subseteq \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathrm{RP}))$ such that for any $E \in \mathrm{Pr}$, $\mathcal{O}[\![G\{E/x\}]\!] \to \emptyset$ if and only if $\emptyset \in \mathbf{S}_G$ and $\mathcal{O}[\![G\{E/x\}]\!] \to \{(a_1,\pi_1),\ldots,(a_m,\pi_m)\}$ if and only if $\{(a_1,\pi^1_G),\ldots,(a_m,\pi^m_G)\} \in \mathbf{S}_G$ where for any $1 \leq i \leq m$ and $F \in \mathrm{Pr}$:*

$$\pi_i(F) = \begin{cases} \pi^i_G(F') & \text{if } F = F'\{E/x\} \text{ for some } F' \in \mathrm{RP} \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 5.5.5 *For any $E \in \mathrm{RP}$ and $F, F' \in \mathrm{Pr}$ such that $E\{F/x\}, E\{F'/x\} \in \mathrm{Pr}$ and $\mathsf{R_{glb}}(F)(t) \leq \mathsf{R_{glb}}(F')(t)$ for all $t \in \mathtt{T}$ then:*

$$\mathsf{R_{glb}}(E\{F/x\})(t) \leq \mathsf{R_{glb}}(E\{F'/x\})(t) \text{ for all } t \in \mathtt{T}.$$

Lemma 5.5.6 *For any $E \in \mathrm{RP}$ and $F, F' \in \mathrm{Pr}$ such that $E\{F/x\}, E\{F'/x\} \in \mathrm{Pr}$ and $\mathsf{R_{lub}}(F)(t) \leq \mathsf{R_{lub}}(F')(t)$ for all $t \in \mathtt{T}$ then:*

$$\mathsf{R_{lub}}(E\{F/x\})(t) \leq \mathsf{R_{lub}}(E\{F'/x\})(t) \text{ for all } t \in \mathtt{T}.$$

Lemma 5.5.7 *For all $E, F \in \mathrm{Pr}$, $\mathcal{O}[\![E]\!] \sqsubseteq^{\mathsf{glb}} \mathcal{O}[\![F]\!]$ if and only if for any $(\!|r|\!) \in \mathtt{T}$ and $S' \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ such that $\mathcal{O}[\![F]\!] \to S'$ there exists $S'' \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ such that $\mathcal{O}[\![E]\!] \to S''$ and $\mathsf{R_{glb}}(S')(r) \geq \mathsf{R_{glb}}(S'')(r)$.*

Proof. First, if $E, F \in \mathrm{Pr}$ and $\mathcal{O}[\![E]\!] \sqsubseteq^{\mathsf{glb}} \mathcal{O}[\![F]\!]$, then for any $(\!|r|\!) \in \mathtt{T}$ and $S' \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ such that $\mathcal{O}[\![F]\!] \to S'$:

$$\begin{array}{rcll} \mathsf{R}_{\mathsf{glb}}(S')(r) & \geq & \min\{\mathsf{R}_{\mathsf{glb}}(S)(r) \mid \mathcal{O}[\![F]\!] \to S\} & \\ & = & \mathsf{R}_{\mathsf{glb}}(F)((\!|r|\!)) & \text{by definition of } \mathsf{R}_{\mathsf{glb}} \\ & \geq & \mathsf{R}_{\mathsf{glb}}(E)((\!|r|\!)) & \text{since } E \sqsubseteq^{\mathsf{glb}} F \\ & = & \min\{\mathsf{R}_{\mathsf{glb}}(S)(r) \mid \mathcal{O}[\![E]\!] \to S\} & \text{by definition of } \mathsf{R}_{\mathsf{glb}} \\ & = & \mathsf{R}_{\mathsf{glb}}(S'')(r) & \text{for some } \mathcal{O}[\![E]\!] \to S'' \end{array}$$

and since this was for any $(\!|r|\!) \in \mathtt{T}$ and $S' \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ such that $\mathcal{O}[\![F]\!] \to S'$, the "if" direction holds.

Second, suppose for any $(\!|r|\!) \in \mathtt{T}$ and $S' \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ such that $\mathcal{O}[\![F]\!] \to S'$ there exists $S'' \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ such that $\mathcal{O}[\![E]\!] \to S''$ and $\mathsf{R}_{\mathsf{glb}}(S')(r) \geq \mathsf{R}_{\mathsf{glb}}(S'')(r)$. Then, $\mathsf{R}_{\mathsf{glb}}(F)((\!|r|\!))$ equals:

$$\begin{array}{cll} = & \min\{\mathsf{R}_{\mathsf{glb}}(S)(r) \mid \mathcal{O}[\![F]\!] \to S\} & \text{by definition of } \mathsf{R}_{\mathsf{glb}} \\ = & \mathsf{R}_{\mathsf{glb}}(S')(r) & \text{for some } S' \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathrm{Pr})) \\ & & \text{such that } F \to S' \\ \geq & \mathsf{R}_{\mathsf{glb}}(S'')(r) & \text{for some } S'' \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathrm{Pr})) \\ & & \text{such that } \mathcal{O}[\![E]\!] \to S'' \text{ by hypothesis} \\ \geq & \min\{\mathsf{R}_{\mathsf{glb}}(S)(r) \mid \mathcal{O}[\![E]\!] \to S\} & \text{since } \mathcal{O}[\![E]\!] \to S'' \\ = & \mathsf{R}_{\mathsf{glb}}(E)((\!|r|\!)) & \text{by definition of } \mathsf{R}_{\mathsf{glb}} \end{array}$$

and since this was for arbitrary $(\!|r|\!) \in \mathtt{T}$, $\mathcal{O}[\![E]\!] \sqsubseteq^{\mathsf{glb}} \mathcal{O}[\![F]\!]$ and hence the "only if" direction holds. □

Lemma 5.5.8 *For all $E, F \in \mathrm{Pr}$, $\mathcal{O}[\![E]\!] \sqsubseteq^{\mathsf{lub}} \mathcal{O}[\![F]\!]$ if and only if for any $(\!|r|\!) \in \mathtt{T}$ and $S' \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ such that $\mathcal{O}[\![E]\!] \to S'$ there exists $S'' \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ such that $\mathcal{O}[\![F]\!] \to S''$ and $\mathsf{R}_{\mathsf{lub}}(S')(r) \leq \mathsf{R}_{\mathsf{lub}}(S'')(r)$.*

Proof. The proof is the dual of Lemma 5.5.7 above. □

Using the lemmas above we can now show that $\sqsubseteq^{\mathsf{r}}$ is a congruence over RP.

Proposition 5.5.9 *The pre-order $\sqsubseteq^{\mathsf{r}}$ is preserved by all contexts in the language* RP*. Formally, if we have that $E_i \sqsubseteq^{\mathsf{r}} F_i$ for all $i \in I$ and $E \sqsubseteq^{\mathsf{r}} F$, then:*

$$\begin{array}{rcl} \mathcal{O}[\![a.\sum_{i\in I}\mu_i.E_i]\!] & \sqsubseteq^{\mathsf{r}} & \mathcal{O}[\![a.\sum_{i\in I}\mu_i.F_i]\!] \\ \mathcal{O}[\![E \,\Box\, G]\!] & \sqsubseteq^{\mathsf{r}} & \mathcal{O}[\![F \,\Box\, G]\!] \\ \mathcal{O}[\![E \sqcap G]\!] & \sqsubseteq^{\mathsf{r}} & \mathcal{O}[\![F \sqcap G]\!] \\ \mathcal{O}[\![E \,\|\, G]\!] & \sqsubseteq^{\mathsf{r}} & \mathcal{O}[\![F \,\|\, G]\!] \\ \mathcal{O}[\![E \upharpoonright B]\!] & \sqsubseteq^{\mathsf{r}} & \mathcal{O}[\![F \upharpoonright B]\!] \\ \mathcal{O}[\![E\,[\lambda]]\!] & \sqsubseteq^{\mathsf{r}} & \mathcal{O}[\![F\,[\lambda]]\!] \\ \mathcal{O}[\![\mathit{fix}_x.E]\!] & \sqsubseteq^{\mathsf{r}} & \mathcal{O}[\![\mathit{fix}_x.F]\!]. \end{array}$$

Proof. The proof follows similarly to the case for $\mathrm{RP_p}$, $\mathrm{RP_d}$ and $\mathrm{RP_{nd}}$ except in the case of $\Box$. In the latter case, suppose $E, F, G \in \mathrm{Pr}$ and $\mathcal{O}[\![E]\!] \sqsubseteq^{\mathsf{r}} \mathcal{O}[\![F]\!]$. Considering any $S' \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ such that $\mathcal{O}[\![F']\!] \to S'$. By definition of the transition rules there exists $S_1, S_2 \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ such that $\mathcal{O}[\![F]\!] \to S_1$, $\mathcal{O}[\![G]\!] \to S_2$ and $(a, \pi) \in S'$ if $(a, \pi) \in S_1$ or $(a, \pi) \in S_2$. Then if $(\!|r|\!) \in \mathtt{T}$, either $r = \bot$, in which case since by construction $\mathcal{O}[\![E \Box G]\!] \to S''$ for some $S'' \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$, we have by definition of $\mathsf{R_{glb}}$:

$$\mathsf{R_{glb}}(S')(\bot) = 1 = \mathsf{R_{glb}}(S'')(\bot),$$

or r is of the form $[a_1.T_1, \ldots, a_m.T_m]$, then putting:

$$r_2 = [a'_1.T'_1, \ldots, a'_{m'}.T'_{m'}]$$

where for any $1 \leq i \leq m'$ there exists a unique $1 \leq j \leq m$ such that $a'_i.T'_i = a_j.T_j$ and $(a_i, \pi) \in S' \cap S_2$ for some $\pi_i \in \mu(\mathrm{RP})$, and putting:

$$r_1 = [a''_1.T''_1, \ldots, a''_{m''}.T''_{m''}]$$

where for any $1 \leq i \leq m''$, there exists a unique $1 \leq j \leq m$ such that $a''_i.T''_i = a_j.T_j$ and $a'_k.T'_k \neq a_j.T_j$ for all $1 \leq k \leq m'$. By definition of $\mathsf{R_{glb}}$ we have:

$$\mathsf{R_{glb}}(S')(r) = \mathsf{R_{glb}}(S_1)(r_1) \cdot \mathsf{R_{glb}}(S_2)(r_2).$$

Moreover, since $\mathcal{O}[\![E]\!] \sqsubseteq^{\mathsf{r}} \mathcal{O}[\![F]\!]$, by definition $\mathcal{O}[\![E]\!] \sqsubseteq^{\mathsf{glb}} \mathcal{O}[\![F]\!]$ and since $\mathcal{O}[\![F]\!] \to S_1$, Lemma 5.5.7 implies there exists $S'_1 \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ such that $\mathcal{O}[\![E]\!] \to S'_1$ and $\mathsf{R_{glb}}(S'_1)(t_1) \leq \mathsf{R_{glb}}(S_1)(t_1)$. Furthermore, it follows by definition of the transition rules that there exists $S'' \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ such that $\mathcal{O}[\![E \Box G]\!] \to S''$ and

$$\mathsf{R_{glb}}(S'')(r) = \mathsf{R_{glb}}(S'_1)(r_1) \cdot \mathsf{R_{glb}}(S_2)(r_2).$$

Combining the above, we have $\mathsf{R_{glb}}(S')(r) \geq \mathsf{R_{glb}}(S'')(r)$. Then since this was for any $t \in \mathtt{T}$ and $S' \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ such that $\mathcal{O}[\![F \Box G]\!] \to S'$, Lemma 5.5.7 implies $\mathcal{O}[\![E \Box G]\!] \sqsubseteq^{\mathsf{glb}} \mathcal{O}[\![F \Box G]\!]$.

Similarly, using Lemma 5.5.8 instead of Lemma 5.5.7 and considering any $S' \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ such that $\mathcal{O}[\![E \Box G]\!] \to S'$, we can show $\mathcal{O}[\![E \Box F]\!] \sqsubseteq^{\mathsf{lub}} \mathcal{O}[\![F \Box G]\!]$, and thus, since $\sqsubseteq^{\mathsf{r}}$ is the intersection of the orderings $\sqsubseteq^{\mathsf{glb}}$ and $\sqsubseteq^{\mathsf{lub}}$, $\mathcal{O}[\![E \Box G]\!] \sqsubseteq^{\mathsf{r}} \mathcal{O}[\![F \Box G]\!]$ as required. $\square$

5.6 Equational Laws

In this section, we investigate equational laws for RP. We note that when restricted to only the syntactic operators of $\mathrm{RP_p}$, $\mathrm{RP_d}$ and $\mathrm{RP_{nd}}$, the laws we derive will hold for these subcalculi. We first define the following "equality" and "ordering" relations co-inductively over the set of processes of RP.

Definition 5.6.1 *A relation* $\equiv^{\mathrm{e}} \subseteq \mathrm{Pr}\times\mathrm{Pr}$ *is a "equality" relation if whenever* $E \equiv^{\mathrm{e}} F$:

$$\begin{array}{ll} (i) & \text{if } \mathcal{O}[\![E]\!] \to S' \text{ then } \mathcal{O}[\![F]\!] \to S'' \text{ such that } S' \equiv^{\mathrm{e}} S'' \\ (ii) & \text{if } \mathcal{O}[\![F]\!] \to S'' \text{ then } \mathcal{O}[\![E]\!] \to S' \text{ such that } S'' \equiv^{\mathrm{e}} S' \end{array}$$

where for any $S', S'' \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathrm{RP}))$, $S' \equiv^{\mathrm{e}} S''$ *if whenever* $(a, \pi') \in S'$ *then* $(a, \pi'') \in S''$ *such that for any* $G' \in \mathrm{RP}$ *there exists* $G'' \in \mathrm{RP}$ *with* $G' \equiv^{\mathrm{e}} G''$ *and* $\pi'(G') = \pi''(G'')$, *and vice versa.*

Furthermore, a relation $\sqsubseteq^{\mathrm{e}} \subseteq \mathrm{Pr}\times\mathrm{Pr}$ *is a "ordering" relation if whenever* $E \sqsubseteq^{\mathrm{e}} F$:

$$\text{if } \mathcal{O}[\![E]\!] \to S' \text{ then } \mathcal{O}[\![F]\!] \to S'' \text{ such that } S' \sqsubseteq^{\mathrm{e}} S''$$

where for any $S', S'' \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathrm{RP}))$, $S' \sqsubseteq^{\mathrm{e}} S''$ *if* $(a, \pi') \in S'$ *implies* $(a, \pi'') \in S''$ *such that for any* $G' \in \mathrm{RP}$ *there exists* $G'' \in \mathrm{RP}$ *with* $G' \sqsubseteq^{\mathrm{e}} G''$ *and* $\pi'(G') = \pi''(G'')$.

Now, following the standard techniques we introduce the maximum such "equivalence" and "ordering" relations as our equality and ordering over RP.

Definition 5.6.2 *Let* $\equiv$ *and* $\sqsubseteq$ *be the maximum "equality" relation and "ordering" relation respectively.*

We now list some of the equational laws of RP in Figure 5.1 below. We see that many of the laws coincide with those for non-probabilistic process calculi. For example, $\sqcap$ is idempotent, symmetric and associative, and both $\Box$ and $\|$ are associative, symmetric and distribute through $\sqcap$. Also, we see that $\Box$ degenerates to $\sqcap$ when processes can perform the same action. Other equational laws for RP include those for restriction and relabelling, which distribute over $\sqcap$, $\Box$ and $\|$.

However, certain rules fail to extend from the non-probabilistic setting, for example $\Box$ is *not* idempotent. To illustrate this consider the process $E = (a.1.\mathbf{0}) \sqcap (b.1.\mathbf{0})$; then by definition of the transition rules we can represent E and $E \,\Box\, E$ graphically as given in Figure 5.2 below.

By definition of $\equiv$, it is clear that $E \,\Box\, E \not\equiv E$.

Another standard CSP law that fails is that $\sqcap$ no longer distributes through $\Box$. To illustrate this, suppose E is the process given above, $F = b.1.\mathbf{0}$ and $G = b.1.\mathbf{0}$. Then

$$
\begin{array}{rcll}
E \sqcap E & \equiv & E & \\
E \sqcap F & \equiv & F \sqcap E & \\
E \sqcap (F \sqcap G) & \equiv & (E \sqcap F) \sqcap G & \\
E \Box F & \equiv & F \Box E & \\
E \Box (F \Box G) & \equiv & (E \Box F) \Box G & \\
E \Box (F \sqcap G) & \equiv & (E \Box F) \sqcap (E \Box G) & \\
E \sqcap \mathbf{0} & \sqsubseteq & E & \\
E \Box \mathbf{0} & \equiv & E & \\
(a.\sum_{i \in I} \mu_i.E_i) \sqcap (b.\sum_{j \in J} \lambda_j.F_j) & \sqsubseteq & (a.\sum_{i \in I} \mu_i.E_i) \Box (b.\sum_{j \in J} \lambda_j.F_j) & \text{if } a \neq b \\
(a.\sum_{i \in I} \mu_i.E_i) \sqcap (a.\sum_{j \in J} \lambda_j.F_j) & \equiv & (a.\sum_{i \in I} \mu_i.E_i) \Box (a.\sum_{j \in J} \lambda_j.F_j) & \\
E \parallel F & \equiv & F \parallel E & \\
E \parallel (F \parallel G) & \equiv & (E \parallel F) \parallel G & \\
E \parallel (F \sqcap G) & \equiv & (E \parallel F) \sqcap (E \parallel F) & \\
E \parallel \mathbf{0} & \equiv & \mathbf{0} & \\
(a.\sum_{i \in I} \mu_i.E_i) \parallel (b.\sum_{j \in J} \lambda_j.F_j) & \equiv & \mathbf{0} & \text{if } a \neq b \\
(a.\sum_{i \in I} \mu_i.E_i) \parallel (a.\sum_{j \in J} \lambda_j.F_j) & \equiv & a.\sum_{i \in I \,\&\, j \in J} (\mu_i \cdot \lambda_j).E_i \parallel F_j & \\
E \restriction \mathcal{A}ct & \equiv & E & \\
(E \restriction B_1) \restriction B_2 & \equiv & E \restriction (B_1 \cap B_2) & \\
E \restriction \emptyset & \equiv & \mathbf{0} & \\
E\,[\mathrm{id}_{\mathcal{A}ct}] & \equiv & E & \\
(E\,[\lambda_1])\,[\lambda_2] & \equiv & E\,[\lambda_2 \circ \lambda_1] & \\
\mathit{fix}_x.E & \equiv & E\{\mathit{fix}_x.E/x\} &
\end{array}
$$

Figure 5.1: Equational Laws of RP.

it is straightforward to show that: $E \sqcap (F \Box G) \equiv E$ and $(E \sqcap F) \Box (E \sqcap G) \equiv E \Box E$, and therefore since $E \not\equiv E \Box E$:

$$E \sqcap (F \Box G) \not\equiv (E \sqcap F) \Box (E \sqcap G).$$

5.7 Adding Additional Syntactic Operators

As we have attempted to define an equivalence to distinguish processes which can only be distinguished by external observations, consequently we have to omit certain operators to ensure our equivalence is a congruence (see discussion in Section 2.4).

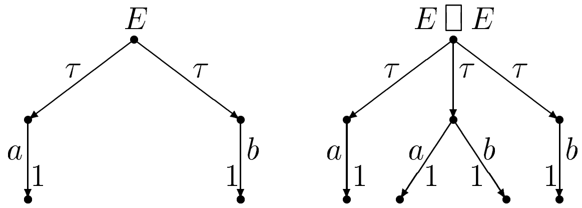


Figure 5.2: Example to show external choice is not idempotent.

For example, if we add a parallel operator which is not fully synchronous to our calculus then $\stackrel{r}{\sim}$ will fail to be a congruence. To illustrate this consider the following processes of RP, where if no probability is given it is assumed to be 1:

$$F_1 = a.\left(b.\left(\tfrac{1}{2}.c.\mathbf{0} + \tfrac{1}{2}.\mathbf{0}\right)\right),\quad F_2 = a.\left(\tfrac{1}{2}.b.c.\mathbf{0} + \tfrac{1}{2}.b.\mathbf{0}\right)\ \text{ and }\ F_3 = d.\mathbf{0}.$$

First, it is straightforward to show that $\mathcal{O}[\![F_1]\!] \stackrel{r}{\sim} \mathcal{O}[\![F_2]\!]$. However, following the expansion law for interleaving we have:

$$F_1 \,|||\, F_3 = \left(a.\left(b.\left(\tfrac{1}{2}.(c.d.\mathbf{0} \Box d.c.\mathbf{0}) + \tfrac{1}{2}d.\mathbf{0}\right) \Box d.\left(b.\left(\tfrac{1}{2}.c.\mathbf{0} + \tfrac{1}{2}.\mathbf{0}\right)\right)\right)\right) \Box d.F_1$$

$$\text{and }\ F_2 \,|||\, F_3 = \left(a.\left(\tfrac{1}{2}.b.(c.d.\mathbf{0} \Box d.c.\mathbf{0}) + \tfrac{1}{2}.(b.d.\mathbf{0} \Box d.b.\mathbf{0})\right)\right) \Box d.F_2.$$

Furthermore, by definition of the transition rules the behaviour of $F_1 \,|||\, F_3$ and $F_2 \,|||\, F_3$ when offered the action a, denoted F_{13} and F_{23} respectively, can be graphically represented in Figure 5.3 below.

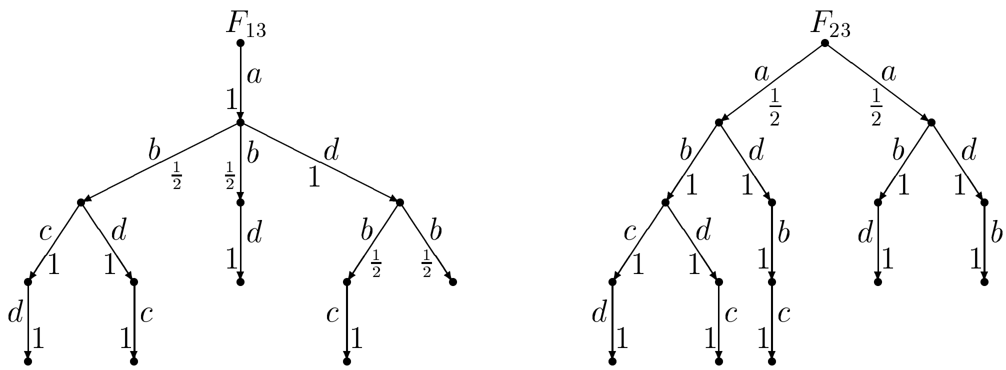


Figure 5.3: Graphical representation of F_{13} and F_{23}.

Then considering the test $t = (\![a.(\![b.(\![d.(\![c.\bot]\!)]\!)]\!), d.(\![b.(\![c.\bot]\!)]\!)]\!)$, it is straightforward to show

$$\mathsf{R}_*(F_1 \,|||\, F_3)(t) = \frac{1}{4} \neq \frac{1}{2} = \mathsf{R}_*(F_2 \,|||\, F_3)(t)$$

where R_* denotes either $\mathsf{R}_{\mathsf{lub}}$ or $\mathsf{R}_{\mathsf{glb}}$. Hence, $\mathcal{O}[\![F_1 \,|||\, F_3]\!] \stackrel{r}{\not\sim} \mathcal{O}[\![F_2 \,|||\, F_3]\!]$, and thus $\stackrel{r}{\sim}$ fails to be a congruence since $\mathcal{O}[\![F_1]\!] \stackrel{r}{\sim} \mathcal{O}[\![F_2]\!]$.

It should also be noted that we have not included the hiding operator, the reason being that our model contains action-guarded probabilistic choice. In we added a hiding operator in this setting, there will exist probabilistic transitions which are hidden, and it would be problematic to test for the probability of such hidden moves. A more appropriate model would be one where probabilistic choices and action transitions are separate, that is, a model that contains both prefixing and an internal probabilistic choice operator. Moreover, we feel that in this model it may be possible to add an interleaving parallel operator to the calculus without losing the congruence property of our equivalence.

One approach to model such a calculus would be to consider a transition system which exhibits probabilistic, internal and action (external) choices. One such candidate could be a transition system $(P, \mathcal{A}ct, \rightarrow)$, where the transition relation is:

$$\rightarrow \subseteq P \times \mu(\mathcal{P}_{fr}(\mathcal{A}ct \times P)).$$

In the above *any* $S \in \mathcal{P}_{fr}(\mathcal{A}ct \times P)$ should be thought of as a deterministic process, where either $S = \{(a_1, E_1), \ldots, (a_m, E_m)\}$, the process which makes an external choice between the actions $\{a_1, \ldots, a_m\}$ and, for any $1 \leq i \leq m$, if S performs the action a_i it will then behave as the process E_i, or $S = \emptyset$, the inactive process. Then any $\pi \in \mu(\mathcal{P}_{fr}(\mathcal{A}ct \times P))$ represents the probabilistic process in which the probability of π behaving as any deterministic process $S \in \mathcal{P}_{fr}(\mathcal{A}ct \times P)$ is given by $\pi(S)$. Finally, internal choice is introduced by allowing choices between probabilistic processes.

If we then consider our testing scenario over the above transition system, one can adapt the maps $\mathsf{R}_{\mathbf{glb}}$ and $\mathsf{R}_{\mathbf{lub}}$, where R_* denotes either $\mathsf{R}_{\mathbf{glb}}$ or $\mathsf{R}_{\mathbf{lub}}$, as follows. For any $E \in P$ put:

$$\mathsf{R}_{\mathbf{glb}}(E)((\!|r|\!)) = \min_{E \rightarrow \pi} \mathsf{R}_{\mathbf{glb}}(\pi)(r), \quad \mathsf{R}_{\mathbf{lub}}(E)((\!|r|\!)) = \max_{E \rightarrow \pi} \mathsf{R}_{\mathbf{lub}}(\pi)(r)$$

$$\text{and} \quad \mathsf{R}_*(E)((t_1, \ldots, t_m)) = \prod_{i=1}^{m} \mathsf{R}_*(E)(t_i)$$

where for any $\pi \in \mu(\mathcal{P}_{fnr}(\mathcal{A}ct \times P))$:

$$\mathsf{R}_{\mathbf{lub}}(\pi)(t) = \sum_{S \in \mathcal{P}_{fr}(\mathcal{A}ct \times P)} \pi(S) \cdot \mathsf{R}_{\mathbf{lub}}(S)(t)$$

and for any $S \in \mathcal{P}_{fr}(\mathcal{A}ct \times P)$ and $1 \leq i \leq m$:

$$\mathsf{R}_*(S)(\perp) = 1, \qquad \mathsf{R}_{\mathbf{lub}}(S)([a_1.T_1, \ldots, a_m.T_m]) = \prod_{i=1}^{m} \mathsf{R}_{\mathbf{lub}}(S)(a_i.T_i)$$

$$\text{and} \qquad \mathsf{R}_{\mathbf{lub}}(S)(a.T) = \begin{cases} \mathsf{R}_{\mathbf{lub}}(F)(T) & \text{if } (a, F) \in S \text{ for some } F \in P \\ 0 & \text{otherwise.} \end{cases}$$

Furthermore, we illustrate how we could give operational semantics to a calculus containing a separate internal probabilistic choice by means of such a transition system, where η_S denotes the point distribution with value 1 at S (see Definition 3.2.2).

- $\mathcal{O}[\![\mathbf{0}]\!] \to \eta_\emptyset$.
- $\mathcal{O}[\![a.E]\!] \to \eta_{\{(a,E)\}}$.
- $\mathcal{O}[\![E\ {}_p\sqcap_q\ F]\!] \to \pi$, if $\mathcal{O}[\![E]\!] \to \pi_1$ and $\mathcal{O}[\![F]\!] \to \pi_2$ such that for any $S \in \mathcal{P}_{fr}(\mathcal{A}ct \times P)$, $\pi(S) = p \cdot \pi_1(S) + q \cdot \pi_2(S)$.

The above is only an outline for how the operational semantics can be constructed, which we feel is worth future investigation.

Note also that we only allow a restricted version of the relabelling operator, that is, we require relabelling functions to be bijective. This again is to preserve the congruence of our equivalence: we feel that in a model with a separate probabilistic choice operator our equivalence may turn out to be a congruence for a weaker notion of relabelling.

Furthermore, as none of our results relating to our orderings depend on the sum of any probability distribution being 1, we can in fact consider *sub-probability distributions* by allowing the syntactic operator a . $\sum_{i\in I}\mu_i.F_i$ where $\sum_{i\in I}\mu_i \leq 1$. This way $1 - \sum_{i\in I}\mu_i$ can be used to model the probability of deadlock, and all results relating to our ordering will still hold.

Chapter 6

Denotational Semantics

In this chapter, we present denotational semantics for our probabilistic calculus RP. As mentioned in Chapter 2, there are several frameworks available and each offers its own advantages. We have chosen the metric-theoretic approach as probabilistic processes are quantitative in nature: the probabilities of transitions occurring are given, which corresponds with the quantitative information contained in the distance between denotations given by a process metric.

To achieve our goal we follow de Bakker and Zucker's metric space construction for denotational semantics of non-probabilistic process calculi [BZ82], which we now outline. First, de Bakker and Zucker consider *simple processes*, that is, those which are derived in the sub-calculus by means of just the syntactic operator used in the inductive step of the transition rules of the calculus. In non-probabilistic calculi, these are the processes which can be derived just using (successive applications of) prefixing. Formally, de Bakker and Zucker introduce the following inductively defined collection of metric spaces.

Definition 6.0.1 (cf. [BZ82]) *Let (P_n, d_n), $n = 0, 1, \ldots$, be a collection of metric spaces defined inductively as follows. Let $P_0 = \{p_0\}$ where $d_0(p', p'') = 0$ for all $p', p'' \in P_0$, and $P_{n+1} = \{p_0\} \cup (A \times P_n)$ where $d_{n+1}(p_0, p_0) = 0$, $d_{n+1}(p_0, (a_1, p_1)) = d_{n+1}((a_1, p_1), p_0) = 0$ and*

$$d_{n+1}((a_1, p_1), (a_2, p_2)) = \begin{cases} 1 & \text{if } a_1 \neq a_2 \\ \frac{1}{2} \cdot d_n(p_1, p_2) & \text{otherwise.} \end{cases}$$

Informally, $P_0 \subseteq P_1 \subseteq \ldots \subseteq P_n \ldots$ form a sequence of sets, where as n increases the number of simple processes which are modelled increases, with P_n modelling the processes capable of performing one action at a time up to *the depth* n.

Following this, de Bakker and Zucker then take the completion of $(\cup_n P_n, \cup_n d_n)$ as the denotational model for simple processes. Intuitively, the denotational model consists of p_0 and all finite sequences $(a_1, (a_2 \ldots (a_n, p_0) \ldots))$ where $n \in \mathbb{N}$, together with all infinite sequences $(a_1, (a_2 \ldots))$. We can think of $(a_1, (a_2 \ldots (a_n, p_0) \ldots))$ as the process that can perform the actions $a_1, a_2 \ldots a_n$ in sequence and then terminate, and $(a_1, (a_2, \ldots))$ can be considered as an infinite process performing the sequence $a_1 a_2 \ldots$

In the second step, to model the whole calculus de Bakker and Zucker "lift" the denotations of simple processes to *sets* using the induced Hausdorff distance between the sets, and add semantic operators to model the remaining syntactic operators of the calculus. This corresponds to the introduction of an appropriate powerset operator $\mathcal{P}$ into the construction as follows:

$$P_{n+1} = \{p_0\} \cup \mathcal{P}_c(A \times P_n)$$

Now set-theoretic union corresponds to the syntactic choice: the denotation $\{(a, p_0)\} \cup \{(b, p_0)\}$ can intuitively be thought of as the process that can either perform the action a and then terminate, or perform the action b and then terminate.

6.1 A Metric for Simple Probabilistic Processes

We first turn our attention to simple probabilistic processes, which should be thought of as suitable generalisations of the simple processes of de Bakker and Zucker [BZ82]. As in the non-probabilistic case, a probabilistic process will be represented by a certain set of such processes. Returning to the transition rules for RP, we see that the inductive step of the transition rules is given by action-guarded probabilistic choice, and we therefore consider simple probabilistic processes as those which are derived in the sub-calculus by means of just this syntactic operator. We denote such a simple probabilistic process p by the pair (a, f), where $a \in A$ is an action type and $f : P \to [0, 1]$ is a probability distribution on the set of simple probabilistic processes P such that for any simple probabilistic process q, $f(q)$ gives the probability of p performing the action a and then behaving as q. Furthermore, to model the inactive process we introduce the distinguished element p_0. Then applying the techniques of [BZ82] this leads us to the following inductively defined collection of carrier sets.

Definition 6.1.1 (Finite simple probabilistic processes) *Let P_n, $n \in \mathbb{N}$, be a collection of carrier sets defined inductively by:*

$$P_0 = \{p_0\} \;\; and \;\; P_{n+1} = \{p_0\} \cup (A \times \mu(P_n))$$

where A is a set of actions. Let $P_\omega = \cup_n P_n$ denote processes of bounded depth.

For simplicity, we consider any $f \in \mu(P_n)$ as the extension of f to P_ω, defined by letting $f(p) = 0$ for any $p \in P_\omega \setminus P_n$.

The next step is to construct a metric on the set of simple probabilistic processes P_ω. To motivate our construction we first consider what properties we would expect of a metric over P_ω. The main tool a metric offers is the notion of convergence, that is, defining Cauchy sequences (see Definition 3.3.4). Therefore, we first consider the Cauchy sequences we would expect a metric over P_ω to give us. One example is given by the sequence $\langle p_n \rangle_{n\in\mathbb{N}}$ of simple processes given in Figure 6.1 below.

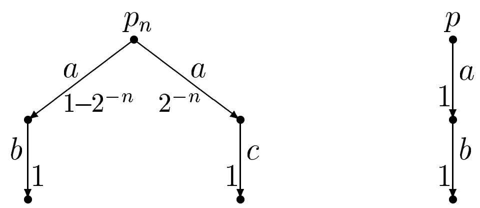


Figure 6.1: Example of a Cauchy sequence and its limit point.

Observe that, as $n \to \infty$, the probability of p_n performing its right branch becomes more and more insignificant, that is, the operational behaviour of p_n *converges* to that of p. Therefore, following Lemma 3.3.5 which states "any convergent sequence in a metric space is Cauchy" we would expect the sequence $\langle p_n \rangle_{n\in\mathbb{N}}$ to be a Cauchy sequence for any intuitively "correct" metric over P_ω.

Following de Bakker and Zucker's construction, we first attempted to define a metric inductively on the sets P_n. Firstly, the case for $n = 0$ is simple, as P_0 is a singleton set, that is, $d_0(p, q) = 0$ for all $p, q \in P_0$. Moreover, similar to de Bakker and Zucker's construction, we can set: $d_{n+1}(p_0, p_0) = 0$, $d_{n+1}(p, p_0) = 1$ if $p \neq p_0$ and $d_{n+1}((a, f), (b, g)) = 0$ if $a \neq b$. This leaves us with defining the case for $d_{n+1}((a, f), (a, g))$ where $f, g \in \mu(P_n)$. However, in this situation things become more complex, since the metric d_{n+1} will need to take into account the distances $d_n(p', q')$ as well as the values $f(p')$ and $g(q')$ for all $p' \in \mathsf{s}(f)$ and $q' \in \mathsf{s}(g)$. Investigating a possible definition of d_{n+1} we found that the metric did not correspond to the operational behaviour of the processes. For example, possible approaches would be to take the minimum, maximum or summation of one of the following:

$$|f(p') - g(q')| \cdot d_n(p', q') \tag{6.1}$$

$$|f(p') - g(q')| + \frac{1}{2} d_n(p', q') \tag{6.2}$$

over all $p', q' \in P_n$. Firstly, if we consider the minimum of either (6.1) or (6.2), it is straightforward to show the resultant "metric" does not satisfy the triangle inequality (M3). On the other hand, if we consider (6.1), the only non-zero value for p_n and p

in Figure 6.1 is $|1 - 2^{-n}|$. Therefore, if we take either the maximum or summation of (6.1), as $n \to \infty$ the resultant distance between p_n and p increases, and therefore the sequence $\langle p_n \rangle_{n \in \mathbb{N}}$ does not converge to p.

We note that if instead we consider the maximum or summation of (6.2) similar problems will be encountered.

Intuitively, the difficulty with these approaches arises from the separation of the distance between the processes in P_n and the probabilities associated with these processes, that is, the values of f and g. For example, there exist cases where $|f(p') - g(q')|$ is small (or zero) and the operational behaviour of p' and q' is different, and cases where $|f(p') - g(q')|$ is large and the operational behaviour of p' and q' is similar (or even equivalent). Thus, calculating the value of (6.1) and (6.2) will yield small values even though the operational behaviour is different.

To overcome these problems, that is, to avoid the above separation, a non-inductive approach is needed. Based on the above discussion, our first attempt, see [KN96b], was to define a metric on simple processes P_ω by means of the following metric on probability distributions.

Proposition 6.1.2 (cf. [KN96b]) *For any set P, the family $\mu(P)$ of probability distributions on P is a metric space with respect to the metric:*

$$d_\mu(f, g) = \frac{1}{2} \sum_{p \in \mathsf{s}(f) \cup \mathsf{s}(g)} |f(p) - g(p)|.$$

Using the metric d_μ of [KN96b] and de Bakker and Zucker's metric we constructed the following metric on finite simple probabilistic processes P_ω.

Definition 6.1.3 (cf. [KN96b]) *Let $(P_n)_{n \in \mathbb{N}}$ and P_ω be the carrier sets defined in Definition 6.1.1. We define the metric $\hat{d}$ on the structure of elements of P_ω by putting $\hat{d}(p_0, p_0) = 0$, $\hat{d}(p_0, (a, f)) = 1$, $\hat{d}((a, f), p_0) = 1$, and*

$$\hat{d}((a, f), (b, g)) = \begin{cases} 1 & \text{if } a \neq b \\ d_\mu(f, g) & \text{otherwise.} \end{cases}$$

An analysis of the metric $\hat{d}$ leads to the following observation. We first consider the simple probabilistic processes p_n and p given in Figure 6.1 which differ on their *first* transition. Calculating the distance we have: $\hat{d}(p_n, p) = 2^{-n}$, and hence $\langle p_n \rangle_{n \in \mathbb{N}}$ is a Cauchy sequence. However, if we now consider the simple probabilistic processes which differ *after* the first transitions given in Figure 6.2 below, the above property relating to convergence no longer holds for the metric $\hat{d}$.

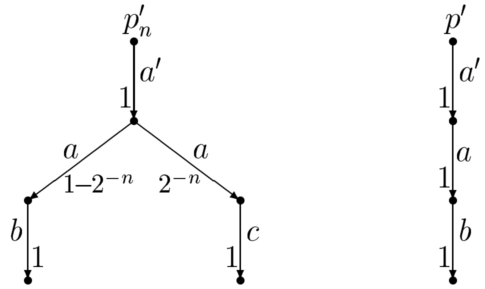


Figure 6.2: Processes differing after the first transition.

Calculating the distances between p'_n and p'_m for any $n \neq m \in \mathbb{N}$ we obtain: $\hat{d}(p'_n, p'_m) = 1$. However, analysing the operational behaviour, similarly to the processes of Figure 6.1, we have that as $n \to \infty$, the behaviour of p'_n becomes more similar to that of p', and hence we would expect $\langle p'_n \rangle_{n \in \mathbb{N}}$ to be Cauchy.

To understand the above we discuss how the metric "works": on the first transitions of simple probabilistic processes the metric considers the difference in the probabilities, and hence we have the "correct" results for Figure 6.1. However, as soon as we go beyond the first transitions, the differences between the probabilistic transitions are only considered with respect to equality. To elaborate on this, consider $\hat{d}(p'_n, p'_m)$ for any $n \neq m \in \mathbb{N}$: we see that p'_n and p'_m can perform the action a' with probability 1 and then behave as the processes p_n and p_m given in Figure 6.1, but the metric only uses the information that $p_n \neq p_m$, and *not* the differences in the probabilities of transitions of p_n and p_m. Thus, the values given by the metric of [KN96b] between simple probabilistic processes do not capture the behaviour of certain simple probabilistic processes, that is, those whose operational behaviour differs after their first transitions. Therefore, if we wish to find a metric to eliminate this problem an alternative approach is required, which we now explain.

The motivation behind the new approach is to develop a representation of simple probabilistic processes which will give us more information about their operational behaviour. To achieve this, instead of modelling a simple probabilistic process by the pair (a, f) of an action symbol and a probability distribution, we consider a simple probabilistic process as sets of (maximal) finite strings over $A \times (0, 1]$, that is, sets of strings of pairs of actions and (non-zero) probabilities of the form: $(a_1, \mu_1)(a_2, \mu_2) \ldots (a_k, \mu_k)$, where $k \in \mathbb{N}$, $a_i \in A$ and $\mu_i \in (0, 1]$ for all $1 \leq i \leq k$. To illustrate this representation, recall the simple probabilistic process given in Figure 6.1; we can represent p_n by the following set of strings:

$$\{(a, 1 - 2^{-n})(b, 1),\ (a, 2^{-n})(c, 1)\}.$$

Formally, using Definition 6.1.1, in order to represent simple probabilistic processes as sets of finite strings over $A \times (0, 1]$, that is, subsets of $(A \times (0, 1])^*$, where to simplify notation let $A^{(0,1]^*} \stackrel{def}{=} (A \times (0,1])^*$, we introduce the following mapping from the set of simple probabilistic processes P_ω to the set of strings described above.

Definition 6.1.4 *Let $\mathcal{S}: P_\omega \to \mathcal{P}_{fn}(A^{(0,1]^*})$ be the map defined inductively on $p \in P_n$ as follows. If $p \in P_0$, then $p = p_0$ and put $\mathcal{S}(p) = \langle\rangle$, and if $p \in P_{n+1} \setminus P_n$, then $p = (a, f)$ for some $a \in A$ and $f \in \mu(P_n)$, and put:*

$$\mathcal{S}(p) = \{(a, f(q))x \mid x \in \mathcal{S}(q) \ \&\ q \in \mathsf{s}(f)\}.$$

Recall $\mathsf{s}(f)$ denotes the support of the distribution f.

Intuitively, for any process $p \in P_\omega$ and $x \in \mathcal{S}(p)$, by construction we have: $x = (a_1, \mu_1)(a_2, \mu_2) \ldots (a_k, \mu_k)$ for some $k \in \mathbb{N}$, where $a_i \in A$ and $\mu_i \in (0, 1]$ for all $1 \leq i \leq k$. The sequence $a_1 \ldots a_k$ is a *complete path* (trace) that p can perform, and $\mu_1 \cdot \mu_2 \cdots \mu_k$ is the *probability* of p performing this path. To make these notions more precise we introduce the following two projections on $A^{(0,1]^*}$.

Definition 6.1.5 *Let $\mathcal{A} : A^{(0,1]^*} \to A^*$ and $\mathcal{V} : A^{(0,1]^*} \to [0, 1]$ be the maps defined as follows. For any $x = (a_1, \mu_1)(a_2, \mu_2) \ldots (a_k, \mu_k) \in A^{(0,1]^*}$ put:*

$$\mathcal{A}(x) = \begin{cases} \langle\rangle & \text{if } k = 0 \\ a_1 a_2 \ldots a_k & \text{otherwise} \end{cases} \quad \text{and} \quad \mathcal{V}(x) = \begin{cases} 1 & \text{if } k = 0 \\ \mu_1 \cdot \mu_2 \cdots \mu_k & \text{otherwise.} \end{cases}$$

The idea behind these mappings is that, if we consider any $p \in P_\omega$ and $x \in \mathcal{S}(p)$, then $\mathcal{A}(x)$ is a path p can perform and $\mathcal{V}(x)$ is the probability of p performing this path. Unfortunately, the situation is more complex, which we demonstrate by the simple probabilistic process given in Figure 6.3.

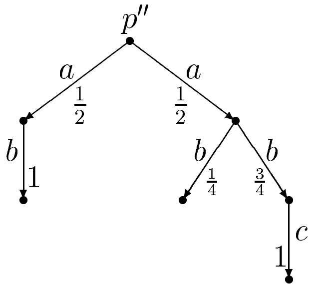


Figure 6.3: Example of a simple probabilistic process.

Then calculating $\mathcal{S}(p'')$ we have:

$$\mathcal{S}(p'') = \left\{(a, \tfrac{1}{2})(b, 1),\ (a, \tfrac{1}{2})(b, \tfrac{1}{4}),\ (a, \tfrac{1}{2})(b, \tfrac{3}{4})(c, 1)\right\}$$

and by definition of $\mathcal{A}$: $\mathcal{A}((a, \frac{1}{2})(b, 1)) = \mathcal{A}((a, \frac{1}{2})(b, \frac{1}{4})) = ab$. Thus, for certain simple probabilistic processes p, there will exist distinct $x, y \in \mathcal{S}(p)$ such that $\mathcal{A}(x) = \mathcal{A}(y)$;

intuitively, in these cases, there will be two (or more) ways that p can perform the path u, and thus the probability of p performing the path u will be $\mathcal{V}(x)+\mathcal{V}(y)$ (or the sum over all $x \in \mathcal{S}(p)$ such that $\mathcal{A}(x) = u$). To make this more formal, we introduce the following definition:

Definition 6.1.6 *For all simple probabilistic processes $p \in P_\omega$ and paths $u \in A^*$, we define the* probability *of p* performing the path *u, denoted $\mathcal{V}(u,p)$, as follows: $\mathcal{V}(u,p) = 0$ if $\mathcal{A}(x) \neq u$ for all $x \in \mathcal{S}(p)$ and*

$$\mathcal{V}(u,p) = \sum_{\substack{x \in \mathcal{S}(p)\,\& \\ \mathcal{A}(x)=u}} \mathcal{V}(x) \quad \textit{otherwise.}$$

By abuse of notation, we have two mappings named $\mathcal{V}$. However, the following lemma leads us towards an alternative characterisation of the map $\mathcal{V}$ given in Definition 6.1.6 which will remove the need for the mappings $\mathcal{S}$, $\mathcal{A}$ and $\mathcal{V}$ (of Definition 6.1.5) and also simplify subsequent work.

Lemma 6.1.7 *For any $p = (a,f) \in P_\omega$ and $u \in A^*$, if $u \neq a\tilde{u}$ for some $\tilde{u} \in A^*$, then $\mathcal{V}(u,p) = 0$. Furthermore, for all $\tilde{u} \in A^*$:*

$$\mathcal{V}(a\tilde{u},p) = \sum_{q \in \mathsf{s}(f)} f(q) \cdot \mathcal{V}(\tilde{u},q).$$

Proof. If $p = (a,f) \in P_\omega$, then by Definition 6.1.4 if $x \in \mathcal{S}(p)$, then $x = (a, f(q))y$ for some $q \in \mathsf{s}(f)$ and $y \in \mathcal{S}(q)$, and therefore $\mathcal{A}(x) = a\mathcal{A}(y)$ for some $y \in \mathcal{S}(q)$ and $q \in \mathsf{s}(f)$. Now considering $u \in A^*$ such that $u \neq a\tilde{u}$ for any $\tilde{u} \in A^*$, from the above we have $\mathcal{A}(x) \neq u$ for all $x \in \mathcal{S}(p)$, and therefore by definition of $\mathcal{V}$, $\mathcal{V}(u,p) = 0$ as required.

For the second part of the lemma, consider any $\tilde{u} \in A^*$, if $a\tilde{u} \neq \mathcal{A}(x)$ for any $x \in \mathcal{S}(p)$. From the first part of the proof we have $\tilde{u} \neq \mathcal{A}(y)$ for all $y \in \mathcal{S}(q)$ and $q \in \mathsf{s}(f)$, and hence by definition of $\mathcal{V}$:

$$\mathcal{V}(a\tilde{u},p) = 0 = \sum_{q \in \mathsf{s}(f)} f(q) \cdot 0 = \sum_{q \in \mathsf{s}(f)} f(q) \cdot \mathcal{V}(\tilde{u},q).$$

On the other hand, if $a\tilde{u} = \mathcal{A}(x)$ for some $x \in \mathcal{S}$, then by Definition 6.1.6:

$$
\begin{aligned}
\mathcal{V}(a\tilde{u}, p) &= \sum_{\substack{x \in \mathcal{S}(p)\,\& \\ A(x) = a\tilde{u}}} \mathcal{V}(x) \\
&= \sum_{\substack{q \in \mathsf{s}(f),\, y \in \mathcal{S}(q)\,\& \\ \mathcal{A}((a, f(q))y) = a\tilde{u}}} \mathcal{V}((a, f(q))y) && \text{by Definition 6.1.4} \\
&= \sum_{\substack{q \in \mathsf{s}(f),\, y \in \mathcal{S}(q) \\ \&\, \mathcal{A}(y) = \tilde{u}}} f(q) \cdot \mathcal{V}(y) && \text{by Definition 6.1.5} \\
&= \sum_{q \in \mathsf{s}(f)} f(q) \cdot \left(\sum_{\substack{y \in \mathcal{S}(q)\,\& \\ \mathcal{A}(y) = \tilde{u}}} \mathcal{V}(y) \right) && \text{rearranging} \\
&= \sum_{q \in \mathsf{s}(f)} f(q) \cdot \mathcal{V}(\tilde{u}, q) && \text{by Definition 6.1.6}
\end{aligned}
$$

as required. □

Using this lemma, we reach the following alternative to Definition 6.1.6.

Definition 6.1.8 *For all $p \in P_\omega$ and $u \in A^*$, we define the probability of p performing the path u, denoted $\mathcal{V}(u, p)$, inductively on $u \in A^n$ as follows. For all $p \in P_\omega$ put:*

$$
\mathcal{V}(\langle\rangle, p) = \begin{cases} 1 & \text{if } p = p_0 \\ 0 & \text{otherwise} \end{cases}
$$

and for all $u \in A^n$ and $a \in A$:

$$
\mathcal{V}(au, p) = \begin{cases} \sum_{q \in P_\omega} f(q) \cdot \mathcal{V}(u, q) & \text{if } p = (a, f) \text{ for some } f \in \mu(P_\omega) \\ 0 & \text{otherwise.} \end{cases}
$$

From the above we reach the following fundamental proposition concerning $\mathcal{V}$.

Proposition 6.1.9 *For all $p \in P_\omega$ the map $\mathcal{V}(\cdot, p) : A^* \to [0, 1]$ is a probability distribution.*

Proof. The proof is by induction on $p \in P_n$. If $n = 0$, then $p = p_0$ and by Definition 6.1.8:

$$
\sum_{u \in A^*} \mathcal{V}(u, p_0) = \mathcal{V}(\langle\rangle, p_0) = 1 \quad \text{as required.}
$$

Now suppose the lemma holds for some $n \in \mathbb{N}$ and consider any $p \in P_{n+1} \setminus P_n$, then $p = (a, f)$ for some $a \in A$ and $f \in \mu(P_n)$, and by definition of $\mathcal{V}$ we have $\mathsf{s}(\mathcal{V}(\cdot, p)) = \{au \mid u \in \mathsf{s}(\mathcal{V}(\cdot, q)) \text{ and } q \in \mathsf{s}(f)\}$ and hence:

$$\begin{aligned}
\sum_{u \in A^*} \mathcal{V}(u,p) &= \sum_{a\tilde{u} \in A^*} \left(\sum_{q \in \mathsf{s}(f)} f(q) \cdot \mathcal{V}(\tilde{u}, q) \right) \\
&= \sum_{q \in \mathsf{s}(f)} f(q) \cdot \left(\sum_{\tilde{u} \in A^*} \mathcal{V}(\tilde{u}, q) \right) && \text{rearranging} \\
&= \sum_{q \in \mathsf{s}(f)} f(q) \cdot 1 && \text{by induction} \\
&= 1 && \text{since } f \in \mu(P_n)
\end{aligned}$$

which completes the proof. □

To recap, we have constructed the map $\mathcal{V}$ from the set of simple probabilistic processes (P_ω) and the set of paths such processes can perform (A^*) to the unit interval, where for any $p \in P_\omega$ and $u \in A^*$ the value given by $\mathcal{V}(u, p)$ is the probability of p performing the path u. Using this map we can now explain the intuition behind the construction of our metric: for any two simple probabilistic processes p and q, to calculate the *distance* between p and q we should compute the *similarities* and *differences* between them. By the construction of simple probabilistic processes, the differences and similarities involve the *paths* that the probabilistic processes can perform and the *probabilities* of performing these paths. Following this argument, using Definition 6.1.8, for any path $u \in A^*$ we can find the difference in the probabilities of p and q performing this path, that is:

$$|\mathcal{V}(u,p) - \mathcal{V}(u,q)|. \tag{6.3}$$

Then summing (6.3) over all possible paths, that is, over $u \in A^*$, gives a candidate value for the distance between p and q which is representative of their similarities and differences. From this intuition, we can now define our metric (in fact a pseudo-metric) on P_ω as follows, where the factor $\frac{1}{2}$ is used to normalise the distance.

Proposition 6.1.10 *P_ω (and P_n for any $n \in \mathbb{N}$) is a pseudo-metric space with respect to the pseudo-metric:*

$$d_{\mathcal{S}}(p,q) = \frac{1}{2} \sum_{u \in A^*} |\, \mathcal{V}(u,p) - \mathcal{V}(u,q) \,|.$$

Furthermore, $0 \leq d_{\mathcal{S}}(p,q) \leq 1$ for all $p, q \in P_\omega$.

Proof. (M1′) For all $p, q \in P_\omega$, $d_{\mathcal{S}}(p,q) \geq 0$ and $d_{\mathcal{S}}(p,p) = 0$ follows by definition of $d_{\mathcal{S}}$.
(M2) For all $p, q \in P_\omega$, $d_{\mathcal{S}}(p,q) = d_{\mathcal{S}}(q,p)$ follows by properties of the Euclidean metric.
(M3) First, by construction $\mathcal{V}(u,s) \in [0,1]$ for all $u \in A^*$ and $s \in P_\omega$, and hence using the properties of the Euclidean metric, we obtain:

$$|\mathcal{V}(u,p) - \mathcal{V}(u,q)| + |\mathcal{V}(u,q) - \mathcal{V}(u,r)| - |\mathcal{V}(u,p) - \mathcal{V}(u,r)| \geq 0 \tag{6.4}$$

for any for any $p, q, r \in P_\omega$ and $u \in A^*$. Now by definition of $d_{\mathcal{S}}$ and rearranging:

$$\begin{aligned}
&d_{\mathcal{S}}(p,q) + d_{\mathcal{S}}(q,r) - d_{\mathcal{S}}(p,r) \\
&\quad = \tfrac{1}{2} \sum_{u \in A^*} \Big(|\mathcal{V}(u,p) - \mathcal{V}(u,q)| + |\mathcal{V}(u,q) - \mathcal{V}(u,r)| - |\mathcal{V}(u,p) - \mathcal{V}(u,r)| \Big) \\
&\quad \geq 0 \quad \text{by (6.4)},
\end{aligned}$$

and hence $d_{\mathcal{S}}(p,q) + d_{\mathcal{S}}(q,r) - d_{\mathcal{S}}(p,r) \geq 0$ as required.
To prove that $d_{\mathcal{S}}$ does not satisfy (M1) we show there exist distinct $p, q \in P_\omega$ such that $d(p,q) = 0$. Consider the simple probabilistic processes given in Figure 6.4.

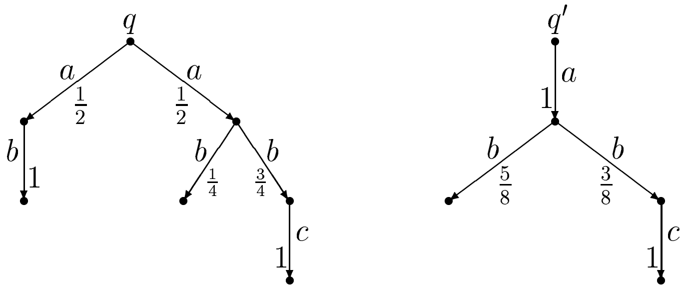


Figure 6.4: Example to show $d_{\mathcal{S}}$ is only a pseudo-metric.

Clearly $q \neq q'$ and by definition of $d_{\mathcal{S}}$ we reach:

$$\begin{aligned}
d_{\mathcal{S}}(q,q') &= \frac{1}{2}\left(\left| \left(\frac{1}{2}\cdot 1 + \frac{1}{2}\cdot\frac{1}{4}\right) - 1\cdot\frac{5}{8} \right| + \left| \frac{1}{2}\cdot\frac{3}{4}\cdot 1 - 1\cdot\frac{3}{8}\cdot 1 \right| \right) \\
&= \frac{1}{2}\left|\frac{5}{8} - \frac{5}{8}\right| + \frac{1}{2}\left|\frac{3}{8} - \frac{3}{8}\right| = 0.
\end{aligned}$$

Finally, to show $0 \leq d_{\mathcal{S}}(p,q) \leq 1$ for all $p, q \in P_\omega$, consider any $p, q \in P_\omega$. By (M1′) $0 \leq d_{\mathcal{S}}(p,q)$ and by definition $d_{\mathcal{S}}(p,q)$ equals:

$$\begin{aligned}
\tfrac{1}{2} \sum_{u \in A^*} |\mathcal{V}(u,p) - \mathcal{V}(u,q)| &\leq \tfrac{1}{2} \sum_{u \in A^*} \mathcal{V}(u,p) + \tfrac{1}{2} \sum_{u \in A^*} \mathcal{V}(u,q) && \text{rearranging} \\
&= \tfrac{1}{2}(1+1) && \text{by Proposition 6.1.9} \\
&= 1
\end{aligned}$$

as required. □

If we now return to Figure 6.1 and Figure 6.2 and calculate the distances between the processes with respect to $d_{\mathcal{S}}$, we obtain for any $n, m \in \mathbb{N}$:

$$d_{\mathcal{S}}(p_n, p_m) = d_{\mathcal{S}}(p'_n, p'_m) = |2^{-n} - 2^{-m}|$$

and so we have constructed a pseudo-metric with the required convergence properties.

The next step is to consider the Cauchy sequences with respect to $d_{\mathcal{S}}$, with which we want to model recursive simple probabilistic processes. As an example we discuss the sequence of simple probabilistic processes $\langle q_n \rangle_n$ in Figure 6.5.

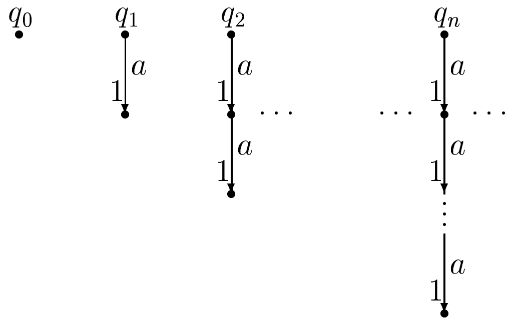


Figure 6.5: Example of recursive simple probabilistic processes.

From the methodology of de Bakker and Zucker, the limit of this sequence will model the recursive simple probabilistic process which repeatedly performs the action a with probability 1. However, it is straightforward to show that for any $n \neq m \in \mathbb{N}$, $d_{\mathcal{S}}(q_n, q_m) = 1$, and thus $\langle q_n \rangle_n$ is not a Cauchy sequence with respect to $d_{\mathcal{S}}$.

As in [KN96b], to solve this problem we introduce *truncations*, where for any $n \in \mathbb{N}$ the nth truncation of a simple probabilistic process p, denoted $p[n]$, gives only the first n *steps* that p performs, as illustrated in Figure 6.6.

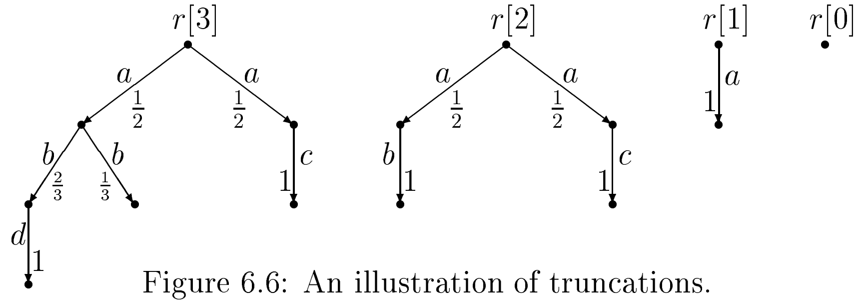


Figure 6.6: An illustration of truncations.

Formally, we define truncations on distributions and simple probabilistic processes as follows.

Definition 6.1.11 (Truncations) *Let $f \in \mu(P_\omega)$. For $k \in \mathbb{N}$ define the kth* truncation *of f, $f[k] : P_\omega \to [0,1]$, as follows. For any $p \in P_\omega$,*

$$f[k](p) = \sum_{\substack{q \in P_\omega \\ \& \, q[k]=p}} f(q)$$

where for $p \in P_\omega$ the truncation on simple probabilistic processes, $p[k]$, is defined inductively on $k \in \mathbb{N}$ by putting $p[0] = p_0$ for all p and

$$p[k+1] = \begin{cases} p_0 & \text{if } p = p_0 \\ (a, f[k]) & \text{if } p = (a,f) \text{ for some } a \in A \text{ and } f \in \mu(P_\omega). \end{cases}$$

The truncation of simple probabilistic processes (and respectively of probabilistic distributions) satisfies the properties given in the proposition below, useful in proofs of properties of our pseudo-metric, as truncations are an integral part of its definition. These properties are, moreover, reminiscent of the properties of projection spaces, for example see [GH90].

Proposition 6.1.12 *For all $p, q \in P_\omega$ and $k, m \in \mathbb{N}$:*

(a) *if $p \in P_m$, then $p[k] \in P_k$ when $k < m$ and $p[k] = p$ otherwise.*
(b) $(p[m])[k] = p[\min\{m,k\}]$.
(c) *$p[m] = q[m]$ if and only if $p[k] = q[k]$ for all $k \leq m$.*
(d) $d_{\mathcal{S}}(p[k], q[k]) \leq d_{\mathcal{S}}(p,q)$.
(e) *if $u \in A^* \setminus A^k$, then $\mathcal{V}(u, p[k]) = 0$.*

However, before we can give a proof of the above proposition we require the following lemma.

Lemma 6.1.13 *For all $p \in P_\omega$, $u \in A^*$ and $k \in \mathbb{N}$:*

$$\mathcal{V}(u, p[k]) = \sum_{\tilde{u} \upharpoonright k = u} \mathcal{V}(\tilde{u}, p).$$

Proof. The proof is by induction on $k \in \mathbb{N}$. The case for $k = 0$ follows by Proposition 6.1.9 and since $p[0] = p_0$ and $u \upharpoonright 0 = \langle\rangle$ for all $p \in P_\omega$ and $u \in A^*$.

Now suppose the lemma is true for $k \in \mathbb{N}$ and consider any $p \in P_\omega$. If $p = p_0$ then, the result follows by definition of truncations and since, for any $u \in A^*$, $u \upharpoonright (k+1) = \langle\rangle$ if and only if $u = \langle\rangle$. On the other hand, if $p = (a, f)$ for some $a \in A$ and $f \in \mu(P_\omega)$, by definition $p[k+1] = (a, f[k])$. If $u \neq au'$ for any $u' \in A^*$, then by Definition 3.1.1 if $\tilde{u} \upharpoonright (k+1) = u$ we have $\tilde{u} \neq au'$ for any $u' \in A^*$, and hence by definition of $\mathcal{V}$:

$$\mathcal{V}(u, p[k+1]) = \sum_{\tilde{u} \upharpoonright (k+1) = u} \mathcal{V}(\tilde{u}, p) = 0.$$

On the other hand, if $u = au'$ for some $u' \in A^*$, by definition of $\mathcal{V}$:

$$\begin{array}{rcll}
\mathcal{V}(au', p[k+1]) & = & \sum_{q \in \mathsf{s}(f)} f(q) \cdot \mathcal{V}(u', q[k]) & \\
& = & \sum_{q \in \mathsf{s}(f)} f(q) \cdot \left(\sum_{\tilde{u} \restriction k = u'} \mathcal{V}(\tilde{u}, q) \right) & \text{by induction} \\
& = & \sum_{a(\tilde{u} \restriction k) = au'} \mathcal{V}(a\tilde{u}, (a, f)) & \text{rearranging} \\
& = & \sum_{\grave{u} \restriction (k+1) = au'} \mathcal{V}(\grave{u}, p) & \text{by Definition 3.1.1}
\end{array}$$

as required. □

Proof. (of Proposition 6.1.12)

(a) The proof is by induction on $p \in P_n$. If $n = 0$, then $p = p_0$ and by Definition 6.1.11 $p_0[k] = p_0$ for all $k \in \mathbb{N}$ as required.

Now suppose that (a) holds for some $n \in \mathbb{N}$ and consider any $p \in P_{n+1} \setminus P_n$. Then p equals (a, f) for some $a \in A$ and $f \in \mu(P_n)$. If $k \leq n+1$, either $k = 0$ and by definition $p[k] = p_0 \in P_0$, or $k \geq 1$ and by definition $p[k] = (a, f[k-1])$. In the second case to prove $p \in P_k$ by definition of P_k it is sufficient to show $f[k-1] \in \mu(P_{k-1})$. By Definition 6.1.11, we have $\mathsf{s}(f[k-1]) = \{q[k-1] \mid q \in \mathsf{s}(f)\}$, then by induction we have $\mathsf{s}(f[k-1]) \subseteq P_{k-1}$. Moreover, by definition of truncations:

$$\begin{array}{rcll}
\sum_{\tilde{q} \in P_\omega} f[k-1](\tilde{q}) & = & \sum_{\tilde{q} \in \mathsf{s}(f[k-1])} f[k-1](\tilde{q}) & \\
& = & \sum_{\tilde{q} \in \mathsf{s}(f[k-1])} \left(\sum_{\substack{q \in P_\omega \,\& \\ q[k-1] = \tilde{q}}} f(p) \right) & \text{by Definition 6.1.11} \\
& = & \sum_{q \in \mathsf{s}(f)} f(q) & \text{from above} \\
& = & 1 & \text{since } f \in \mu(P_n)
\end{array}$$

and thus $p[k] \in P_k$ as required. The case for $k \geq n+1$ follows similarly by induction.

(b) The proof is by induction on $k \in \mathbb{N}$. If $k = 0$ the proof follows by definition of truncations. Now suppose the result is true for $k \in \mathbb{N}$ and consider any $p \in P_\omega$. Then either $p = p_0$ and by Definition 6.1.11 $(p[m])[k+1] = p[\min\{m, k+1\}] = p_0$. Or $p = (a, f)$ for some $a \in A$ and $f \in \mu(P_\omega)$, in which case $(p[m])[k+1] =$

$(a, (f[m-1])[k])$ and $p[\min\{m, k+1\}] = (a, f[\min\{m-1, k\}])$. Therefore, to show (b) holds it is sufficient to show $(f[m-1])[k] = f[\min\{m-1, k\}]$ and by Definition 6.1.11 we have:

$$\begin{aligned}
\mathsf{s}((f[m-1])[k]) &= \{\tilde{q}[k] \mid \tilde{q} \in \mathsf{s}(f[m-1])\} \\
&= \{(q[m-1])[k] \mid q \in \mathsf{s}(f)\} && \text{by Definition 6.1.11} \\
&= \{q[\min\{m-1, k\}] \mid q \in \mathsf{s}(f)\} && \text{by induction} \\
&= \mathsf{s}(f[\min\{m-1, k\}]).
\end{aligned}$$

Similarly, using induction we can show $(f[m-1])[k](q) = f[\min\{m-1, k\}](q)$ for all $q \in P_\omega$, and hence $(p[m])[k+1] = p[\min\{m, k+1\}]$ as required.

(c) The proof follows techniques similar to (a) and (b), using induction on $m \in \mathbb{N}$.

(d) Consider any $p, q \in P_\omega$ and $k \in \mathbb{N}$, then by definition of $d_\mathcal{S}$:

$$\begin{aligned}
d_\mathcal{S}(p[k], q[k]) &= \tfrac{1}{2} \sum_{u \in A^*} |\, \mathcal{V}(u, p[k]) - \mathcal{V}(u, q[k]) \,| \\
&= \tfrac{1}{2} \sum_{u \in A^*} \left| \sum_{\tilde{u} \restriction k = u} \mathcal{V}(\tilde{u}, p) - \sum_{\tilde{u} \restriction k = u} \mathcal{V}(\tilde{u}, q) \right| && \text{by Lemma 6.1.13} \\
&\leq \tfrac{1}{2} \sum_{u \in A^*} \left(\sum_{\tilde{u} \restriction k = u} |\mathcal{V}(\tilde{u}, p) - \mathcal{V}(\tilde{u}, q)| \right) && \text{rearranging} \\
&= \tfrac{1}{2} \sum_{\tilde{u} \in A^*} |\mathcal{V}(\tilde{u}, p) - \mathcal{V}(\tilde{u}, q)| \\
&= d_\mathcal{S}(p, q)
\end{aligned}$$

as required.

(e) Consider any $p \in P_\omega$, $k \in \mathbb{N}$ and $u \in A^* \setminus A^k$, then by Definition 3.1.1 $\tilde{u} \restriction k \neq u$ for any $\tilde{u} \in A^*$ and hence:

$$\begin{aligned}
0 &= \sum_{\tilde{u} \restriction k = u} \mathcal{V}(\tilde{u}, p) \\
&= \mathcal{V}(u, p[k]) && \text{by Lemma 6.1.13}
\end{aligned}$$

as required.

□

Using truncations we reach the following classical definition of an ultra-metric d_t, which is the metric Baier and Kwiatkowska use to give denotational semantics to a probabilistic version of CCS [BK97].

Definition 6.1.14 *For all p and $q \in P_\omega$:*

$$d_t(p,q) = \begin{cases} 0 & \text{if } p = q \\ 2^{1-\min\{k \mid p[k] \neq q[k]\}} & \text{otherwise.} \end{cases}$$

If we return to the recursive processes given in Figure 6.5, we have $d_t(q_m, q_n) = 2^{-m}$ for any $m \leq n \in \mathbb{N}$, and hence $\langle q_n \rangle_{n \in \mathbb{N}}$ is a Cauchy sequence with respect to d_t. However, if we calculate the values of d_t on the processes in Figure 6.1 and Figure 6.2 then:

$$d_t(p_n, p_m) = \frac{1}{2} \text{ and } d_t(p'_n, p'_m) = \frac{1}{4}$$

for any $n \neq m \in \mathbb{N}$. Thus, we lose the convergence properties of the pseudo-metric $d_{\mathcal{S}}$, that is, $\langle p_n \rangle_n$ and $\langle p'_n \rangle_n$ are no longer Cauchy sequences converging to p and p' respectively. To keep the *properties* of $d_{\mathcal{S}}$, and also to incorporate the required Cauchy sequences, we define a pseudo-metric on P_ω as follows.

Definition 6.1.15 *For all $p, q \in P_\omega$, we define $d_\omega : P_\omega \times P_\omega \to [0,1]$ as follows:*

$$d_\omega(p,q) = \sum_{k=0}^{\infty} 2^{-k} d_{\mathcal{S}}(p[k], q[k]).$$

Proposition 6.1.16 *(P_ω, d_ω) (and (P_n, d_ω) for any $n \in \mathbb{N}$) is a pseudo-metric space. Furthermore, $0 \leq d_\omega(p,q) \leq 1$ for all $p, q \in P_\omega$.*

Proof. (M1′) For all $p, q \in P_\omega$, $d_\omega(p,q) \geq 0$ and $d_\omega(p,p) = 0$ follows from Proposition 6.1.12(a) and since $d_{\mathcal{S}}$ satisfies (M1′).
(M2) For all $p, q \in P_\omega$, $d_\omega(p,q) = d_\omega(q,p)$ follows from Proposition 6.1.12(a) and since $d_{\mathcal{S}}$ satisfies (M2).
(M3) Consider any p, q and $r \in P_\omega$, then by Proposition 6.1.12(a), $p[k]$, $q[k]$ and $r[k] \in P_\omega$ for all $k \in \mathbb{N}$, and since $d_{\mathcal{S}}$ is a pseudo-metric on P_ω we have:

$$d_{\mathcal{S}}(p[k], q[k]) + d_{\mathcal{S}}(q[k], r[k]) - d_{\mathcal{S}}(p[k], r[k]) \geq 0$$

for all $k \in \mathbb{N}$, and hence,

$$\sum_{k=1}^{\infty} 2^{-k}\Big(d_{\mathcal{S}}(p[k], q[k]) + d_{\mathcal{S}}(q[k], r[k]) - d_{\mathcal{S}}(p[k], r[k])\Big) \geq 0.$$

Rearranging, we have:

$$\sum_{k=1}^{\infty} 2^{-k} d_{\mathcal{S}}(p[k], q[k]) + \sum_{k=1}^{\infty} 2^{-k} d_{\mathcal{S}}(q[k], r[k]) \geq \sum_{k=1}^{\infty} 2^{-k} d_{\mathcal{S}}(p[k], r[k]),$$

that is, $d_\omega(p,q) + d_\omega(q,r) \geq d_\omega(p,r)$ as required.
The proof that d_ω does not satisfy (M1) follows from the case for $d_\mathcal{S}$ using Proposition 6.1.12(a) and Proposition 6.1.12(d).
Finally, for all $p,q \in P_\omega$ $0 \leq d_\omega(p,q)$ is a result of (M1$'$). To show $d_\omega(p,q) \leq 1$ for all $p,q \in P_\omega$, consider any $p,q \in P_\omega$, then from the definition of truncations, $p[0] = q[0] = p_0$, and hence since $d_\mathcal{S}$ is a pseudo-metric, $d_\mathcal{S}(p[0], q[0]) = 0$. Substituting this into the definition of d_ω, we have:

$$\begin{aligned} d_\omega(p,q) &= \sum_{k=1}^{\infty} 2^{-k} d_\mathcal{S}(p[k], q[k]) \\ &\leq \sum_{k=1}^{\infty} 2^{-k} && \text{by Proposition 6.1.10} \\ &= 1 \end{aligned}$$

as required. □

If we now consider the processes in Figure 6.1, Figure 6.2 and Figure 6.5 and calculate the distance between the processes with respect to the pseudo-metric d_ω, we have:

$$d_\omega(p_n, p_m) = |2^{-n} - 2^{-m}|, \quad d_\omega(p'_n, p'_m) = \frac{1}{2}|2^{-n} - 2^{-m}|$$

$$\text{and} \quad d_\omega(q_m, q_n) = \begin{cases} 0 & \text{if } m = n \\ 2^{-\min\{n,m\}} & \text{otherwise} \end{cases}$$

and hence d_ω has captured both the properties of $d_\mathcal{S}$ and d_t.

Our pseudo-metric nevertheless specialises to the metric of de Bakker and Zucker [BZ82]. To see this consider a restriction, for each $n \in \mathbb{N}$, of the set $\mu(P_n)$ to the set of *point distributions* of P_n (see Definition 3.2.2), that is, the set $\{\eta_p \,|\, p \in P_n\}$. As before, we inductively denote $\{p_0\} \cup A \times \{\eta_p \,|\, p \in P^\eta_n\}$ by P^η_{n+1} and put $P^\eta_\omega = \cup_n P^\eta_n$. Intuitively, if $p = (a, \eta_q) \in P^\eta_n$ then the probability of p performing the action a and becoming q is 1, and the probability of p becoming any other process is 0. This can be compared with de Bakker and Zucker's construction of simple processes, where the elements are of the form $p = p_0$ or $p = (a,q)$, for a action and q process. Formally, we have the following lemma and proposition.

Lemma 6.1.17 *For all $p,q \in P^\eta_\omega$:*

$$d_\mathcal{S}(p,q) = \begin{cases} 0 & \textit{if } p = q \\ 1 & \textit{otherwise.} \end{cases}$$

Proof. The proof is by induction on $p,q \in P_n$. If $n = 0$, then $p = q = p_0$ and the lemma holds since $d_\mathcal{S}$ is a pseudo-metric.

Now suppose the lemma holds for some $n \in \mathbb{N}$ and consider any $p, q \in P_{n+1}$. If $p = q$, then since $d_{\mathcal{S}}$ is a pseudo-metric $d_{\mathcal{S}}(p,q) = 0$. On the other hand, if $p \neq q$, without loss of generality we have the following three cases to consider.

1. $p \neq q = p_0$, then by definition of $\mathcal{V}$, if $\mathcal{V}(u,p) > 0$, then $\mathcal{V}(u,q) = 0$ and vice versa. Substituting this into the definition of $d_{\mathcal{S}}$ we have:

$$\begin{aligned} d_{\mathcal{S}}(p,q) &= \tfrac{1}{2}\left(\sum_{u \in A^*} \mathcal{V}(u,p) + \sum_{u \in A^*} \mathcal{V}(u,q)\right) \\ &= \tfrac{1}{2}(1+1) && \text{by Proposition 6.1.9} \\ &= 1. \end{aligned}$$

2. $p = (a, \eta_{p'})$ and $q = (b, \eta_{q'})$ such that $a \neq b \in A$ and $p', q' \in P_n$, then by definition of $\mathcal{V}$ if $\mathcal{V}(u,p) > 0$, $\mathcal{V}(u,q) = 0$ and vice versa, and hence as in the first case we have $d_{\mathcal{S}}(p,q) = 1$.

3. $p = (a, \eta_{p'})$ and $q = (a, \eta_{q'})$ such that $a \in A$ and $p' \neq q' \in P_n$, then by definition of $\mathcal{V}$ and $d_{\mathcal{S}}$:

$$\begin{aligned} d_{\mathcal{S}}(p,q) &= \tfrac{1}{2} \sum_{au \in A^*} |1 \cdot \mathcal{V}(u,p') - 1 \cdot \mathcal{V}(u,q')| \\ &= \tfrac{1}{2} \sum_{u \in A^*} |\mathcal{V}(u,p') - \mathcal{V}(u,q')| && \text{rearranging} \\ &= d_{\mathcal{S}}(p',q') && \text{by definition of } d_{\mathcal{S}} \\ &= 1 && \text{by induction.} \end{aligned}$$

Since these are all the possible cases the lemma is proved by induction. □

Proposition 6.1.18 *The pseudo-metric d_ω is equivalent to the metric of de Bakker and Zucker (see Definition 6.0.1) on the subspace P_ω^η of P_ω.*

Proof. First, classical results have shown us that the metric of de Bakker and Zucker given in Definition 6.0.1 is equivalent to the metric d_t given in Definition 6.1.14. It is therefore sufficient to prove that d_ω is equivalent to d_t on the subspace P_ω^η of P_ω. Now, consider any $p, q \in P_\omega^\eta$, then if $p = q$, it follows that $d_\omega(p,q) = 0$ since d_ω is a pseudo-metric. On the other hand, if $p \neq q$, using Proposition 6.1.12(c) and Lemma 6.1.17 and letting $m = \min\{k \mid p[k] \neq q[k]\}$, by definition of d we have:

$$d_\omega(p,q) = \sum_{k=m}^{\infty} 2^{-k} = 2^{1-m}$$

and hence, d_ω is equivalent to the metric d_t on the subspace P_ω^η of P_ω as required. □

We now consider some of the properties of the pseudo-metrics $d_{\mathcal{S}}$ and d_ω on elements of P_ω.

Lemma 6.1.19 *For all* $f, g \in \mu(P_\omega)$ *and* $a \neq b \in A$: $d_{\mathcal{S}}((a, f), (b, g)) = 1$.

Proof. Consider any $f, g \in \mu(P_\omega)$ and $a \neq b \in A$, then by definition of $d_{\mathcal{S}}$ and $\mathcal{V}$:

$$\begin{aligned} d_{\mathcal{S}}((a,f),(b,g)) &= \tfrac{1}{2} \sum_{au \in A^*} |\mathcal{V}(au,(a,f)) - 0| + \tfrac{1}{2} \sum_{bu \in A^*} |0 - \mathcal{V}(bu,(a,g))| \\ &= \tfrac{1}{2} \sum_{au \in A^*} \mathcal{V}(au,(a,f)) + \sum_{bu \in A^*} \mathcal{V}(bu,(a,g)) \\ &= \tfrac{1}{2}(1+1) \quad \text{by Proposition 6.1.9} \\ &= 1 \end{aligned}$$

as required. □

Lemma 6.1.20 *Let* a *and* b *be distinct elements of* A, $f, g \in \mu(P_\omega)$, $p \in P_\omega$ *and* $m \in \mathbb{N}$, *then*

$$d_\omega((a,f),(b,g)) = d_\omega(p_0,(a,f)) = 1, \;\; d_\omega((a,f),(a,g)) \leq \frac{1}{2} \;\; \textit{and} \;\; d_\omega(p,p[m]) \leq \frac{1}{2^m}.$$

Proof. Consider any $f, g \in \mu(P_\omega)$ and distinct $a, b \in A$, then by Lemma 6.1.19 and Proposition 6.1.12(a):

$$d_{\mathcal{S}}((a,f)[k+1],(b,g)[k+1]) = d_{\mathcal{S}}((a,f[k]),(b,g[k])) = 1$$

for all $k \geq 1$. Substituting this and the fact that $(a,f)[0] = (b,g)[0] = p_0$ into the definition of d_ω we have:

$$d_\omega((a,f),(b,g)) = \sum_{k=1}^{\infty} 2^{-k} = 1.$$

Similarly, we can show that $d_\omega(p_0,(a,f)) = 1$.

For the third part, since $P_0 = \{p_0\}$, using Proposition 6.1.12(a) we have $f[0] = g[0]$, and therefore $(a,f)[1] = (a,g)[1]$ by definition of truncations. Hence, by definition of d_ω we have:

$$\begin{aligned} d_\omega((a,f),(a,g)) &= \sum_{k=2}^{\infty} 2^{-k} d_{\mathcal{S}}((a,f)[k],(b,g)[k]) \\ &\leq \sum_{k=2}^{\infty} 2^{-k} \qquad \text{by Proposition 6.1.16} \\ &= \tfrac{1}{2} \end{aligned}$$

as required.

Finally, consider any $p \in P_\omega$ and $m \in \mathbb{N}$, then by definition of d_ω:

$$\begin{aligned} d_\omega(p,p[k]) &= \sum_{k=0}^{\infty} 2^{-k} d_{\mathcal{S}}(p[k],(p[m])[k]) \\ &= \sum_{k=0}^{\infty} 2^{-k} d_{\mathcal{S}}(p[k],(p[\min\{m,k\}]) \quad \text{by Proposition 6.1.12}(b) \\ &= \sum_{k=m+1}^{\infty} 2^{-k} d_{\mathcal{S}}(p[k],(p[k]) \quad \text{since } d_{\mathcal{S}} \text{ is a pseudo-metric} \\ &\leq \sum_{k=m+1}^{\infty} 2^{-k} \qquad \text{by Proposition 6.1.16} \\ &= \tfrac{1}{2^m} \end{aligned}$$

as required. □

We now apply the standard metric completion technique to derive the metric space (P, d) of (finite and infinite) simple probabilistic processes.

Definition 6.1.21 *Define the space* (P, d) *of* simple probabilistic processes *as the metric completion of* (P_ω, d_ω).

Applying the standard completion techniques (see Theorem 3.3.7), P consists of the set of equivalence classes of Cauchy sequences of P_ω under the equivalence $\sim$, where

$$\langle p_n \rangle_{n\in\mathbb{N}} \sim \langle q_n \rangle_{n\in\mathbb{N}} \quad \text{if and only if} \quad \lim_{n\to\infty} d_\omega(p_n, q_n) = 0,$$

and for any Cauchy sequences $\langle p_n \rangle_{n\in\mathbb{N}}$ and $\langle q_n \rangle_{n\in\mathbb{N}}$ the metric d is given by:

$$d(\langle p_n \rangle_{n\in\mathbb{N}}, \langle q_n \rangle_{n\in\mathbb{N}}) = \lim_{n\to\infty} d_\omega(p_n, q_n).$$

Categorical techniques of [AR89] have not been used to derive a domain equation for simple probabilistic processes as it is unclear how to define a functor to represent this construction; this is due to the fact that our pseudo-metric d_ω is not defined inductively in correspondence with the inductively defined metric spaces.

We now introduce some useful lemmas concerning the Cauchy sequences of P_ω.

Lemma 6.1.22 *For all* $p \in P_\omega$, $\langle p[n] \rangle_n$ *is a Cauchy sequence.*

Proof. Consider any $p \in P_\omega$ and $n, m, k \in \mathbb{N}$, then $(p[n])[k] = p[\min\{n, k\}]$ and $(p[m])[k] = p[\min\{m, k\}]$ by Proposition 6.1.12(b). Therefore, since $d_{\mathcal{S}}$ is a pseudo-metric for any $k \leq \min\{n, m\}$:

$$d_{\mathcal{S}}((p[n])[k], (p[m])[k]) = d_{\mathcal{S}}(p[k], p[k]) = 0.$$

and substituting this into the definition of d_ω we have:

$$\begin{aligned} d_\omega(p[n], p[m]) &= \sum_{k=1+\min\{m,n\}}^{\infty} 2^{-k} d_{\mathcal{S}}(p[\min\{n,k\}], p[\min\{m,k\}]) \\ &\leq \sum_{k=1+\min\{m,n\}}^{\infty} 2^{-k} \quad \text{by Proposition 6.1.10} \\ &= 2^{-\min\{m,n\}} \end{aligned}$$

and thus $\langle p[n] \rangle_n$ is a Cauchy sequence. □

Lemma 6.1.23 *If* $\langle p_n \rangle_{n\in\mathbb{N}}$ *is a sequence in* P_ω *such that* $p_{n+1}[n] = p_n[n]$ *for all* $n \in \mathbb{N}$, *then* $\langle p_n \rangle_{n\in\mathbb{N}}$ *is Cauchy and* $p_m[n] = p_n[n]$ *for all* $m \geq n \in \mathbb{N}$. *Furthermore, if* $\langle q_n \rangle_{n\in\mathbb{N}}$ *is a sequence in* P_ω *such that* $q_{n+1}[n] = q_n[n]$ *for all* $n \in \mathbb{N}$ *and* $\langle p_n \rangle_{n\in\mathbb{N}} \sim \langle q_n \rangle_{n\in\mathbb{N}}$, *then* $d_\omega(p_n[n], q_n[n]) = 0$ *for all* $n \in \mathbb{N}$.

Proof. First, if $\langle p_n \rangle_{n\in\mathbb{N}}$ is a sequence in P_ω such that $p_{n+1}[n] = p_n[n]$ for all $n \in \mathbb{N}$, then since $d_{\mathcal{S}}$ is a pseudo-metric and using Proposition 6.1.12(c) we have:

$$d_{\mathcal{S}}(p_{n+1}[k], p_n[k]) = 0 \text{ for all } k \leq n \text{ and } n \in \mathbb{N}.$$

Then, substituting this into the definition of d_ω, for any $n \in \mathbb{N}$:

$$\begin{array}{rcll} d_\omega(p_{n+1}, p_n) & = & \sum_{k=n+1}^{\infty} 2^{-k} d_{\mathcal{S}}(p_{n+1}[k], p_n[k]) & \\ & \leq & \sum_{k=n+1}^{\infty} 2^{-k} & \text{by Proposition 6.1.10} \\ & = & 2^{-n} & \end{array}$$

and hence $\langle p_n \rangle_{n\in\mathbb{N}}$ is Cauchy.

Next, we prove $p_m[n] = p_n[n]$ for all $m \geq n \in \mathbb{N}$, by induction on $m \geq n$. If $m = n$ the result is trivial. Now suppose that $p_m[n] = p_n[n]$ for for some $m \geq n$, then:

$$\begin{array}{rcll} p_{m+1}[n] & = & p_{m+1}[\min\{m, n\}] & \\ & = & (p_{m+1}[m])[n] & \text{by Proposition 6.1.12}(b) \\ & = & p_m[n] & \text{by hypothesis} \\ & = & p_n[n] & \text{by induction.} \end{array}$$

and since $n \in \mathbb{N}$ was arbitrary, this part of the lemma holds by induction.

Finally, if $\langle q_n \rangle_{n\in\mathbb{N}}$ is a sequence in P_ω such that $q_{n+1}[n] = q_n[n]$ for all $n \in \mathbb{N}$ and $\langle p_n \rangle_{n\in\mathbb{N}} \sim \langle q_n \rangle_{n\in\mathbb{N}}$. Then, using the second part of the lemma, we have:

$$p_m[n] = p_n[n] \text{ and } q_m[n] = q_n[n] \text{ for all } m \geq n \in \mathbb{N} \tag{6.5}$$

and using Proposition 6.1.12(d), for any $n, k \in \mathbb{N}$:

$$d_\omega(p_k[n], q_k[n]) \leq d_\omega(p_k, q_k).$$

Therefore, since $\langle p_n \rangle_{n\in\mathbb{N}} \sim \langle q_n \rangle_{n\in\mathbb{N}}$, by definition of $\sim$:

$$\begin{array}{rcll} \lim_{k\to\infty} d_\omega(p_k, q_k) = 0 & \Rightarrow & \lim_{k\to\infty} d_\omega(p_k[n], q_k[n]) = 0 & \\ & \Rightarrow & \lim_{k\to\infty} d_\omega(p_n[n], q_n[n]) = 0 & \text{by (6.5)} \\ & \Rightarrow & d_\omega(p_n[n], q_n[n]) = 0 & \end{array}$$

as required. □

Lemma 6.1.24 *If $\langle p_n \rangle_{n\in\mathbb{N}}$ and $\langle q_n \rangle_{n\in\mathbb{N}}$ are Cauchy sequence and $\langle p_n \rangle_{n\in\mathbb{N}} \not\sim \langle q_n \rangle_{n\in\mathbb{N}}$, then there exists $n \in \mathbb{N}$ such that $p_n[n] \neq q_n[n]$.*

Proof. The proof is by contradiction, suppose $\langle p_n\rangle_{n\in\mathbb{N}}$ and $\langle q_n\rangle_{n\in\mathbb{N}}$ are Cauchy sequence such that $\langle p_n\rangle_{n\in\mathbb{N}} \not\sim \langle q_n\rangle_{n\in\mathbb{N}}$ and $p_n[n] = q_n[n]$ for all $n \in \mathbb{N}$. Then, since $d_{\mathcal{S}}$ is a pseudo-metric and using Proposition 6.1.12(c):

$$d_{\mathcal{S}}(p_n[k], q_n[k]) = 0 \text{ for all } k \leq n \text{ and } n \in \mathbb{N}$$

and hence by definition of d_ω for any $n \in \mathbb{N}$:

$$\begin{array}{rcll} d_\omega(p_n, q_n) & = & \sum\limits_{k=0}^{\infty} 2^{-k} d_{\mathcal{S}}(p_n[k], q_n[k]) & \\ & = & \sum\limits_{k=n+1}^{\infty} 2^{-k} d_{\mathcal{S}}(p_n[k], q_n[k]) & \text{from above} \\ & \leq & \sum\limits_{k=n+1}^{\infty} 2^{-k} & \text{by Proposition 6.1.10} \\ & = & 2^{-n}. & \end{array}$$

Now, by definition of d we have:

$$\begin{array}{rcll} d(\langle p_n\rangle_{n\in\mathbb{N}}, \langle q_n\rangle_{n\in\mathbb{N}}) & = & \lim\limits_{n\to\infty} d_\omega(p_n, q_n) & \\ & \leq & \lim\limits_{n\to\infty} 2^{-n} & \text{from above} \\ & = & 0 & \end{array}$$

that is $\langle p_n\rangle_{n\in\mathbb{N}} \sim \langle q_n\rangle_{n\in\mathbb{N}}$ which contradicts the hypothesis, and therefore $p_n[n] \neq q_n[n]$ for some $n \in \mathbb{N}$. $\square$

6.2 Denotational Semantics for $\mathrm{RP_p}$

Using the complete metric space (P, d), we can now give denotational semantics for our language $\mathrm{RP_p}$, assuming $A = \mathcal{A}ct$. The first step is the introduction of the semantic operators: synchronous parallel ($\|$), restriction ($\upharpoonright$), and relabelling ($[\lambda]$), where following the definition of RP we require that $\lambda : A \to A$ is bijective. However, before we can do this we require the following definition.

Definition 6.2.1 *The* degree *of a process $p \in P_\omega$ is defined inductively by putting $deg(p_0) = 0$ and $deg(p) = n+1$ if $p \in P_{n+1} \setminus P_n$ for some $n \in \mathbb{N}$.*

We can now define the semantic operators on the pseudo-metric space P_ω by induction on the degree.

Definition 6.2.2 (Parallel Operator) *Let $p \,\|\, p_0 = p_0 \,\|\, p = p_0$ and*

$$(a, f) \,\|\, (b, g) = \begin{cases} (a, f \,\|\, g) & \text{if } a = b \\ p_0 & \text{if } a \neq b \end{cases} \quad \textit{where} \quad (f \,\|\, g)(r) = \sum_{\substack{r_1, r_2 \in P_\omega \\ \& \, r_1 \| r_2 = r}} f(r_1) \cdot g(r_2)$$

for any $r \in P_\omega$.

We now investigate properties of Definition 6.2.2 with respect to the map $\mathcal{V}$. Recall that for any $u_1, u_2 \in A^*$, $u_1 \cap u_2$ denotes the largest common prefix of u_1 and u_2.

Lemma 6.2.3 *For all* $p, q \in P_\omega$ *and* $u \in A^*$:

$$\mathcal{V}(u, p \,\|\, q) = \sum_{u_1 \cap u_2 = u} \mathcal{V}(u_1, p) \cdot \mathcal{V}(u_2, q).$$

Proof. The lemma is proved by induction on $deg(p \,\|\, q)$. If $deg(p \,\|\, q) = 0$, then $p \,\|\, q = p_0$ and by Definition 6.2.2 without loss of generality we have the following two cases to consider:

1. $p = p_0$, then for any $u \in A^*$, if $u \neq \langle\rangle$ and $u_1 \cap u_2 = u$ by Definition 3.1.1 $u_1 \neq \langle\rangle$, and hence by definition of $\mathcal{V}$:

$$\mathcal{V}(u, p \,\|\, q) = \sum_{u_1 \cap u_2 = u} \mathcal{V}(u_1, p) \cdot \mathcal{V}(u_2, q) = 0.$$

On the other hand, if $u = \langle\rangle$, using the above we have:

$$\begin{aligned}
\sum_{u_1 \cap u_2 = \langle\rangle} \mathcal{V}(u_1, p) \cdot \mathcal{V}(u_2, q) &= \sum_{u_1, u_2 \in A^*} \mathcal{V}(u_1, p) \cdot \mathcal{V}(u_2, q) \\
&= \left(\sum_{u_1 \in A^*} \mathcal{V}(u_1, p) \right) \cdot \left(\sum_{u_2 \in A^*} \mathcal{V}(u_2, q) \right) && \text{rearranging} \\
&= 1 \cdot 1 && \text{by Proposition 6.1.9} \\
&= \mathcal{V}(\langle\rangle, p_0) && \text{by Definition 6.1.8} \\
&= \mathcal{V}(\langle\rangle, p \,\|\, q) && \text{by hypothesis.}
\end{aligned}$$

2. $p = (a, f)$ and $q = (b, g)$ for some distinct $a, b \in A$ and $f, g \in \mu(P_\omega)$. Consider any $u \in A^*$, then if $u \neq \langle\rangle$ we have $u = cu'$ for some $c \in A$ and by Definition 3.1.1 if $u_1 \cap u_2 = u$ then $u_1 = cu'_1$ and $u_2 = cu'_2$ such that $u'_1 \cap u'_2 = u'$. Without loss of generality, we can suppose $c \neq a$ and therefore $\sum_{u_1 \cap u_2 = u} \mathcal{V}(u_1, p) \cdot \mathcal{V}(u_2, q)$ equals:

$$\begin{aligned}
\sum_{u'_1 \cap u'_2 = u'} \mathcal{V}(cu'_1, p) \cdot \mathcal{V}(cu'_2, q) &= \sum_{u'_1 \cap u'_2 = u'} 0 \cdot \mathcal{V}(cu'_2, q) && \text{by Definition 6.1.8 since } c \neq a \\
&= 0 \\
&= \mathcal{V}(cu', p_0) && \text{by Definition 6.1.8} \\
&= \mathcal{V}(u, p \,\|\, q) && \text{by hypothesis.}
\end{aligned}$$

On the other hand, if $u = \langle\rangle$, similarly to the first case we have:

$$\sum_{u_1 \cap u_2 = \langle\rangle} \mathcal{V}(u_1, p) \cdot \mathcal{V}(u_2, q) = \mathcal{V}(u, p \,\|\, q) = 1.$$

Then since these are all the possible cases, the lemma holds for $n = 0$.

Now, suppose the lemma holds for some $n \in \mathbb{N}$, and consider any $p, q \in P$ such that $deg(p \,\|\, q) = n + 1$. Then, by Definition 6.2.2, $p \,\|\, q = (a, f \,\|\, g)$ for some $a \in A$ and $f, g \in \mu(P_\omega)$ such that $p = (a, f)$ and $q = (a, g)$. Now considering any $u \in A^*$, if $u \neq au'$ for some $u' \in A^*$ and $u_1 \cap u_2 = u$, by Definition 3.1.1 without loss of generality we can suppose $u_1 \neq au'$ for any $u' \in A^*$, and hence by Definition 6.1.8 we have:

$$\sum_{u_1 \cap u_2 = u} \mathcal{V}(u_1, p) \cdot \mathcal{V}(u_2, q) = \sum_{u_1 \cap u_2 = u} 0 \cdot \mathcal{V}(u_2, q) = 0 = \mathcal{V}(u, p \,\|\, q).$$

On the other hand if $u = au'$ for some $u' \in A^*$ and $u_1 \cap u_2 = u$, by Definition 3.1.1 $u_1 = au_1'$ and $u_2 = au_2'$ such that $u_1' \cap u_2' = u'$, and from Definition 6.2.2:

$$\begin{aligned}
\mathcal{V}(au', p \,\|\, q) &= \sum_{\substack{p' \in \mathsf{s}(f) \\ \& \, q' \in \mathsf{s}(g)}} \Big(f(p') \cdot g(q')\Big) \cdot \mathcal{V}(u', p' \,\|\, q') \\
&= \sum_{\substack{p' \in \mathsf{s}(f) \\ \& \, q' \in \mathsf{s}(g)}} \Big(f(p') \cdot g(q')\Big) \cdot \left(\sum_{u_1' \cap u_2' = u'} \mathcal{V}(u_1', p') \cdot \mathcal{V}(u_2', q') \right) && \text{by induction} \\
&= \sum_{u_1' \cap u_2' = u'} \left(\sum_{p' \in \mathsf{s}(f)} f(p') \cdot \mathcal{V}(u_1', p') \right) \cdot \left(\sum_{q' \in \mathsf{s}(g)} g(q') \cdot \mathcal{V}(u_2', q')) \right) \\
&= \sum_{u_1' \cap u_2' = u'} \mathcal{V}(au_1', p) \cdot \mathcal{V}(au_2', q) && \text{by Definition 6.1.8} \\
&= \sum_{u_1 \cap u_2 = au'} \mathcal{V}(u_1, p) \cdot \mathcal{V}(u_2, q) && \text{from above}
\end{aligned}$$

as required. □

Lemma 6.2.4 *For all* $p, q \in P_\omega$ *and* $k \in \mathbb{N}$: $(p \,\|\, q)[k] = p[k] \,\|\, q[k]$.

Proof. The proof is by induction on $k \in \mathbb{N}$. If $k = 0$, then by definition of truncations and $\|$: $(p \,\|\, q)[0] = p[0] \,\|\, q[0] = p_0$.

Now, suppose the lemma holds for some $k \in \mathbb{N}$ and consider any $p, q \in P_\omega$. If $p \,\|\, q = p_0$, then the result follows by Definition 6.1.11 and Definition 6.2.2. On the other hand, if $p \,\|\, q \neq p_0$, then $p \,\|\, q = (a, f \,\|\, g)$ for some $a \in A$ and $f, g \in \mu(P_\omega)$ and by Definition 6.2.2 to prove $(p \,\|\, q)[k+1] = p[k+1] \,\|\, q[k+1]$ it is enough to show $(f \,\|\, g)[k] = f[k] \,\|\, g[k]$. By Definition 6.2.2 we have:

$$\begin{aligned}
\mathsf{s}(f[k] \,\|\, g[k]) &= \{\tilde{p} \,\|\, \tilde{q} \mid \tilde{p} \in \mathsf{s}(f[k]) \text{ and } \tilde{q} \in \mathsf{s}(g[k])\} \\
&= \{\hat{p}[k] \,\|\, \hat{q}[k] \mid \hat{p} \in \mathsf{s}(f) \text{ and } \hat{q} \in \mathsf{s}(g)\} && \text{by Definition 6.1.11} \\
&= \{(\hat{p} \,\|\, \hat{q})[k] \mid \hat{p} \in \mathsf{s}(f) \text{ and } \hat{q} \in \mathsf{s}(g)\} && \text{by induction} \\
&= \mathsf{s}((f \,\|\, g)[k]) && \text{by Definition 6.1.11.}
\end{aligned}$$

Similarly, we can show $(f \,\|\, g)[k](r) = (f[k] \,\|\, g[k])(r)$ for all $r \in P_\omega$, and thus,

$$(p \,\|\, q)[k+1] = p[k+1] \,\|\, q[k+1]$$

as required. $\square$

Proposition 6.2.5 $\|$ *is continuous and well-defined on* (P_ω, d_ω).

Proof. Consider any p, q and $r \in P_\omega$ and $k \in \mathbb{N}$, then by Lemma 6.2.4 we have:

$$
\begin{aligned}
&d_{\mathcal{S}}((p \,\|\, r)[k], (q \,\|\, r)[k]) = d_{\mathcal{S}}(p[k] \,\|\, r[k], q[k] \,\|\, r[k]) \\
&= \tfrac{1}{2} \sum_{u \in A^*} |\mathcal{V}(u, p[k] \,\|\, r[k]) - \mathcal{V}(u, q[k] \,\|\, r[k])| && \text{by definition of } d_{\mathcal{S}} \\
&= \tfrac{1}{2} \sum_{u \in A^*} \left| \sum_{u_1 \cap u_2 = u} \Big(\mathcal{V}(u_1, p[k]) \cdot \mathcal{V}(u_2, r[k]) - \mathcal{V}(u_1, q[k]) \cdot \mathcal{V}(u_2, r[k]) \Big) \right| \\
& && \text{by Lemma 6.2.3} \\
&\leq \tfrac{1}{2} \sum_{u \in A^*} \left(\sum_{u_1 \cap u_2 = u} \mathcal{V}(u_2, r[k]) \cdot |\mathcal{V}(u_1, p[k]) - \mathcal{V}(u_1, q[k])| \right) \\
&= \tfrac{1}{2} \sum_{u_1, u_2 \in A^*} \mathcal{V}(u_2, r[k]) \cdot |\mathcal{V}(u_1, p[k]) - \mathcal{V}(u_1, q[k])| && \text{rearranging} \\
&= \tfrac{1}{2} \sum_{u \in A^*} 1 \cdot |\mathcal{V}(u, p[k]) - \mathcal{V}(u, q[k])| && \text{by Proposition 6.1.9} \\
&= d_{\mathcal{S}}(p[k], q[k]) && \text{by definition of } d_{\mathcal{S}}
\end{aligned}
$$

and since this was for any $k \in \mathbb{N}$ by definition of d_ω:

$$
\begin{aligned}
d_\omega(p \,\|\, r, q \,\|\, r) &= \sum_{k=0}^{\infty} 2^{-k} d_{\mathcal{S}}((p \,\|\, r)[k], (q \,\|\, r)[k]) \\
&\leq \sum_{k=1}^{\infty} 2^{-k} d_{\mathcal{S}}(p[k], q[k]) && \text{from above} \\
&= d_\omega(p, q) && \text{by definition.}
\end{aligned}
$$

Therefore, if p, p', q and $q' \in P_\omega$ we have:

$$
\begin{aligned}
d_\omega(p \,\|\, q, p' \,\|\, q') &\leq d_\omega(p \,\|\, q, p' \,\|\, q) + d_\omega(p' \,\|\, q, p' \,\|\, q') && \text{by the triangle inequality} \\
&\leq d_\omega(p, p') + d_\omega(q, q') && \text{from above}
\end{aligned}
$$

and thus $\|$ is continuous if well defined.

To complete the proof we show $p \,\|\, q \in P_\omega$ for all $p, q \in P_\omega$ by induction on n where $n = \max\{deg(p), deg(q)\}$. If $n = 0$, then $p = q = p_0$, and thus $p \,\|\, q \in P$ as required.

Now suppose the proposition holds for n and consider any $p,q \in P_\omega$ such that $n+1 = \max\{deg(p), deg(q)\}$, then by definition of $\|$ either $p \,\|\, q = p_0$ and hence $p||q \in P_\omega$, or $p \,\|\, q = (a, f \,\|\, g)$ for some $a \in A$ and $f,g \in \mu(P_\omega)$ such that $p = (a,f)$ and $q = (a,g)$ for some $a \in \mathcal{A}ct$ and $f,g \in \mu(P_n)$. Therefore, in the second case, by Definition 6.2.2 $p||q = (a, f||g)$, and hence to prove $p \,\|\, q \in P_\omega$, it is sufficient to show $f \,\|\, g \in \mu(P_\omega)$. First, by Definition 6.2.2 it follows that:

$$\mathsf{s}(f \,\|\, g) = \{\tilde{p} \,\|\, \tilde{q} \mid \tilde{p} \in \mathsf{s}(f) \text{ and } \tilde{q} \in \mathsf{s}(g)\} \tag{6.6}$$

and therefore by induction $\tilde{p} \,\|\, \tilde{q} \in P_\omega$ for all $\tilde{p} \in \mathsf{s}(f)$ and $\tilde{q} \in \mathsf{s}(g)$, and hence $\mathsf{s}(f \,\|\, g) \subseteq P_\omega$. Moreover, by (6.6):

$$\begin{aligned}
\sum_{r \in \mathsf{s}(f \,\|\, g)} (f \,\|\, g)(r) &= \sum_{\substack{\tilde{p} \in \mathsf{s}(f)\, \& \\ \tilde{q} \in \mathsf{s}(g)}} (f \,\|\, g)(\tilde{p} \,\|\, \tilde{q}) \\
&= \sum_{\substack{\tilde{p} \in \mathsf{s}(f)\, \& \\ \tilde{q} \in \mathsf{s}(g)}} f(\tilde{p}) \cdot g(\tilde{q}) && \text{by Definition 6.2.2} \\
&= \left(\sum_{\tilde{p} \in \mathsf{s}(f)} f(\tilde{p}) \right) \cdot \left(\sum_{\tilde{q} \in \mathsf{s}(g)} g(\tilde{q}) \right) && \text{rearranging} \\
&= 1 && \text{since } f,g \in \mu(P_\omega)
\end{aligned}$$

and thus $f \,\|\, g \in \mu(P_\omega)$ as required.

□

The next semantic operator we introduce is restriction, which we again define inductively on the degree of processes.

Definition 6.2.6 (Restriction Operator) *For any $B \subseteq A$, let:*

$$p_0 \restriction B = p_0 \quad \textit{and} \quad (a,f) \restriction B = \begin{cases} (a, f \restriction B) & \textit{if } a \in B \\ p_0 & \textit{otherwise} \end{cases} \quad \textit{where } f \restriction B(q) = \sum_{\substack{r \in P_\omega\, \& \\ r \restriction B = q}} f(r)$$

for any $q \in P_\omega$.

To investigate properties of this semantic operator, as for the case involving parallel composition we first consider a connection between $\mathcal{V}$ and the restriction operator. Recall that for any $u \in A^*$, $u \restriction B$ denotes the largest prefix of u such that all its elements are in the set B.

Lemma 6.2.7 *For all $p \in P_\omega$, $u \in A^*$ and $B \subseteq A$:*

$$\mathcal{V}(u, p \restriction B) = \sum_{u' \restriction B = u} \mathcal{V}(u', p).$$

Proof. The proof is by induction on $u \in A^n$. If $u \in A^0$, then $u = \langle\rangle$ and if $u' \restriction B = u$ for any $u' \in A^*$, either $u' = \langle\rangle$ or $u' = au''$ for some $a \notin B$. Now considering any $p \in P_\omega$, we have the following three cases:

1. $p = p_0$, then by Definition 6.2.6 $p \restriction B = p_0$ and by definition of $\mathcal{V}$ since $\langle\rangle \restriction B = \langle\rangle$:
$$\mathcal{V}(u, p \restriction B) = \sum_{u' \restriction B = u} \mathcal{V}(u', p) = 1.$$
2. $p = (a, f)$ and $a \in B$, then by Definition 6.2.6 $p \restriction B = (a, f \restriction B)$ and since $(au) \restriction B \neq \langle\rangle$ for any $u \in A^*$, by definition of $\mathcal{V}$:
$$\mathcal{V}(u, p \restriction B) = \sum_{u' \restriction B = u} \mathcal{V}(u', p) = 0.$$
3. $p = (a, f)$ and $a \notin B$, then since $(au') \restriction B = \langle\rangle$ for all $u' \in A^*$ and by definition of $\mathcal{V}$, $\mathcal{V}(u, p) = 0$ if $u \neq au'$ for some $u' \in A^*$:
$$\begin{aligned}\sum_{u' \restriction B = u} \mathcal{V}(u, p) &= \sum_{u \in A^*} \mathcal{V}(u, p) && \\ &= 1 && \text{by Proposition 6.1.9} \\ &= \mathcal{V}(\langle\rangle, p_0) && \text{by Definition 6.1.8} \\ &= \mathcal{V}(\langle\rangle, p \restriction B) && \text{by Definition 6.2.6 since } a \notin B.\end{aligned}$$

Since these are all the possible cases the lemma holds for $n = 0$.

Now suppose the lemma holds for $n \in \mathbb{N}$ and consider any $u \in A^{n+1} \setminus A^n$, then $u = a\tilde{u}$ for some $a \in A$ and $\tilde{u} \in A^n$. If $a \notin B$ by Definition 3.1.1 $u' \restriction B \neq u$ for any $u' \in A^*$. Moreover, for any $p \in P_\omega$, by Definition 6.2.6 $p \restriction B \neq (a, f)$ for any $f \in \mu(P_\omega)$, and hence by definition of $\mathcal{V}$:

$$\sum_{u' \restriction B = u} \mathcal{V}(u', p) = \mathcal{V}(u, p \restriction B) = 0.$$

On the other hand, if $a \in B$, then for any $p \in P_\omega$, either $p \neq (a, f)$ for any $f \in \mu(P_\omega)$ and by Definition 3.1.1:

$$\begin{aligned}\sum_{u' \restriction B = u} \mathcal{V}(u', p) &= \sum_{\tilde{u}' \restriction B = \tilde{u}} \mathcal{V}(a\tilde{u}', p) && \\ &= 0 && \text{since } p \neq (a, f) \text{ for any } f \in \mu(P_\omega) \\ &= \mathcal{V}(a\tilde{u}, p_0) && \text{by definition of } \mathcal{V} \\ &= \mathcal{V}(a\tilde{u}, p \restriction B) && \text{by Definition 6.2.6,}\end{aligned}$$

or $p = (a, f)$ for some $f \in \mu(P_\omega)$, in which case by Definition 6.2.6 and $\mathcal{V}$:

$$\begin{aligned}
\mathcal{V}(u, p\upharpoonright B) &= \sum_{q\in \mathsf{s}(f)} f(q)\cdot \mathcal{V}(\tilde{u}, q\upharpoonright B) \\
&= \sum_{q\in \mathsf{s}(f)} f(q)\cdot \left(\sum_{\tilde{u}'\upharpoonright B=\tilde{u}} \mathcal{V}(\tilde{u}', q)\right) && \text{by induction} \\
&= \sum_{\tilde{u}'\upharpoonright B=\tilde{u}} \left(\sum_{q\in \mathsf{s}(f)} f(q)\cdot \mathcal{V}(\tilde{u}', q)\right) && \text{rearranging} \\
&= \sum_{\tilde{u}'\upharpoonright B=\tilde{u}} \mathcal{V}(a\tilde{u}', p) && \text{by Definition 6.1.8} \\
&= \sum_{u'\upharpoonright B=a\tilde{u}} \mathcal{V}(u', p) && \text{by Definition 3.1.1 since } a \in B.
\end{aligned}$$

Thus, the lemma is proved by induction. □

Lemma 6.2.8 *For all $p \in P_\omega$, $B \subseteq A$ and $k \in \mathbb{N}$: $(p\upharpoonright B)[k] = p[k]\upharpoonright B$.*

Proof. The proof is by induction on $k \in \mathbb{N}$ and follows similarly to Lemma 6.2.4. □

Proposition 6.2.9 *For all $B \subseteq A$, $\upharpoonright B$ is continuous and well-defined on (P_ω, d_ω).*

Proof. Consider any $p, q \in P_\omega$ and $k \in \mathbb{N}$, then by Lemma 6.2.8:

$$\begin{aligned}
&d_{\mathcal{S}}((p\upharpoonright B)[k], (q\upharpoonright B)[k]) = d_{\mathcal{S}}(p[k]\upharpoonright B, q[k]\upharpoonright B) \\
&\quad= \tfrac{1}{2}\sum_{u\in A^*} |\mathcal{V}(u, p[k]\upharpoonright B) - \mathcal{V}(u, q[k]\upharpoonright B)| && \text{by definition of } d_{\mathcal{S}} \\
&\quad= \tfrac{1}{2}\sum_{u\in A^*} \left|\sum_{u'\upharpoonright B=u} \mathcal{V}(u', p[k]) - \sum_{u'\upharpoonright B=u} \mathcal{V}(u', q[k])\right| && \text{by Lemma 6.2.7} \\
&\quad\le \tfrac{1}{2}\sum_{u\in A^*} \left(\sum_{u'\upharpoonright B=u} |\mathcal{V}(u', p[k]) - \mathcal{V}(u', q[k])|\right) && \text{rearranging} \\
&\quad= \tfrac{1}{2}\sum_{u'\in A^*} |\mathcal{V}(u', p[k]) - \mathcal{V}(u', q[k])| \\
&\quad= d_{\mathcal{S}}(p[k], q[k]) && \text{by definition of } d_{\mathcal{S}}
\end{aligned}$$

and since this was for any $k \in \mathbb{N}$, similarly to Proposition 6.2.5 we have $d_\omega(p\upharpoonright B, q\upharpoonright B) \le d_\omega(p, q)$, that is $\upharpoonright$ is continuous on (P_ω, d_ω).

To show $p\restriction B \in P_\omega$ for all $p \in P_\omega$ follows similarly to Proposition 6.2.5 above using induction on $deg(p)$. $\square$

Finally, we introduce the semantic operator for relabelling defined inductively on the degree of processes as follows.

Definition 6.2.10 (Relabelling Operator) *For any $\lambda\colon A \to A$, let $p_0\,[\lambda] = p_0$ and $(a, f)\,[\lambda] = (\lambda(a), f\,[\lambda])$, where for any $q \in P_\omega$:*

$$f\,[\lambda](q) = \sum_{\substack{r\in P_\omega\ \&\\ r\,[\lambda]=q}} f(r).$$

To show the above operator is continuous and well-defined on (P_ω, d_ω), we first extend any function $\lambda : A \to A$ to $\lambda : A^* \to A^*$ as follows: for any $a \in A$ and $u \in A^*$: $\lambda(\langle\rangle) = \langle\rangle$ and $\lambda(au) = \lambda(a)\lambda(u)$. Using this extension, we reach the following lemma.

Lemma 6.2.11 *For all $p \in P_\omega$, $u \in A^*$ and $\lambda\colon A \to A$: $\mathcal{V}(u, p\,[\lambda]) = \mathcal{V}(\lambda^{-1}(u), p)$.*

Proof. The proof is by induction on $u \in A^n$. If $u \in A^0$, then for any $p \in P$ by definition of $\mathcal{V}$:

$$\begin{aligned}
\mathcal{V}(\langle\rangle, p\,[\lambda]) &= \begin{cases} 1 & \text{if } p\,[\lambda] = p_0 \\ 0 & \text{otherwise} \end{cases} \\
&= \begin{cases} 1 & \text{if } p = p_0 \\ 0 & \text{otherwise} \end{cases} && \text{by Definition 6.2.10} \\
&= \mathcal{V}(\langle\rangle, p) && \text{by definition of } \mathcal{V} \\
&= \mathcal{V}(\lambda^{-1}(\langle\rangle), p)
\end{aligned}$$

as required.

Now suppose the lemma holds for any $n \in \mathbb{N}$ and consider any $u \in A^{n+1} \setminus A^n$, then $u = au'$ for some $a \in A$ and if $p \in P_\omega$ by definition of $\mathcal{V}$ we have:

$$\mathcal{V}(au', p\,[\lambda]) = \begin{cases} \sum_{q\in\mathsf{s}(f)} f(q)\cdot\mathcal{V}(u', q) & \text{if } p\,[\lambda] = (a, f) \text{ for some } f \in \mu(P) \\ 0 & \text{otherwise} \end{cases}$$

$$= \begin{cases} \sum_{q \in \mathsf{s}(f)} f(q) \cdot \mathcal{V}(u', q\,[\lambda]) & \text{if } p = (\lambda^{-1}(a), f) \\ & \text{for some } f \in \mu(P) \\ 0 & \text{otherwise} \end{cases} \qquad \text{by Definition 6.2.10}$$

$$= \begin{cases} \sum_{q \in \mathsf{s}(f)} f(q) \cdot \mathcal{V}(\lambda^{-1}(u), q) & \text{if } p = (\lambda^{-1}(a), f) \\ & \text{for some } f \in \mu(P) \\ 0 & \text{otherwise} \end{cases} \qquad \text{by induction}$$

$$\begin{aligned} &= \mathcal{V}(\lambda^{-1}(a)\lambda^{-1}(u'), p) && \text{by Definition 6.1.8} \\ &= \mathcal{V}(\lambda^{-1}(au'), p) && \text{rearranging} \end{aligned}$$

as required. □

Lemma 6.2.12 *For all* $p \in P_\omega$, $\lambda\colon A \to A$ *and* $k \in \mathbb{N}$: $(p\,[\lambda])[k] = (p[k])\,[\lambda]$.

Proof. The proof is by induction on $k \in \mathbb{N}$ and again follows similarly to Lemma 6.2.4. □

Proposition 6.2.13 *For all* $\lambda\colon A \to A$, $[\lambda]$ *is continuous and well-defined on* (P_ω, d_ω).

Proof. The proof follows similarly to Proposition 6.2.5 and Proposition 6.2.9 using Lemma 6.2.7 and Lemma 6.2.8 lemmas above. □

We are now in a position to give denotational semantics to the guarded expressions $\mathcal{G}^{\mathrm{p}}$ of $\mathrm{RP_p}$. We accomplish this by defining a map $\mathcal{D}$ from $\mathrm{RP_p}$ to P, but only consider properties of this map over guarded terms. By construction, the element of P are the equivalence classes of the Cauchy sequences of (P_ω, d_ω) under the equivalence relation $\sim$, and we therefore first construct a sequence of maps $(\mathcal{D}_n)_{n\in\mathbb{N}}$ from $\mathrm{RP_p}$ to P_ω such that $\langle \mathcal{D}[\![E]\!]\rangle_{n\in\mathbb{N}}$ is Cauchy for any $E \in \mathcal{G}^{\mathrm{p}}$, and then set $\mathcal{D}[\![E]\!] = [\langle \mathcal{D}[\![E]\!]\rangle_{n\in\mathbb{N}}]_\sim$ for any $E \in \mathcal{G}^{\mathrm{p}}$.

As usual, in order to handle the variables x in the expressions $\mathrm{RP_p}$, we introduce environments Env, ranged over by ρ, defined by $\mathrm{Env} = \mathcal{X} \to P$. Similar to the above discussion, for any $\rho \in \mathrm{Env}$ we can suppose that there exists a sequence of maps $(\rho_n)_{n\in\mathbb{N}}$ such that $\rho_n : \mathcal{X} \to P_\omega$ for all $n \in \mathbb{N}$, $\langle \rho_n(x)\rangle_{n\in\mathbb{N}}$ is Cauchy in (P_ω, d_ω) and $\rho(x) = [\langle \rho_n(x)\rangle_{n\in\mathbb{N}}]_\sim$ for all $x \in \mathcal{X}$

In addition, we shall require the following auxiliary function.

Definition 6.2.14 *For any set* P *and family* $\langle \mu_i, p_i\rangle_{i\in I}$ *where* $\langle \mu_i, p_i\rangle \in ((0,1] \times P)$ *for all* $i \in I$, *let:* $\Phi_P(\langle \mu_i, p_i\rangle_{i\in I})(q) = \sum\{\mu_j \mid i \in I \text{ and } q = p_i\}$.

Lemma 6.2.15 *If* $\sum_{i\in I}\mu_i = 1$ *for some family* $\langle\mu_i, p_i\rangle_{i\in I}$*, then* $\Phi_P(\langle\mu_i, p_i\rangle_{i\in I}) \in \mu(P)$.

Proof. By definition of Φ_P, if $\langle\mu_i, p_i\rangle_{i\in I} \in ((0,1]\times P)^*$ we obtain:

$$\sum_{q\in P}\Phi_P(\langle\mu_i, p_i\rangle_{i\in I})(q) = \sum_{i\in I}\mu_i$$

and hence $\Phi_P(\langle\mu_i, p_i\rangle_{i\in I}) \in \mu(P)$ by the hypothesis. □

We can now define denotational metric semantics for $\mathrm{RP_p}$.

Definition 6.2.16 (Denotational Semantics) *Let* $\mathcal{D}_n : \mathrm{RP_p} \to (\mathrm{Env} \to P_\omega)$*,* $n \in \mathbb{N}$*, be the collection of maps defined inductively as follows. Put* $\mathcal{D}_0[\![E]\!] = p_0$ *for all* $E \in \mathrm{RP_p}$*, and* $\mathcal{D}_{n+1}$ *be defined inductively on the structure of elements of* $\mathrm{RP_p}$ *as follows:*

$$\begin{array}{rcl}
\mathcal{D}_{n+1}[\![x]\!](\rho) & = & \rho_{n+1}(x) \\
\mathcal{D}_{n+1}[\![\mathbf{0}]\!](\rho) & = & p_0 \\
\mathcal{D}_{n+1}[\![a.\sum_{i\in I}\mu_i.E_i]\!](\rho) & = & (a, \Phi_{P_\omega}(\langle\mu_i, \mathcal{D}_n[\![E_i]\!](\rho)\rangle_{i\in I})) \\
\mathcal{D}_{n+1}[\![E_1 \parallel E_2]\!](\rho) & = & \mathcal{D}_{n+1}[\![E_1]\!](\rho) \parallel \mathcal{D}_{n+1}[\![E_2]\!](\rho) \\
\mathcal{D}_{n+1}[\![E \upharpoonright B]\!](\rho) & = & \mathcal{D}_{n+1}[\![E]\!](\rho) \upharpoonright B \\
\mathcal{D}_{n+1}[\![E\,[\lambda]]\!](\rho) & = & \mathcal{D}_{n+1}[\![E]\!](\rho)\,[\lambda] \\
\mathcal{D}_{n+1}[\![\mathit{fix}_x.E]\!](\rho) & = & \mathcal{D}_{n+1}[\![E]\!](\rho\{\mathcal{D}_n[\![\mathit{fix}_x.E]\!](\rho)/x\}).
\end{array}$$

Furthermore, let $\mathcal{D} : \mathrm{RP_p} \to (\mathrm{Env} \to P)$ *be the map defined as follows, for any* $E \in \mathrm{RP_p}$ *put:* $\mathcal{D}[\![E]\!](\rho) = [\langle\mathcal{D}_n[\![E]\!](\rho)\rangle_{n\in\mathbb{N}}]_\sim$.

To prove the well-definedness of the semantic map we shall require the following technical lemmas.

Lemma 6.2.17 *For all* $E \in \mathrm{RP_p}$, $p \in P_\omega$, $\rho \in \mathrm{Env}$ *and* $k \le n \in \mathbb{N}$:

$$\mathcal{D}_k[\![E]\!](\rho\{p[n]/x\})[k] = \mathcal{D}_k[\![E]\!](\rho\{p/x\})[k].$$

Proof. If $k = 0$, the result follows by definition of truncations. Now consider any $k, n \in \mathbb{N}$ such that $k + 1 \le n$, we prove this case by induction on the structure of $E \in \mathrm{RP_p}$.

1. If $E \in \mathcal{X}$, then by definition for any $k \le n \in \mathbb{N}$:

$$\mathcal{D}_{k+1}[\![E]\!](\rho\{p[n]/x\})[k+1] = \begin{cases} (p[n])[k+1] & \text{if } E = x \\ \rho_{k+1}(E)[k+1] & \text{otherwise} \end{cases}$$

$$= \begin{cases} p[\min\{n, k+1\}] & \text{if } E = x \\ \rho_{k+1}(E)[k+1] & \text{otherwise} \end{cases} \quad \text{by Proposition 6.1.12}(b)$$

$$= \begin{cases} p[k+1] & \text{if } E = x \\ \rho_{k+1}(E)[k+1] & \text{otherwise} \end{cases} \quad \text{by hypothesis}$$

$$= \mathcal{D}_{k+1}[\![E]\!](\rho\{p/x\})[k+1] \quad \text{by definition of } \mathcal{D}_{k+1}.$$

2. If $E = \mathbf{0}$, the result follows by definition of $\mathcal{D}_{k+1}$.
3. If $E = a.\sum_{i\in I}\mu_i.E_i$, then by definition of $\mathcal{D}_{k+1}$:

$$\begin{aligned} \mathcal{D}_{k+1}[\![E]\!](\rho\{p/x\})[k+1] &= \Big(a, \Phi_{P_\omega}(\langle\mu_i, \mathcal{D}_k[\![E_i]\!](\rho\{p/x\})\rangle_{i\in I})\Big)[k+1] \\ &= \Big(a, \Phi_{P_\omega}(\langle\mu_i, \mathcal{D}_k[\![E_i]\!](\rho\{p/x\})\rangle_{i\in I})[k]\Big) \end{aligned}$$

by Definition 6.1.11 and similarly, for any $n \in \mathbb{N}$:

$$\mathcal{D}_{k+1}[\![E]\!](\rho\{p[n]/x\})[k+1] = \Big(a, \Phi_{P_\omega}(\langle\mu_i, \mathcal{D}_k[\![E_i]\!](\rho\{p[n]/x\})\rangle_{i\in I})[k]\Big)$$

Therefore, to show the lemma holds in this case, by definition of Φ_{P_ω} it is sufficient to prove that for all $k+1 \leq n$ and $i \in I$:

$$\mathcal{D}_k[\![E_i]\!](\rho\{p[n]/x\})[k] = \mathcal{D}_k[\![E_i]\!](\rho\{p/x\})[k]$$

which follows by induction since $k \leq k+1 \leq n$.
4. If $E = E_1 \,\|\, E_2$, then for any $k+1 \leq n \in \mathbb{N}$ we have $\mathcal{D}_{k+1}[\![E]\!](\rho\{p[n]/x\})[k+1]$ equals:

$$\begin{aligned} &= \Big(\mathcal{D}_{k+1}[\![E_1]\!](\rho\{p[n]/x\}) \,\|\, \mathcal{D}_{k+1}[\![E_2]\!](\rho\{p[n]/x\})\Big)[k+1] && \text{by definition of } \mathcal{D}_{k+1} \\ &= \mathcal{D}_{k+1}[\![E_1]\!](\rho\{p[n]/x\})[k+1] \,\|\, \mathcal{D}_{k+1}[\![E_2]\!](\rho\{p[n]/x\})[k+1] && \text{by Lemma 6.2.4} \\ &= \mathcal{D}_{k+1}[\![E_1]\!](\rho\{p/x\})[k+1] \,\|\, \mathcal{D}_{k+1}[\![E_2]\!](\rho\{p/x\})[k+1] && \text{by induction} \\ &= \Big(\mathcal{D}_{k+1}[\![E_1]\!](\rho\{p/x\}) \,\|\, \mathcal{D}_{k+1}[\![E_2]\!](\rho\{p/x\})\Big)[k+1] && \text{by Lemma 6.2.4} \\ &= \mathcal{D}_{k+1}[\![E_1 \,\|\, E_2]\!](\rho\{p/x\})[k+1] && \text{by definition of } \mathcal{D}_{k+1}. \end{aligned}$$

5. If $E = F\lceil B$ or $E = F\,[\lambda]$, the proof follows a similar argument to the case above replacing Lemma 6.2.4 by Lemma 6.2.8 and Lemma 6.2.12 respectively.
6. If $E = \mathit{fix}_y.F$, then either $x = y$ and by definition of $\mathcal{D}_{k+1}$ we have $\mathcal{D}_{k+1}[\![E]\!](\rho\{q/x\}) = \mathcal{D}_{k+1}[\![E]\!](\rho)$ for any $q \in P$, and hence the lemma holds in this case, or $x \neq y$, in which

by definition of D_{k+1}:

$$\begin{array}{rcll}\mathcal{D}_{k+1}[\![E]\!](\rho\{p[n]/x\})[k+1] &=& \mathcal{D}_{k+1}[\![F]\!](\rho\{\mathcal{D}_k[\![E]\!](\rho)/y\}\{p[n]/x\})[k+1] & \\ &=& \mathcal{D}_{k+1}[\![F]\!](\rho\{p[n]/x\}\{\mathcal{D}_k[\![E]\!](\rho)/y\})[k+1] & \text{since } x \neq y \\ &=& \mathcal{D}_{k+1}[\![F]\!](\rho\{p/x\}\{\mathcal{D}_k[\![E]\!](\rho)/y\})[k+1] & \text{by induction} \\ &=& \mathcal{D}_{k+1}[\![F]\!](\rho\{\mathcal{D}_k[\![E]\!](\rho)/y\}\{p/x\})[k+1] & \text{since } x \neq y \\ &=& \mathcal{D}_{k+1}[\![E]\!](\rho\{p/x\})[k+1] & \text{by definition.}\end{array}$$

Since these are all the possible cases the lemma holds by induction. □

Lemma 6.2.18 *For all $E \in \mathcal{G}^{\mathrm{p}}$, $p \in P_\omega$, $\rho \in \mathrm{Env}$ and $k \in \mathbb{N}$:*

$$\mathcal{D}_k[\![E]\!](\rho\{p/x\})[k+1] = \mathcal{D}_k[\![E]\!](\rho\{p[k]/x\})[k+1].$$

Proof. The proof is by induction on the structure of $E \in \mathcal{G}^{\mathrm{p}}$ and follows similarly to Lemma 6.2.17 above except in the case when $E = a.\sum_{i\in I}\mu_i.E_i$. In this case, similarly to Lemma 6.2.18 and replacing n by k, to show the lemma holds it is sufficient to prove $\mathcal{D}_k[\![E_i]\!](\rho\{p/x\})[k] = \mathcal{D}_k[\![E_i]\!](\rho\{p[k]/x\})[k]$ for all $i \in I$, which follows by Lemma 6.2.17 since $E_i \in \mathrm{RP}^{\mathrm{p}}$ for all $i \in I$ and $k \leq k$. □

Lemma 6.2.19 *For all $E \in \mathcal{G}^{\mathrm{p}}$, $\rho \in \mathrm{Env}$ and $k \in \mathbb{N}$: $\mathcal{D}_{k+1}[\![E]\!](\rho)[k] = \mathcal{D}_k[\![E]\!](\rho)[k]$.*

Proof. We prove the lemma by induction on $k \in \mathbb{N}$. The case for $k = 0$ follows by definition of truncations.

Now suppose the lemma holds for some $k \in \mathbb{N}$, then we prove the lemma by induction on the structure of $E \in \mathcal{G}^{\mathrm{p}}$. The proof follows similarly to Lemma 6.2.17 above except in the case when $E = \mathit{fix}_x.F$, which we now prove. If $E = \mathit{fix}_x.F$, then by definition of $\mathcal{D}_{k+2}$:

$$\begin{array}{rcll}\mathcal{D}_{k+2}[\![E]\!](\rho)[k+1] &=& \mathcal{D}_{k+2}[\![F]\!](\rho\{\mathcal{D}_{k+1}[\![E]\!](\rho)/x\})[k+1] & \\ &=& \mathcal{D}_{k+2}[\![F]\!](\rho\{\mathcal{D}_{k+1}[\![E]\!](\rho)[k]/x\})[k+1] & \text{by Lemma 6.2.18} \\ &=& \mathcal{D}_{k+2}[\![F]\!](\rho\{\mathcal{D}_k[\![E]\!](\rho)[k]/x\})[k+1] & \text{by induction on } k \in \mathbb{N} \\ &=& \mathcal{D}_{k+2}[\![F]\!](\rho\{\mathcal{D}_k[\![E]\!](\rho)/x\})[k+1] & \text{by Lemma 6.2.18} \\ &=& \mathcal{D}_{k+1}[\![F]\!](\rho\{\mathcal{D}_k[\![E]\!](\rho)/x\})[k+1] & \text{by induction on } F \\ &=& \mathcal{D}_{k+1}[\![E]\!](\rho)[k+1] & \text{by definition}\end{array}$$

which completes the proof. □

Lemma 6.2.20 *For all $E \in \mathrm{RP_p}$, $F \in \mathrm{Pr}^{\mathrm{p}}$, $\rho \in Env$ and $n \in \mathbb{N}$:*

$$\mathcal{D}_n[\![E\{F/x\}]\!](\rho)[n] = \mathcal{D}_n[\![E]\!](\rho\{D_n[\![F]\!]/x\})[n].$$

Furthermore, if $E \in \mathcal{G}^{\mathrm{p}}$ then:

$$\mathcal{D}_{n+1}[\![E\{F/x\}]\!](\rho)[n+1] = \mathcal{D}_{n+1}[\![E]\!](\rho\{D_n[\![F]\!]/x\})[n+1].$$

Proof. The proof is by induction on the structure of E and follows a similar proof to Lemma 6.2.17 and Lemma 6.2.18. $\square$

Proposition 6.2.21 *$\mathcal{D}$ is well-defined on the set of guarded expressions of* $\mathrm{RP_p}$.

Proof. First, we prove that $\mathcal{D}_n[\![E]\!](\rho) \in P_\omega$ for all $E \in \mathcal{G}^{\mathrm{p}}$ and $n \in \mathbb{N}$ by induction on n. The case for $n = 0$ is trivial.

Now suppose $\mathcal{D}_n[\![E]\!](\rho) \in P_\omega$ for all $E \in \mathcal{G}^{\mathrm{p}}$ and some $n \in \mathbb{N}$, we prove the case for $n+1$ by induction on the structure of $E \in \mathcal{G}^{\mathrm{p}}$.

1. If $E = \mathbf{0}$, then by definition $\mathcal{D}_{n+1}[\![\mathbf{0}]\!](\rho) = p_0 \in P_\omega$.
2. If $E = a.\sum_{i\in I}\mu_i.E_i$, then by induction $\mathcal{D}_n[\![E_i]\!](\rho) \in P_\omega$ for all $i \in I$, and since by construction $\sum_{i\in I}\mu_i = 1$, using Lemma 6.2.15 we have:
$$\Phi_{P_\omega}(\langle \mu_i, \mathcal{D}[\![E_i]\!](\rho)\,\rangle_{i\in I}) \in \mu(P_\omega).$$
and therefore, $\mathcal{D}[\![E]\!](\rho) \in P_\omega$ by definition of $\mathcal{D}_{n+1}$.
3. If $E = E_1 \,\|\, E_2$, $E = \tilde{E}\!\upharpoonright\! B$ or $E = \tilde{E}\,[\lambda]$, the proposition holds by definition of $\mathcal{D}_{n+1}$, the well-definedness of the semantic operators and induction.
4. If $E = \mathit{fix}_x.E'$, then by induction on E' and $n \in \mathbb{N}$ we have $\mathcal{D}_{n+1}[\![E']\!](\rho) \in P_\omega$ and $\mathcal{D}_n[\![E]\!](\rho) \in P_\omega$ respectively, and hence $\mathcal{D}_{n+1}[\![E]\!](\rho) \in P_\omega$, by definition of $\mathcal{D}_{n+1}$.

Finally to prove that $\mathcal{D}$ is well defined, we show that for any $E \in \mathcal{G}^{\mathrm{p}}$: $\langle D_n[\![E]\!]\rangle_{n\in\mathbb{N}}$ is Cauchy in (P_ω, d_ω) which follows from the continuity of the semantic operators, Lemma 6.1.23 and Lemma 6.2.19. $\square$

6.2.1 Full Abstraction

In this section we show that the above denotational model is fully abstract, that is, two $\mathrm{RP_p}$ expressions are equivalent with respect to $\overset{\mathrm{p}}{\sim}$ if and only if their denotations (under the semantic map $\mathcal{D}$) have distance zero. By definition the operational equivalence $\overset{\mathrm{p}}{\sim}$ and metric d are based on the mappings P and $\mathcal{V}$ respectively, where

$$\mathsf{P} : \Big(\{\mathcal{O}[\![E]\!] \mid E \in \mathrm{Pr}^{\mathrm{p}}\} \times \mathtt{T}^{\mathrm{p}}\Big) \to [0,1] \quad \text{and} \quad \mathcal{V} : \Big(A^* \times \{\mathcal{D}_n[\![E]\!] \mid E \in \mathrm{Pr}^{\mathrm{p}}\}\Big) \to [0,1].$$

Therefore, to reach a full abstraction result, we first relate the semantic maps $\mathcal{O}$ and $\mathcal{D}$ and our testing language $\mathtt{T}^{\mathrm{p}}$ and the set of strings A^*, then, using these results, the maps P and $\mathcal{V}$. This leads to a connection between $\overset{\mathrm{p}}{\sim}$ and the metric d, and hence the full abstraction result. Formally, we have the following lemmas and definition.

Lemma 6.2.22 *For all $E \in \mathrm{Pr^p}$ and $\rho \in \mathrm{Env}$, $\mathcal{O}[\![E]\!] = \emptyset$ if and only if $\mathcal{D}_{n+1}[\![E]\!](\rho) = p_0$ for all $n \in \mathbb{N}$, and $\mathcal{O}[\![E]\!] = (a, \pi)$ if and only if $\mathcal{D}_{n+1}[\![E]\!](\rho) = (a, f_n)$ for all $n \in \mathbb{N}$ such that for any $n \in \mathbb{N}$ and $q \in P_\omega$:*

$$f_n[n](q) = \sum_{\substack{F \in \mathrm{Pr^p}\ \& \\ \mathcal{D}_n[\![F]\!](\rho)[n]=q}} \pi(F).$$

Proof. Consider any $E \in \mathrm{Pr^p}$, $\rho \in \mathrm{E}nv$ and $n \in \mathbb{N}$, we prove the lemma by induction on the structure of $E \in \mathrm{Pr^p}$.

1. If $E = \mathbf{0}$, then $\mathcal{O}[\![E]\!] = \emptyset$ and $\mathcal{D}_{n+1}[\![\mathbf{0}]\!](\rho) = p_0$ as required.

2. If $E = \sum_{i \in I} a_{\mu_i}.E_i$, then by the transition rules $\mathcal{O}[\![E]\!] = (a, \pi)$, where for any $F \in \mathrm{Pr^p}$:
$$\pi(E) = \sum_{\substack{i \in I\ \& \\ E_i = E}} \mu_i.$$
On the other hand:
$$\mathcal{D}_{n+1}[\![a.\textstyle\sum_{i \in I} \mu_i.E_i]\!](\rho) = \Big(a, \Phi_{P_\omega}(\langle \mu_i, \mathcal{D}_n[\![E_i]\!](\rho)\rangle_{i \in I})\Big)$$
by definition of $\mathcal{D}_{n+1}$ and letting $f_n \equiv \Phi_{P_\omega}(\langle \mu_i, \mathcal{D}_n[\![E_i]\!](\rho)\rangle_{i \in I})$, we obtain $\mathcal{D}_n[\![E]\!] = (a, f_n)$. Thus, for any $n \in \mathbb{N}$ and $q \in P_\omega$ we have:
$$f_n[n](q) = \sum_{\substack{F \in \mathrm{Pr^p}\ \& \\ \mathcal{D}_n[\![F]\!](\rho)[n]=q}} \pi(F)$$
by definition of Φ_{P_ω} and π.

3. If $E = E_1 \,\|\, E_2$, then either $\mathcal{O}[\![E]\!] = \emptyset$ or $\mathcal{O}[\![E]\!] = (a, \pi)$ for some $a \in \mathcal{A}ct$ and $\pi \in \mu(\mathrm{Pr^p})$. First consider when $\mathcal{O}[\![E]\!] = \emptyset$, then by definition of the transition rules one of the following two cases must hold.
   - $\mathcal{O}[\![E_1]\!] = \emptyset$ or $\mathcal{O}[\![E_2]\!] = \emptyset$, then by induction either $\mathcal{D}_{n+1}[\![E_1]\!](\rho) = p_0$ or $\mathcal{D}_{n+1}[\![E_2]\!](\rho) = p_0$, and therefore $\mathcal{D}_{n+1}[\![E_1 \,\|\, E_2]\!](\rho) = p_0$ by definition of $\mathcal{D}_{n+1}$ and the semantic operator $\|$.
   - $\mathcal{O}[\![E_1]\!] = (a_1, \pi_1)$ and $\mathcal{O}[\![E_2]\!] = (a_2, \pi_2)$ for some $\pi_1, \pi_2 \in \mu(\mathrm{Pr^p})$ such that $a_1 \neq a_2$. Then by induction, the definition of $\mathcal{D}_{n+1}$ and the semantic operator $\|$, $\mathcal{D}_{n+1}[\![E_1 \,\|\, E_2]\!](\rho) = p_0$.

   Secondly, if $\mathcal{O}[\![E]\!] = (a, \pi)$, then by definition of the transition rules $\mathcal{O}[\![E_1]\!] = (a, \pi_1)$ and $\mathcal{O}[\![E_2]\!] = (a, \pi_2)$ for some $\pi_1, \pi_2 \in \mu(\mathrm{Pr^p})$. Then by induction and the definition of the semantic operator $\|$: $\mathcal{D}_{n+1}[\![E_1 \| E_2]\!](\rho) = (a, f_n \| g_n)$, where $\mathcal{D}_{n+1}[\![E_1]\!](\rho) = (a, f_n)$ and $\mathcal{D}_{n+1}[\![E_2]\!](\rho) = (a, g_n)$. Moreover, for any $q \in P$ by Definition 6.2.2:

$$
\begin{aligned}
(f_n[n] \| g_n[n])(q) &= \sum_{\substack{q_1,q_2 \in P \\ \& \, q_1 \| q_2 = q}} f_n[n](q_1) \cdot g_n[n](q_2) \\
&= \sum_{\substack{q_1,q_2 \in P \\ \& \, q_1 \| q_2 = q}} \left(\sum_{\substack{F_1 \in \mathrm{Pr^p} \, \& \\ \mathcal{D}_n[\![F_1]\!](\rho)[n] = q_1}} \pi_1(F_1) \right) \cdot \left(\sum_{\substack{F_2 \in \mathrm{Pr^p} \, \& \\ \mathcal{D}_n[\![F_2]\!](\rho)[n] = q_2}} \pi_2(F_2) \right) && \text{by induction} \\
&= \sum_{\substack{F_1,F_2 \in \mathrm{Pr^p} \, \& \\ (\mathcal{D}_n[\![F_1]\!](\rho) \| \mathcal{D}_n[\![F_2]\!](\rho))[n] = q}} \pi_1(F_1) \cdot \pi_2(F_2) && \text{by Lemma 6.2.4} \\
&= \sum_{\substack{F_1,F_2 \in \mathrm{Pr^p} \, \& \\ \mathcal{D}_n[\![F_1 \| F_2]\!](\rho)[n] = q}} \pi_1(F_1) \cdot \pi_2(F_2) && \text{by definition of } \mathcal{D}_n \\
&= \sum_{\substack{F \in \mathrm{Pr^p} \, \& \\ \mathcal{D}_n[\![F]\!](\rho)[n] = q}} \pi(F) && \text{by the transition rules.}
\end{aligned}
$$

4. If $E = E' \restriction B$, then either $\mathcal{O}[\![E]\!] = \emptyset$ or $\mathcal{O}[\![E]\!] = (a, \pi)$ for some $a \in \mathcal{A}ct$ and $\pi \in \mu(\mathrm{Pr^p})$. Considering when $\mathcal{O}[\![E]\!] = \emptyset$, by definition of the transition rules: $\mathcal{O}[\![E']\!] = \emptyset$ or $\mathcal{O}[\![E']\!] = (a, \pi)$ for some $a \in A \setminus B$, in both cases by definition of the semantic operator for restriction and induction $\mathcal{D}_{n+1}[\![E]\!](\rho) = p_0$.

   On the other hand, if $\mathcal{O}[\![E]\!] = (a, \pi)$ then by definition of the transition rules: $a \in B$ such that $\mathcal{O}[\![E']\!] = (a, \pi')$. Furthermore, by induction $\mathcal{D}_{n+1}[\![E']\!](\rho) = (a, f_n)$, and hence by definition of the semantic operator for restriction $\mathcal{D}_{n+1}[\![E]\!](\rho) = (a, f_n \restriction B)$ and for any $n \in \mathbb{N}$ and $q \in P$:

$$
\begin{aligned}
(f_n \restriction B)[n](q) &= \sum_{\substack{p \in P \, \& \\ p[n] \restriction B = q}} f_n[n](p) \\
&= \sum_{\substack{p \in P \, \& \\ p[n] \restriction B = q}} \left(\sum_{\substack{F \in \mathrm{Pr^p} \, \& \\ \mathcal{D}_n[\![F]\!](\rho)[n] = p}} \pi'(F) \right) && \text{by induction} \\
&= \sum_{\substack{F \in \mathrm{Pr^p} \, \& \\ \mathcal{D}_n[\![F]\!](\rho) \restriction B[n] = q}} \pi'(F) && \text{by Lemma 6.2.8} \\
&= \sum_{\substack{F \in \mathrm{Pr^p} \, \& \\ \mathcal{D}_n[\![F \restriction B]\!](\rho)[n] = q}} \pi'(F) && \text{by definition of } \mathcal{D}_n \\
&= \sum_{\substack{F \in \mathrm{Pr^p} \, \& \\ \mathcal{D}_n[\![F]\!](\rho)[n] = q}} \pi(F) && \text{by the transition rules.}
\end{aligned}
$$

5. If $E = E'[\lambda]$, either $\mathcal{O}[\![E]\!] = \emptyset$ and $\mathcal{O}[\![E']\!] = \emptyset$ in which case the result follows by induction, or $\mathcal{O}[\![E]\!] = (a, \pi)$ and $\mathcal{O}[\![E']\!] = (\lambda^{-1}(a), \pi')$, then by induction $\mathcal{D}_{n+1}[\![E]\!](\rho) = (a, f_n[\lambda])$, and for any $q \in P_\omega$, by Definition 6.2.10:

$$\begin{aligned}
f_n[n][\lambda](q) &= \sum_{\substack{p \in P_\omega \,\&\\ p[n][\lambda]=q}} f_n[n](p) \\
&= \sum_{\substack{p \in P_\omega \,\&\\ p[\lambda]=q}} \left(\sum_{\substack{F \in \mathrm{Pr^p} \,\&\\ \mathcal{D}_n[\![F]\!](\rho)[n]=p}} \pi'(F) \right) && \text{by induction} \\
&= \sum_{\substack{F \in \mathrm{Pr^p} \,\&\\ \mathcal{D}_n[\![F]\!](\rho)[\lambda][n]=q}} \pi'(F) && \text{by Lemma 6.2.12} \\
&= \sum_{\substack{F \in \mathrm{Pr^p} \,\&\\ \mathcal{D}_n[\![F[\lambda]]\!](\rho)[n]=q}} \pi'(F) && \text{by definition of } \mathcal{D}_n \\
&= \sum_{\substack{F \in \mathrm{Pr^p} \,\&\\ \mathcal{D}_n[\![F]\!](\rho)[n]=q}} \pi(F) && \text{by the transition rules.}
\end{aligned}$$

6. If $E = \mathit{fix}_x.E'$, the lemma follows by induction on the structure $E' \in \mathcal{G}^{\mathrm{p}}$, similarly to the cases above and using Lemma 6.2.20.

Since these are all the possible forms of E the lemma is proved by induction on the structure of E. □

Definition 6.2.23 *We define the following map* $\xi : A^* \to \mathtt{T}^{\mathrm{p}}$ *inductively on* $u \in A^n$. *Let* $\xi(\langle\rangle) = \bot$ *and* $\xi(au) = a.\xi(u)$.

Lemma 6.2.24 *The mapping* ξ *is bijective.*

Proof. The proof follows by definition of A^* and $\mathtt{T}^{\mathrm{p}}$, and since $A = \mathcal{A}ct$. □

As discussed earlier, we are now in a position to reach a connection between the maps P and $\mathcal{V}$. Recall that for any $u, v \in A^*$, $u \leq v$ if u is a prefix of v.

Lemma 6.2.25 *For all* $E \in \mathrm{Pr^p}$, $\rho \in \mathrm{Env}$, $u \in A^n$ *and* $n \in \mathbb{N}$*:*

$$\sum_{\substack{u' \in A^n \\ \& \, u \leq u'}} \mathcal{V}(u', \mathcal{D}_n[\![E]\!](\rho)[n]) = \mathsf{P}(E)(\xi(u)).$$

Proof. The proof is by induction on $n \in \mathbb{N}$, where we remove ρ for simplicity. Consider any $E \in \mathrm{Pr^p}$ and $u \in A^0$, then since $A^0 = \{\langle\rangle\}$:

$$\begin{array}{rcll}
\sum_{\substack{u' \in A^0 \\ \& \langle\rangle \leq u'}} \mathcal{V}(u', \mathcal{D}_0[\![E]\!][0]) & = & \mathcal{V}(\langle\rangle, \mathcal{D}_0[\![E]\!][0]) & \\
& = & \mathcal{V}(\langle\rangle, p_0) & \text{by Definition 6.1.11} \\
& = & 1 & \text{by Definition 6.1.8} \\
& = & \mathsf{P}(E)(\perp) & \text{by definition of } \mathsf{P} \\
& = & \mathsf{P}(E)(\xi(\langle\rangle)) & \text{by definition of } \xi.
\end{array}$$

Now suppose the result holds for n and consider any $E \in \mathrm{Pr^p}$ and $u \in A^{n+1}$. If $u = \langle\rangle$, then since $\langle\rangle \leq u'$ for all $u \in A^{n+1}$:

$$\begin{array}{rcll}
\sum_{\substack{u' \in A^{n+1} \\ \& \langle\rangle \leq u'}} \mathcal{V}(u, \mathcal{D}_{n+1}[\![E]\!][n+1]) & = & \sum_{u' \in A^{n+1}} \mathcal{V}(u, \mathcal{D}_{n+1}[\![E]\!][n+1]) & \\
& = & \sum_{u' \in A^{*}} \mathcal{V}(u, \mathcal{D}[\![E]\!][n+1]) & \text{by Proposition 6.1.12}(e) \\
& = & 1 & \text{by Proposition 6.1.9} \\
& = & \mathsf{P}(E)(\perp) & \text{by definition of } \mathsf{P} \\
& = & \mathsf{P}(E)(\xi(\langle\rangle)) & \text{by definition of } \xi.
\end{array}$$

On the other hand, if $u \neq \langle\rangle$ then $u = a\tilde{u}$ for some $a \in \mathcal{A}ct$ and $\tilde{u} \in A^n$, and in this case by definition of $\mathcal{V}$, ξ and Lemma 6.2.22, if $\mathcal{O}[\![E]\!] \neq (a, \pi)$ for any $\pi \in \mu(\mathrm{Pr^p})$:

$$\sum_{\substack{u' \in A^{n+1} \\ \& u \leq u'}} \mathcal{V}(u, \mathcal{D}_{n+1}[\![E]\!][n+1]) = \mathsf{P}(E)(\xi(u)) = 0.$$

We are therefore left with the case when $\mathcal{O}[\![E]\!] = (a, \pi)$ for some $\pi \in \mu(\mathrm{Pr^p})$. Using Lemma 6.2.22, Definition 3.1.1 and since $u = a\tilde{u}$ we have:

$$\sum_{\substack{u' \in A^{n+1} \\ \& \, u \leq u'}} \mathcal{V}(u', \mathcal{D}[\![E]\!][n+1]) = \sum_{\substack{u' \in A^{n} \\ \& \, \tilde{u} \leq u'}} \mathcal{V}(au', (a, f_n)[n+1])$$

$$\begin{array}{lll}
= & \displaystyle\sum_{\substack{u' \in A^{n} \\ \& \, \tilde{u} \leq u'}} \mathcal{V}(au', (a, f_n[n])) & \text{by Definition 6.1.11} \\
= & \displaystyle\sum_{\substack{u' \in A^{n} \\ \& \, \tilde{u} \leq u'}} \left(\sum_{q \in P_\omega} f_n[n](q) \cdot \mathcal{V}(u', q) \right) & \text{by definition of } \mathcal{V} \\
= & \displaystyle\sum_{\substack{u' \in A^{n} \\ \& \, \tilde{u} \leq u'}} \left(\sum_{q \in P_\omega} \left(\sum_{\substack{F \in \mathrm{Pr^p} \, \& \\ \mathcal{D}_n[\![F]\!][n] = q}} \pi(F) \right) \cdot \mathcal{V}(u', q) \right) & \text{by Lemma 6.2.22} \\
= & \displaystyle\sum_{F \in \mathrm{Pr^p}} \pi(F) \cdot \left(\sum_{\substack{u' \in A^{n} \\ \& \, \tilde{u} \leq u'}} \mathcal{V}(u', \mathcal{D}_n[\![F]\!][n]) \right) & \text{rearranging} \\
= & \displaystyle\sum_{F \in \mathrm{Pr^p}} \pi(F) \cdot \mathsf{P}(F)(\xi(\tilde{u})) & \text{by induction} \\
= & \mathsf{P}(E)(a.\xi(\tilde{u})) & \text{by definition of } \mathsf{P} \\
= & \mathsf{P}(E)(\xi(a\tilde{u})) & \text{by definition of } \xi \\
= & \mathsf{P}(E)(\xi(u)) & \text{by hypothesis}
\end{array}$$

and thus we have proved the lemma by induction on $n \in \mathbb{N}$. $\Box$

Finally, using the above lemmas we reach the following full abstraction result.

Theorem 6.2.26 (Full Abstraction) *For all $E, F \in \mathcal{G}^{\mathrm{p}}$:*

$$\mathcal{O}[\![E]\!] \overset{\mathrm{p}}{\sim} \mathcal{O}[\![F]\!] \textit{ if and only if } \mathcal{D}[\![E]\!](\rho) = \mathcal{D}[\![F]\!](\rho) \textit{ for all } \rho \in \mathrm{Env}.$$

Proof. We only consider the case for $E, F \in \mathrm{Pr^p}$, as the case for $E, F \in \mathcal{G}^{\mathrm{p}} \setminus \mathrm{Pr^p}$ follows by definition of $\overset{\mathrm{p}}{\sim}$ on $\mathcal{G}^{\mathrm{p}}$ (we remove ρ for simplicity). First, consider any $E, F \in \mathrm{Pr^p}$ such that $\mathcal{D}[\![E]\!] = \mathcal{D}[\![F]\!]$. Then using Lemma 6.1.23 and Lemma 6.2.19 we have $d_\omega(\mathcal{D}_n[\![E]\!][n], \mathcal{D}_n[\![F]\!][n]) = 0$ for all $n \in \mathbb{N}$, and hence by definition of d and $d_{\mathcal{S}}$:

$$|\mathcal{V}(u, \mathcal{D}_n[\![E]\!][n]) - \mathcal{V}(u, \mathcal{D}_n[\![F]\!][n])| = 0 \;\; \forall u \in A^n \;\&\; n \in \mathbb{N}$$

$$\Rightarrow \quad \mathcal{V}(u, \mathcal{D}_n[\![E]\!][n]) = \mathcal{V}(u, \mathcal{D}_n[\![F]\!][n]) \;\; \forall u \in A^n \;\&\; n \in \mathbb{N}$$

$$\Rightarrow \quad \sum_{\substack{u' \in A^* \\ \& \, u \leq u'}} \mathcal{V}(u', \mathcal{D}_n[\![E]\!][n]) = \sum_{\substack{u' \in A^n \\ \& \, u \leq u'}} \mathcal{V}(u', \mathcal{D}_n[\![F]\!][n]) \;\; \forall u \in A^n \;\&\; n \in \mathbb{N}$$

$$\begin{array}{lll}
\Rightarrow & \mathsf{P}(E)(\xi(u)) = \mathsf{P}(F)(\xi(u)) \;\; \forall u \in A^n \;\&\; n \in \mathbb{N} & \text{by Lemma 6.2.25} \\
\Rightarrow & \mathsf{P}(E)(\xi(u)) = \mathsf{P}(F)(\xi(u)) \;\; \forall u \in A^* & \text{rearranging} \\
\Rightarrow & \mathsf{P}(E)(t) = \mathsf{P}(F)(t) \;\; \forall t \in \mathtt{T}^{\mathrm{p}} & \text{by Lemma 6.2.24} \\
\Rightarrow & \mathcal{O}[\![E]\!] \overset{\mathrm{p}}{\sim} \mathcal{O}[\![F]\!] & \text{by definition of } \overset{\mathrm{p}}{\sim}
\end{array}$$

as required.

For the other direction, suppose $\mathcal{D}[\![E]\!] \neq \mathcal{D}[\![F]\!]$, then by definition of (P, d): $\lim_{n\to\infty} d_\omega(\mathcal{D}_n[\![E]\!], \mathcal{D}_n[\![F]\!]) \neq 0$, and hence using Lemma 6.1.24 there exists $n \in \mathbb{N}$ such that $d_{\mathcal{S}}(\mathcal{D}_n[\![E]\!][n], \mathcal{D}_n[\![F]\!][n]) \neq 0$. Therefore, by definition of $d_{\mathcal{S}}$ there exists $u \in A^*$ such that $\mathcal{V}(u, \mathcal{D}_n[\![E]\!][n]) \neq \mathcal{V}(u, \mathcal{D}_n[\![F]\!][n])$. Now by construction $\mathcal{A}ct$ is finite and $\mathcal{A}ct = A$, and therefore A^n is finite and using Proposition 6.1.12(e), without loss of generality we can suppose $u \in A^n$ and that:

$$\mathcal{V}(u', \mathcal{D}_n[\![E]\!][n]) = \mathcal{V}(u', \mathcal{D}_n[\![F]\!][n]) \quad \text{for all } u' \in A^n \text{ such that } u < u'. \tag{6.7}$$

Moreover, Lemma 6.2.24 implies $\xi(u) \in \mathtt{T}^{\mathrm{p}}$, and therefore by Lemma 6.2.25:

$$\begin{array}{rcll}
\mathsf{P}(E)(\xi(u)) & = & \sum_{\substack{u' \in A^n \\ \& \, u \leq u'}} \mathcal{V}(u', \mathcal{D}_n[\![E]\!][n]) & \\
& = & \mathcal{V}(u, \mathcal{D}_n[\![E]\!][n]) + \sum_{\substack{u' \in A^n \\ u < u'}} \mathcal{V}(u', \mathcal{D}_n[\![E]\!][n]) & \text{rearranging} \\
& = & \mathcal{V}(u, \mathcal{D}_n[\![E]\!][n]) + \sum_{\substack{u' \in A^n \\ u < u'}} \mathcal{V}(u', \mathcal{D}_n[\![F]\!][n]) & \text{by (6.7)} \\
& \neq & \mathcal{V}(u, \mathcal{D}_n[\![F]\!][n]) + \sum_{\substack{u' \in A^n \\ u < u'}} \mathcal{V}(u', \mathcal{D}_n[\![F]\!][n]) & \text{by hypothesis} \\
& = & \sum_{\substack{u' \in A^n \\ \& \, u \leq u'}} \mathcal{V}(u', \mathcal{D}_n[\![F]\!][n]) & \text{rearranging} \\
& = & \mathsf{P}(F)(\xi(u)) & \text{by Lemma 6.2.25}
\end{array}$$

thus, $\mathcal{O}[\![E]\!] \overset{\mathrm{p}}{\not\sim} \mathcal{O}[\![F]\!]$ as required. □

6.3 A Metric for Deterministic Probabilistic Processes

Observe that simple probabilistic processes (the elements of P) are represented either by p_0 (termination), or are limits $\lim_{n\to\infty} p_n$ of Cauchy sequences of (finite) processes, where with out loss of generality, we can suppose $p_{n+1} = (a, f_n)$ for some $a \in A$ and $f_n \in \mu(P_\omega)$ for all $n \in \mathbb{N}$, and thus initially can only perform the action a. To represent choice it is necessary to use *sets* of elements of P as denotations for probabilistic processes. As we wish to model deterministic probabilistic processes (that is, processes that can make external choices), in the light of the definition of deterministic probabilistic transition systems such sets must satisfy the *reactiveness* condition.

We note that since this construction is based on the construction of the denotational model for purely probabilistic processes, in certain cases the results will overlap and in such cases we omit the proofs.

We now proceed with the construction involving sets of P, as opposed to just elements, to give a denotational semantics for deterministic probabilistic processes. The difference between the equation below and that in Definition 6.1.1 is the presence of the power set operator $\mathcal{P}_{fnr}(\cdot \times \cdot)$ (finite non-empty reactive subsets).

Definition 6.3.1 (Finite deterministic probabilistic processes) *Let D_n, $n \in \mathbb{N}$, be a collection of carrier sets defined inductively by*

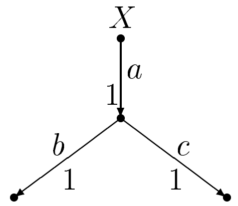
$$D_0 = \{\{p_0\}\} \ \ \textit{and} \ \ D_{n+1} = \{\{p_0\}\} \cup \mathcal{P}_{fnr}\,(A \times \mu(D_n))$$

where A is a set of actions. Furthermore, let $D_\omega = \cup_n D_n$ denote deterministic probabilistic processes of bounded depth.

To simplify notation, we define D^s_ω, where s is intended to denote the singleton elements of D_ω, as the elements of the form p_0 or (a, f) for some $a \in A$ and $f \in \mu(D_\omega)$. Intuitively, we can think of an element of D^s_ω as a finite deterministic probabilistic process whose first transition can only be of one action type and the total probability of this action taking place is 1. Furthermore, let D_ω be ranged over by $X, Y \ldots$ and $p, q \ldots$ range over D^s_ω.

When constructing a pseudo-metric over P_ω, recall that we first considered processes as sets of strings of the type $(A \times (0, 1])^*$ by means of the mapping $\mathcal{S}$, and using this representation we could then calculate the probability of processes performing a given path. Later on we showed that we could, in fact, calculate the probabilities of paths being performed without the need for the mapping $\mathcal{S}$, by induction on the depth of paths (see Definition 6.1.8). Now we extend this definition to our current setting. The next step is therefore to consider the possible paths of deterministic probabilistic processes.

At first sight it may seem feasible to extend our pseudo-metric on simple probabilistic processes by means of the Hausdorff distance. However, if we consider possible paths of deterministic probabilistic processes, as opposed to simple probabilistic processes, we see that the situation is more complex, since there is now external choice, as well as (internal action-guarded) probabilistic choice. We demonstrate this by means of an example. Consider the deterministic probabilistic process X given below:



To incorporate the external choice we consider *deterministic trees*, as opposed to strings, since we cannot consider the paths that X can perform as elements of A^*: X can perform the action a and then make an external choice between b and c, which will be denoted by the tree $a\{b\langle\rangle, c\langle\rangle\}$, and thus we need to add sets to the definition of A^*. Intuitively, we need to add this extra level of complexity as our pseudo-metric is not inductive, whereas de Bakker and Zucker's construction does not require this as their metric is inductive, and so they can use the Hausdorff metric inductively to capture the branching behaviour. Formally, we define A^*_{d}, the set of trees that deterministic processes can perform as follows.

Definition 6.3.2 *Let A^n_{d}, $n \in \mathbb{N}$, be a collection of sets defined inductively as follows. Let*

$$A^0_{\mathrm{d}} = \{\langle\rangle\} \;\; \textit{and} \;\; A^{n+1}_{\mathrm{d}} = A \times (\mathcal{P}_{fnr}(A^n_{\mathrm{d}}) \cup \{\langle\rangle\}).$$

Furthermore, let $A^*_{\mathrm{d}} = \cup_n A^n_{\mathrm{d}}$.

Using A^*_{d} we are now in a position to extend $\mathcal{V}$ (Definition 6.1.8) to deterministic probabilistic processes and deterministic trees as follows, where multiplication is used for the same intuitive reasons it is used in the definition of D on deterministic probabilistic transition systems.

Definition 6.3.3 *For all $p \in D^s_\omega$, $u \in A^*_{\mathrm{d}}$, and $n \in \mathbb{N}$, we define the* probability *of p* performing the "deterministic tree" *u, denoted $\mathcal{V}(u, p)$, as follows:*

$$\mathcal{V}(\langle\rangle, p) = \begin{cases} 1 & \textit{if } p = p_0 \\ 0 & \textit{otherwise} \end{cases}$$

Then for all $p \in D^s_\omega$ and $aU \in A^{n+1}_{\mathrm{d}}$ put:

$$\mathcal{V}(aU, p) = \begin{cases} \sum_{X \in D_\omega} f(X) \cdot \mathcal{V}(U, X) & \textit{if } p = (a, f) \textit{ for some } f \in \mu(D_\omega) \\ 0 & \textit{otherwise} \end{cases}$$

where, for all $X \in D_\omega$ *and* $U \in \mathcal{P}_{fnr}(A^n_{\mathrm{d}}) \cup \{\langle\rangle\}$, *either* $U = \{a_1U_1, \ldots, a_mU_m\} \in \mathcal{P}_{fnr}(A^n_{\mathrm{d}})$ *and*

$$\mathcal{V}(U, X) = \begin{cases} \prod_{i=1}^{m} \mathcal{V}(a_iU_i, (a_i, f_i)) & \textit{if } X = \{(a_1, f_1), \ldots, (a_m, f_m)\} \\ & \textit{for some } \{f_1, \ldots, f_m\} \subseteq \mu(D) \\ 0 & \textit{otherwise} \end{cases}$$

or $U = \langle\rangle$, *and then put:*

$$\mathcal{V}(\langle\rangle, X) = \begin{cases} 1 & \textit{if } X = \{p_0\} \\ 0 & \textit{otherwise.} \end{cases}$$

We next introduce the following extension of Proposition 6.1.9 to the deterministic case.

Proposition 6.3.4 *For all* $p \in D^s_\omega$ *and* $X \in D_\omega$, *the maps* $\mathcal{V}(\cdot, p) : A^*_{\mathrm{d}} \to [0, 1]$ *and* $\mathcal{V}(\cdot, X) : \mathcal{P}_{fnr}(A^*_{\mathrm{d}}) \cup \{\langle\rangle\} \to [0, 1]$ *are probability distributions.*

Proof. The proof is by induction on $p \in D^s_n$ and $X \in D_n$. If $n = 0$ the lemma follows similarly to Proposition 6.1.9.

Now, suppose that the proposition holds for some $n \in \mathbb{N}$, then again similarly to Proposition 6.1.9 we can show that $\mathcal{V}(\cdot, p) \in \mu(A^*_{\mathrm{d}})$ for all $p \in D^s_{n+1}$. Next consider any $X \in D_{n+1} \setminus D_n$, then $X = \{(a_1, f_1), \ldots, (a_m, f_m)\}$ for some $m \in \mathbb{N}$, where $(a_i, f_i) \in D^s_{n+1}$ for all $1 \leq i \leq m$. Letting $p_i = (a_i, f_i)$, $p_i \in D^s_{n+1}$ and hence from above $\mathcal{V}(\cdot, p_i) \in \mu(A^*_{\mathrm{d}})$ for all $1 \leq i \leq m$. By Definition 6.3.3:

$$\begin{aligned} \sum_{U \in \mathcal{P}_{fnr}(A^*_{\mathrm{d}}) \cup \{\langle\rangle\}} \mathcal{V}(U, X) &= \sum_{\cup_{i=1}^m a_iU_i \in \mathcal{P}_{fnr}(A^*_{\mathrm{d}})} \left(\prod_{i=1}^{m} \mathcal{V}(a_iU_i, p_i) \right) \\ &= \prod_{i=1}^{m} \left(\sum_{a_iU_i \in A^*_{\mathrm{d}}} \mathcal{V}(a_iU_i, p_i) \right) && \text{rearranging} \\ &= \prod_{i=1}^{m} \left(\sum_{u \in A^*_{\mathrm{d}}} \mathcal{V}(u, p_i) \right) && \text{by Definition 6.3.3 since } p_i = (a_i, f_i) \\ &= \prod_{i=1}^{m} 1 && \text{since } \mathcal{V}(\cdot, p_i) \in \mu(A^*_{\mathrm{d}}) \text{ for all } 1 \leq i \leq m \\ &= 1 \end{aligned}$$

as required. □

Following the construction for the metric space (P, d) of simple probabilistic processes, we next define a pseudo-metric on D_ω. We achieve this by first defining a pseudo-metric on D^s_ω based on the pseudo-metric $d_{\mathcal{S}}$ on P_ω, and then extend this pseudo-metric to all of D_ω using the Hausdorff distance.

Proposition 6.3.5 *D^s_ω is a pseudo-metric space with respect to the pseudo-metric:*

$$d_{\mathcal{S}}(p,q) = \frac{1}{2} \sum_{u \in A^*_{\mathrm{d}}} |\, \mathcal{V}(u,p) - \mathcal{V}(u,q)\,|.$$

Furthermore, for all $p, q \in D^s_\omega$, $0 \leq d_{\mathcal{S}}(p,q) \leq 1$.

We note that, since $A^* \subseteq A^*_{\mathrm{d}}$ and the fact that $\mathcal{V}$ (defined over deterministic probabilistic processes) when restricted to simple probabilistic processes coincides with the definition of $\mathcal{V}$ over simple probabilistic processes, the above pseudo-metric is equivalent to the pseudo-metric given in Proposition 6.1.10 defined over simple probabilistic processes.

Again, following the methodology for the construction of P, we next extend the definition of truncations on P_ω to D_ω as follows.

Definition 6.3.6 *For any $f \in \mu(D_\omega)$, $p \in D^s_\omega$ and $k \in \mathbb{N}$, $f[k]$ and $p[k]$ are as defined in Definition 6.1.11. Furthermore, for any $X \in D_\omega$ put $X[n] = \{p[n] \mid p \in X\}$.*

Using the above definition and Definition 6.3.3, similarly to Lemma 6.1.13 and Proposition 6.1.12 for P_ω we have the following lemma and proposition connecting truncations and deterministic probabilistic processes.

Lemma 6.3.7 *For all $p \in D^s_\omega$, $X \in D_\omega$, $u \in A^*_{\mathrm{d}}$ and $U \in \mathcal{P}_{fnr}(A^*_{\mathrm{d}}) \cup \{\langle\rangle\}$:*

$$\mathcal{V}(u, p[k]) = \sum_{\tilde{u}\restriction k = u} \mathcal{V}(\tilde{u}, p) \;\; \textit{and} \;\; \mathcal{V}(U, X[k]) = \sum_{\tilde{U}\restriction k = U} \mathcal{V}(\tilde{U}, X).$$

Proposition 6.3.8 *For all $p, q \in D^s_\omega$ and $k, m \in \mathbb{N}$:*

- (a) *if $p \in D^s_m$, then $p[k] \in D^s_k$ when $k < m$ and $p[k] = p$ otherwise.*
- (b) *$(p[m])[k] = p[\min\{m,k\}]$.*
- (c) *$p[m] = q[m]$ if and only if $p[k] = q[k]$ for all $k \leq m$.*
- (d) *$d_{\mathcal{S}}(p[k], q[k]) \leq d_{\mathcal{S}}(p,q)$.*
- (e) *if $u \in A^*_{\mathrm{d}} \setminus A^k_{\mathrm{d}}$, then $\mathcal{V}(u, p[k]) = 0$.*

Similarly to the case for simple probabilistic processes, to obtain the required Cauchy sequences we consider the pseudo-metric d_ω (see Definition 6.1.15) over D^s_ω, incorporating both the pseudo-metric $d_{\mathcal{S}}$ and truncations. We reach the following proposition.

Proposition 6.3.9 *D^s_ω (and D^s_n for any $n \in \mathbb{N}$) is a pseudo-metric space with respect the pseudo-metric:*

$$d_\omega(p,q) = \sum_{k=0}^{\infty} 2^{-k} d_{\mathcal{S}}(p[k], q[k]).$$

We are now in a position to extend d_ω from D^s_ω to D_ω as follows.

Theorem 6.3.10 *(D_ω, d_ω) (and (D_n, d_ω) for any $n \in \mathbb{N}$) is a pseudo-metric space, where d_ω is the Hausdorff metric with respect to d_ω on D^s_ω. Furthermore, for all $p, q \in D^s_\omega$ and $X, Y \in D_\omega$, $0 \leq d_\omega(p,q), d_\omega(X,Y) \leq 1$.*

Proof. If we consider any $X \in D_\omega$ then either $X = \{p_0\}$ or, by definition of $\mathcal{P}_{fnr}(\cdot \times \cdot)$, X is a non-empty finite set of elements, and hence closed. Then, since this is the case for any $X \in D_\omega$, Lemma 3.3.10 implies that d_ω is a pseudo-metric on D_ω. To show $0 \leq d_\omega(p,q), d_\omega(X,Y) \leq 1$ for all $p, q \in D^s_\omega$ and $X, Y \in D_\omega$ we use an argument similar to that for Proposition 6.1.16 together with the definition of the Hausdorff distance. □

We now investigate the properties of the pseudo-metric d_ω on D_ω.

Lemma 6.3.11 *Let a and b be distinct elements of A, $f, g \in \mu(D_\omega)$, $p \in D^s_\omega$ and $m \in \mathbb{N}$, then*

$$d_\omega((a,f),(b,g)) = d_\omega(p_0,(a,f)) = 1, \;\; d_\omega((a,f),(a,g)) \leq \frac{1}{2} \;\; \textit{and} \;\; d_\omega(p, p[m]) \leq \frac{1}{2^m}.$$

Moreover, for all $X, Y (\neq \{p_0\}) \in D_\omega$: $d_\omega(X,Y) \leq \frac{1}{2}$ if and only if

$$X = \{(a_1, f_1), \ldots, (a_m, f_m)\} \;\; \textit{and} \;\; Y = \{(a_1, g_1), \ldots, (a_m, g_m)\}$$

for some $m \in \mathbb{N}$, where $a_i \in A$ and f_i, $g_i \in \mu(D_\omega)$ for all $1 \leq i \leq m$.

Proof. For the proof of the first part of the lemma see Lemma 6.1.20. For the second part of the lemma and its "if" direction suppose:

$$X = \{(a_1, f_1), \ldots, (a_m, f_m)\} \;\text{ and }\; Y = \{(a_1, g_1), \ldots, (a_m, g_m)\}.$$

Hence, if $p \in X$ then $p = (a_i, f_i)$ for some $1 \leq i \leq m$, and therefore by definition of the Hausdorff distance:

$$\begin{array}{rcll} d_\omega(p, Y) & = & inf\{d_\omega(p,q) \,|\, q \in Y\} & \\ & \leq & d_\omega((a_i, f_i),(a_i, g_i)) & \text{since } p = (a_i, f_i) \text{ and } (a_i, g_i) \in Y \\ & \leq & \frac{1}{2} & \text{by the first part of the lemma} \end{array}$$

and since this was for any $p \in X$, $\sup_{p \in X} d_\omega(p, Y) \leq \frac{1}{2}$. Furthermore, by symmetry we have $\sup_{q \in Y} d_\omega(q, X) \leq \frac{1}{2}$, and hence by definition of the Hausdorff distance $d_\omega(X,Y) \leq \frac{1}{2}$ as required.

For the "only if" direction, consider any $X, Y (\neq \{p_0\}) \in D_\omega$ not of the form given in the hypothesis, then without loss of generality we can suppose that there exists

$p \in X$ such that $p = (a, f)$ for some $a \in A$ and $f \in \mu(D_\omega)$, and for all $q \in Y$, $q \neq (a, g)$ for any $g \in \mu(D_\omega)$. Then, by definition of the Hausdorff distance:

$$\begin{aligned} d_\omega(X,Y) &\geq inf\{d_\omega(q,p) \mid q \in Y\} \\ &= 1 \qquad\qquad \text{by the first part of the lemma.} \end{aligned}$$

Moreover, by Proposition 6.3.5, $d_\omega(X,Y) \leq 1$, and thus $d_\omega(X,Y) = 1$ as required. □

As before, we now apply the standard completion techniques to derive the metric space (D, d) of deterministic probabilistic processes.

Definition 6.3.12 *Let (D, d), the metric-space of* deterministic probabilistic processes*, be the completion of (D_ω, d_ω).*

Note that, as for the case for simple probabilistic processes, D consists of the set of equivalence classes of Cauchy sequences of D_ω under the equivalence $\sim$, where

$$\langle X_n \rangle_{n \in \mathbb{N}} \sim \langle Y_n \rangle_{n \in \mathbb{N}} \quad \text{if and only if} \quad \lim_{n \to \infty} d_\omega(X_n, Y_n) = 0,$$

and for any Cauchy sequences $\langle X_n \rangle_{n \in \mathbb{N}}$ and $\langle Y_n \rangle_{n \in \mathbb{N}}$ the metric d is given by:

$$d(\langle X_n \rangle_{n \in \mathbb{N}}, \langle Y_n \rangle_{n \in \mathbb{N}}) = \lim_{n \to \infty} d_\omega(X_n, Y_n).$$

Before we introduce denotational semantics for $\mathrm{RP_d}$, we first require the following technical lemmas.

Lemma 6.3.13 *For all $X \in D_\omega$, $\langle X[n] \rangle_n$ is a Cauchy sequence.*

Lemma 6.3.14 *If $\langle X_n \rangle_{n \in \mathbb{N}}$ is a sequence in D_ω such that $X_{n+1}[n] = X_n[n]$ for all $n \in \mathbb{N}$, then $\langle X_n \rangle_{n \in \mathbb{N}}$ is Cauchy and $X_m[n] = X_n[n]$ for all $m \geq n \in \mathbb{N}$. Furthermore, if $\langle q_n \rangle_{n \in \mathbb{N}}$ is a sequence in D_ω such that $Y_{n+1}[n] = Y_n[n]$ for all $n \in \mathbb{N}$ and $\langle X_n \rangle_{n \in \mathbb{N}} \sim \langle Y_n \rangle_{n \in \mathbb{N}}$, then $d_\omega(X_n[n], Y_n[n]) = 0$ for all $n \in \mathbb{N}$.*

Lemma 6.3.15 *If $\langle X_n \rangle_{n \in \mathbb{N}}$ and $\langle Y_n \rangle_{n \in \mathbb{N}}$ are Cauchy sequence and $\langle X_n \rangle_{n \in \mathbb{N}} \not\sim \langle Y_n \rangle_{n \in \mathbb{N}}$, then there exists $n \in \mathbb{N}$ such that $X_n[n] \neq Y_n[n]$.*

6.4 Denotational Semantics for $\mathrm{RP_d}$

Similarly to the case for P we can now give denotational semantics for our language $\mathrm{RP_d}$ based on D (assuming $A = \mathrm{Act}$). The first step is to add an operator for external choice and extend the semantic operators defined over P_ω. Similar to the case for P_ω we define the operators by induction on the *degree* of a processes $X \in D_\omega$, which we now define.

Definition 6.4.1 *The* degree *of a process* $X \in D_\omega$ *is defined inductively by putting* $deg(\{p_0\}) = 0$ *and* $deg(X) = n+1$ *if* $X \in D_{n+1} \setminus D_n$ *for some* $n \in \mathbb{N}$.

Definition 6.4.2 (External Choice) *Let* $\{p_0\} \oplus \{p_0\} = \{p_0\}$ *and if* $X, Y \in D_\omega$ *with non-zero degree, then* $X \oplus \{p_0\} = \{p_0\} \oplus X = X$ *and* $X \oplus Y$ *is the set theoretic union of the two sets* X *and* Y.

To show $\oplus$ is well-defined, we first require the following lemma:

Lemma 6.4.3 *For all* X, $\tilde{X}$, Y *and* $\tilde{Y} \in D_\omega$:

$$d_\omega(X \oplus Y, \tilde{X} \oplus \tilde{Y}) \leq \max\{d_\omega(X, \tilde{X}), d_\omega(Y, \tilde{Y})\}.$$

Proof. If X, $\tilde{X}$, Y, $\tilde{Y} \in D_\omega$, then without loss of generality either $X = \{p_0\}$ and the result follows from Lemma 6.3.11. or X, $\tilde{X}$, Y and $\tilde{Y}$ are not equal to $\{p_0\}$. In this case, by definition of the Hausdorff distance and $\oplus$ we obtain:

$$d_\omega(p, \tilde{X} \oplus \tilde{Y}) = d_\omega(p, \tilde{X} \cup \tilde{Y}) \leq d_\omega(p, \tilde{X}) \leq d_\omega(X, \tilde{X}) \leq \max\{d_\omega(X, \tilde{X}), d_\omega(Y, \tilde{Y})\}$$

for any $p \in X$. Taking the supremum of $p \in X$ we have

$$sup_{p \in X} d_\omega(p, \tilde{X} \oplus \tilde{Y}) \leq \max\{d_\omega(X, \tilde{X}), d_\omega(Y, \tilde{Y})\}.$$

Then similarly:

$$\begin{array}{rcl}
\sup_{q \in Y} d_\omega(q, \tilde{X} \oplus \tilde{Y}) & \leq & \max\{d_\omega(X, \tilde{X}), d_\omega(Y, \tilde{Y})\} \\
\sup_{\tilde{p} \in \tilde{X}} d_\omega(\tilde{p}, X \oplus Y) & \leq & \max\{d_\omega(X, \tilde{X}), d_\omega(Y, \tilde{Y})\} \\
\sup_{\tilde{q} \in \tilde{Y}} d_\omega(\tilde{q}, X \oplus Y) & \leq & \max\{d_\omega(X, \tilde{X}), d_\omega(Y, \tilde{Y})\}.
\end{array}$$

Now taking the maximum of the left hand sides of the above four inequalities, the lemma follows by definition of the Hausdorff distance. □

We note that, Lemma 6.4.3 above can be generalize to: for all X, $\tilde{X}$, Y and $\tilde{Y} \in D_\omega$:

$$d_\omega(X \oplus Y, \tilde{X} \oplus \tilde{Y}) \leq \max\{d_\omega(X, \tilde{X}), d_\omega(X, \tilde{Y}), d_\omega(Y, \tilde{X}), d_\omega(Y, \tilde{Y})\}.$$

Proposition 6.4.4 $\oplus$ *is continuous and well-defined on* (D_ω, d_ω), *with the restriction that* $X \oplus Y$ *is only considered if* $X \oplus Y$ *satisfies the reactiveness condition.*

Proof. The proof that $\oplus$ is continuous in both arguments is a direct result of Lemma 6.4.3. Furthermore, with the above restriction, it is clear that $X \oplus Y \in D_\omega$ for all $X, Y \in D_\omega$ as required. □

Before we consider the semantic operators $||$ and $\lceil$ with respect to D_ω, following the techniques used for simple probabilistic processes we lift the operators $\cap$ and $\lceil B$ for any $B \subseteq A$ on A^* to A^*_{d} by induction as follows.

Definition 6.4.5 *For any* $U, \tilde{U} \in \mathcal{P}_{fnr}(A_{\mathrm{d}}^{n+1})$ *and* $B \subseteq A$:

$$U \cap \tilde{U} = \begin{cases} \langle\rangle & \text{if } u \cap \tilde{u} = \langle\rangle \text{ for all } u \in U \;\&\; \tilde{u} \in \tilde{U} \\ \{u \cap \tilde{u} \mid u \cap \tilde{u} \neq \langle\rangle,\ u \in U \;\&\; \tilde{u} \in \tilde{U}\} & \text{otherwise} \end{cases}$$

and

$$U \restriction B = \begin{cases} \langle\rangle & \text{if } u \restriction B = \langle\rangle \text{ for all } u \in U \\ \{u \restriction B \mid u \restriction B \neq \langle\rangle \;\&\; u \in U\} & \text{otherwise.} \end{cases}$$

We next introduce the semantic operator for synchronous parallel.

Definition 6.4.6 (Parallel) *We extend the definition of the semantic operator* $\|$ *on* P_ω *to* D_ω *by setting:* $X \| Y = \oplus\{p \| q \mid p \in X \;\&\; q \in Y\}$ *for any* $X, Y \in D_\omega$.

We next investigate the connections between $\|$ and $\mathcal{V}$. First we require the following lemma.

Lemma 6.4.7 *For all* $X = X_1 \cup X_2 \in D_\omega$*, such that* X_1 *and* X_2 *are of the form* $\{(a_1, f_1), \ldots, (a_m, f_m)\}$ *and* $\{(b_1, g_1), \ldots, (b_{\tilde{m}}, g_{\tilde{m}})\}$ *respectively, and* U_1, $U_2 \in \mathcal{P}_{fr}(A_{\mathrm{d}}^*)$ *such that* U_1 *and* U_2 *are of the form* $\{a_1V_1, \ldots, a_mV_m\}$ *and* $\{b_1W_1, \ldots, b_{\tilde{m}}W_{\tilde{m}}\}$ *respectively:*

$$\mathcal{V}(U_1 \cup U_2, X) = \mathcal{V}(U_1, X_1) \cdot \mathcal{V}(U_2, X_2),$$

and moreover:

$$\sum_{U_1 \subseteq U} \mathcal{V}(U, X) = \mathcal{V}(U_1, X_1).$$

Proof. Consider any $X \in D_\omega$ and $U_1, U_2 \in \mathcal{P}_{fr}(A_{\mathrm{d}}^*)$ of the form given above. Then Definition 6.3.3 implies:

$$\begin{aligned} \mathcal{V}(U_1 \cup U_2, X) &= \prod_{i=1}^{m} \prod_{j=1}^{\tilde{m}} \left(\mathcal{V}(a_iV_i, (a_i, f_i)) \cdot \mathcal{V}(b_jW_j, (b_j, g_j))\right) \\ &= \left(\prod_{i=1}^{m} \mathcal{V}(a_iV_i, (a_i, f_i))\right) \cdot \left(\prod_{j=1}^{\tilde{m}} \mathcal{V}(b_jW_j, (b_j, g_j))\right) && \text{rearranging} \\ &= \mathcal{V}(U_1, X_1) \cdot \mathcal{V}(U_2, X_2) && \text{as required.} \end{aligned}$$

For the proof of the second part of the lemma, since $X \in D_\omega$, by the reactiveness condition $a_i \neq a_j$ for all $1 \leq i \leq m$ and $1 \leq j \leq \tilde{m}$. Moreover, by definition of $\mathcal{V}$, if $U \in \mathcal{P}_{fnr}(A_{\mathrm{d}}^*)$ and $U \neq U_1 \cup U_2$ for some U_1, $U_2 \in \mathcal{P}_{fnr}(A_{\mathrm{d}}^*)$ of the form given in the hypothesis, we obtain $\mathcal{V}(U, X)$ therefore equals 0. Supposing U_2 varies according to the form given in the hypothesis, the term $\sum_{U_1 \subseteq U} \mathcal{V}(U, X)$ therefore equals:

$$\begin{aligned} \sum_{U_2 \in \mathcal{P}_{fnr}(A_{\mathrm{d}}^*)} \mathcal{V}(U_1 \cup U_2, X) &= \sum_{U_2 \in \mathcal{P}_{fnr}(A_{\mathrm{d}}^*)} \mathcal{V}(U_1, X_1) \cdot \mathcal{V}(U_2, X_2) && \text{from above} \\ &= \mathcal{V}(U_1, X_1) \cdot \left(\sum_{U_2 \in \mathcal{P}_{fnr}(A_{\mathrm{d}}^*)} \mathcal{V}(U_2, X_2)\right) && \text{rearranging} \\ &= \mathcal{V}(U_1, X_1) && \text{by Proposition 6.3.4} \end{aligned}$$

as required. □

Lemma 6.4.8 *For all $p, q \in D^s_\omega$, $X, Y \in D_\omega$, $u \in A^*_\mathrm{d}$ and $U \in \mathcal{P}_{fnr}(A^*_\mathrm{d}) \cup \{\langle\rangle\}$:*

$$\mathcal{V}(u, p \,\|\, q) = \sum_{u_1 \cap u_2 = u} \mathcal{V}(u_1, p) \cdot \mathcal{V}(u_2, q) \quad \textit{and}$$

$$\mathcal{V}(U, X \,\|\, Y) = \sum_{U_1 \cap U_2 = U} \mathcal{V}(U_1, X) \cdot \mathcal{V}(U_2, Y).$$

Proof. The proof is by induction on $deg(p \,\|\, q)$ and $deg(X \,\|\, Y)$. Similarly to the proof of Lemma 6.2.3 we can show that the lemma holds for any $p, q \in D^s_\omega$ and $X, Y \in D_\omega$ such that $deg(p \,\|\, q) = deg(X \,\|\, Y) = 0$. Suppose that the lemma holds for some $n \in \mathbb{N}$ for any $p, q \in D^s_\omega$ such that $deg(p \,\|\, q) = n + 1$, and $u \in A^*_\mathrm{d}$:

$$\mathcal{V}(u, p \,\|\, q) = \sum_{u_1 \cap u_2 = u} \mathcal{V}(u_1, p) \cdot \mathcal{V}(u_2, q). \tag{6.8}$$

To complete the proof, consider any $X, Y \in D_\omega$ such that $deg(X \,\|\, Y) = n + 1$. By definition of $\|$, $X \,\|\, Y = \{(a_1, f_1 \,\|\, g_1), \ldots, (a_m, f_m \,\|\, g_m)\}$ for some $m \in \mathbb{N}$ such that:

$$X = \{(a_1, f_1), \ldots, (a_m, f_m), (b_1, \tilde{f}_1), \ldots, (b_{m_1}, \tilde{f}_{m_1})\}$$

and

$$Y = \{(a_1, g_1), \ldots, (a_m, g_m), (c_1, \tilde{g}_1), \ldots, (c_{m_2}, \tilde{g}_{m_2})\}$$

where $m_1, m_2 \in \mathbb{N}$, $b_i \neq c_j$ for all $1 \leq i \leq m_1$ and $1 \leq j \leq m_2$. By definition of $\mathcal{V}$ and Definition 6.4.5:

$$\mathcal{V}(U, X \,\|\, Y) = \sum_{U_1 \cap U_2 = U} \mathcal{V}(U_1, X) \cdot \mathcal{V}(U_2, Y) = 0$$

for any $U \in \mathcal{P}_{fnr}(A^*_\mathrm{d})$ not of the form $\{a_1U_1, \ldots, a_mU_m\}$.

On the other hand if U is of the form $\{a_1U_1, \ldots, a_mU_m\}$ then:

$$\begin{aligned}
\mathcal{V}(U, X \,\|\, Y) &= \prod_{i=1}^{m} \mathcal{V}(a_iU_i, (a_i, f_i \,\|\, g_i)) \\
&= \prod_{i=1}^{m} \left(\sum_{v_i \cap w_i = a_iU_i} \mathcal{V}(v_i, (a_i, f_i)) \cdot \mathcal{V}(w_i, (a_i, g_i)) \right) && \text{by (6.8)} \\
&= \prod_{i=1}^{m} \left(\sum_{a_iV_i \cap a_iW_i = a_iU_i} \mathcal{V}(a_iV_i, (a_i, f_i)) \cdot \mathcal{V}(a_iW_i, (a_i, g_i)) \right) && \text{by Definition 6.4.5} \\
&= \sum_{\substack{a_iV_i \cap a_iW_i = a_iU_i \\ \forall\, 1 \le i \le m}} \mathcal{V}\left(\bigcup_{i=1}^{m} a_iV_i, \bigcup_{i=1}^{m} (a_i, f_i) \right) \cdot \mathcal{V}\left(\bigcup_{i=1}^{m} a_iW_i, \bigcup_{i=1}^{m} (a_i, g_i) \right) \\
&= \sum_{\substack{a_iV_i \cap a_iW_i = a_iU_i \\ \forall\, 1 \le i \le m}} \left(\sum_{\cup_{i=1}^{m} a_iV_i \subseteq V} \mathcal{V}(V, X) \right) \cdot \left(\sum_{\cup_{i=1}^{m} a_iW_i \subseteq W} \mathcal{V}(W, Y) \right) && \text{by Lemma 6.4.7} \\
&= \sum_{V \cap W = U} \mathcal{V}(V, X) \cdot \mathcal{V}(W, Y) && \text{by Definition 6.4.5.}
\end{aligned}$$

□

Lemma 6.4.9 *For all* $p, q \in D^s_\omega$ *and* $k \in \mathbb{N}$ *we have* $(p \,\|\, q)[k] = p[k] \,\|\, q[k]$.

Proposition 6.4.10 $\|$ *is continuous and well-defined on* (D_ω, d_ω).

The next semantic operator we introduce is restriction.

Definition 6.4.11 (Restriction) *We extend the definition of the semantic operator* $\restriction$ *by setting:* $X \restriction B = \oplus\{p \restriction B \mid p \in X\}$ *for any* $X \in D_\omega$.

We now investigate properties of this operator.

Lemma 6.4.12 *For all* $p \in D^s_\omega$, $X \in D_\omega$, $u \in A^*$, $U \in \mathcal{P}_{fnr}(A^*_{\mathrm{d}})$ *and* $B \subseteq A$:

$$\mathcal{V}(u, p \restriction B) = \sum_{u' \restriction B = u} \mathcal{V}(u', p) \quad \textit{and} \quad \mathcal{V}(u, X \restriction B) = \sum_{U' \restriction B = U} \mathcal{V}(U', X).$$

Furthermore, for any $k \in \mathbb{N}$: $(p \restriction B)[k] = p[k] \restriction B$.

Proposition 6.4.13 *For all* $B \subseteq A$, *the map* $\restriction B$ *is continuous and well-defined on* (D_ω, d_ω).

As for the case concerning P_ω, the final semantic operator we introduce is that of relabelling.

Definition 6.4.14 (Relabelling) *For all* $\lambda\colon A \to A$ *we extend Definition 6.2.10, by setting* $X\,[\lambda] = \oplus\{p\,[\lambda] \mid p \in X\}$ *for any* $X \in D_\omega$.

To show that the above operator is continuous and well-defined we need the following lemma.

Lemma 6.4.15 *For all* $p \in D^s_\omega$, $u \in A^*_{\mathrm{d}}$, $\lambda : A \to A$ *and* $k \in \mathbb{N}$: $\mathcal{V}(u, p\,[\lambda]) = \mathcal{V}(\lambda^{-1}(u), p)$ *and* $(p\,[\lambda])[k] = (p[k])\,[\lambda]$.

Proposition 6.4.16 *For all* $\lambda\colon A \to A$, $[\lambda]$ *is continuous and well-defined on* (D_ω, d_ω).

We can now define denotational metric semantics for $\mathrm{RP_d}$ by extending the definition of the semantic map $\mathcal{D}$ given earlier for $\mathrm{RP_p}$.

Definition 6.4.17 (Denotational Semantics) *Let* $\mathcal{D}_n : \mathrm{RP_d} \to (\mathrm{Env} \to D_\omega)$, $n \in \mathbb{N}$, *be the collection of maps defined inductively as follows. Put* $\mathcal{D}_0[\![E]\!] = \{p_0\}$ *for all* $E \in \mathrm{RP_d}$, *and* $\mathcal{D}_{n+1}$ *be defined inductively on the structure of elements of* $\mathrm{RP_d}$ *as follows:*

$$
\begin{array}{rcl}
\mathcal{D}_{n+1}[\![x]\!](\rho) & = & \rho_{n+1}(x) \\
\mathcal{D}_{n+1}[\![\mathbf{0}]\!](\rho) & = & \{p_0\} \\
\mathcal{D}_{n+1}[\![a.\sum_{i\in I}\mu_i.E_i]\!](\rho) & = & \{(a, \Phi_{D_\omega}(\langle \mu_i, \mathcal{D}_n[\![E_i]\!](\rho)\rangle_{i\in I}))\} \\
\mathcal{D}_{n+1}[\![E_1 \,\Box\, E_2]\!](\rho) & = & \mathcal{D}_{n+1}[\![E_1]\!](\rho) \oplus \mathcal{D}_{n+1}[\![E_2]\!](\rho) \\
\mathcal{D}_{n+1}[\![E_1 \parallel E_2]\!](\rho) & = & \mathcal{D}_{n+1}[\![E_1]\!](\rho) \parallel \mathcal{D}_{n+1}[\![E_2]\!](\rho) \\
\mathcal{D}_{n+1}[\![E \upharpoonright B]\!](\rho) & = & \mathcal{D}_{n+1}[\![E]\!](\rho) \upharpoonright B \\
\mathcal{D}_{n+1}[\![E\,[\lambda]]\!](\rho) & = & \mathcal{D}_{n+1}[\![E]\!](\rho)\,[\lambda] \\
\mathcal{D}_{n+1}[\![\mathit{fix}_x.E]\!](\rho) & = & \mathcal{D}_{n+1}[\![E]\!](\rho\{\mathcal{D}_n[\![\mathit{fix}_x.E]\!](\rho)/x\}).
\end{array}
$$

Furthermore, let $\mathcal{D} : \mathrm{RP_d} \to (\mathrm{Env} \to D)$ *be the map defined as follows, for any* $E \in \mathrm{RP_d}$ *put:* $\mathcal{D}[\![E]\!](\rho) = [\langle \mathcal{D}_n[\![E]\!](\rho)\rangle_{n\in\mathbb{N}}]_\sim$.

As before, to prove the well-definedness of the semantic map we must first demonstrate the following results.

Lemma 6.4.18 *For all* $E \in \mathcal{G}^{\mathrm{d}}$, $\rho \in \mathrm{Env}$ *and* $k \in \mathbb{N}$: $\mathcal{D}_{k+1}[\![E]\!](\rho)[k] = \mathcal{D}_k[\![E]\!](\rho)[k]$.

Lemma 6.4.19 *For all* $E \in \mathrm{RP_d}$, $F \in \mathrm{Pr}^{\mathrm{d}}$, $\rho \in Env$ *and* $n \in \mathbb{N}$:

$$\mathcal{D}_n[\![E\{F/x\}]\!](\rho)[n] = \mathcal{D}_n[\![E]\!](\rho\{D_n[\![F]\!]/x\})[n].$$

Furthermore, if $E \in \mathcal{G}^{\mathrm{d}}$ *then:*

$$\mathcal{D}_{n+1}[\![E\{F/x\}]\!](\rho)[n+1] = \mathcal{D}_{n+1}[\![E]\!](\rho\{D_n[\![F]\!]/x\})[n+1].$$

Moreover, since we have added deterministic choice to our model, we also require the following lemma.

Lemma 6.4.20 *For all $E \in \mathcal{G}^{\mathrm{d}}$, $\rho \in \mathrm{Env}$ and $a \in \mathcal{A}ct$: $a \in \mathrm{init}(E)$ if and only if $(a, f_n) \in \mathcal{D}_{n+1}[\![E]\!](\rho)$ for some $f_n \in \mu(D_\omega)$ for all $n \in \mathbb{N}$.*

Proof. The proof is by induction on the structure of $E \in \mathcal{G}^{\mathrm{d}}$ and follows from the definition of init $\mathcal{D}_{n+1}$ and the semantic operators on D_ω. □

Proposition 6.4.21 *$\mathcal{D}$ is well-defined on the guarded expressions of $\mathrm{RP_d}$.*

Proof. The proof follows similarly to the one of Proposition 6.2.21, with the following additional inductive step. If $E = E_1 \,\Box\, E_2$, then by induction on E_1 and E_2, $\mathcal{D}_{k+1}[\![E_1]\!](\rho) \in D_\omega$ and $\mathcal{D}_{k+1}[\![E_2]\!](\rho) \in D_\omega$. Furthermore, by Lemma 6.4.20 and since $\mathrm{init}(E_1) \cap \mathrm{init}(E_2) = \emptyset$ by construction of $\mathrm{RP_d}$, we have that $\mathcal{D}_{k+1}[\![E_1]\!](\rho) \cup \mathcal{D}_{k+1}[\![E_2]\!](\rho)$ satisfies the reactiveness condition and hence $\mathcal{D}_{k+1}[\![E]\!](\rho) \in D_\omega$ by definition of $\mathcal{D}_{k+1}$ and $\oplus$. □

6.4.1 Full Abstraction

To prove full abstraction we first require the following lemmas and definitions where we remove the proofs if they are simple extensions of the corresponding proofs in Subsection 6.2.1.

Lemma 6.4.22 *For all $E \in \mathrm{Pr^p}$ and $\rho \in \mathrm{Env}$, $\mathcal{O}[\![E]\!] = \emptyset$ if and only if $\mathcal{D}_n[\![E]\!](\rho) = \{p_0\}$ for all $n \in \mathbb{N}$ and $\mathcal{O}[\![E]\!] = \{(a_1, \pi_1), \ldots, (a_m, \pi_m)\}$ if and only if $\mathcal{D}_{n+1}[\![E]\!](\rho) = \{(a_1, f_n^1), \ldots, (a_m, f_n^m)\}$ for all $n \in \mathbb{N}$ such that for any $n \in \mathbb{N}$, $1 \le i \le m$ and $Y \in D$:*

$$f_n^i[n](Y) = \sum_{\substack{F \in \mathrm{Pr^d}\ \& \\ \mathcal{D}[\![F]\!](\rho)[n] = Y}} \pi_i(F).$$

We next extend our mapping $\xi : A^* \to \mathtt{T}^{\mathrm{p}}$ to $A_{\mathrm{d}}^* \to \mathtt{T}^{\mathrm{d}}$ as follows: for any $U = \{u_1, \ldots, u_m\} \in \mathcal{P}_{fnr}(A_{\mathrm{d}}^*)$ put:

$$\xi(U) \stackrel{def}{=} (\xi(u_1), \ldots, \xi(u_m)).$$

Furthermore, we extend $\le$ to A_{d}^* by letting: $\langle\rangle \le u$ for all $u \in A_{\mathrm{d}}^*$ and $aU \le u'$ if $u' = aU'$ for some $U' \in \mathcal{P}_{fnr}(A_{\mathrm{d}}^*) \cup \{\langle\rangle\}$ such that for all $\tilde{u} \in U$ there exists $\tilde{u}' \in U'$ such that $\tilde{u} \le \tilde{u}'$. Then we have the following lemmas.

Lemma 6.4.23 *The mapping ξ is bijective.*

Lemma 6.4.24 *For all* $E \in \mathrm{Pr^d}$ *and* $\rho \in \mathrm{Env}$, *if* $\mathcal{O}[\![E]\!] = \{(a_1, \pi_1), \ldots, (a_m, \pi_m)\}$, *then* $\mathcal{D}_{n+1}[\![E]\!](\rho) = \{(a_1, f_n^1), \ldots, (a_m, f_n^m)\}$ *for any* $n \in \mathbb{N}$ *(by Lemma 6.4.22) and for any* $1 \leq i \leq m$, $U \in \mathcal{P}_{fnr}(A_\mathrm{d}^n) \cup \{\langle\rangle\}$ *and* $n \in \mathbb{N}$:

$$\sum_{\substack{u \in A_\mathrm{d}^{n+1} \\ \& \, a_i U \leq u}} \mathcal{V}(u, (a_i, f_n^i[n])) = \mathsf{D}(E)(\xi(u)).$$

Proof. Consider any $E \in \mathrm{Pr^d}$ and $\rho \in \mathrm{Env}$, such that $\mathcal{O}[\![E]\!] = \{(a_1, \pi_1), \ldots, (a_m, \pi_m)\}$. We prove the lemma by induction on $n \in \mathbb{N}$ and we ignore ρ for simplicity. If $n = 0$, then by definition of A_d^0, if $U \in \mathcal{P}_{fnr}(A_\mathrm{d}^n) \cup \{\langle\rangle\}$, then $U = \{\langle\rangle\}$ and by Definition 6.4.5 for any $1 \leq i \leq m$:

$$\sum_{\substack{u \in A_\mathrm{d}^1 \\ \& \, a_i \{\langle\rangle\} \leq u}} \mathcal{V}(u, (a_i, f_1^i[0])) \;\; = \;\; \mathcal{V}(a_i\{\langle\rangle\}, (a_i, f_1^i[0])).$$

Now, by definition of $\mathcal{V}$ and D we have: $\mathcal{V}(a_i\{\langle\rangle\}, (a_i, f_1^i[0])) = \mathsf{D}(E)(a_i.(\bot)) = 1$ and since $\xi(a_i\{\langle\rangle\}) = a_i.(\bot)$, the lemma holds for $n = 0$.

Now suppose the lemma holds for some $n \in \mathbb{N}$ and consider any $F \in \mathrm{Pr^d}$ and $U \in \mathcal{P}_{fnr}(A_\mathrm{d}^{n+1}) \cup \{\langle\rangle\}$. Then either $U = \langle\rangle$, and since $\langle\rangle \leq U'$ for all $U' \in \mathcal{P}_{fnr}(A_\mathrm{d}^{n+1}) \cup \{\langle\rangle\}$:

$$\begin{aligned}
\sum_{\substack{U' \in \mathcal{P}_{fnr}(A_\mathrm{d}^{n+1}) \cup \{\langle\rangle\} \\ \& \, \langle\rangle \leq U'}} \mathcal{V}(U', \mathcal{D}_{n+1}[\![F]\!][n+1]) &= \sum_{U' \in \mathcal{P}_{fnr}(A_\mathrm{d}^{n+1}) \cup \{\langle\rangle\}} \mathcal{V}(U', \mathcal{D}_{n+1}[\![F]\!][n+1]) \\
&= \sum_{U' \in \mathcal{P}_{fnr}(A_\mathrm{d}^{*}) \cup \{\langle\rangle\}} \mathcal{V}(U', \mathcal{D}_{n+1}[\![F]\!][n+1]) \quad \text{by Proposition 6.3.8}(e) \\
&= 1 \quad \text{by Proposition 6.3.4} \\
&= \mathsf{D}(F)(\bot) \quad \text{by definition of } \mathsf{P} \\
&= \mathsf{D}(F)(\xi(\langle\rangle)) \quad \text{by definition of } \xi,
\end{aligned}$$

or $U = \{b_1 U_1, \ldots, b_k U_k\}$ for some $k \in \mathbb{N}$, such that $b_i U_i \in A_\mathrm{d}^{n+1}$ for all $1 \leq i \leq k$. If $\{(b_1, \pi_1), \ldots, (b_k, \pi_k)\} \subseteq \mathcal{O}[\![F]\!]$ for some $\{\pi_1, \ldots \pi_k\} \subseteq \mu(\mathrm{Pr}^{\mathbf{d}})$, then Lemma 6.4.22

entails $(b_i, f_n^i) \in \mathcal{D}_{n+1}[\![F]\!]$ for some $f_n^i \in \mu(D_\omega)$ for all $1 \leq i \leq k$, and in this case:

$$\begin{aligned}
& \sum_{\substack{U' \in \mathcal{P}_{fnr}(A_{\mathrm{d}}^{n+1}) \cup \{\langle\rangle\} \\ \& \, U \leq U'}} \mathcal{V}(U, \mathcal{D}_{n+1}[\![F]\!][n+1]) \\
= & \sum_{\substack{b_i U_i' \in A_{\mathrm{d}}^{n+1} \\ \& \, b_i U_i \leq b_i U_i' \\ \forall 1 \leq i \leq k}} \left(\sum_{\substack{U' \in \mathcal{P}_{fnr}(A_{\mathrm{d}}^{n+1}) \cup \{\langle\rangle\} \\ \cup_{i=1}^{k} b_i U_i' \subseteq U'}} \mathcal{V}(U', \mathcal{D}_{n+1}[\![F]\!][n+1]) \right) && \text{by definition of } \leq \\
= & \sum_{\substack{b_i U_i' \in A_{\mathrm{d}}^{n+1} \\ \& \, b_i U_i \leq b_i U_i' \\ \forall 1 \leq i \leq k}} \prod_{i=1}^{k} \mathcal{V}(b_i U_i', (b_i, f_n^i)[n+1]) && \text{by Lemma 6.4.7} \\
= & \prod_{i=1}^{k} \left(\sum_{\substack{b_i U_i' \in A_{\mathrm{d}}^{n+1} \\ \& \, b_i U_i \leq b_i U_i'}} \mathcal{V}(b_i U_i', (b_i, f_n^i)[n+1]) \right) && \text{rearranging} \\
= & \prod_{i=1}^{k} \left(\sum_{\substack{u_i' \in A_{\mathrm{d}}^{n+1} \\ \& \, b_i U_i \leq u_i'}} \mathcal{V}(u_i', (b_i, f_n^i)[n+1]) \right) && \text{by definition of } \leq \\
= & \prod_{i=1}^{k} \mathsf{D}(F)(\xi(b_i U_i)) && \text{by induction} \\
= & \mathsf{D}(F)((\xi(b_1 U_1), \ldots, \xi(b_k U_k))) && \text{by definition of } \mathsf{D} \\
= & \mathsf{D}(F)(\xi(U)) && \text{by definition of } \xi.
\end{aligned}$$

On the other hand, if $(b_i, \pi_i) \notin \mathcal{O}[\![F]\!]$ for some $1 \leq i \leq k$ and all $\pi_i \in \mu(\mathrm{Pr^d})$, then $(b_i, f) \notin \mathcal{D}_{n+1}[\![F]\!]$ for any $f \in \mu(D_\omega)$ by Lemma 6.4.22 and therefore:

$$\sum_{\substack{U' \in \mathcal{P}_{fnr}(A_{\mathrm{d}}^{n+1}) \cup \{\langle\rangle\} \\ \& \, U \leq U'}} \mathcal{V}(U', \mathcal{D}_{n+1}[\![F]\!][n+1]) = \mathsf{D}(F)(\xi(U)) = 0$$

by definition of D and $\mathcal{V}$. Putting this together, we have:

$$\sum_{\substack{U' \in \mathcal{P}_{fnr}(A_{\mathrm{d}}^{n+1}) \cup \{\langle\rangle\} \\ \& \, U \leq U'}} \mathcal{V}(U, \mathcal{D}_{n+1}[\![F]\!][n+1]) = \mathsf{D}(F)(\xi(U))$$

for all $F \in \mathrm{Pr^d}$ and $U \in \mathcal{P}_{fnr}(A_{\mathrm{d}}^{n+1}) \cup \{\langle\rangle\}$. Using the latter the remainder of the proof follows similarly to Lemma 6.2.25. $\square$

Theorem 6.4.25 (Full Abstraction) *For all $E, F \in \mathcal{G}^{\mathrm{d}}$:*

$$\mathcal{O}[\![E]\!] \overset{\mathsf{d}}{\sim} \mathcal{O}[\![F]\!] \text{ if and only if } \mathcal{D}[\![E]\!](\rho) = \mathcal{D}[\![F]\!](\rho) \text{ for all } \rho \in \mathrm{Env}.$$

Proof. As for the purely probabilistic case, we only consider when $E, F \in \mathrm{Pr}^{\mathrm{d}}$ (we remove ρ for simplicity). First, consider any $E, F \in \mathrm{Pr}^{\mathrm{d}}$ such that $\mathcal{D}[\![E]\!] = \mathcal{D}[\![F]\!]$, then using Lemma 6.3.14 and Lemma 6.4.18 we have $d_\omega(\mathcal{D}_n[\![E]\!][n], \mathcal{D}_n[\![F]\!][n]) = 0$ for all $n \in \mathbb{N}$. Furthermore, by Lemma 6.3.11 and Lemma 6.4.18 either $\mathcal{D}_{n+1}[\![E]\!] = \mathcal{D}_{n+1}[\![F]\!] = \{p_0\}$, in which case $\mathcal{O}[\![E]\!] = \mathcal{O}[\![F]\!] = \emptyset$ by Lemma 6.4.22, and hence $\mathcal{O}[\![E]\!] \overset{\mathsf{d}}{\sim} \mathcal{O}[\![F]\!]$, or

$$\mathcal{D}_{n+1}[\![E]\!] = \{(a_1, f_n^1), \ldots, (a_m, f_n^m)\} \text{ and } \mathcal{D}_{n+1}[\![F]\!] = \{(a_1, g_n^1), \ldots, (a_m, g_n^m)\}$$

for some $m \in \mathbb{N}$, such that $d_\omega((a_i, f_n^i)[n+1], (a_i, g_n^i)[n+1]) = 0$ for all $1 \leq i \leq m$ and $n \in \mathbb{N}$. In the latter case, again using Lemma 6.4.22 we have:

$$\mathcal{O}[\![E]\!] = \{(a_1, \pi_1), \ldots, (a_m, \pi_m)\} \text{ and } \mathcal{O}[\![F]\!] = \{(a_1, \pi'_1), \ldots, (a_m, \pi'_m)\} \tag{6.9}$$

such that π_i, $\pi'_i \in \mu(\mathrm{Pr}^{\mathrm{p}})$ for all $1 \leq i \leq m$. Now, by definition of d_ω for any $n \in \mathbb{N}$:

$$\begin{aligned}
& d_\omega((a_i, f_n^i)[n+1], (a_i, g_n^i)[n+1]) = 0 \\
& \Rightarrow \ \mathcal{V}(aU, (a_i, f_n^i)[n+1]) = \mathcal{V}(a_iU, (a_i, f_n^i)[n+1]) \quad \forall\, a_iU \in A_{\mathrm{d}}^{n+1} \\
& \Rightarrow \sum_{\substack{u \in A_{\mathrm{d}}^{n+1} \\ \&\, a_iU \leq u}} \mathcal{V}(u, (a_i, f_n^i)[n+1]) = \sum_{\substack{u \in A_{\mathrm{d}}^{n+1} \\ \&\, a_iU \leq u}} \mathcal{V}(u, (a_i, g_n^i)[n+1]) \quad \forall\, a_iU \in A_{\mathrm{d}}^{n+1} \\
& \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{by Definition 6.4.5} \\
& \Rightarrow \ \mathsf{D}(E)(\xi(a_iU)) = \mathsf{D}(F)(\xi(a_iU)) \quad \forall\, a_iU \in A_{\mathrm{d}}^{n+1} \quad \text{by Lemma 6.4.24}
\end{aligned}$$

and since this was for any $n \in \mathbb{N}$ and $1 \leq i \leq m$ we have:

$$\mathsf{D}(E)(\xi(a_iU)) = \mathsf{D}(F)(\xi(a_iU)) \quad \forall\, a_iU \in A_{\mathrm{d}}^* \text{ and } 1 \leq i \leq m.$$

Now considering any $u \in A_{\mathrm{d}}^*$ not of the form a_iU for some $1 \leq i \leq m$, then either $u = \langle\rangle$, and hence $\mathsf{D}(E)(\xi(u)) = \mathsf{D}(F)(\xi(u)) = 1$ by definition of D since $\xi(u) = \bot$, or u is of the form aU where $a \notin \{a_1, \ldots, a_m\}$. In the latter case, we have $\mathsf{D}(E)(\xi(u)) = \mathsf{D}(F)(\xi(u)) = 0$ by definition of ξ, D and using (6.9). Putting the above together we have:

$$\begin{aligned}
\mathsf{D}(E)(\xi(u)) = \mathsf{D}(F)(\xi(u)) \ \ \forall u \in A_{\mathrm{d}}^* \ &\Rightarrow \ \mathsf{D}(E)(t) = \mathsf{D}(t) \ \ \forall t \in \mathsf{T}^{\mathrm{d}} && \text{by Lemma 6.4.23} \\
&\Rightarrow \ \mathcal{O}[\![E]\!] \overset{\mathsf{d}}{\sim} \mathcal{O}[\![F]\!] && \text{by definition}
\end{aligned}$$

as required.

The reverse direction follows a similar argument to the proof of Theorem 6.2.26 using the definition of the Hausdorff distance and Lemma 6.4.24. □

6.5 A Metric for Non-deterministic Probabilistic Processes

Similarly to the deterministic case, to add internal choice it is necessary to use sets of elements of P. We proceed with the construction involving sets of P to give a denotational semantics for non-deterministic probabilistic processes, as an alternative to deterministic probabilistic processes, by introducing finite non-deterministic probabilistic processes as follows. We note that certain proofs below follow similar arguments to the relevant proofs for P and D, and we therefore omit these.

Definition 6.5.1 (Finite non-deterministic probabilistic processes) *Let N_n, $n \in \mathbb{N}$, be a collection of carrier sets defined inductively by*

$$N_0 = \{\{p_0\}\} \ \ and \ \ N_{n+1} = \mathcal{P}_{fn}\Big(\{p_0\} \cup (A \times \mu(N_n))\Big)$$

where A is a set of actions. Furthermore, let $N_\omega = \cup_n N_n$ denote non-deterministic probabilistic processes of bounded depth.

The difference between the above definition and the corresponding definition for the deterministic case results from the fact that non-deterministic probabilistic processes are able to perform two distinct transitions of the same action type, whereas deterministic probabilistic processes cannot. For this reason, we remove the reactiveness condition from the powerset operator to allow transitions of this type to occur. A further change is in where p_0 (the inactive process) appears in the two definitions. This difference again arises from the difference between external and internal choice, since in the process calculus RP we have the following absorption law $E \,\Box\, \mathbf{0} \equiv E$, whereas $E \sqcap \mathbf{0} \not\equiv \mathbf{0}$; the result of this is that when we model non-deterministic probabilistic processes, we must allow processes of the form $\{(a, f), p_0\}$, whereas, when considering deterministic probabilistic processes, $\{(a, f), p_0\}$ can be represented as $\{(a, f)\}$.

Following the construction of P, the next step is to introduce the set of "trees" which processes can perform and then define a map $\mathcal{V}$ which calculates the probability of processes performing these trees. Following this we will then define a pseudo-metric over processes using the map $\mathcal{V}$. However, as we are considering processes which exhibit non-deterministic behaviour, we are unable to calculate the *exact* probability of processes performing trees. This is similar to our construction of the ordering $\sqsubseteq^{nd}$ over non-deterministic probabilistic transition systems. To overcome this, instead of the map $\mathcal{V}$ taking values in $[0, 1]$, we will let $\mathcal{V}$ take values in the set of closed intervals (subsets) of $[0, 1]$, that is, the set $\mathcal{I}$ (see Definition 3.3.11), and use our metric $d_{\mathcal{I}}$ on

$\mathcal{I}$ (see Definition 3.3.13) to formulate a pseudo-metric over finite non-deterministic probabilistic processes. Recall that for any $[a,b],[c,d] \in \mathcal{I}$:

$$d_{\mathcal{I}}([a,b],[c,d]) = \max\{|a-c|, |b-d|\}.$$

Intuitively, for any process and tree, the probability of the process performing the tree will always lie inside the interval given by the map $\mathcal{V}$.

As the above will lead to a more complex model than in the cases for P and D, instead of considering closed trees, we will only work with the set of open trees, by removing $\langle\rangle$ from the definition below. This is to simplify the formalism.

Definition 6.5.2 *Let A^n_{nd}, $n \in \mathbb{N}$, be the sets inductively defined as follows. Put:*

$$A^0_{\mathrm{nd}} = A \;\; \textit{and} \;\; A^{n+1}_{\mathrm{nd}} = (A \times \mathcal{P}_{fnr}(A^n_{\mathrm{nd}})) \cup A.$$

Furthermore, let $A^*_{\mathrm{nd}} = \cup_n A^n_{\mathrm{nd}}$.

As described above, we now introduce the map $\mathcal{V}$ from the set of trees A^*_{nd} and N_ω to $\mathcal{I}$, where summation, multiplication and union take the meaning given in Definition 3.3.11.

Definition 6.5.3 *Let $\mathcal{V} : (A^*_{\mathrm{nd}} \times N_\omega) \to \mathcal{I}$ be the mapping defined inductively on A^n_{nd} as follows. For all $p \in N^s_\omega$, $a \in A$ and $V \in \mathcal{P}_{fnr}(A^n_{\mathrm{nd}})$ put:*

$$\mathcal{V}(a,p) \;\; = \;\; \begin{cases} [1,1] & \textit{if } p = (a,f) \textit{ for some } f \in \mu(N_\omega) \\ [0,0] & \textit{otherwise.} \end{cases}$$

and

$$\mathcal{V}(aV,p) \;\; = \;\; \begin{cases} \sum_{Y \in N_\omega} f(Y) \cdot \mathcal{V}(V,Y) & \textit{if } p = (a,f) \textit{ for some } f \in \mu(N_\omega) \\ [0,0] & \textit{otherwise} \end{cases}$$

where for all $X \in N_\omega$ put:

$$\mathcal{V}(V,X) = \prod_{v \in V} \mathcal{V}(v,X) \;\; \textit{and} \;\; \mathcal{V}(aV,X) = \bigsqcup_{p \in X} \mathcal{V}(aV,p).$$

We now introduce an important lemma concerning the above definition.

Lemma 6.5.4 *For all $X \in N_\omega$ and $v \in A^*_{\mathrm{nd}}$: $\mathcal{V}(v,X) \subseteq [0,1]$.*

Proof. The proof is by induction on $v \in A^n_{\mathrm{nd}}$. If $n = 0$ then $v = a$ and the lemma holds by definition of $\mathcal{V}$.

Now suppose the lemma holds for $n \in \mathbb{N}$ and consider any $X \in N_\omega$ and $V \in \mathcal{P}_{fnr}(A^n_{\mathrm{nd}})$, then by definition of $\mathcal{V}$ and induction:

$$\mathcal{V}(V,X) = \prod_{v \in V} \mathcal{V}(v,X) \subseteq \prod_{v \in V} [0,1] = [0,1]. \tag{6.10}$$

Next consider any $p \in N^s_\omega$ and $v \in A^{n+1}_{\mathrm{nd}} \setminus A^n_{\mathrm{nd}}$, then $v = aV$ for some $a \in A$ and $V \in \mathcal{P}_{fnr}(A^n_{\mathrm{nd}})$ and either $p \neq (a,f)$ for all $f \in \mu(N_\omega)$, or there exists $f \in \mu(N_\omega)$ such that $p = (a,f)$. In the first case by definition of $\mathcal{V}$, $\mathcal{V}(aV,p) = [0,0]$, whereas in the second case:

$$\begin{aligned}
\mathcal{V}(aV,p) &= \sum_{Y \in N_\omega} f(Y) \cdot \mathcal{V}(V,Y) && \text{by definition of } \mathcal{V} \\
&\subseteq \sum_{Y \in N_\omega} f(Y) \cdot [0,1] && \text{by (6.10)} \\
&\subseteq \left[\sum_{Y \in N_\omega} f(Y) \cdot 0, \sum_{Y \in N_\omega} f(Y) \cdot 1\right] && \text{by Definition 3.3.11} \\
&= [0,1] && \text{since } f \in \mu(N_\omega).
\end{aligned}$$

Finally, for any $X \in N_\omega$, by definition of $\mathcal{V}$:

$$\begin{aligned}
\mathcal{V}(v,X) &= \bigsqcup_{p \in X} \mathcal{V}(v,p) \\
&\subseteq \bigsqcup_{p \in X} [0,1] && \text{from above} \\
&= [0,1] && \text{by Definition 3.3.11}
\end{aligned}$$

as required. □

We are now ready to introduce our pseudo-metric over non-deterministic probabilistic processes. As in the previous models, the intuitive understanding behind the pseudo-metric is that the distance between any processes X and Y should correspond to the differences or similarities between X and Y. Using the map $\mathcal{V}$ and the metric $d_{\mathcal{I}}$, a candidate value corresponding to the difference in the probabilities of X and Y performing the tree v, is the value of $d_{\mathcal{I}}(\mathcal{V}(v,X), \mathcal{V}(v,Y))$. In previous models, we then took the sum over all trees, that is, in this case over all $v \in A^*_{\mathrm{nd}}$, giving:

$$d'(X,Y) = \sum_{v \in A^*_{\mathrm{nd}}} d_{\mathcal{I}}(\mathcal{V}(v,X), \mathcal{V}(v,Y))$$

as our candidate for a pseudo-metric over non-deterministic probabilistic processes. This was a suitable definition in the cases before, as the sum over all trees of the probability of trees being performed was 1. However, due to the difference between non-deterministic probabilistic processes and the processes considered so far, this result will not hold in this case and, in fact, the value of $d'(X,Y)$ above will be unbounded (even if we were to replace A^*_{nd} by a set of closed trees, that is, introduce $\langle\rangle$ into the definition of A^*_{nd}). To prevent our pseudo-metric from being unbounded, we calculate the *maximum* difference in the probabilities of processes performing trees. Formally, we define the following pseudo-metric over non-deterministic probabilistic processes.

Proposition 6.5.5 *N_ω (and N_n for any $n \in \mathbb{N}$) is a pseudo-metric space with respect to the pseudo-metric:*

$$d_{\mathcal{V}}(X,Y) = \max_{v \in A^*_{\mathrm{nd}}} d_{\mathcal{I}}(\mathcal{V}(v,X), \mathcal{V}(v,Y)).$$

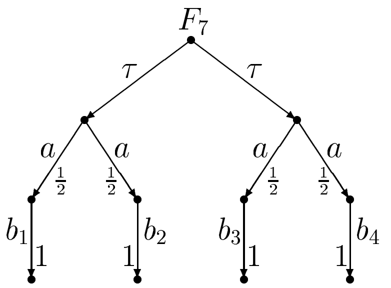
Furthermore, $0 \leq d_{\mathcal{V}}(X,Y) \leq 1$ for all $X, Y \in N_\omega$.

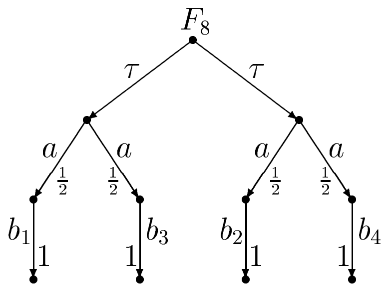
Proof. (M1$'$) For all $X, Y \in N_\omega$ $d_{\mathcal{V}}(X,Y) \geq 0$ and $d_{\mathcal{V}}(X,X) = 0$ follows by definition of $d_{\mathcal{V}}$ and since $d_{\mathcal{I}}$ is a metric on $\mathcal{I}$.
(M2) For all $X, Y \in N_\omega$ the expressions $d_{\mathcal{V}}(X,Y)$ and $d_{\mathcal{V}}(Y,X)$ are equal by definition of $d_{\mathcal{V}}$ and since $d_{\mathcal{I}}$ is a metric on $\mathcal{I}$.
(M3) Consider any X, Y and $Z \in N_\omega$, and $v \in A^*_{\mathrm{nd}}$, then since $d_{\mathcal{I}}$ is a metric (see Proposition 3.3.14) we get:

$$\begin{aligned} d_{\mathcal{I}}(\mathcal{V}(v,X), \mathcal{V}(v,Z)) &\leq d_{\mathcal{I}}(\mathcal{V}(v,X), \mathcal{V}(v,Y)) + d_{\mathcal{I}}(\mathcal{V}(v,Y), \mathcal{V}(v,Z)) \\ &\leq \max_{v \in A^*_{\mathrm{nd}}} d_{\mathcal{I}}(\mathcal{V}(v,X), \mathcal{V}(v,Y)) + \max_{v \in A^*_{\mathrm{nd}}} d_{\mathcal{I}}(\mathcal{V}(v,Y), \mathcal{V}(v,Z)) \\ &= d_{\mathcal{V}}(X,Y) + d_{\mathcal{V}}(Y,Z) \quad \text{by definition of } d_{\mathcal{V}}. \end{aligned}$$

Since $v \in A^*_{\mathrm{nd}}$ was arbitrary, we have $d_{\mathcal{V}}(X,Z) \leq d_{\mathcal{V}}(X,Y) + d_{\mathcal{V}}(Y,Z)$ by taking the maximum over all $v \in A^*_{\mathrm{nd}}$ as required.
To show that $d_{\mathcal{V}}$ is only a pseudo-metric we can use the processes in Figure 6.4 given in the proof of Proposition 6.1.16.
Finally, $0 \leq d_{\mathcal{V}}(X,Y) \leq 1$ for all $X, Y \in N_\omega$ follows by (M1$'$), Lemma 6.5.4 and the property of the metric $d_{\mathcal{I}}$ given by Lemma 3.3.15. □

If we were to follow our construction of the pseudo-metric over D_ω, we would instead construct the pseudo-metric $d_{\mathcal{V}}$ over the singleton elements of N_ω, that is, over $\{p_0\} \cup (A \times \mu(N_\omega))$, and then employ the Hausdorff distance of this pseudo-metric over N_ω. However, if we took this approach we would have defined a pseudo-metric with respect to which processes with equivalent operational behaviour have a non-zero distance. To illustrate this we return to the processes in Figure 4.9, namely:





Then, as discussed earlier, these processes have equivalent observable behaviour. If we consider their denotations in N_ω, then F_7 and F_8 will be represented by the sets: $\{(a, f_{1,2}), (a, f_{3,4})\}$ and $\{(a, f_{1,3}), (a, f_{2,4})\}$ respectively, where for any $Y \in N_\omega$:

$$f_{i,j}(Y) = \begin{cases} \frac{1}{2} & \text{if } Y = \{(b_k, \eta_{\{p_0\}})\} \text{ and } k \in \{i, j\} \\ 0 & \text{otherwise.} \end{cases}$$

Then by simple calculations we have $d_{\mathcal{V}}((a, f_{i,j}), (a, f_{k,l})) \neq 0$ for any $\{i, j\} \neq \{k, l\}$, and hence by definition of the Hausdorff distance, the distance between the denotations of F_7 and F_8 will be non-zero.

We now investigate the properties of the pseudo-metric $d_{\mathcal{V}}$. Firstly, we need to check that the properties of our pseudo-metric defined for simple probabilistic processes still hold. We therefore return to the example which distinguishes between our pseudo-metric and the classical ultra-metric construction given in Figure 6.2. Calculating the non-zero values of $\mathcal{V}$ for p'_n and $v \in A^*_{\mathrm{nd}}$ we have:

v	a'	$a'a$	$a'ab$	$a'ac$
$\mathcal{V}(v, p'_n)$	$[1, 1]$	$[1, 1]$	$[1 - 2^{-n}, 1 - 2^{-n}]$	$[2^{-n}, 2^{-n}]$

and by definition of $d_{\mathcal{V}}$ we have $d_{\mathcal{V}}(p'_n, p'_m) = |2^{-n} - 2^{-m}|$ for any $m, n \in \mathbb{N}$, and hence the pseudo-metric $d_{\mathcal{V}}$ keeps the properties of $d_{\mathcal{S}}$ while at the same time extending it to non-deterministic probabilistic processes.

Similarly to the earlier construction, to model recursive processes we introduce the definition of truncations which corresponds to the definition for D. Moreover, as before, the following proposition holds.

Proposition 6.5.6 *For all $X, Y \in N_\omega$ and $k, m \in \mathbb{N}$:*

- (a) *if $X \in N_m$, then $X[k] \in N_k$ when $k < m$ and $X[k] = X$ otherwise.*
- (b) $(X[m])[k] = X[\min\{m, k\}]$.
- (c) *$X[m] = Y[m]$ if and only if $X[k] = Y[k]$ for all $k \leq m$.*
- (d) $d_{\mathcal{V}}(X[k], Y[k]) \leq d_{\mathcal{V}}(X, Y)$.

The proofs follow similarly to the case concerning simple probabilistic processes and using the following lemma to prove part (d).

Lemma 6.5.7 *For all $X \in N_\omega$, $v \in A^*_{\text{nd}}$ and $k \in \mathbb{N}$: $\mathcal{V}(v, X[0]) = [0,0]$ and*

$$\mathcal{V}(v, X[k+1]) = \begin{cases} \mathcal{V}(v, X) & \textit{if } v \in A^k_{\text{nd}} \\ [0,0] & \textit{otherwise.} \end{cases}$$

Proof. The first part of the lemma follows by definition of $\mathcal{V}$ and since $X[0] = \{p_0\}$ for all $X \in N_\omega$.

We now prove the second part of the lemma by induction on $k \in \mathbb{N}$. Firstly consider any $p \in N^s_\omega$ and $v \in A^0_{\text{nd}}$. Then $v = a$ for some $a \in A$ and by definition of $\mathcal{V}$:

$$\begin{aligned}
\mathcal{V}(a,p) &= \begin{cases} [1,1] & \text{if } (a,f) \in p \text{ for some } f \in \mu(N_\omega) \\ [0,0] & \text{otherwise} \end{cases} \\
&= \begin{cases} [1,1] & \text{if } (a,f[0]) \in p[1] \text{ for some } f \in \mu(N_\omega) \\ [0,0] & \text{otherwise} \end{cases} && \text{by Definition 6.1.11} \\
&= \mathcal{V}(a, p[1]) && \text{by definition of } \mathcal{V}
\end{aligned}$$

and therefore, by definition of truncations and $\mathcal{V}$ for any $X \in N_\omega$:

$$\begin{aligned}
\mathcal{V}(a,X) &= \bigsqcup_{p \in X} \mathcal{V}(a,p) \\
&= \bigsqcup_{p \in X} \mathcal{V}(a,p[1]) && \text{from above} \\
&= \mathcal{V}(a, X[1]) && \text{by definition of truncations and } \mathcal{V}.
\end{aligned}$$

On the other hand, if $v \notin A^0_{\text{nd}}$, then $v = aV$ for some $a \in A$ and $V \in \mathcal{P}_{fnr}(A^*_{\text{nd}})$ and in this case:

$$\begin{aligned}
\mathcal{V}(aV, p[1]) &= \begin{cases} \sum_{Y \in \mathsf{s}(f[0])} f[0](Y) \cdot \mathcal{V}(V,Y) & \text{if } (a,f[0]) \in p[1] \text{ for some } f \in \mu(N_\omega) \\ [0,0] & \text{otherwise} \end{cases} \\
&= \begin{cases} 1 \cdot \mathcal{V}(V,p_0) & \text{if } (a,f[0]) \in p[1] \text{ for some } f \in \mu(N_\omega) \\ [0,0] & \text{otherwise} \end{cases} \\
& \qquad \text{by Proposition 6.5.6}(a) \\
&= \begin{cases} 1 \cdot [0,0] & \text{if } (a,f[0]) \in p[1] \text{ for some } f \in \mu(N_\omega) \\ [0,0] & \text{otherwise} \end{cases} \\
& \qquad \text{by the first part of the lemma} \\
&= [0,0].
\end{aligned}$$

Then, similarly to the first case and using the above, for any $X \in N_\omega$ we have:

$$\begin{aligned}\mathcal{V}(v, X[1]) &= \bigsqcup_{p \in X} [0,0] \\ &= [0,0] \qquad \text{by Definition 3.3.11}\end{aligned}$$

and since this was for any $X \in N_\omega$ hence the lemma holds for $n = 0$.

Now suppose the lemma holds for any $k \in \mathbb{N}$ and consider any $V \in \mathcal{P}_{fnr}(A^*_{\text{nd}})$, if $V \in \mathcal{P}_{fnr}(A^k_{\text{nd}})$:

$$\begin{aligned}\mathcal{V}(V, X[k+1]) &= \prod_{v \in V} \mathcal{V}(v, X[k+1]) \\ &= \prod_{v \in V} \mathcal{V}(v, X) && \text{by induction} \\ &= \mathcal{V}(V, X) && \text{by definition of } \mathcal{V}.\end{aligned}$$

On the other hand, if $V \notin \mathcal{P}_{fnr}(A^k_{\text{nd}})$ then there exists $\tilde{v} \in V$ such that $\tilde{v} \notin A^k_{\text{nd}}$, and in this case:

$$\begin{aligned}\mathcal{V}(V, X[k+1]) &= \prod_{v \in V} \mathcal{V}(v, X[k+1]) \\ &= \mathcal{V}(\tilde{v}, X[k+1]) \cdot \left(\prod_{v \in V \setminus \{\tilde{v}\}} \mathcal{V}(v, X[k+1]) \right) && \text{rearranging} \\ &= [0,0] \cdot \left(\prod_{v \in V \setminus \{\tilde{v}\}} \mathcal{V}(v, X[k+1]) \right) && \text{by induction} \\ &= [0,0] && \text{by Definition 3.3.11.}\end{aligned}$$

Next, consider any $v \in A^*_{\text{nd}}$. Then if $v = a$ for some $a \in \mathcal{A}ct$ the proof follows similarly to the case when $k = 0$. On the other hand, if $v = aV$ for some $a \in A$ and $V \in \mathcal{P}_{fnr}(A^*_{\text{nd}})$, then for any $p \in X$, either $p \neq (a, f)$ for any $f \in \mu(N_\omega)$, and hence by definition of $\mathcal{V}$: $\mathcal{V}(aV, p[k+2]) = \mathcal{V}(aV, p) = [0,0]$, or $p = (a, f)$ for some $f \in \mu(N_\omega)$, and in this case since $p[k+2] = (a, f[k+1])$ we obtain:

$$\mathcal{V}(aV, p[k+2]) = \sum_{Y \in \mathsf{s}(f[k+1])} f(Y) \cdot \mathcal{V}(aV, Y)$$

$$= \sum_{Y \in \mathsf{s}(f)} f(Y) \cdot \mathcal{V}(aV, Y[k+1]) \qquad \text{by definition of truncations}$$

$$= \begin{cases} \sum_{Y \in \mathsf{s}(f)} f(Y) \cdot \mathcal{V}(V, Y) & \text{if } V \in \mathcal{P}_{fnr}(A^k_{\text{nd}}) \\ \sum_{Y \in \mathsf{s}(f)} f(Y) \cdot [0,0] & \text{otherwise} \end{cases} \qquad \text{from above}$$

$$= \begin{cases} \sum_{Y \in \mathsf{s}(f)} f(Y) \cdot \mathcal{V}(V, Y) & \text{if } V \in \mathcal{P}_{fnr}(A^k_{\text{nd}}) \\ [0,0] & \text{otherwise} \end{cases} \qquad \text{rearranging}$$

$$= \begin{cases} \mathcal{V}(aV, p) & \text{if } aV \in A^{k+1}_{\text{nd}} \\ [0,0] & \text{otherwise} \end{cases} \qquad \text{by definition of } A^{k+1}_{\text{nd}}.$$

Using the above the remainder of the proof follows similarly to the case for $k = 0$. $\square$

The above lemma also leads to the following connection between truncations and our pseudo-metric $d_{\mathcal{V}}$.

Proposition 6.5.8 *For all $X, Y \in N_\omega$ and $k \in \mathbb{N}$:*

$$d_{\mathcal{V}}(X[k+1], Y[k+1]) = \max_{v \in A^k_{\text{nd}}} d_{\mathcal{I}}(\mathcal{V}(v, X), \mathcal{V}(v, Y)).$$

Proof. Consider any $X, Y \in N_\omega$ and $v \in A^*_{\text{nd}}$. By Lemma 6.5.7:

$$\begin{aligned} & d_{\mathcal{I}}(\mathcal{V}(v, X[k+1]), \mathcal{V}(v, Y[k+1])) \\ &\quad = \begin{cases} d_{\mathcal{I}}(\mathcal{V}(v, X), \mathcal{V}(v, Y)) & \text{if } v \in A^k_{\text{nd}} \\ d_{\mathcal{I}}([0,0],[0,0]) & \text{otherwise} \end{cases} \\ &\quad = \begin{cases} d_{\mathcal{I}}(\mathcal{V}(v, X), \mathcal{V}(v, Y)) & \text{if } v \in A^k_{\text{nd}} \\ 0 & \text{otherwise} \end{cases} \qquad \text{by Definition 3.3.13.} \end{aligned} \tag{6.11}$$

Therefore, $d_{\mathcal{V}}(X[k+1], Y[k+1])$ equals:

$$\begin{aligned} &= \max_{v \in A^*_{\text{nd}}} d_{\mathcal{I}}(\mathcal{V}(v, X[k+1]), \mathcal{V}(v, Y[k+1])) && \text{by definition of } d_{\mathcal{V}} \\ &= \max\left\{ \max_{v \in A^k_{\text{nd}}} d_{\mathcal{I}}(\mathcal{V}(v, X), \mathcal{V}(v, Y)),\ 0 \right\} && \text{by (6.11)} \\ &= \max_{v \in A^k_{\text{nd}}} d_{\mathcal{I}}(\mathcal{V}(v, X), \mathcal{V}(v, Y)) && \text{by Lemma 3.3.15} \end{aligned}$$

as required. $\square$

As in the case of our pseudo-metric for simple probabilistic processes P, we combine both the pseudo-metric $d_{\mathcal{V}}$ and truncations to formulate a pseudo-metric for non-deterministic processes.

Definition 6.5.9 *For all $X, Y \in N_\omega$, we define $d_\omega : N_\omega \times N_\omega \longrightarrow [0, 1]$ as follows:*

$$d_\omega(X, Y) = \sum_{k=1}^{\infty} 2^{-k} d_{\mathcal{V}}(X[k], Y[k]).$$

Proposition 6.5.10 *(N_ω, d_ω) (and (N_n, d_ω) for any $n \in \mathbb{N}$) is a pseudo-metric space. Furthermore, $0 \leq d_\omega(X, Y) \leq 1$ for all $X, Y \in N_\omega$.*

We now continue applying the standard completion techniques (see Theorem 3.3.7), to construct the metric space of non-deterministic probabilistic processes.

Definition 6.5.11 *Let (N, d) be the completion of (N_ω, d_ω).*

Before we give denotation semantics to $\mathrm{RP}_{\mathrm{nd}}$, we introduce the following lemmas.

Lemma 6.5.12 *For all $X \in N_\omega$, $\langle X[n] \rangle_n$ is a Cauchy sequence.*

Lemma 6.5.13 *If $\langle X_n \rangle_{n \in \mathbb{N}}$ is a sequence in N_ω such that $X_{n+1}[n] = X_n[n]$ for all $n \in \mathbb{N}$, then $\langle X_n \rangle_{n \in \mathbb{N}}$ is Cauchy and $X_m[n] = X_n[n]$ for all $m \geq n \in \mathbb{N}$. Furthermore, if $\langle q_n \rangle_{n \in \mathbb{N}}$ is a sequence in N_ω such that $Y_{n+1}[n] = Y_n[n]$ for all $n \in \mathbb{N}$ and $\langle X_n \rangle_{n \in \mathbb{N}} \sim \langle Y_n \rangle_{n \in \mathbb{N}}$, then $d_\omega(X_n[n], Y_n[n]) = 0$ for all $n \in \mathbb{N}$.*

Lemma 6.5.14 *If $\langle X_n \rangle_{n \in \mathbb{N}}$ and $\langle Y_n \rangle_{n \in \mathbb{N}}$ are Cauchy sequence and $\langle X_n \rangle_{n \in \mathbb{N}} \not\sim \langle Y_n \rangle_{n \in \mathbb{N}}$, then there exists $n \in \mathbb{N}$ such that $X_n[n] \neq Y_n[n]$.*

6.6 Denotational Semantics for $\mathrm{RP}_{\mathrm{nd}}$

As for the cases concerning P and D, we now introduce the semantic operators on N. We first introduce the semantic operator for internal choice.

Definition 6.6.1 (Internal Choice Operator) *For any $X, Y \in N_\omega$, let $X \cup Y$ be set theoretic union.*

Lemma 6.6.2 *For all $X, Y \in N_\omega$ and $k \in \mathbb{N}$: $(X \cup Y)[k] = X[k] \cup Y[k]$.*

Proposition 6.6.3 *$\cup$ is continuous and well-defined on (N_ω, d_ω).*

Proof. Consider any $X, Y, Z \in N_\omega$, $v \in A^*_{\mathrm{nd}}$ and $k \in \mathbb{N}$. Then Lemma 6.6.2 entails:

$$\begin{array}{lll} & d_{\mathcal{I}}(\mathcal{V}(v, (X \cup Z)[k]), \mathcal{V}(v, (Y \cup Z)[k])) & \\ = & d_{\mathcal{I}}(\mathcal{V}(v, X[k] \cup Z[k]), \mathcal{V}(v, Y[k] \cup Z[k])) & \\ = & d_{\mathcal{I}}(\mathcal{V}(v, X[k]) \sqcup \mathcal{V}(v, Z[k]), \mathcal{V}(v, Y[k]) \sqcup \mathcal{V}(v, Z[k])) & \text{by definition of } \mathcal{V} \\ \leq & d_{\mathcal{I}}(\mathcal{V}(v, X[k]), \mathcal{V}(v, Y[k])) & \text{by Proposition 3.3.16}(ii) \\ \leq & \max_{v \in A^*_{\mathrm{nd}}} d_{\mathcal{I}}(\mathcal{V}(v, X[k]), \mathcal{V}(v, Y[k])) & \\ = & d_{\mathcal{V}}(X, Y) & \text{by definition.} \end{array}$$

Since this was for arbitrary $v \in A^*_{\mathrm{nd}}$:

$$d_{\mathcal{V}}((X \cup Z)[k], (Y \cup Z)[k]) \leq d_{\mathcal{V}}(X[k], Y[k])$$

follows by definition of $d_{\mathcal{V}}$. Furthermore, since this was for any $k \in \mathbb{N}$, we have: $d_\omega(X \cup Z, Y \cup Z) \leq d_\omega(X, Y)$ by definition of d. The rest of the lemma follows similarly to the deterministic case. $\square$

For the remaining semantic operators have definitions equivalent to the deterministic case with $\oplus$ replaced by $\cup$. We now turn our attention to the semantic operator for synchronous parallel. To show this operator is well-defined and continuous we first require the following lemmas.

Lemma 6.6.4 *For all* $X, Y \in N_\omega$ *and* $v \in A^*_{\mathrm{nd}}$: $\mathcal{V}(v, X \parallel Y) = \mathcal{V}(v, X) \cdot \mathcal{V}(v, Y)$.

Proof. The proof is by induction on $v \in A^n_{\mathrm{nd}}$. If $v \in A^0_{\mathrm{nd}}$ then $v = a$ for some $a \in \mathcal{A}ct$ and the lemma follows by definition of $\mathcal{V}$ and the semantic operator $\parallel$.

Now suppose the lemma holds for any $n \in \mathbb{N}$ and consider any $X, Y \in N_\omega$ and $V \in \mathcal{P}_{fnr}(A^n_{\mathrm{nd}})$, then by definition of $\mathcal{V}$:

$$\begin{array}{rcll} \mathcal{V}(V, X \parallel Y) & = & \prod_{v \in V} \mathcal{V}(v, X \parallel Y) & \\ & = & \prod_{v \in V} (\mathcal{V}(v, X) \cdot \mathcal{V}(v, Y)) & \text{by induction} \\ & = & \left(\prod_{v \in V} \mathcal{V}(v, X)\right) \cdot \left(\prod_{v \in V} \mathcal{V}(v, X)\right) & \text{rearranging} \\ & = & \mathcal{V}(V, X) \cdot \mathcal{V}(V, Y) & \text{by definition of } \mathcal{V}. \end{array}$$

Next consider any $p, q \in N^s_\omega$ and $v \in A^{n+1}_{\mathrm{nd}} \setminus A^n_{\mathrm{nd}}$, then $v = aV$ for some $a \in A$. Now if $p \parallel q = (a, h)$ for some $h \in \mu(N_\omega)$, then $h = f \parallel g$ where $p = (a, f)$ and $q = (a, g)$, in which case:

$$\begin{array}{rcll}
\mathcal{V}(aV, p \,\|\, q) & = & \sum_{Z \in N_\omega} (f \,\|\, g)(Z) \cdot \mathcal{V}(V, Z) & \\
& = & \sum_{X \,\|\, Y \in N_\omega} \Big(f(X) \cdot g(Y)\Big) \cdot \mathcal{V}(V, X \,\|\, Y) & \text{by definition of } \| \\
& = & \sum_{X \,\|\, Y \in N_\omega} \Big(f(X) \cdot g(Y)\Big) \cdot \Big(\mathcal{V}(V, X) \cdot \mathcal{V}(V, Y)\Big) & \text{by induction} \\
& = & \left(\sum_{X \in N_\omega} f(X) \cdot \mathcal{V}(V, X)\right) \cdot \left(\sum_{Y \in N_\omega} g(Y) \cdot \mathcal{V}(V, Y)\right) & \text{rearranging} \\
& = & \mathcal{V}(aV, p) \cdot \mathcal{V}(aV, q) & \text{by definition of } \mathcal{V}.
\end{array}$$

On the other hand, if $p \,\|\, q \neq (a, f)$ for any $f \in \mu(N_\omega)$, without loss of generality we can suppose $p \neq (a, f)$ for any $f \in \mu(N_\omega)$. By definition of $\mathcal{V}$ we therefore obtain:

$$\mathcal{V}(aV, p \,\|\, q) = [0, 0] = [0, 0] \cdot \mathcal{V}(aV, q) = \mathcal{V}(aV, p) \cdot \mathcal{V}(aV, q).$$

Finally for any $X, Y \in N_\omega$ and $v \in A_{\mathrm{nd}}^{n+1}$:

$$\begin{array}{rcll}
\mathcal{V}(v, X \,\|\, Y) & = & \sqcup\{\mathcal{V}(v, r) \mid r \in X \,\|\, Y\} & \text{by definition of } \mathcal{V} \\
& = & \sqcup\{\mathcal{V}(v, p \,\|\, q) \mid p \in X \;\&\; q \in Y\} & \text{by definition of } \| \\
& = & \sqcup\{\mathcal{V}(v, p) \cdot \mathcal{V}(v, q) \mid p \in X \;\&\; q \in Y\} & \text{from above} \\
& = & \Big(\sqcup_{p \in X} \mathcal{V}(v, p)\Big) \cdot \Big(\sqcup_{q \in Y} \mathcal{V}(v, q)\Big) & \text{rearranging} \\
& = & \mathcal{V}(v, X) \cdot \mathcal{V}(v, Y) & \text{by definition of } \mathcal{V}.
\end{array}$$

Hence, we have proved the lemma by induction on $v \in A_{\mathrm{nd}}^n$. □

Lemma 6.6.5 *For all* $X, Y \in N_\omega$ *and* $k \in \mathbb{N}$: $(X \,\|\, Y)[k] = X[k] \,\|\, Y[k]$.

Proposition 6.6.6 $\|$ *is continuous and well-defined on* (N_ω, d_ω).

Proof. Consider any X, Y and $Z \in N_\omega$, $k \in \mathbb{N}$ and $v \in A_{\mathrm{nd}}^*$. By Lemma 6.6.5:

$$\begin{array}{cll}
\multicolumn{3}{l}{d_{\mathcal{I}}(\mathcal{V}(v, (X \,\|\, Z)[k]), \mathcal{V}(v, (Y \,\|\, Z)[k]))} \\
= & d_{\mathcal{I}}(\mathcal{V}(v, X[k] \,\|\, Z[k]), \mathcal{V}(v, Y[k] \,\|\, Z[k])) & \\
= & d_{\mathcal{I}}(\mathcal{V}(v, X[k]) \cdot \mathcal{V}(v, Z[k]), \mathcal{V}(v, Y[k]) \cdot \mathcal{V}(v, Z[k])) & \text{by Lemma 6.6.4} \\
\leq & d_{\mathcal{I}}(\mathcal{V}(v, X[k]), \mathcal{V}(v, Y[k])) & \text{by Proposition 3.3.16}(i) \\
\leq & \max_{v \in A_{\mathrm{nd}}^*} d_{\mathcal{I}}(\mathcal{V}(v, X[k]), \mathcal{V}(v, Y[k])) & \\
= & d_{\mathcal{V}}(X, Y) & \text{by definition of } d_{\mathcal{V}}
\end{array}$$

Then since this was for any $v \in A^*_{\mathrm{nd}}$ and $k \in \mathbb{N}$, similarly to proving that $\cup$ was continuous, $\|$ is continuous. The fact that $\|$ is well-defined follows similarly to Proposition 6.2.5. □

Next we consider the operator for restriction, for which we require the following lemma before we can verify that this operator is well-defined.

Lemma 6.6.7 *For all $X \in N_\omega$, $v \in A^*_{\mathrm{nd}}$ and $B \subseteq A$:*

$$\mathcal{V}(v, X \upharpoonright B) = \begin{cases} [0,0] & \text{if } a \in v \text{ for some } a \in A \setminus B \\ \mathcal{V}(v, X) & \text{otherwise.} \end{cases}$$

Moreover, for any $k \in \mathbb{N}$: $(X \upharpoonright B)[k] = X[k] \upharpoonright B$.

Proposition 6.6.8 *For all $B \subseteq A$, $\upharpoonright B$ is continuous and well-defined on (N_ω, d_ω).*

Proof. Consider any $X, Y \in N_\omega$, $v \in A^*_{\mathrm{nd}}$, $k \in \mathbb{N}$ and $B \subseteq A$. Using Lemma 6.6.7 we infer:

$$\begin{array}{lll} \multicolumn{3}{l}{d_{\mathcal{I}}(\mathcal{V}(v, (X \upharpoonright B)[k]), \mathcal{V}(v, (Y \upharpoonright B)[k]))} \\ = & d_{\mathcal{I}}(\mathcal{V}(v, X[k] \upharpoonright B), \mathcal{V}(v, Y[k] \upharpoonright B)) & \\ = & \begin{cases} d_{\mathcal{I}}(\mathcal{V}(v, X[k]), \mathcal{V}(v, Y[k])) & \text{if } a \in V \text{ for some } a \notin B \\ 0 & \text{otherwise.} \end{cases} & \text{by Lemma 6.6.7} \\ \leq & d_{\mathcal{I}}(\mathcal{V}(v, X[k]), \mathcal{V}(v, Y[k])) & \text{rearranging} \\ \leq & \max\limits_{v \in A^*_{\mathrm{nd}}} d_{\mathcal{I}}(\mathcal{V}(v, X[k]), \mathcal{V}(v, Y[k])) & \\ = & d_{\mathcal{V}}(X, Y) & \text{by definition of } d_{\mathcal{V}}. \end{array}$$

Since this was for any $V \in A^*_{\mathrm{nd}}$ and $k \in \mathbb{N}$, we have that $\upharpoonright$ is continuous as required. It follows that $\upharpoonright$ is well-defined by an argument similar to Theorem 6.2.7. □

Finally, we consider relabelling.

Lemma 6.6.9 *For all $X \in N_\omega$, $v \in A^*_{\mathrm{nd}}$, $\lambda : A \to A$ and $k \in \mathbb{N}$: $\mathcal{V}(v, X[\lambda]) = \mathcal{V}(\lambda^{-1}(v), X)$ and $(X[\lambda])[k] = (X[k])[\lambda]$.*

Proposition 6.6.10 *For all $\lambda : A \to A$, $[\lambda]$ is continuous and well-defined on (N_ω, d_ω).*

Proof. The proof follows from Lemma 6.6.9 above and a similar proof for the deterministic case. □

Using the above semantic operators we can now define denotational metric semantics for the expressions of our process calculus $\mathrm{RP_{nd}}$.

Definition 6.6.11 (Denotational Semantics) *Let $\mathcal{D}_n : \mathrm{RP_{nd}} \to (\mathrm{Env} \to N_\omega)$, $n \in \mathbb{N}$, be the collection of maps defined inductively as follows. Put $\mathcal{D}_0[\![E]\!] = \{p_0\}$ for all $E \in \mathrm{RP_{nd}}$, and $\mathcal{D}_{n+1}$ be defined inductively on the structure of elements of $\mathrm{RP_{nd}}$ as follows:*

$$\begin{array}{rcl}
\mathcal{D}_{n+1}[\![x]\!](\rho) &=& \rho_{n+1}(x)\\
\mathcal{D}_{n+1}[\![\mathbf{0}]\!](\rho) &=& \{p_0\}\\
\mathcal{D}_{n+1}[\![\sum_{i\in I} a_{\mu_i}.E_i]\!](\rho) &=& \{(a, \Phi_{N_\omega}(\langle \mu_i, \mathcal{D}_n[\![E_i]\!](\rho)\rangle_{i\in I}))\}\\
\mathcal{D}_{n+1}[\![E_1 \sqcap E_2]\!](\rho) &=& \mathcal{D}_{n+1}[\![E_1]\!](\rho) \cup \mathcal{D}_{n+1}[\![E_2]\!](\rho)\\
\mathcal{D}_{n+1}[\![E_1 \parallel E_2]\!](\rho) &=& \mathcal{D}_{n+1}[\![E_1]\!](\rho) \parallel \mathcal{D}_{n+1}[\![E_2]\!](\rho)\\
\mathcal{D}_{n+1}[\![E \upharpoonright B]\!](\rho) &=& \mathcal{D}_{n+1}[\![E]\!](\rho) \upharpoonright B\\
\mathcal{D}_{n+1}[\![E\,[\lambda]]\!](\rho) &=& \mathcal{D}_{n+1}[\![E]\!](\rho)\,[\lambda]\\
\mathcal{D}_{n+1}[\![\mathit{fix}_x.E]\!](\rho) &=& \mathcal{D}_{n+1}[\![E]\!](\rho\{\mathcal{D}_n[\![\mathit{fix}_x.E]\!](\rho)/x\}).
\end{array}$$

Furthermore, let $\mathcal{D} : \mathrm{RP_{nd}} \to (\mathrm{Env} \to N)$ be the map defined as follows, for any $E \in \mathrm{RP_{nd}}$ put: $\mathcal{D}[\![E]\!](\rho) = [\langle \mathcal{D}_n[\![E]\!](\rho)\rangle_{n\in\mathbb{N}}]_\sim$.

To prove the well-definedness of this semantic map, we first need to reach the following technical lemma, similarly to the cases before.

Lemma 6.6.12 *For all $E \in \mathcal{G}^{\mathrm{nd}}$, $\rho \in \mathrm{Env}$ and $k \in \mathbb{N}$: $\mathcal{D}_{k+1}[\![E]\!](\rho)[k] = \mathcal{D}_k[\![E]\!](\rho)[k]$.*

Lemma 6.6.13 *For any $E \in \mathrm{RP_{nd}}$, $F \in \mathrm{Pr}^{nd}$, $\rho \in Env$ and $n \in \mathbb{N}$:*

$$\mathcal{D}_n[\![E\{F/x\}]\!](\rho)[n] = \mathcal{D}_n[\![E]\!](\rho\{D_n[\![F]\!]/x\})[n].$$

Furthermore, if $E \in \mathcal{G}^{\mathrm{nd}}$ then:

$$\mathcal{D}_{n+1}[\![E\{F/x\}]\!](\rho)[n+1] = \mathcal{D}_{n+1}[\![E]\!](\rho\{D_n[\![F]\!]/x\})[n+1].$$

Proposition 6.6.14 *$\mathcal{D}$ is well-defined on the guarded expressions of $\mathrm{RP_{nd}}$.*

6.6.1 Full Abstraction

To show that the above denotational model is fully abstract with respect to our equivalence $\overset{\mathsf{nd}}{\sim}$ we first require the following lemmas and definition.

Lemma 6.6.15 *For all $E \in \mathrm{Pr}^{\mathrm{nd}}$, $\rho \in \mathrm{Env}$ and $s \in (\mathcal{A}ct \times \mu(\mathrm{Pr}^{\mathrm{nd}})) \cup \{\emptyset\}$, we have $\mathcal{O}[\![E]\!] \to s$ if and only if $p^s_{n+1} \in \mathcal{D}_{n+1}[\![E]\!](\rho)$ for all $n \in \mathbb{N}$ such that if $s = \emptyset$, then $p^s_{n+1} = p_0$, and if $s = (a, \pi)$, then $p^s_{n+1} = (a, f_n)$, where for any $Y \in P$:*

$$f_n[n](Y) = \sum_{\substack{F \in \mathrm{Pr}^{\mathrm{nd}}\, \& \\ \mathcal{D}[\![F]\!](\rho)[n] = Y}} \pi(F).$$

Definition 6.6.16 *Let* $\varphi : A^*_{\mathrm{nd}} \to \mathtt{T}^{\mathrm{nd}} \setminus \{(\!|\bot|\!)\}$ *be the following map between trees and tests defined inductively as follows:* $\varphi(a) = (\!|a.(\!|\bot|\!)|\!)$ *and* $\varphi(aV) = (\!|a.\varphi(V)|\!)$*, where* $\varphi(\{v_1, \ldots, v_m\}) = (\varphi(v_1), \ldots, \varphi(v_m))$*.*

Lemma 6.6.17 *The map* φ *is bijective.*

Lemma 6.6.18 *For all* $E \in \mathrm{Pr}^{\mathrm{nd}}$*,* $\rho \in \mathrm{Env}$*,* $v \in A^n_{\mathrm{nd}}$ *and* $n \in \mathbb{N}$*:*

$$\mathcal{V}(v, \mathcal{D}_{n+1}[\![E]\!](\rho)[n+1]) = [\mathsf{N_{glb}}(E)(\varphi(v)), \mathsf{N_{lub}}(E)(\varphi(v))].$$

Proof. The proof is by induction on $n \in \mathbb{N}$. If $v \in A^0_{\mathrm{nd}}$, then $v = a$ for some $a \in \mathbb{N}$ and by definition $\varphi(a) = (\!|a.(\!|\bot|\!)|\!)$. Considering any $s \in (\mathcal{A}ct \times \mu(\mathrm{Pr}^{nd})) \cup \{\bot\}$:

$$\mathsf{N_{lub}}(s)(a.(\!|\bot|\!)) = \mathsf{N_{glb}}(s)(a.(\!|\bot|\!)) = \begin{cases} 1 & \text{if } s = (a, \pi) \text{ for some } \pi \in \mu(\mathrm{Pr}^{nd}) \\ 0 & \text{otherwise} \end{cases} \tag{6.12}$$

by definition of $\mathsf{N_{lub}}$ and $\mathsf{N_{glb}}$. For any $s \in (\mathcal{A}ct \times \mu(\mathrm{Pr}^{nd})) \cup \{\emptyset\}$ using the notation of Lemma 6.6.15 above we have:

$$\begin{aligned}
\mathcal{V}(v, p^s_1[1]) &= \begin{cases} [1,1] & \text{if } p^1_s = (a, f_0) \text{ for some } f_0 \in \mu(N_\omega) \\ [0,0] & \text{otherwise} \end{cases} \\
&= \begin{cases} [1,1] & \text{if } s = (a, \pi) \text{ for some } \pi \in \mu(\mathrm{Pr}^{nd}) \\ [0,0] & \text{otherwise} \end{cases} && \text{by Lemma 6.6.15} \\
&= [\mathsf{N_{glb}}(s)(a.(\!|\bot|\!)), \mathsf{N_{lub}}(s)(a.(\!|\bot|\!))] && \text{by (6.12).} \qquad (6.13)
\end{aligned}$$

Then for any $E \in \mathrm{Pr}^{nd}$:

$$\begin{aligned}
\mathcal{V}(v, \mathcal{D}_1[\![E]\!][1]) &= \sqcup\{\mathcal{V}(v, p^s_1[1]) \mid \mathcal{O}[\![E]\!] \to s\} && \text{by Lemma 6.6.15} \\
&= \left[\min_{\mathcal{O}[\![E]\!]\to s} \mathcal{V}(v, p^s_1[1]), \max_{\mathcal{O}[\![E]\!]\to s} \mathcal{V}(v, p^s_1[1])\right] && \text{by Definition 3.3.11} \\
&= \left[\min_{\mathcal{O}[\![E]\!]\to s} \mathsf{N_{glb}}(s)(a.(\!|\bot|\!)), \max_{\mathcal{O}[\![E]\!]\to s} \mathsf{N_{lub}}(s)(a.(\!|\bot|\!))\right] && \text{by (6.13)} \\
&= [\mathsf{N_{glb}}(E)((\!|a.(\!|\bot|\!)|\!)), \mathsf{N_{lub}}(E)((\!|a.(\!|\bot|\!)|\!))] && \text{by definition of } \mathsf{N}_* \\
&= [\mathsf{N_{glb}}(E)(\varphi(a)), \mathsf{N_{lub}}(E)(\varphi(a))] && \text{by definition of } \varphi
\end{aligned}$$

and thus the lemma holds for $n = 0$.

Now suppose the lemma holds for some $n \in \mathbb{N}$ and consider any $V = \{v_1, \ldots, v_m\} \in \mathcal{P}_{fnr}(A^n_{\mathrm{nd}})$. Then:

$$\begin{aligned}
\mathcal{V}(V, \mathcal{D}_{n+1}[\![E]\!][n+1]) &= \prod_{i=1}^{m} \mathcal{V}(v_i, \mathcal{D}_{n+1}[\![E]\!][n+1]) && \text{by definition of } \mathcal{V} \\
&= \prod_{i=1}^{m} [\mathsf{N}_{\mathbf{glb}}(E)(\varphi(v_i)), \mathsf{N}_{\mathbf{lub}}(E)(\varphi(v_i))] && \text{by induction} \\
&= \left[\prod_{i=1}^{m} \mathsf{N}_{\mathbf{glb}}(E)(\varphi(v_i)), \prod_{i=1}^{m} \mathsf{N}_{\mathbf{lub}}(E)(\varphi(v_i))\right] && \text{by Definition 3.3.11} \\
&= [\mathsf{N}_{\mathbf{glb}}(E)(\varphi(V)), \mathsf{N}_{\mathbf{lub}}(E)(\varphi(V))] && \text{by definition of } \varphi.
\end{aligned}$$

Next consider any $v \in A^{n+1}_{\mathrm{nd}}$. Then either $v = a$ for some $a \in A$ in which case the result follows similarly to the case when $n = 0$, or $v = aV$ for some $a \in \mathcal{A}ct$ and $V \in \mathcal{P}_{fnr}(A^n_{\mathrm{nd}})$. In the second case, for any $E \in \mathrm{Pr}^{\mathrm{n}d}$ and $s \in (\mathcal{A}ct \times \mu(\mathrm{Pr}^{\mathrm{n}d})) \cup \{\emptyset\}$ such that $\mathcal{O}[\![E]\!] \to s$ we have the following two possibilities:

1. $s \neq (a, \pi)$ for any $\pi \in \mu(\mathrm{Pr}^{\mathrm{n}d})$, and hence by definition of N_*, $\mathcal{V}$, φ and Lemma 6.6.15:

$$\begin{aligned}
\mathcal{V}(aV, p^s_{n+2}[n+2]) &= [0, 0] && \text{by definition of } \mathcal{V} \\
&= [\mathsf{N}_{\mathbf{glb}}(s)(a.\varphi(V)), \mathsf{N}_{\mathbf{lub}}(s)(a.\varphi(V))] && \text{by definition of } \mathsf{N}_* \\
&= [\mathsf{N}_{\mathbf{glb}}(s)(\varphi(aV)), \mathsf{N}_{\mathbf{lub}}(s)(\varphi(aV))] && \text{by definition of } \varphi.
\end{aligned}$$

2. $s = (a, \pi)$ for some $\pi \in \mu(\mathrm{Pr}^{\mathrm{n}d})$, in which case using Lemma 6.6.15 $p^s_{n+2} =$

$(a, f_{n+1}) \in \mathcal{D}[\![E]\!]$, and therefore $\mathcal{V}(aV, p_s[n+2])$ equals:

$$
\begin{aligned}
&= \sum_{Y \in N_\omega} f_{n+1}[n+1](Y) \cdot \mathcal{V}(V, Y) && \text{by definition of } \mathcal{V} \\
&= \sum_{Y \in N_\omega} \left(\sum_{\substack{F \in \mathrm{Pr}^{nd} \& \\ \mathcal{D}[\![F]\!][n+1] = Y}} \pi(F) \right) \cdot \mathcal{V}(V, Y) && \text{by Lemma 6.6.15} \\
&= \sum_{F \in \mathrm{Pr}^{nd}} \pi(F) \cdot \mathcal{V}(V, \mathcal{D}[\![F]\!][n+1]) && \text{rearranging} \\
&= \sum_{F \in \mathrm{Pr}^{nd}} \pi(F) \cdot [\mathsf{N}_{\mathbf{glb}}(F)(\varphi(V)), \mathsf{N}_{\mathbf{lub}}(F)(\varphi(V))] && \text{from above} \\
&= \left[\sum_{F \in \mathrm{Pr}^{nd}} \pi(F) \cdot \mathsf{N}_{\mathbf{glb}}(F)(\varphi(V)), \sum_{F \in \mathrm{Pr}^{nd}} \pi(F) \cdot \mathsf{N}_{\mathbf{lub}}(F)(\varphi(V)) \right] \\
& && \text{by Definition 3.3.11} \\
&= [\mathsf{N}_{\mathbf{glb}}(s)(a.\varphi(V)), \mathsf{N}_{\mathbf{lub}}(s)(a.\varphi(V))] && \text{by definition of } \mathsf{N}_* \\
&= [\mathsf{N}_{\mathbf{glb}}(s)(\varphi(aV)), \mathsf{N}_{\mathbf{lub}}(s)(\varphi(aV))] && \text{by definition of } \varphi.
\end{aligned}
$$

The remainder of the proof follows as for the case when $n = 0$. □

Theorem 6.6.19 *For all $E, F \in \mathcal{G}^{\mathrm{nd}}$:*

$$\mathcal{O}[\![E]\!] \overset{\mathsf{nd}}{\approx} \mathcal{O}[\![F]\!] \text{ if and only if } \mathcal{D}[\![E]\!](\rho) = \mathcal{D}[\![F]\!](\rho) \text{ for all } \rho \in \mathrm{Env}.$$

Proof. As before, we only prove the case for $E, F \in \mathrm{Pr}^{\mathrm{nd}}$ removing ρ for simplicity. First, consider any $E, F \in \mathrm{Pr}^{nd}$ such that $\mathcal{D}[\![E]\!] = \mathcal{D}[\![F]\!]$. Then using Lemma 6.5.13 and Lemma 6.6.13 we have $d_\omega(\mathcal{D}_n[\![E]\!][n], \mathcal{D}_n[\![F]\!][n]) = 0$ for all $n \in \mathbb{N}$, and hence by definition of d and $d_{\mathcal{V}}$:

$$|\mathcal{V}(v, \mathcal{D}_{n+1}[\![E]\!][n+1]) - \mathcal{V}(v, \mathcal{D}_{n+1}[\![F]\!][n+1])| = 0 \ \ \forall v \in A_{\mathrm{nd}}^{n+1} \ \& \ n \in \mathbb{N}$$

$$
\begin{array}{ll}
\Rightarrow \ \mathcal{V}(v, \mathcal{D}_{n+1}[\![E]\!][n+1]) = \mathcal{V}(v, \mathcal{D}_{n+1}[\![F]\!][n+1]) \ \ \forall v \in A_{\text{nd}}^{n+1} \ \& \ n \in \mathbb{N} & \\
\Rightarrow \ \mathsf{N}_{\text{glb}}(E)(\varphi(v)) = \mathsf{N}_{\text{glb}}(F)(\varphi(v)) \ \& \ \mathsf{N}_{\text{lub}}(E)(\varphi(v)) = \mathsf{N}_{\text{lub}}(F)(\varphi(v)) \ \ \forall v \in A_{\text{nd}}^{*} & \\
& \text{by Lemma 6.6.18 and} \\
& \text{definition of } A_{\text{nd}}^{*} \\
\Rightarrow \ \mathsf{N}_{\text{glb}}(E)(t) = \mathsf{N}_{\text{glb}}(F)(t) \ \& \ \mathsf{N}_{\text{lub}}(E)(t) = \mathsf{N}_{\text{lub}}(F)(t) \ \ \forall t \in \mathtt{T}^{\text{nd}} \setminus (\!|\bot|\!) & \\
& \text{by Lemma 6.6.17} \\
\Rightarrow \ \mathsf{N}_{\text{glb}}(E)(t) = \mathsf{N}_{\text{glb}}(F)(t) \ \& \ \mathsf{N}_{\text{lub}}(E)(t) = \mathsf{N}_{\text{lub}}(F)(t) \ \ \forall t \in \mathtt{T}^{\text{nd}} & \\
& \text{by definition of } \mathsf{N}_{\text{glb}} \text{ and } \mathsf{N}_{\text{lub}} \\
\Rightarrow \ \mathcal{O}[\![E]\!] \overset{\mathsf{n}d}{\sim} \mathcal{O}[\![F]\!] & \text{by definition of } \overset{\mathsf{n}d}{\sim}
\end{array}
$$

as required.

On the other hand, if $E, F \in \text{Pr}^{\text{n}d}$ and $\mathcal{O}[\![E]\!] \overset{\mathsf{n}d}{\sim} \mathcal{O}[\![F]\!]$, then by definition of $\overset{\mathsf{n}d}{\sim}$ and Lemma 6.6.17 for any $n \in \mathbb{N}$:

$$
\begin{array}{ll}
\mathsf{N}_{\text{glb}}(E)(\varphi(v)) = \mathsf{N}_{\text{lub}}(E)(\varphi(v)) \ \text{ and } \ \mathsf{N}_{\text{glb}}(F)(\varphi(v)) = \mathsf{N}_{\text{lub}}(F)(\varphi(v)) \ \ \forall v \in A_{\text{nd}}^{n} & \\
\quad \Rightarrow \ \mathcal{V}(v, \mathcal{D}_{n+1}[\![E]\!][n+1]) = \mathcal{V}(v, \mathcal{D}_{n+1}[\![F]\!][n+1]) \ \ \forall v \in A_{\text{nd}}^{n} & \text{by Lemma 6.6.18} \\
\quad \Rightarrow \ \mathcal{V}(v, \mathcal{D}_{n+1}[\![E]\!][n+1]) = \mathcal{V}(v, \mathcal{D}_{n+1}[\![F]\!][n+1]) \ \ \forall v \in A_{\text{nd}}^{*} & \text{by Lemma 6.5.7} \\
\quad \Rightarrow \ d_{\mathcal{V}}(\mathcal{D}_{n+1}[\![E]\!][n+1], \mathcal{D}_{n+1}[\![F]\!][n+1]) = 0 & \text{by definition of } d_{\mathcal{V}}
\end{array}
$$

and substituting this into the definition of d_ω we have:

$$
\begin{array}{rcll}
d_\omega(\mathcal{D}_{n+1}[\![E]\!], \mathcal{D}_{n+1}[\![F]\!]) & \leq & \sum\limits_{k=n+2}^{\infty} 2^{-k} d_{\mathcal{V}}(\mathcal{D}_{n+1}[\![E]\!][k], \mathcal{D}_{n+1}[\![F]\!][k]) & \\
& \leq & \sum\limits_{k=n+2}^{\infty} 2^{-k} & \text{by Proposition 6.5.5} \\
& = & 2^{-(n+1)} & \text{rearranging}
\end{array}
$$

Then, since this was for arbitrary $n \in \mathbb{N}$, by definition of d we have:

$$
d(\mathcal{D}[\![E]\!], \mathcal{D}[\![F]\!]) \leq \lim_{n \to \infty} 2^{-n} = 0.
$$

and thus, $\mathcal{D}[\![E]\!] = \mathcal{D}[\![F]\!]$ since d is a metric. □

6.7 A Metric for Reactive Probabilistic Processes

In this section, we outline the construction of a metric space for reactive probabilistic processes, based on our previous constructions, where we remove the proofs when they are simple extensions of the cases discussed earlier. First, we combine the definitions of finite deterministic and non-deterministic probabilistic processes (D_ω and N_ω respectively) to form the set of finite reactive probabilistic processes as follows.

Definition 6.7.1 (Finite reactive probabilistic processes) *Let R_n, $n \in \mathbb{N}$, be a collection of carrier sets defined inductively by:*

$$R_0 = \{\{p_0\}\} \;\; \text{and} \;\; R_{n+1} = \mathcal{P}_{fn}\Big(\{\{p_0\}\} \cup \mathcal{P}_{fnr}(A \times \mu(R_n))\Big).$$

Furthermore, let $R_\omega = \cup_n R_n$ denote reactive probabilistic processes of bounded depth.

To ease the notation, we let $X, Y \ldots$ range over R_ω, $x, y \ldots$ range over the elements of $X \in R_\omega$, that is, over $\{\{p_0\}\} \cup \mathcal{P}_{fnr}(A \times \mu(R_n))$, and p, q range over the elements of $x \in X \in R_\omega$, that is, the elements of the form p_0 or (a, f) for some $a \in A$ and $f \in \mu(R_\omega)$.

We next introduce the set of (open) trees reactive probabilistic processes can perform, and then using this definition extend the map $\mathcal{V}$ to this setting. We note that since the processes exhibit internal choices the map $\mathcal{V}$ takes values in the set of closed intervals $\mathcal{I}$, as for the case concerning N_ω.

Definition 6.7.2 *Let A_{r}^n, $n \in \mathbb{N}$, be the sets inductively defined as follows. Put:*

$$A_{\mathrm{r}}^0 = \mathcal{P}_{fnr}(A) \;\; \text{and} \;\; A_{\mathrm{r}}^{n+1} = \mathcal{P}_{fnr}\left((A \times \mathcal{P}_{fnr}(A_{\mathrm{r}}^n)) \cup A\right).$$

Furthermore, let $A_{\mathrm{r}}^* = \cup_n A_{\mathrm{r}}^n$.

Definition 6.7.3 *Let $\mathcal{V} : (A_{\mathrm{r}}^* \times R_\omega) \to \mathcal{I}$ be the mapping defined inductively on A_{r}^n as follows. For all $x \in \{\{p_0\}\} \cup \mathcal{P}_{fnr}(A \times \mu(R_\omega))$, $a \in A$, $V \in A_{\mathrm{r}}^n$ and $\mathbf{V} \in \mathcal{P}_{fnr}(A_{\mathrm{r}}^n)$ put:*

$$\begin{aligned}
\mathcal{V}(a, x) &= \begin{cases} [1,1] & \text{if } (a,f) \in x \text{ for some } f \in \mu(R_\omega) \\ [0,0] & \text{otherwise} \end{cases} \\
\mathcal{V}(a\mathbf{V}, x) &= \begin{cases} \sum_{Y \in R_\omega} f(Y) \cdot \mathcal{V}(\mathbf{V}, Y) & \text{if } (a,f) \in x \text{ for some } f \in \mu(R_\omega) \\ [0,0] & \text{otherwise} \end{cases} \\
\mathcal{V}(V, x) &= \prod_{v \in V} \mathcal{V}(v, x)
\end{aligned}$$

and furthermore, for all $X \in R_\omega$ put:

$$\mathcal{V}(\mathbf{V}, X) = \prod_{V \in \mathbf{V}} \mathcal{V}(V, X) \;\; \text{and} \;\; \mathcal{V}(V, X) = \bigsqcup_{x \in X} \mathcal{V}(V, x).$$

As for the non-deterministic case, the following lemma holds concerning the map $\mathcal{V}$.

Lemma 6.7.4 *For all $X \in R_\omega$ and $V \in A_{\mathrm{r}}^*$: $\mathcal{V}(V, X) \subseteq [0, 1]$.*

Then, for reasons similar to the non-deterministic case, we define our pseudo-metric over reactive probabilistic processes based on the metric $d_{\mathcal{I}}$ as follows.

Proposition 6.7.5 *R_ω (and R_n for any $n \in \mathbb{N}$) is a pseudo-metric space with respect to the pseudo-metric:*

$$d_{\mathcal{V}}(X,Y) = \max_{V \in A_{\mathrm{r}}^*} d_{\mathcal{I}}(\mathcal{V}(V,X), \mathcal{V}(V,Y)).$$

Furthermore, $0 \leq d_{\mathcal{V}}(X,Y) \leq 1$ for all $X, Y \in R_\omega$.

As before, to model recursive processes we introduce the definition of truncations, for which the proposition below holds.

Definition 6.7.6 *For all $f \in \mu(R_\omega)$, truncations are defined as in Definition 6.1.11, with the additional case that for all $X \in R_\omega$, $X[n] = \{x[n] \mid x \in X\}$, and for all $x \in X$, $x[n] = \{p[n] \mid p \in x\}$.*

Proposition 6.7.7 *For all $X, Y \in R_\omega$ and $k, m \in \mathbb{N}$:*

- (a) *if $X \in R_m$, then $X[k] \in R_k$ when $k < m$ and $X[k] = X$ otherwise.*
- (b) $(X[m])[k] = X[\min\{m,k\}]$.
- (c) *$X[m] = Y[m]$ if and only if $X[k] = Y[k]$ for all $k \leq m$.*
- (d) $d_{\mathcal{V}}(X[k], Y[k]) \leq d_{\mathcal{V}}(X,Y)$.

The proofs of (a), (b) and (c) follow similarly to the case concerning simple probabilistic processes and the proof of (d) follows from the lemma below.

Lemma 6.7.8 *For all $X \in R_\omega$, $V \in A_{\mathrm{r}}^*$ and $k \in \mathbb{N}$: $\mathcal{V}(V, X[0]) = [0,0]$ and*

$$\mathcal{V}(V, X[k+1]) = \begin{cases} \mathcal{V}(V,X) & \text{if } V \in A_{\mathrm{r}}^k \\ [0,0] & \text{otherwise.} \end{cases}$$

Following our construction, we next combine our pseudo-metric $d_{\mathcal{V}}$ with truncations to reach the following pseudo-metric over reactive processes.

Definition 6.7.9 *For all $X, Y \in R_\omega$, we define $d_\omega : R_\omega \times R_\omega \longrightarrow [0,1]$ as follows:*

$$d_\omega(X,Y) = \sum_{k=1}^{\infty} 2^{-k} d_{\mathcal{V}}(X[k], Y[k]).$$

Proposition 6.7.10 *(R_ω, d_ω) (and (R_n, d_ω) for any $n \in \mathbb{N}$) is a pseudo-metric space. Furthermore, $0 \leq d_\omega(X,Y) \leq 1$ for all $X, Y \in R_\omega$.*

To construct denotational semantics for RP, we first construct the metric space of reactive probabilistic processes as the completion of the metric space (R_ω, d_ω).

Definition 6.7.11 *Let (R, d) be the completion of (R_ω, d_ω).*

Before we introduce denotational semantics for RP, we first require the following technical lemmas.

Lemma 6.7.12 *For all $X \in R_\omega$, $\langle X[n] \rangle_n$ is a Cauchy sequence.*

Lemma 6.7.13 *If $\langle X_n \rangle_{n\in\mathbb{N}}$ is a sequence in R_ω such that $X_{n+1}[n] = X_n[n]$ for all $n \in \mathbb{N}$, then $\langle X_n \rangle_{n\in\mathbb{N}}$ is Cauchy and $X_m[n] = X_n[n]$ for all $m \geq n \in \mathbb{N}$. Furthermore, if $\langle q_n \rangle_{n\in\mathbb{N}}$ is a sequence in R_ω such that $Y_{n+1}[n] = Y_n[n]$ for all $n \in \mathbb{N}$ and $\langle X_n \rangle_{n\in\mathbb{N}} \sim \langle Y_n \rangle_{n\in\mathbb{N}}$, then $d_\omega(X_n[n], Y_n[n]) = 0$ for all $n \in \mathbb{N}$.*

Lemma 6.7.14 *If $\langle X_n \rangle_{n\in\mathbb{N}}$ and $\langle Y_n \rangle_{n\in\mathbb{N}}$ are Cauchy sequence and $\langle X_n \rangle_{n\in\mathbb{N}} \not\sim \langle Y_n \rangle_{n\in\mathbb{N}}$, then there exists $n \in \mathbb{N}$ such that $X_n[n] \neq Y_n[n]$.*

6.8 Denotational Semantics for RP

Similarly to the cases before we can introduce the definition of the *degree* of a process and then define semantic operators on reactive processes by induction on their degree. We note that the definitions and proofs concerning semantic operators are omitted when they are the expected extensions.

Definition 6.8.1 *For any $X, Y \in R_\omega$, let $X \cup Y$ be set-theoretic union.*

Lemma 6.8.2 *For all $X, Y \in R_\omega$ and $k \in \mathbb{N}$: $(X \cup Y)[k] = X[k] \cup Y[k]$.*

Proposition 6.8.3 *$\cup$ is continuous and well-defined on (R_ω, d_ω).*

We next introduce the semantic operator for external choice.

Definition 6.8.4 (External Choice Operator) *For any $X, Y \in R_\omega$, let*

$$X \Box Y = \{z \mid z \in x \Box y,\ x \in X \text{ and } y \in Y\}$$

where $\{p_0\} \Box \{p_0\} = \{\{p_0\}\}$, and if $x, y \in \mathcal{P}_{fnr}(A \times \mu(R_\omega))$ put $\{p_0\} \Box x = x \Box \{p_0\} = \{x\}$ and $x \Box y$ to be the set of maximal reactive subsets of $x \cup y$.

Lemma 6.8.5 *For all $X, Y \in R_\omega$ and $V \in A_{\mathrm{r}}^*$:*

$$\mathcal{V}(V, X \Box Y) = \bigsqcup_{\substack{V_1 \cup V_2 = V \\ \& \ V_1 \cap V_2 = \emptyset}} \mathcal{V}(V_1, X) \cdot \mathcal{V}(V_2, Y)$$

where $V_1, V_2 \in A_{\mathrm{r}}^* \cup \{\emptyset\}$ and $\mathcal{V}(\emptyset, Z) \stackrel{\text{def}}{=} [1, 1]$ for any $Z \in R_\omega$.

Proof. Consider any $X, Y \in R_\omega$ and $V \in A^*_{\mathrm{r}}$, then:

$$\mathcal{V}(V, X \square Y) = \bigsqcup_{z \in X \square Y} \mathcal{V}(V, z)$$

by definition of $\mathcal{V}$ and, using Proposition 3.3.12, it is sufficient to prove that:

$$\min_{\substack{V_1 \cup V_2 = V \\ \& \, V_1 \cap V_2 = \emptyset}} \mathcal{V}(V_1, X) \cdot \mathcal{V}(V_2, Y) =_{\mathrm{left}} \min_{z \in X \square Y} \mathcal{V}(V, z)$$

and

$$\max_{\substack{V_1 \cup V_2 = V \\ \& \, V_1 \cap V_2 = \emptyset}} \mathcal{V}(V_1, X) \cdot \mathcal{V}(V_2, Y) =_{\mathrm{right}} \max_{z \in X \square Y} \mathcal{V}(V, z).$$

We only prove the case for max as the case for min follows similarly. First, consider any $z \in X \square Y$, then by Definition 6.8.4 there exists $x \in X$ and $y \in Y$ such that $z \in x \square y$. Now setting:

$$V_1 = \{a\mathbf{V} \,|\, a\mathbf{V} \in V \text{ and } (a, f) \in x \cap z\} \;\text{ and }\; V_2 = V \setminus V_1$$

we have:

$$\begin{array}{rcll} \mathcal{V}(V, z) & = & \mathcal{V}(V_1, x) \cdot \mathcal{V}(V_2, y) & \text{by definition of } \mathcal{V} \\ & \leq_{\mathrm{right}} & \max_{x \in X} \mathcal{V}(V_1, x) \cdot \max_{y \in Y} \mathcal{V}(V_2, y) & \text{since } x \in X \text{ and } y \in Y \\ & =_{\mathrm{right}} & \mathcal{V}(V_1, X) \cdot \mathcal{V}(V_2, Y) & \text{by definition of } \mathcal{V} \\ & \leq_{\mathrm{right}} & \max\limits_{\substack{V_1 \cup V_2 = V \\ \& \, V_1 \cap V_2 = \emptyset}} \mathcal{V}(V_1, X) \cdot \mathcal{V}(V_2, Y) & \text{since } V_1 \cup V_2 = V \text{ and } V_1 \cap V_2 = \emptyset. \end{array}$$

In either case, since this is valid we infer:

$$\max_{z \in X \square Y} \mathcal{V}(V, z) \leq_{\mathrm{right}} \max_{V_1 \cup V_2 = V} \mathcal{V}(V_1, X) \cdot \mathcal{V}(V_2, Y). \tag{6.14}$$

On the other hand, considering any $V_1, V_2 \in A^*_{\mathrm{r}} \cup \{\emptyset\}$ such that $V_1 \cup V_2 = V$ and $V_1 \cap V_2 = \emptyset$, either $\mathcal{V}(V_1, X) \cdot \mathcal{V}(V_2, Y) = [0, 0]$ and thus:

$$\mathcal{V}(V_1, X) \cdot \mathcal{V}(V_2, Y) \leq_{\mathrm{right}} \max_{z \in X \square Y} \mathcal{V}(V, z)$$

by Lemma 6.7.4, or $\mathcal{V}(V_1, X) \cdot \mathcal{V}(V_2, Y) \neq [0, 0]$, and then, by definition of $\mathcal{V}$, there exist $x \in X$ and $y \in Y$ such that $\mathcal{V}(V_1, X) =_{\mathrm{right}} \mathcal{V}(V_1, x)$, $\mathcal{V}(V_2, Y) =_{\mathrm{right}} \mathcal{V}(V_2, Y)$, where $a\mathbf{V} \in V_1$ if $(a, f) \in x$ for some $f \in \mu(R_\omega)$ and $a\mathbf{V} \in V_2$ if $(a, f) \in y$ for some $f \in \mu(P_\omega)$. Then, let z be the element of $\mathcal{P}_{fnr}(A \times \mu(R_\omega))$ such that $z \in (a, f)$ if and only if one of the following holds:

- $(a, f) \in x$ and $a\mathbf{V} \in V_1$ for some $\mathbf{V} \in \mathcal{P}_{fnr}(A^*_{\mathrm{r}})$

- $(a, f) \in y$ and $a\mathbf{V} \in V_2$ for some $\mathbf{V} \in \mathcal{P}_{fnr}(A^*_{\mathrm{r}})$
- $(a, f) \in x$ or $(a, f) \in y$ and $a\mathbf{V} \notin V$ for all $\mathbf{V} \in \mathcal{P}_{fnr}(A^*_{\mathrm{r}})$.

By definition of $\Box$, $z \in x \Box y$, and hence since $x \in X$ and $y \in Y$: $z \in X \Box Y$. Then, similarly to the above, we have:

$$\begin{array}{rcl} \mathcal{V}(V_1, x) \cdot \mathcal{V}(V_2, y) & = & \mathcal{V}(V, z) \\ & \leq_{\mathrm{right}} & \max_{z \in X \Box Y} \mathcal{V}(V, z) \quad \text{since } z \in X \Box Y. \end{array}$$

Since this was for any $V_1, V_2 \in A^*_{\mathrm{r}} \cup \{\emptyset\}$ with $V_1 \cup V_2 = V$ we obtain:

$$\max_{\substack{V_1 \cup V_2 = V \\ \& V_1 \cap V_2 = \emptyset}} \mathcal{V}(V_1, X) \cdot \mathcal{V}(V_2, Y) \leq_{\mathrm{right}} \max_{z \in X \Box Y} \mathcal{V}(V, z). \tag{6.15}$$

Putting (6.14) and (6.15) together we have:

$$\max_{\substack{V_1 \cup V_2 = V \\ \& V_1 \cap V_2 = \emptyset}} \mathcal{V}(V_1, X) \cdot \mathcal{V}(V_2, Y) =_{\mathrm{right}} \max_{z \in X \Box Y} \mathcal{V}(V, z)$$

as required. $\Box$

Lemma 6.8.6 *For all $X, Y \in R_\omega$ and $k \in \mathbb{N}$: $(X \Box Y)[k] = X[k] \Box Y[k]$.*

Proposition 6.8.7 *$\Box$ is continuous and well-defined on (R_ω, d_ω).*

Proof. The proof that dc is continuous follows from Lemma 6.8.5 and properties of $d_{\mathcal{I}}$ (see Proposition 3.3.16 and Proposition 3.3.17). $\Box$

Lemma 6.8.8 *For all $X, Y \in R_\omega$ and $V \in A^*_{\mathrm{r}}$ and $k \in \mathbb{N}$: $\mathcal{V}(V, X \parallel Y) = \mathcal{V}(V, X) \cdot \mathcal{V}(V, Y)$ and $(X \parallel Y)[k] = X[k] \parallel Y[k]$.*

Proposition 6.8.9 *$\parallel$ is continuous and well-defined on (R_ω, d_ω).*

Lemma 6.8.10 *For all $X \in R_\omega$, $V \in A^*_{\mathrm{r}}$, $B \subseteq A$ and $k \in \mathbb{N}$:*

$$\mathcal{V}(V, X \upharpoonright B) = \begin{cases} [0,0] & \textit{if } a \in V \textit{ for some } a \notin B \\ \mathcal{V}(V, X) & \textit{otherwise} \end{cases}$$

and $(X \upharpoonright B)[k] = X[k] \upharpoonright B$.

Proposition 6.8.11 *For all $B \subseteq A$, $\upharpoonright B$ is continuous and well-defined on (R_ω, d_ω).*

Lemma 6.8.12 *For all $X \in R_\omega$, $V \in A^*_{\mathrm{r}}$, $\lambda : A \to A$ and $k \in \mathbb{N}$: $\mathcal{V}(V, X\,[\lambda]) = \mathcal{V}(\lambda^{-1}(V), X)$ and $(X\,[\lambda])[k] = (X[k])\,[\lambda]$.*

Proposition 6.8.13 *For all* $\lambda\colon A \to A$, $[\lambda]$ *is continuous and well-defined on* (R_ω, d_ω).

We now use the above semantic operators to define denotational semantics for the set of expressions $\mathcal{E}$ of our process calculus RP.

Definition 6.8.14 (Denotational Semantics) *Let* $\mathcal{D}_n : \mathrm{RP} \to (\mathrm{Env} \to R_\omega)$, $n \in \mathbb{N}$, *be the collection of maps defined inductively as follows. Put* $\mathcal{D}_0[\![E]\!] = \{\{p_0\}\}$ *for all* $E \in \mathrm{RP}$, *and* $\mathcal{D}_{n+1}$ *be defined inductively on the structure of elements of* RP *as follows:*

$$\begin{array}{rcl}
\mathcal{D}_{n+1}[\![x]\!](\rho) & = & \rho_{n+1}(x) \\
\mathcal{D}_{n+1}[\![\mathbf{0}]\!](\rho) & = & \{\{p_0\}\} \\
\mathcal{D}_{n+1}[\![\sum_{i\in I} a_{\mu_i}.E_i]\!](\rho) & = & \{\{(a, \Phi_{R_\omega}(\langle \mu_i, \mathcal{D}_n[\![E_i]\!](\rho)\rangle_{i\in I}))\}\} \\
\mathcal{D}_{n+1}[\![E_1 \,\Box\, E_2]\!](\rho) & = & \mathcal{D}_{n+1}[\![E_1]\!](\rho) \,\Box\, \mathcal{D}_{n+1}[\![E_2]\!](\rho) \\
\mathcal{D}_{n+1}[\![E_1 \sqcap E_2]\!](\rho) & = & \mathcal{D}_{n+1}[\![E_1]\!](\rho) \cup \mathcal{D}_{n+1}[\![E_2]\!](\rho) \\
\mathcal{D}_{n+1}[\![E_1 \parallel E_2]\!](\rho) & = & \mathcal{D}_{n+1}[\![E_1]\!](\rho) \parallel \mathcal{D}_{n+1}[\![E_2]\!](\rho) \\
\mathcal{D}_{n+1}[\![E \restriction B]\!](\rho) & = & \mathcal{D}_{n+1}[\![E]\!](\rho) \restriction B \\
\mathcal{D}_{n+1}[\![E\,[\lambda]]\!](\rho) & = & \mathcal{D}_{n+1}[\![E]\!](\rho)\,[\lambda] \\
\mathcal{D}_{n+1}[\![\mathit{fix}_x.E]\!](\rho) & = & \mathcal{D}_{n+1}[\![E]\!](\rho\{\mathcal{D}_n[\![\mathit{fix}_x.E]\!](\rho)/x\}).
\end{array}$$

Furthermore, let $\mathcal{D} : \mathrm{RP} \to (\mathrm{Env} \to R)$ *be the map defined as follows, for any* $E \in \mathrm{RP}$ *put:* $\mathcal{D}[\![E]\!](\rho) = [\langle \mathcal{D}_n[\![E]\!](\rho)\rangle_{n\in\mathbb{N}}]_\sim$.

To prove the well-definedness of the semantic map $\mathcal{D}$, as before we first require the following lemma.

Lemma 6.8.15 *For all* $E \in \mathcal{G}$, $\rho \in \mathrm{Env}$ *and* $k \in \mathbb{N}$: $\mathcal{D}_{k+1}[\![E]\!](\rho)[k] = \mathcal{D}_k[\![E]\!](\rho)[k]$.

Lemma 6.8.16 *For all* $E \in \mathrm{RP}$, $F \in \mathrm{Pr}$, $\rho \in Env$ *and* $n \in \mathbb{N}$*:*

$$\mathcal{D}_n[\![E\{F/x\}]\!](\rho)[n] = \mathcal{D}_n[\![E]\!](\rho\{D_n[\![F]\!]/x\})[n].$$

Furthermore, if $E \in \mathcal{G}$ *then:*

$$\mathcal{D}_{n+1}[\![E\{F/x\}]\!](\rho)[n+1] = \mathcal{D}_{n+1}[\![E]\!](\rho\{D_n[\![F]\!]/x\})[n+1].$$

Proposition 6.8.17 $\mathcal{D}$ *is well-defined on the guarded expressions of* RP.

6.8.1 Full Abstraction

To show that the above denotational model is fully abstract we first require the following extensions of the lemmas and the definition of the map φ from the non-deterministic case.

Lemma 6.8.18 *For all $E \in \mathrm{Pr}$, $\rho \in \mathrm{Env}$ and $S \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$, we have $\mathcal{O}[\![E]\!] \to S$ if and only if $x_n^S \in \mathcal{D}_{n+1}[\![E]\!](\rho)$ for all $n \in \mathbb{N}$ such that if $S = \emptyset$ then $x_{n+1}^S = \{p_0\}$, and if $S = \{(a_1, \pi_1), \ldots (a_m, \pi_m)\}$ then x_{n+1}^S is of the form $\{(a_1, f_n^1), \ldots, (a_m, f_n^m)\}$, and for any $1 \leq i \leq m$ and $Y \in R$:*

$$f_n^i[n](Y) = \sum_{\substack{F \in \mathrm{RP}\ \& \\ \mathcal{D}_n[\![F]\!](\rho)[n] = Y}} \pi_i(F).$$

Definition 6.8.19 *Let $\varphi : A_{\mathrm{r}}^* \to \mathtt{T} \setminus \{(\!|\bot|\!)\}$ be the mapping defined inductively as follows: $\varphi(\{a_1, \ldots, a_m\}) = (\!|[a_1.(\!|\bot|\!), \ldots, a_m.(\!|\bot|\!)]|\!)$ and*

$$\varphi(\{a_1\mathbf{V}_1, \ldots, a_m\mathbf{V}_m\}) = (\!|[a_1.\varphi(\mathbf{V}_1), \ldots a_m.\varphi(\mathbf{V}_m)]|\!),$$

where $\varphi_(\{V_1, \ldots, V_m\}) = (\varphi(V_1), \ldots, \varphi(V_{m'}))$.

Lemma 6.8.20 *The mapping φ is bijective.*

Lemma 6.8.21 *For all $E \in \mathrm{Pr}$, $\rho \in \mathrm{Env}$, $V \in A_{\mathrm{r}}^n$ and $n \in \mathbb{N}$:*

$$\mathcal{V}(V, \mathcal{D}_{n+1}[\![E]\!](\rho)[n+1]) = [\mathsf{R}_{\mathbf{glb}}(E)(\varphi(V)), \mathsf{R}_{\mathbf{lub}}(E)(\varphi(V))].$$

Theorem 6.8.22 *For all $E, F \in \mathcal{G}$:*

$$\mathcal{O}[\![E]\!] \stackrel{r}{\sim} \mathcal{O}[\![F]\!] \text{ if and only if } \mathcal{D}[\![E]\!](\rho) = \mathcal{D}[\![F]\!](\rho) \text{ for all } \rho \in \mathrm{Env}.$$

6.9 Discussion

As already mentioned in Section 5.7, one possible topic of future research is to consider a process calculus with a separate probabilistic choice operator based on the operational model and our metric space construction for the calculus RP. The first step would be to consider simple probabilistic processes, which can be considered as any $f \in \mu(\{p_0\} \cup (A \times P))$ such that for any simple process g, $f((a, g))$ is the probability that f will perform the action a and then behave as g, and $f(p_0)$ is the probability that f behaves as the inactive process. This then gives:

$$P_{n+1} = \mu(\{p_0\} \cup (A \times P_n))$$

as a candidate for the carrier set construction for simple probabilistic processes. Then we could introduce a pseudo-metric ($d_{\mathcal{S}}$) based on the mapping $\mathcal{V} : A^* \times P \to [0, 1]$, where for any μ:

$$\mathcal{V}(\langle\rangle, f) = f(p_0) \text{ and } \mathcal{V}(au, f) = \sum_{(a,g) \in \mathsf{s}(f)} f((a, g)) \cdot \mathcal{V}(u, g).$$

Extending this to respectively allow external choice, internal choice and both types of choice, we would expect to arrive at the following carrier set constructions:

$$
\begin{aligned}
D_{n+1} &= \mu(\{\{p_0\}\} \cup \mathcal{P}_{fnr}(A \times D_n)),\\
N_{n+1} &= \mathcal{P}_{fn}\Big(\mu(\{\{p_0\}\} \cup (A \times N_n))\Big),\\
R_{n+1} &= \mathcal{P}_{fn}\Big(\mu(\{\{p_0\}\} \cup \mathcal{P}_{fnr}(A \times R_n))\Big).
\end{aligned}
$$

Also, as mentioned in Section 5.7, we can formulate an operational model containing sub-probability distributions. However, if we consider the full abstraction results we see that the cases relating to P and D depend on the summation of distributions being one, whereas the cases for N and R do not. Thus, to formulate a fully abstract model for purely probabilistic and deterministic probabilistic process calculi containing sub-probability distributions we will need to use a psudeo-metric in the spirit of $d_{\mathcal{V}}$, as opposed to $d_{\mathcal{S}}$, that is, remove the null string $(\langle\rangle)$ from the definitions of A^* and $A^*_{\mathbf{d}}$ and then consider the maximum difference between the probabilities of processes performing these paths instead of a summation over all paths.

Chapter 7

Logical Semantics

In this chapter we give a logical semantics to reactive probabilistic transition systems using Hennessy-Milner Logic (HML) [HM85] and adapting Huth and Kwiatkowska's non-standard interpretation [HK97] for HML over processes of Larsen and Skou's probabilistic transition systems [LS91] to our reactive probabilistic transition systems. Similarly to the operational and denotational approaches, we first consider purely probabilistic transition systems, and in this case give a logical semantics to these transition systems by means of a sublanguage of HML. We next consider suitable extensions of this sublanguage of HML to extend our semantics to both deterministic and non-deterministic probabilistic transition systems, and then finally combine these sublanguages to give semantics to all reactive probabilistic transition systems.

7.1 Preliminaries

In this section, we introduce the logic HML and give this logic Huth and Kwiatkowska's non-standard interpretation originally introduced for Larsen and Skou's probabilistic transition systems. Moreover, we state definitions that will be needed to give our reactive probabilistic transition systems a logical semantics.

Definition 7.1.1 (Hennessy-Milner Logic [HM85]) *The logic* HML *is defined inductively on the syntax:*

$$\phi \ ::= \ \mathtt{true} \mid \langle a \rangle \phi \mid \neg \phi \mid \phi \wedge \phi$$

where a ranges over a set of actions $\mathcal{A}ct$.

We note that we only consider the finitary version of conjunction as we only consider finite external and internal choices.

Definition 7.1.2 *Let* $[\![.]\!] : (\texttt{HML} \times P) \to [0,1]$ *be the mapping defined inductively on formulae of* HML *for any probabilistic transition system* (P, Act, Can, μ) *and* $E \in P$ *as follows:*

$$\begin{array}{rcl} [\![\texttt{true}]\!]E & = & 1 \\ [\![\langle a\rangle\phi]\!]E & = & \sum_{F\in P}\{\mu \cdot [\![\psi]\!]F \mid E \xrightarrow{a}_{\mu} F\} \\ [\![\neg\phi]\!]E & = & 1 - [\![\phi]\!]E \\ [\![\phi_1 \wedge \phi_2]\!]E & = & [\![\phi_1]\!]E \cdot [\![\phi_2]\!]E. \end{array}$$

We note that in [HK97] Huth and Kwiatkowska also consider additional alternative operators, for example disjunction ($\vee$) and fixed point operators.

Definition 7.1.3 *Let* $\mathrm{a}ct : \texttt{HML} \to \mathcal{P}_f(\mathcal{A}ct)$ *be the mapping defined inductively on the syntax of* HML *as follows:*

$$\begin{array}{rcl} \mathrm{a}ct(\texttt{true}) & = & \emptyset \\ \mathrm{a}ct(\langle a\rangle\phi) & = & \{a\} \\ \mathrm{a}ct(\neg\phi) & = & \mathrm{a}ct(\phi) \\ \mathrm{a}ct(\phi_1 \wedge \phi_2) & = & \mathrm{a}ct(\phi_1) \cup \mathrm{a}ct(\phi_2). \end{array}$$

Definition 7.1.4 *We define the* height *of a formula* ϕ *of* HML*,* $\mathrm{h}t(\phi) \in \mathbb{N}$*, by induction on the syntax of* HML *as follows:*

$$\begin{array}{rcl} \mathrm{h}t(\texttt{true}) & = & 0 \\ \mathrm{h}t(\langle a\rangle\phi) & = & \mathrm{h}t(\phi) + 1 \\ \mathrm{h}t(\neg\phi) & = & \mathrm{h}t(\phi) + 1 \\ \mathrm{h}t(\phi_1 \wedge \phi_2) & = & \max\{\mathrm{h}t(\phi_1),\, \mathrm{h}t(\phi_2)\} + 1. \end{array}$$

7.2 Purely Probabilistic Transition Systems

First, since the interpretation $[\![\cdot]\!]$ of HML (see Definition 7.1.2) is given for probabilistic transition systems, we adapt it to purely probabilistic transition systems. Let $(\mathcal{R}^{\mathrm{p}}, \mathcal{A}ct, \to)$ be a purely probabilistic transition system and $E \in \mathcal{R}^{\mathrm{p}}$; we need to replace the clause for $\langle a\rangle\phi$ in Definition 7.1.2 by:

$$[\![\langle a\rangle\phi]\!]E \stackrel{def}{=} \begin{cases} \sum\limits_{F\in\mathcal{R}^{\mathrm{p}}} \pi(F) \cdot [\![\phi]\!]F & \text{if } E = (a,\pi) \text{ for some } \pi \in \mu(\mathcal{R}^{\mathrm{p}}) \\ 0 & \text{otherwise.} \end{cases}$$

As mentioned above, to characterise our equivalence over purely probabilistic transition systems we need only consider a sublanguage of HML, denoted $\texttt{HML}_{\mathrm{p}}$, defined as follows.

Definition 7.2.1 *The sublanguage* $\mathtt{HML}_{\mathrm{p}}$ *of* $\mathtt{HML}$ *is the language defined inductively on the syntax:*

$$\phi \ ::= \ \mathtt{true} \mid \langle a \rangle \phi$$

where $a \in \mathcal{A}ct$.

The following connections between the map P on purely probabilistic tests and $\mathtt{HML}_{\mathrm{p}}$ with its interpretation on $\mathcal{R}^{\mathrm{p}}$ given above can be proved.

Proposition 7.2.2 *For all* $t \in \mathtt{T}^{\mathrm{p}}$ *there exists* $\phi_t \in \mathtt{HML}_{\mathrm{p}}$ *such that* $[\![\phi_t]\!]E = \mathsf{P}(E)(t)$ *for all* $E \in \mathcal{R}^{\mathrm{p}}$.

Proof. The proposition is proved by induction on $t \in \mathtt{T}^{\mathrm{p}}$, where for any $t \in \mathtt{T}^{\mathrm{p}}$ we set:

$$\phi_t = \begin{cases} \mathtt{true} & \text{if } t = \bot \\ \langle a \rangle \phi_{t'} & \text{if } t = a.t'. \end{cases}$$

If $t = \bot$, then $\phi_\bot = \mathtt{true}$ and we conclude by definition of P and $[\![\cdot]\!]$ that $[\![\phi_\bot]\!]E = \mathsf{P}(E)(\bot) = 1$ for all $E \in \mathcal{R}^{\mathrm{p}}$.

If $t = a.t'$ for some $a \in \mathcal{A}ct$, then $\phi_{a.t'} = \langle a \rangle \phi_{t'}$ and by induction we have $\phi_{a.t'} \in \mathtt{HML}_{\mathrm{p}}$. Furthermore, by definition of P and $[\![\cdot]\!]$ for any $E \in \mathcal{R}^{\mathrm{p}}$:

$$\mathsf{P}(E)(a.t') = \begin{cases} \sum_{F \in \mathcal{R}^{\mathrm{p}}} \pi(F) \cdot \mathsf{P}(F)(t') & \text{if } E = (a, \pi) \text{ for some } \pi \in \mu(\mathcal{R}^{\mathrm{p}}) \\ 0 & \text{otherwise.} \end{cases}$$

$$\begin{aligned} &= \begin{cases} \sum_{F \in \mathcal{R}^{\mathrm{p}}} \pi(F) \cdot [\![\phi_{t'}]\!]F & \text{if } E = (a, \pi) \text{ for some } \pi \in \mu(\mathcal{R}^{\mathrm{p}}) \\ 0 & \text{otherwise.} \end{cases} && \text{by induction} \\ &= [\![\langle a \rangle \phi_{t'}]\!]E && \text{by definition of } [\![\cdot]\!] \end{aligned}$$

and hence the proposition is proved by induction on $n \in \mathbb{N}$. □

Proposition 7.2.3 *For all* $\phi \in \mathtt{HML}_{\mathrm{p}}$ *there exists* $t_\phi \in \mathtt{T}^{\mathrm{p}}$ *such that* $[\![\phi]\!]E = \mathsf{P}(E)(t_\phi)$ *for all* $E \in \mathcal{R}^{\mathrm{p}}$.

Proof. The proof follows by arguments similar to the proof of Proposition 7.2.2 above by induction on the height of formulae of $\mathtt{HML}_{\mathrm{p}}$, where for any $\phi \in \mathtt{HML}_{\mathrm{p}}$:

$$t_\phi = \begin{cases} \bot & \text{if } \phi = \mathtt{true} \\ a.t_\psi & \text{if } \phi = \langle a \rangle \psi. \end{cases}$$

□

Theorem 7.2.4 *For all $E, F \in \mathcal{R}^{\mathrm{p}}$, $E \sqsubseteq^{\mathsf{p}} F$ if and only if $[\![\phi]\!]E \leq [\![\phi]\!]F$ for all $\phi \in \mathtt{HML}_{\mathrm{p}}$.*

Proof. First consider $E, F \in \mathcal{R}^{\mathrm{p}}$ such that $E \sqsubseteq^{\mathsf{p}} F$, then for any $\phi \in \mathtt{HML}_{\mathrm{p}}$:

$$\begin{array}{rcll} [\![\phi]\!]E & = & \mathsf{P}(E)(t_\phi) & \text{by Proposition 7.2.3} \\ & \leq & \mathsf{P}(F)(t_\phi) & \text{since } E \sqsubseteq^{\mathsf{p}} F \\ & = & [\![\phi]\!]F & \text{by Proposition 7.2.3.} \end{array}$$

Conversely, suppose $E, F \in \mathcal{R}^{\mathrm{p}}$ and $[\![\phi]\!]E \leq [\![\phi]\!]F$ for all $\phi \in \mathtt{HML}_{\mathrm{p}}$. Then for any $t \in \mathtt{T}^{\mathrm{p}}$:

$$\begin{array}{rcll} \mathsf{P}(E)(t) & = & [\![\phi_t]\!]E & \text{by Proposition 7.2.2} \\ & \leq & [\![\phi_t]\!]F & \text{by hypothesis} \\ & = & \mathsf{P}(F)(t) & \text{by Proposition 7.2.2} \end{array}$$

and since this was for arbitrary $t \in \mathtt{T}^{\mathrm{p}}$, we obtain $E \sqsubseteq^{\mathsf{p}} F$ as required. $\square$

7.3 Deterministic Probabilistic Transition Systems

In this section we consider a deterministic probabilistic transition system $(\mathcal{R}^{\mathrm{d}}, \mathcal{A}ct, \rightarrow)$ and first extend the subset $\mathtt{HML}_{\mathrm{p}}$ of $\mathtt{HML}$, to $\mathtt{HML}_{\mathrm{d}}$, defined as follows.

Definition 7.3.1 *The sublanguage $\mathtt{HML}_{\mathrm{d}}$ of $\mathtt{HML}$ is the language defined inductively on the syntax:*

$$\phi \ ::= \ \mathtt{true} \mid \phi \wedge \phi \mid \langle a \rangle \phi$$

where, for any ϕ_1 and $\phi_2 \in \mathtt{HML}_{\mathrm{d}}$, $\phi_1 \wedge \phi_2$ exists in $\mathtt{HML}_{\mathrm{d}}$ if and only if $\mathrm{act}(\phi_1) \cap \mathrm{act}(\phi_2) = \emptyset$.

We can state the following connections between the function D and $\mathtt{HML}_{\mathrm{d}}$. Recall that for any independent $T_1, T_2 \in \mathtt{T}^{\mathrm{d}}_{\omega}$, $T_1 \parallel T_2$ denotes the composition of the tests T_1 and T_2.

Proposition 7.3.2 *For all $t \in \mathtt{T}^{\mathrm{d}}$ there exists $\phi_t \in \mathtt{HML}_{\mathrm{d}}$ such that $[\![\phi_t]\!]E = \mathsf{D}(E)(t)$ for all $E \in \mathcal{R}^{\mathrm{d}}$, and if t is of the form $a.T$ then $\mathrm{act}(\phi_t) = a$.*

Proof. The proof is by induction on $t \in \mathtt{T}^{\mathrm{d}}$, where for any $t \in \mathtt{T}^{\mathrm{d}}$ we set:

$$\phi_t = \begin{cases} \mathtt{true} & \text{if } t = \bot \\ \langle a \rangle \phi_T & \text{if } t = a.T \end{cases} \qquad \text{and} \qquad \phi_{(t_1,\ldots,t_m)} = \bigwedge_{i=1}^{m} \phi_{t_i}.$$

The case for $t = \bot$ follows similarly to Proposition 7.2.2. If $t = a.T$ for some $a \in \mathcal{A}ct$, then T is of the form $(t_1, \ldots, t_n)$ such that $t_i \in \mathtt{T}^{\mathrm{d}}$ for all $1 \leq i \leq m$, and each t_i

is of the form $a_i.T_i$ such that $a_i \neq a_j$ for all $1 \leq i \neq j \leq m$. By induction we have $\phi_{t_i} \in \mathtt{HML_d}$ and $act(\phi_{t_i}) = a_i$ for all $1 \leq i \leq m$, therefore $\phi_T \in \mathtt{HML_d}$ since $a_j \neq a_j$ for all $1 \leq i \neq j \leq m$. Hence, by the construction given above, $\phi_t \in \mathtt{HML_d}$. Moreover, it follows by definition of $[\![\cdot]\!]$ and D that $[\![\phi_t]\!]E = \mathsf{D}(E)(t)$ for any $E \in \mathcal{R}^{\mathrm{d}}$, and hence the proposition is proved by induction. □

Proposition 7.3.3 *For all $\phi \in \mathtt{HML_d}$ there exists $T_\phi \in \mathtt{T}^{\mathrm{d}}_\omega$ such that $[\![\phi]\!]E = \mathsf{D}(E)(T_\phi)$ for all $E \in \mathcal{R}^{\mathrm{d}}$, where T_ϕ is of the form $(a_1.T_1, \ldots, a_m.T_m)$ if $act(\phi) = \{a_1, \ldots, a_m\}$ and $T_\phi = (\bot)$ if $act(\phi) = \emptyset$.*

Proof. The proof is by induction on $n \in \mathbb{N}$ where $n = ht(\phi)$. Put:

$$T_\phi = \begin{cases} (\bot) & \text{if } \phi = \mathtt{true} \\ (a.T_\psi) & \text{if } \phi = \langle a \rangle \psi \\ T_{\phi_1} \,\|\, T_{\phi_2} & \text{if } \phi = \phi_1 \wedge \phi_2. \end{cases}$$

The proof now follows similarly to Proposition 7.2.3, except in the inductive step when supposing the proposition holds for all formulae of height n and ϕ is of the form $\phi_1 \wedge \phi_2$ for some $\phi_1, \phi_2 \in \mathtt{HML_d}$ and $ht(\phi) = n + 1$. In this case $T_{\phi_1} \,\|\, T_{\phi_2}$ is well-defined by induction and since, by definition of $\mathtt{HML_d}$, $act(\phi_1) \cap act(\phi_2) = \emptyset$. Therefore, from our construction above, we have $T_\phi \in \mathtt{T}^{\mathrm{d}}_\omega$ and is of the required form since $act(\phi_1 \wedge \phi_2) = act(\phi_1) \cup act(\phi_2)$. Moreover, for any $E \in \mathcal{R}^{\mathrm{d}}$:

$$\begin{array}{rcll} [\![\phi]\!]E & = & [\![\phi_1 \wedge \phi_2]\!]E & \\ & = & [\![\phi_1]\!]E \cdot [\![\phi_2]\!]E & \text{by definition of } [\![\cdot]\!] \\ & = & \mathsf{D}(E)(T_{\phi_1}) \cdot \mathsf{D}(E)(T_{\phi_2}) & \text{by induction} \\ & = & \mathsf{D}(E)(T_{\phi_1} \,\|\, T_{\phi_2}) & \text{by Lemma 4.3.6} \\ & = & \mathsf{D}(E)(T_\phi) & \text{by construction} \end{array}$$

as required. □

Using Proposition 7.3.2 and Proposition 7.3.3 we reach the following theorem connecting $\mathtt{HML_d}$ and our operational ordering $\sqsubseteq^{\mathsf{d}}$.

Theorem 7.3.4 *For all $E, F \in \mathcal{R}^{\mathrm{d}}$, $E \sqsubseteq^{\mathsf{d}} F$ if and only if $[\![\phi]\!]E \leq [\![\phi]\!]F$ for all $\phi \in \mathtt{HML_d}$.*

Proof. The proof follows similarly to that of Theorem 7.2.4. □

7.4 Non-deterministic Probabilistic Transition Systems

We now consider a logical semantics for non-deterministic probabilistic transition systems. In non-probabilistic transition systems internal behaviour is often represented by processes being able to perform hidden actions, that is, τ actions. When formulating logical semantics over such transition systems, an operator of the form $\langle\varepsilon\rangle\phi$ is added to the syntax of HML (for example, when giving a logical characterisation of weak bisimulation [Mil89]), where for any labelled transition system $(T, \mathcal{A}ct \cup \{\tau\}, \rightarrow)$ and $P \in T$, $\langle\varepsilon\rangle\phi$ is interpreted as follows:

$$[\![\langle\varepsilon\rangle\phi]\!]P \stackrel{def}{=} \max\{[\![\phi]\!]Q \mid P \Rightarrow Q\}.$$

Here $P \Rightarrow Q$ if there exists a path from P to Q consisting of an arbitrary number (≥ 0) of τ-steps. Intuitively, a process P satisfies the formula $\langle\varepsilon\rangle\phi$, that is, $[\![\langle\varepsilon\rangle\phi]\!]P = 1$, if P *can* make an internal choice to evolve as a process which will satisfy ϕ. Adapting this to a non-deterministic probabilistic transition system $(\mathcal{R}^{\mathrm{n}d}, \mathcal{A}ct, \rightarrow)$, we have the following interpretation of $\langle\varepsilon\rangle\phi$ for any $E \in \mathcal{R}^{\mathrm{nd}}$:

$$[\![\langle\varepsilon\rangle\phi]\!]E \stackrel{def}{=} \max\{[\![\phi]\!]s \mid E \rightarrow s\}$$

since E makes an internal choice between behaving as any $s \in (\mathcal{A}ct \times \mu(\mathcal{R}^{\mathrm{n}d})) \cup \{\emptyset\}$ such that $E \rightarrow s$.

Furthermore, we also add the dual of $\langle\varepsilon\rangle\phi$, namely $[\varepsilon]\phi$, where, intuitively, a (non-probabilistic) process P satisfies the formula $[\varepsilon]\phi$ if *all* the processes that P can evolve to by making an internal choice satisfy ϕ. Since by definition of HML $[.] = \neg\langle.\rangle\neg$, we reach the desired interpretation of $[\varepsilon]\phi$ over non-deterministic probabilistic transition systems by means of the following proposition.

Proposition 7.4.1 *For all $E \in \mathcal{R}^{\mathrm{nd}}$ and $\phi \in$ HML: $[\![[\varepsilon]\phi]\!]E = \min\{[\![\phi]\!]s \mid E \rightarrow s\}$.*

Proof. Consider any $E \in \mathcal{R}^{\mathrm{n}d}$ and $\phi \in$ HML, then by definition of $[\![\cdot]\!]$:

$$\begin{array}{rcll} [\![[\varepsilon]\phi]\!]E & = & [\![\neg\langle\varepsilon\rangle\neg\phi]\!]E & \\ & = & 1 - \max\{[\![\neg\phi]\!]s \mid E \rightarrow s\} & \text{by definition of } [\![\cdot]\!] \\ & = & 1 - \max\{1 - [\![\phi]\!]s \mid E \rightarrow s\} & \text{by definition of } [\![\cdot]\!] \\ & = & 1 - (1 - \min\{[\![\phi]\!]s \mid E \rightarrow s\}) & \text{rearranging} \\ & = & \min\{[\![\phi]\!]s \mid E \rightarrow s\} & \end{array}$$

as required. $\square$

Furthermore, since any $s \in (\mathcal{A}ct \times \mu(\mathcal{R}^{\mathrm{nd}})) \cup \{\emptyset\}$ can be considered as a purely probabilistic process and can therefore perform no internal choices, we can set:

$$[\![\langle\varepsilon\rangle\phi]\!]s \stackrel{def}{=} [\![\phi]\!]s \text{ and } [\![[\varepsilon]\phi]\!]s \stackrel{def}{=} [\![\phi]\!]s.$$

We also set $[\![\langle a\rangle\phi]\!]s$ to have the same interpretation as when we considered purely probabilistic transition systems.

As we have added $\langle\varepsilon\rangle\phi$ to $\mathtt{HML}$, we therefore extend our definition of the maps $\mathrm{a}ct(\cdot)$ and $\mathrm{h}t(\cdot)$ as follows. For any $\phi \in \mathtt{HML}$:

$$\mathrm{a}ct(\langle\varepsilon\rangle\phi) \stackrel{def}{=} \mathrm{a}ct(\phi) \text{ and } \mathrm{h}t(\langle\varepsilon\rangle\phi) \stackrel{def}{=} \mathrm{h}t(\phi)$$

Using this operator, we reach the following two extensions of $\mathtt{HML}_{\mathrm{p}}$, denoted $\mathtt{HML}_{\mathrm{nd}}^{\langle\varepsilon\rangle}$ and $\mathtt{HML}_{\mathrm{nd}}^{[\varepsilon]}$, where intuitively the meaning of $\mathtt{HML}_{\mathrm{nd}}^{\langle\varepsilon\rangle}$ and $\mathtt{HML}_{\mathrm{nd}}^{[\varepsilon]}$ respectively is that processes *may* or *must* validate a formula.

Definition 7.4.2 *The sublanguage $\mathtt{HML}_{\mathrm{nd}}^{\langle\varepsilon\rangle}$ of $\mathtt{HML}$ is the language defined inductively on the syntax:*

$$\phi \ ::= \ \mathtt{true} \mid \langle\varepsilon\rangle\langle a\rangle\phi \mid \phi \wedge \phi$$

where, for any ϕ_1 and $\phi_2 \in \mathtt{HML}_{\mathrm{nd}}^{\langle\varepsilon\rangle}$, $\phi_1 \wedge \phi_2$ exists in $\mathtt{HML}_{\mathrm{nd}}^{\langle\varepsilon\rangle}$ if and only if $\mathrm{a}ct(\phi_1) \cap \mathrm{a}ct(\phi_2) = \emptyset$.

Definition 7.4.3 *The sublanguage $\mathtt{HML}_{\mathrm{nd}}^{[\varepsilon]}$ of $\mathtt{HML}$ is the language defined inductively on the syntax:*

$$\psi \ ::= \ \mathtt{true} \mid [\varepsilon]\langle a\rangle\psi \mid \psi \wedge \psi$$

where, for any ψ_1 and $\psi_2 \in \mathtt{HML}_{\mathrm{nd}}^{[\varepsilon]}$, $\psi_1 \wedge \psi_2$ exists in $\mathtt{HML}_{\mathrm{nd}}^{[\varepsilon]}$ if and only if $\mathrm{a}ct(\psi_1) \cap \mathrm{a}ct(\psi_2) = \emptyset$.

We now state the following relationship between $\mathtt{HML}_{\mathrm{nd}}^{\langle\varepsilon\rangle}$ and $\mathsf{N}_{\mathbf{lub}}$, and $\mathtt{HML}_{\mathrm{nd}}^{[\varepsilon]}$ and $\mathsf{N}_{\mathbf{glb}}$.

Proposition 7.4.4 *For all $t \in \mathtt{T}^{\mathrm{nd}}$ there exists $\phi_t \in \mathtt{HML}_{\mathrm{nd}}^{\langle\varepsilon\rangle}$ such that for all $E \in \mathcal{R}^{nd}$, $[\![\phi_t]\!]E = \mathsf{N}_{\mathbf{lub}}(E)(t)$, and if t is of the form $(\!|a.T|\!)$ for some $a \in \mathcal{A}ct$, then $\mathrm{a}ct(\phi_t) = \{a\}$.*

Proof. The proposition is proved by induction on $t \in \mathtt{T}_n^{\mathrm{nd}}$ by setting:

$$\phi_r = \begin{cases} \mathtt{true} & \text{if } r = \bot \\ \langle a\rangle\phi_T & \text{if } r = a.T, \end{cases} \qquad \phi_{(\!|r|\!)} = \langle\varepsilon\rangle\phi_r \quad \text{and} \quad \phi_{(t_1,\ldots,t_m)} = \bigwedge_{i=1}^{m}\phi_{t_i}.$$

□

Proposition 7.4.5 *For all $t \in \mathtt{T}^{\mathrm{nd}}$ there exists $\psi_t \in \mathtt{HML}_{\mathrm{nd}}^{[\varepsilon]}$ such that for all $E \in \mathcal{R}^{nd}$, $[\![\psi_t]\!]E = \mathsf{N}_{\mathbf{glb}}(E)(t)$, and if $t = (\!|a.T|\!)$ for some $a \in \mathcal{A}ct$, then $\mathrm{a}ct(\psi_t) = \{a\}$.*

Proof. The proposition is proved by induction on $t \in \mathtt{T}_n^{\mathrm{nd}}$ similarly to Proposition 7.4.4 above using Proposition 7.4.1 and replacing $\langle\varepsilon\rangle$ with $[\varepsilon]$. □

Proposition 7.4.6 *For all $\phi \in \mathtt{HML}_{\mathrm{nd}}^{\langle\varepsilon\rangle}$ there exists $T_\phi \in \mathtt{T}_\omega^{\mathrm{nd}}$ such that $\mathsf{N}_{\mathbf{lub}}(E)(T_\phi) = [\![\phi]\!]E$ for all $E \in \mathcal{R}^{\mathrm{nd}}$, where T_ϕ is of the form $((\!|a_1.T_1|\!), \ldots, (\!|a_m.T_m|\!))$ if $\mathrm{act}(\phi) = \{a_1, \ldots, a_m\}$ and $T_\phi = (\perp)$ if $\mathrm{act}(\phi) = \emptyset$.*

Proof. The proof follows by induction on the height of formulae similarly to Proposition 7.3.3, using Lemma 4.4.6 instead of Lemma 4.3.6, and putting:

$$T_\phi = \begin{cases} ((\!|\perp|\!)) & \text{if } \phi = \mathtt{true} \\ ((\!|a.T_{\phi'}|\!)) & \text{if } \phi = \langle\varepsilon\rangle\langle a\rangle\phi' \\ T_{\phi_1} \,\|\, T_{\phi_2} & \text{if } \phi = \phi_1 \wedge \phi_2. \end{cases}$$

□

Proposition 7.4.7 *For all $\psi \in \mathtt{HML}_{\mathrm{nd}}^{[\varepsilon]}$ there exists $T_\psi \in \mathtt{T}_\omega^{\mathrm{nd}}$ such that $\mathsf{N}_{\mathbf{glb}}(E)(T_\psi) = [\![\psi]\!]E$ for all $E \in \mathcal{R}^{\mathrm{nd}}$, where T_ψ is of the form $((\!|a_1.T_1|\!), \ldots, (\!|a_m.T_m|\!))$ if $\mathrm{act}(\psi) = \{a_1, \ldots, a_m\}$ and $T_\psi = (\perp)$ if $\mathrm{act}(\psi) = \emptyset$.*

Using the above propositions, we reach the following theorem connecting $\mathtt{HML}_{\mathrm{nd}}^{\langle\varepsilon\rangle} \cup \mathtt{HML}_{\mathrm{nd}}^{[\varepsilon]}$ and $\sqsubseteq^{\mathsf{nd}}$.

Theorem 7.4.8 *For all $E, F \in \mathcal{R}^{\mathrm{nd}}$, $E \sqsubseteq^{\mathsf{nd}} F$ if and only if $[\![\phi]\!]E \leq [\![\phi]\!]F$ for all $\phi \in \mathtt{HML}_{\mathrm{nd}}^{\langle\varepsilon\rangle}$ and $[\![\psi]\!]E \leq [\![\psi]\!]F$ for all $\psi \in \mathtt{HML}_{\mathrm{nd}}^{[\varepsilon]}$.*

Proof. First consider $E, F \in \mathcal{R}^{\mathrm{nd}}$ such that $E \sqsubseteq^{\mathsf{nd}} F$, then for any $\phi \in \mathtt{HML}_{\mathrm{nd}}^{\langle\varepsilon\rangle}$:

$$\begin{array}{rcll} [\![\phi]\!]E & = & \mathsf{N}_{\mathbf{lub}}(E)(T_\phi) & \text{by Proposition 7.4.6} \\ & \leq & \mathsf{N}_{\mathbf{lub}}(F)(T_\phi) & \text{since } E \sqsubseteq^{\mathsf{nd}} F \\ & = & [\![\phi]\!]F & \text{by Proposition 7.4.6} \end{array}$$

and hence $[\![\phi]\!]E \leq [\![\phi]\!]F$ for all $\phi \in \mathtt{HML}_{\mathrm{nd}}^{\langle\varepsilon\rangle}$. To show $[\![\psi]\!]E \leq [\![\psi]\!]F$ for all $\psi \in \mathtt{HML}_{\mathrm{nd}}^{[\varepsilon]}$ follows a similar argument using Proposition 7.4.7 instead of Proposition 7.4.6.

Conversely, suppose $E, F \in \mathcal{R}^{\mathrm{nd}}$ and $[\![\phi]\!]E \leq [\![\phi]\!]F$ for all $\phi \in \mathtt{HML}_{\mathrm{nd}}^{\langle\varepsilon\rangle}$ and $[\![\psi]\!]E \leq [\![\psi]\!]F$ for all $\psi \in \mathtt{HML}_{\mathrm{nd}}^{[\varepsilon]}$, then for any $t \in \mathtt{T}^{\mathrm{nd}}$:

$$\begin{array}{rcll} \mathsf{N}_{\mathbf{lub}}(E)(t) & = & [\![\phi_t]\!]E & \text{by Proposition 7.4.4} \\ & \leq & [\![\phi_t]\!]F & \text{by hypothesis} \\ & = & \mathsf{N}_{\mathbf{lub}}(F)(t) & \text{by Proposition 7.4.4.} \end{array}$$

Similarly using Proposition 7.4.5, we can show $\mathsf{N}_{\mathbf{glb}}(E)(t) \leq \mathsf{N}_{\mathbf{glb}}(F)(t)$, and since this was for arbitrary $t \in \mathtt{T}^{\mathrm{nd}}$, we get $E \sqsubseteq^{\mathsf{nd}} F$ as required. □

7.5 Reactive Probabilistic Transition Systems

To consider reactive probabilistic transition systems we first extend the interpretation of $\langle\varepsilon\rangle\phi$ from non-deterministic probabilistic transition systems to reactive probabilistic transition systems as follows. For any reactive probabilistic transition system $(\mathcal{R}, \mathcal{A}ct, \rightarrow)$ and $E \in \mathcal{R}$:

$$[\![\langle\varepsilon\rangle\phi]\!]E \stackrel{def}{=} \max\{[\![\phi]\!]S \mid E \rightarrow S\}$$

since E makes an internal choice between behaving as any $S \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathcal{R}))$ such that $E \rightarrow S$.

Again, we can consider the dual of $\langle\varepsilon\rangle\phi$, namely $[\varepsilon]\phi$, and we reach the interpretation of $[\varepsilon]\phi$ over reactive probabilistic transition systems by means of the following proposition.

Proposition 7.5.1 *For all $E \in \mathcal{R}$ and $\phi \in$ HML: $[\![[\varepsilon]\phi]\!]E = \min\{[\![\phi]\!]S \mid E \rightarrow S\}$.*

Furthermore, since any $S \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathcal{R}))$ can be considered as a deterministic probabilistic process, for any $S \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathcal{R}))$ we set:

$$[\![\langle\varepsilon\rangle\phi]\!]S \stackrel{def}{=} [\![\phi]\!]S \quad \text{and} \quad [\![[\varepsilon]\phi]\!]S \stackrel{def}{=} [\![\phi]\!]S.$$

Furthermore, $[\![\langle a\rangle\phi]\!]S$ has the same interpretation as when we considered deterministic probabilistic transition systems.

We next combine the sublanguages of HML, $\mathtt{HML_d}$ and $\mathtt{HML}_{\mathrm{nd}}^{\langle\varepsilon\rangle}$, and $\mathtt{HML_d}$ and $\mathtt{HML}_{\mathrm{nd}}^{[\varepsilon]}$ to form the following two sublanguages of HML.

Definition 7.5.2 *The sublanguage $\mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$ of* HML *is the language defined inductively on the syntax:*

$$\phi \ ::= \ \mathtt{true} \mid \langle\varepsilon\rangle\langle a\rangle\phi \mid \phi \wedge \phi \mid \langle\varepsilon\rangle(\phi \wedge \phi)$$

where, for any ϕ_1 and $\phi_2 \in \mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$, $\phi_1 \wedge \phi_2$ and $\langle\varepsilon\rangle(\phi_1 \wedge \phi_2)$ exists in $\mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$ if and only if $\mathrm{a}ct(\phi_1) \cap \mathrm{a}ct(\phi_2) = \emptyset$.

Definition 7.5.3 *The sublanguage $\mathtt{HML}_{\mathrm{r}}^{[\varepsilon]}$ of* HML *is the language defined inductively on the syntax:*

$$\psi \ ::= \ \mathtt{true} \mid [\varepsilon]\langle a\rangle\psi \mid \psi \wedge \psi \mid [\varepsilon](\psi \wedge \psi)$$

where, for any ψ_1 and $\psi_2 \in \mathtt{HML}_{\mathrm{r}}^{[\varepsilon]}$, $\psi_1 \wedge \psi_2$ and $[\varepsilon](\psi_1 \wedge \psi_2)$ exists in $\mathtt{HML}_{\mathrm{r}}^{[\varepsilon]}$ if and only if $\mathrm{a}ct(\psi_1) \cap \mathrm{a}ct(\psi_2) = \emptyset$.

Before we consider the relationship between $\mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$ and $\mathsf{R_{lub}}$ and between $\mathtt{HML}_{\mathrm{r}}^{[\varepsilon]}$ and $\mathsf{R_{glb}}$, we first prove the following lemmas.

Lemma 7.5.4 *For any* $\{\phi_1, \ldots, \phi_m\} \subseteq \mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$, *if* $\mathrm{a}ct(\phi_i) \cap \mathrm{a}ct(\phi_j) = \emptyset$ *for all* $1 \leq i \leq m$ *then there exists* $\phi \in \mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$ *such that*

$$\mathrm{a}ct(\phi) = \bigcup_{i=1}^{m} \mathrm{a}ct(\phi_i), \quad [\![\phi]\!]E = \left[\!\!\left[\langle\varepsilon\rangle \left(\bigwedge_{i=1}^{m} \phi_i\right)\right]\!\!\right] E \quad \textit{and} \quad [\![\phi]\!]S = \left[\!\!\left[\bigwedge_{i=1}^{m} \phi_i\right]\!\!\right] S$$

for all $E \in \mathcal{R}$ *and* $S \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathcal{R}))$.

Proof. The proof is by induction on $m \in \mathbb{N}$. The case for $m = 1$ follows by definition of $\mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$ and $[\![\cdot]\!]$.

Now suppose the lemma holds for some $m \in \mathbb{N}$ and consider any $\{\phi_1, \ldots, \phi_{m+1}\} \subseteq \mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$ such that $\mathrm{a}ct(\phi_i) \cap \mathrm{a}ct(\phi_j)$ for all $1 \leq i \leq m+1$. Then by induction there exists $\phi' \in \mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$ such that:

$$\mathrm{a}ct(\phi') = \bigcup_{i=1}^{m} \mathrm{a}ct(\phi_i), \quad [\![\phi']\!]E = \left[\!\!\left[\langle\varepsilon\rangle \left(\bigwedge_{i=1}^{m} \phi_i\right)\right]\!\!\right] E \quad \text{and} \quad [\![\phi']\!]S = \left[\!\!\left[\bigwedge_{i=1}^{m} \phi_i\right]\!\!\right] S$$

for all $E \in \mathcal{R}$ and $S \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathcal{R}))$. Now setting:

$$\phi = \langle\varepsilon\rangle\,(\phi' \wedge \phi_{m+1})$$

it follows that $\phi \in \mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$ by the induction hypothesis and since $\mathrm{a}ct(\phi_i) \cap \mathrm{a}ct(\phi_j)$ for all $1 \leq i \leq m+1$. Furthermore, by definition of $[\![\cdot]\!]$, for any $S \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathcal{R}))$:

$$\begin{aligned}
[\![\phi]\!]S &= [\![\phi' \wedge \phi_{m+1}]\!]S \\
&= [\![\phi']\!]S \cdot [\![\phi_{m+1}]\!]S \\
&= \left[\!\!\left[\bigwedge_{i=1}^{m} \phi_i\right]\!\!\right] S \cdot [\![\phi_{m+1}]\!]S && \text{by induction} \\
&= \left[\!\!\left[\bigwedge_{i=1}^{m+1} \phi_i\right]\!\!\right] S && \text{by definition of } [\![\cdot]\!].
\end{aligned}$$

Then, for any $E \in \mathcal{R}$:

$$\begin{aligned}
[\![\phi]\!]E &= \max_{E \to S} [\![\phi' \wedge \phi_{m+1}]\!]S && \text{by definition of } [\![\cdot]\!] \\
&= \max_{E \to S} \left[\!\!\left[\bigwedge_{i=1}^{m+1} \phi_i\right]\!\!\right] S && \text{from above} \\
&= \left[\!\!\left[\langle\varepsilon\rangle \left(\bigwedge_{i=1}^{m+1} \phi_i\right)\right]\!\!\right] E && \text{by definition of } [\![\cdot]\!]
\end{aligned}$$

and hence the lemma is proved by induction on $n \in \mathbb{N}$. $\square$

Lemma 7.5.5 *For any* $\{\psi_1, \dots, \psi_m\} \subseteq \mathtt{HML}_{\mathrm{r}}^{[\varepsilon]}$*, if* $\mathrm{act}(\psi_i) \cap \mathrm{act}(\psi_j) = \emptyset$ *for all* $1 \leq i \leq m$ *then there exists* $\psi \in \mathtt{HML}_{\mathrm{r}}^{[\varepsilon]}$ *such that*

$$\mathrm{act}(\psi) = \bigcup_{i=1}^{m} \mathrm{act}(\psi_i), \quad [\![\psi]\!]E = \left[\!\!\left[[\varepsilon] \left(\bigwedge_{i=1}^{m} \psi_i \right) \right]\!\!\right] E \quad \text{and} \quad [\![\psi]\!]S = \left[\!\!\left[\bigwedge_{i=1}^{m} \psi_i \right]\!\!\right] S$$

for all $E \in \mathcal{R}$ *and* $S \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathcal{R}))$*.*

Proof. The proof follows similarly to Lemma 7.5.4 above replacing max by min, and $\langle\varepsilon\rangle$ by $[\varepsilon]$. □

Using Lemma 7.5.4 and Lemma 7.5.5, we are now in a position to state a connection between the map $\mathsf{R}_{\mathbf{glb}}$ and $\mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$, and between the map $\mathsf{R}_{\mathbf{lub}}$ and $\mathtt{HML}_{\mathrm{r}}^{[\varepsilon]}$.

Proposition 7.5.6 *For all* $t \in \mathtt{T}$ *there exists* $\phi_t \in \mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$ *such that for all* $E \in \mathcal{R}$*,* $[\![\phi_t]\!]E = \mathsf{R}_{\mathbf{lub}}(E)(t)$*, and if* t *is of the form* $(\![[a_1.T_1, \dots, a_m.T_m]]\!)$ *then* $\mathrm{act}(\phi_t) = \{a_1, \dots, a_m\}$*.*

Proof. The proposition is proved by induction on $t \in \mathtt{T}$, where for any $(\![r]\!) \in \mathtt{T}$, if $r = \perp$ we set $\phi_t = \mathtt{true}$, and if $r = [a_1.T_1, \dots, a_m.T_m]$ using Lemma 7.5.4 we set ϕ_t to the formula of $\mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$ such that:

$$[\![\phi_t]\!]E = \left[\!\!\left[\langle\varepsilon\rangle \left(\bigwedge_{i=1}^{m} (\langle a_i \rangle \phi_{T_i}) \right) \right]\!\!\right] E$$

for all $E \in \mathcal{R}$, where $\phi_{T_i} = \bigwedge_{j=1}^{m_i} \phi_{t_j^i}$ if $T_i = (t_1^i, \dots, t_{m_i}^i)$. □

Proposition 7.5.7 *For all* $t \in \mathtt{T}$ *there exists* $\psi_t \in \mathtt{HML}_{\mathrm{r}}^{[\varepsilon]}$ *such that for all* $E \in \mathcal{R}$*,* $[\![\psi_t]\!]E = \mathsf{R}_{\mathbf{glb}}(E)(t)$ *and if* t *is of the form* $(\![[a_1.T_1, \dots, a_m.T_m]]\!)$ *then* $\mathrm{act}(\psi_t) = \{a_1, \dots, a_m\}$*.*

Proof. The proposition is proved by induction on $t \in \mathtt{T}_n$ similarly to Proposition 7.5.6 above using Proposition 7.5.1 and replacing $\langle\varepsilon\rangle$ with $[\varepsilon]$. □

Proposition 7.5.8 *For all* $\phi \in \mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$ *there exists* $(\![r_\phi]\!) \in \mathtt{T}$ *and* $T_\phi \in \mathtt{T}_\omega$ *such that* $[\![\phi]\!]S = \mathsf{R}_{\mathbf{lub}}(S)(r_\phi)$ *for all* $S \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathcal{R}))$*, and* $[\![\phi]\!]E = \mathsf{R}_{\mathbf{lub}}(E)(T_\phi)$ *for all* $E \in \mathcal{R}$*.*

Proof. The proof follows by induction on $n \in \mathbb{N}$, where n is the height of formulae of $\mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$, by combining the proofs of Proposition 7.3.3 and Proposition 7.4.6 and using

Lemma 4.5.10 and Lemma 4.5.11 instead of Lemma 4.3.6 and Lemma 4.4.6, and for any $\phi \in \mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$ putting:

$$r_\phi = \begin{cases} \bot & \text{if } \phi = \mathtt{true} \\ [a.T_{\phi'}] & \text{if } \phi = \langle\varepsilon\rangle\langle a\rangle\phi' \\ r_{\phi_1} \,\|\, r_{\phi_2} & \text{if } \phi = \phi_1 \wedge \phi_2 \\ r_{\phi_1} \,\|\, r_{\phi_2} & \text{if } \phi = \langle\varepsilon\rangle(\phi_1 \wedge \phi_2) \end{cases}$$

and

$$T_\phi = \begin{cases} (\llparenthesis\bot\rrparenthesis) & \text{if } \phi = \mathtt{true} \\ (\llparenthesis[a.T_{\phi'}]\rrparenthesis) & \text{if } \phi = \langle\varepsilon\rangle\langle a\rangle\phi' \\ T_{\phi_1} \,\|\, T_{\phi_2} & \text{if } \phi = \phi_1 \wedge \phi_2 \\ (\llparenthesis r_{\phi_1} \,\|\, r_{\phi_2}\rrparenthesis) & \text{if } \phi = \langle\varepsilon\rangle(\phi_1 \wedge \phi_2). \end{cases}$$

□

Proposition 7.5.9 *For all $\psi \in \mathtt{HML}_{\mathrm{r}}^{[\varepsilon]}$ there exists $\llparenthesis r_\psi \rrparenthesis \in \mathtt{T}$ and $T_\psi \in \mathtt{T}_\omega$ such that $[\![\psi]\!]S = \mathsf{R}_{\mathbf{glb}}(S)(r_\psi)$ for all $S \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathcal{R}))$ and $[\![\psi]\!]E = \mathsf{R}_{\mathbf{glb}}(E)(T_\psi)$ for all $E \in \mathcal{R}$.*

Proof. The proof follows similarly to Proposition 7.5.8. □

We now give some examples of the mappings between the testing language $\mathtt{T}_\omega$ and the logics $\mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$ and $\mathtt{HML}_{\mathrm{r}}^{[\varepsilon]}$, by means of the following table.

$\mathtt{T}_\omega$	$\mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$	$\mathtt{HML}_{\mathrm{r}}^{[\varepsilon]}$
$(\llparenthesis[a.\llparenthesis[b.\bot]\rrparenthesis]\rrparenthesis)$	$\langle\varepsilon\rangle\langle a\rangle\langle\varepsilon\rangle\langle b\rangle\mathtt{true}$	$[\varepsilon]\langle a\rangle[\varepsilon]\langle b\rangle\mathtt{true}$
$(\llparenthesis[a.\bot]\rrparenthesis, \llparenthesis[b.\bot]\rrparenthesis)$	$\langle\varepsilon\rangle\langle a\rangle\mathtt{true} \wedge \langle\varepsilon\rangle\langle b\rangle\mathtt{true}$	$[\varepsilon]\langle a\rangle\mathtt{true} \wedge [\varepsilon]\langle b\rangle\mathtt{true}$
$(\llparenthesis[a.\bot, b.\bot]\rrparenthesis)$	$\langle\varepsilon\rangle(\langle\varepsilon\rangle\langle a\rangle\mathtt{true} \wedge \langle\varepsilon\rangle\langle b\rangle\mathtt{true})$	$[\varepsilon]([\varepsilon]\langle a\rangle\mathtt{true} \wedge ([\varepsilon]\langle b\rangle\mathtt{true})$

Finally, using Proposition 7.5.6, Proposition 7.5.7, Proposition 7.5.8 and Proposition 7.5.9 we reach the following theorem connecting $\mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle} \cup \mathtt{HML}_{\mathrm{r}}^{[\varepsilon]}$ and $\sqsubseteq^{\mathsf{r}}$.

Theorem 7.5.10 *For all $E, F \in \mathcal{R}$, $E \sqsubseteq^{\mathsf{r}} F$ if and only if $[\![\phi]\!]E \leq [\![\phi]\!]F$ for all $\phi \in \mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$ and $[\![\psi]\!]E \leq [\![\psi]\!]F$ for all $\psi \in \mathtt{HML}_{\mathrm{r}}^{[\varepsilon]}$.*

Proof. The proof follows similarly to Theorem 7.4.8 using Lemma 4.5.5. □

7.6 Fixed Point Operators

In this section we add a fixed point operator to the logics $\mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$ and $\mathtt{HML}_{\mathrm{r}}^{[\varepsilon]}$ and compare the results with our maps $\mathsf{R}_{\mathbf{lub}}$ and $\mathsf{R}_{\mathbf{glb}}$ respectively. We note that we only prove results relating to $\mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$ and $\mathsf{R}_{\mathbf{lub}}$, as the results for $\mathtt{HML}_{\mathrm{r}}^{[\varepsilon]}$ and $\mathsf{R}_{\mathbf{glb}}$ are dual.

To add a fixed point operator to our logic we must first add variables (ranged over by $\mathtt{Var}$) to the syntax of $\mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$and extend the definition of $\mathrm{h}t$ by setting $\mathrm{h}t(x) = 0$ for any $x \in \mathtt{Var}$. To compare the tests of $\mathtt{T}$ to fixed point operators of $\mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$, we construct *unfoldings* of formulae, and using the map between formulae of $\mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$ and $\mathtt{T}$ given in Proposition 7.5.8 we then consider these unfoldings as elements of our testing language. Formally, we have the following definitions.

Definition 7.6.1 *For any $\phi \in \mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$, let $(\!|r_\phi|\!) \in \mathtt{T}$ and $T_\phi \in \mathtt{T}_\omega$ be the tests defined by induction on the height of ϕ as follows:*

$$r_\phi = \begin{cases} \bot & \text{if } \phi = \mathtt{true} \\ [a.T_{\phi'}] & \text{if } \phi = \langle\varepsilon\rangle\langle a\rangle\phi' \\ r_{\phi_1} \parallel r_{\phi_2} & \text{if } \phi = \phi_1 \wedge \phi_2 \text{ or } \phi = \langle\varepsilon\rangle(\phi_1 \wedge \phi_2) \end{cases}$$

$$\text{and} \quad T_\phi = \begin{cases} ((\!|\bot|\!)) & \text{if } \phi = \mathtt{true} \\ ((\!|[a.T_{\phi'}]|\!)) & \text{if } \phi = \langle\varepsilon\rangle\langle a\rangle\phi' \\ T_{\phi_1} \parallel T_{\phi_2} & \text{if } \phi = \phi_1 \wedge \phi_2 \\ ((\!|r_{\phi_1} \parallel r_{\phi_2}|\!)) & \text{if } \phi = \langle\varepsilon\rangle(\phi_1 \wedge \phi_2). \end{cases}$$

Definition 7.6.2 *For all $\phi \in \mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$ and $x \in \mathtt{Var}$, we define ϕ_x^n by induction on $n \in \mathbb{N}$ as follows: $\phi_x^0 = \mathtt{true}$ and $\phi_x^{n+1} = \phi\{\phi_x^n/x\}$.*

Using the sequence of formulae given in Definition 7.6.2 and the map between formulae and tests given in Definition 7.6.1, we reach the following sequences of tests $\langle r_{\phi_x}^n\rangle_{n\in\mathbb{N}}$, $\langle T_{\phi_x}^n\rangle_{n\in\mathbb{N}}$. Considering these unfolding with respect to the map $\mathsf{R}_{\mathbf{lub}}$, we have the following lemma and proposition. Its importance is that successive unfoldings improve the probability upper bound obtained with the help of the map $\mathsf{R}_{\mathbf{lub}}$.

Lemma 7.6.3 *If $\phi, \theta_1, \theta_2 \in \mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$ and $x \in \mathtt{Var}$ such that $\mathsf{R}_{\mathbf{lub}}(S)(r_{\theta_1}) \leq \mathsf{R}_{\mathbf{lub}}(S)(r_{\theta_2})$ and $\mathsf{R}_{\mathbf{lub}}(E)(T_{\theta_1}) \leq \mathsf{R}_{\mathbf{lub}}(E)(T_{\theta_2})$ for all $S \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathcal{R}))$ and $E \in \mathcal{R}$, then $\mathsf{R}_{\mathbf{lub}}(S)(r_{\phi\{\theta_1/x\}}) \leq \mathsf{R}_{\mathbf{lub}}(S)(r_{\phi\{\theta_2/x\}})$ and $\mathsf{R}_{\mathbf{lub}}(E)(T_{\phi\{\theta_1/x\}}) \leq \mathsf{R}_{\mathbf{lub}}(E)(T_{\phi\{\theta_2/x\}})$ for all $S \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathcal{R}))$ and $E \in \mathcal{R}$.*

Proof. The proof follows by induction on $n \in \mathbb{N}$, where n is the height of the formula $\phi \in \mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$. □

Proposition 7.6.4 *For all $S \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathcal{R}))$, $E \in \mathcal{R}$, $\phi, \theta \in \mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$ and $x \in \mathtt{Var}$: $\mathsf{R}_{\mathbf{lub}}(S)(r_{\theta\{\phi_x^{n+1}/x\}}) \leq \mathsf{R}_{\mathbf{lub}}(S)(r_{\theta\{\phi_x^n/x\}})$ and $\mathsf{R}_{\mathbf{lub}}(E)(T_{\theta\{\phi_x^{n+1}/x\}}) \leq \mathsf{R}_{\mathbf{lub}}(E)(T_{\theta\{\phi_x^n/x\}})$.*

Proof. The proof is by induction on the height of θ, where we suppose the only variable in θ is x. If $\theta \in \mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$ and $\mathrm{h}t(\phi) = 0$, then by hypothesis we have the following two cases to consider.

1. If $\theta = \texttt{true}$, then $\theta\{\phi_x^n/x\} = \texttt{true}$ for all $n \in \mathbb{N}$, and hence the lemma holds.

2. If $\theta \in \texttt{Var}$, then by the hypothesis $\theta = x$, and in this case we prove the lemma by induction on $n \in \mathbb{N}$. We only consider the case for $S \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathcal{R}))$ since the case for $E \in \mathcal{R}$ follows similarly. If $n = 0$ then since $\theta = x$ for any $S \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathcal{R}))$:

$$\begin{array}{rcll} \mathsf{R}_{\mathbf{lub}}(S)(r_{\theta\{\phi_x^1/x\}}) & = & \mathsf{R}_{\mathbf{lub}}(S)(r_{\phi_x^1}) & \\ & \leq & 1 & \text{by construction of } \mathsf{R}_{\mathbf{lub}} \\ & = & \mathsf{R}_{\mathbf{lub}}(S)(\bot) & \text{by definition of } \mathsf{R}_{\mathbf{lub}} \\ & = & \mathsf{R}_{\mathbf{lub}}(S)(r_{\texttt{true}}) & \text{by Definition 7.6.1} \\ & = & \mathsf{R}_{\mathbf{lub}}(S)(r_{\theta\{\phi_x^0/x\}}) & \text{by Definition 7.6.2.} \end{array}$$

Now suppose the lemma holds for some $n \in \mathbb{N}$, then similarly to the above we have:

$$\begin{array}{rcll} \mathsf{R}_{\mathbf{lub}}(S)(r_{\theta\{\phi_x^{n+2}/x\}}) & = & \mathsf{R}_{\mathbf{lub}}(S)(r_{\phi_x^{n+2}}) & \\ & = & \mathsf{R}_{\mathbf{lub}}(S)(r_{\phi\{\phi_x^{n+1}/x\}}) & \text{by Definition 7.6.2} \\ & \leq & \mathsf{R}_{\mathbf{lub}}(S)(r_{\phi\{\phi_x^{n}/x\}}) & \text{by induction and Lemma 7.6.3} \\ & = & \mathsf{R}_{\mathbf{lub}}(S)(r_{\phi_x^{n+1}}) & \text{by Definition 7.6.2} \\ & = & \mathsf{R}_{\mathbf{lub}}(S)(r_{\theta\{\phi_x^{n+1}/x\}}) & \text{since } \theta = x. \end{array}$$

Then, since these are all the possible cases, the lemma holds for all formulae of height 0.

Now suppose the lemma holds for all formulae of $\texttt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$ of height less than or equal to some $k \in \mathbb{N}$. Consider any $\theta \in \texttt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$ of height $k+1$. Then we have the following three cases to consider.

1. If $\theta = \langle\varepsilon\rangle\langle a\rangle\theta'$ for some $a \in \mathcal{A}ct$ and $\theta' \in \texttt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$ of height k, then by Definition 7.6.1 for any $n \in \mathbb{N}$:

$$T_{\theta\{\phi_x^n/x\}} = (\!(r_{\theta\{\phi_x^n/x\}})\!) = (\!([a.T_{\theta'\{\phi_x^n/x\}}])\!) \tag{7.1}$$

Therefore, if we consider any $S \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathcal{R}))$ then either $(a, \pi) \notin S$ for all $\pi \in \mu(\mathcal{R})$ and by definition of $\mathsf{R}_{\mathbf{lub}}$ for any $n \in \mathbb{N}$:

$$\mathsf{R}_{\mathbf{lub}}(S)([a.T_{\theta'\{\phi_x^n/x\}}]) = 0,$$

or $(a, \pi) \in S$ for some $\pi \in \mu(\mathcal{R})$, and in this case by definition of $\mathsf{R}_{\mathbf{lub}}$ for any $n \in \mathbb{N}$:

$$\begin{array}{rcll} \mathsf{R}_{\mathbf{lub}}(S)([a.T_{\theta'\{\phi_x^{n+1}/x\}}]) & = & \sum_{F \in \mathcal{R}} \pi(F) \cdot \mathsf{R}_{\mathbf{lub}}(F)(T_{\theta'\{\phi_x^{n+1}/x\}}) & \\ & \leq & \sum_{F \in \mathcal{R}} \pi(F) \cdot \mathsf{R}_{\mathbf{lub}}(F)(T_{\theta'\{\phi_x^{n}/x\}}) & \text{by induction} \\ & = & \mathsf{R}_{\mathbf{lub}}(S)([a.T_{\theta'\{\phi_x^n/x\}}]) & \text{by definition of } \mathsf{R}_{\mathbf{lub}}. \end{array}$$

Putting this together and using (7.1) we have:

$$\mathsf{R}_{\mathbf{lub}}(S)(r_{\theta\{\phi_x^{n+1}/x\}}) \leq \mathsf{R}_{\mathbf{lub}}(S)(r_{\theta\{\phi_x^{n}/x\}}) \tag{7.2}$$

for all $S \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathcal{R}))$. Then for any $E \in \mathcal{R}$ and $n \in \mathbb{N}$:

$$\begin{array}{rcll} \mathsf{R}_{\mathbf{lub}}(E)(T_{\theta\{\phi_x^{n+1}/x\}}) & = & \mathsf{R}_{\mathbf{lub}}(E)(((\![a.T_{\theta\{\phi_x^n/x\}}]\!))) & \text{by (7.1)} \\ & = & \max_{E \to S} \mathsf{R}_{\mathbf{lub}}(S)(r_{\theta\{\phi_x^{n+1}/x\}}) & \text{by definition of } \mathsf{R}_{\mathbf{lub}} \\ & \leq & \max_{E \to S} \mathsf{R}_{\mathbf{lub}}(S)(r_{\theta\{\phi_x^{n}/x\}}) & \text{by (7.2)} \\ & = & \mathsf{R}_{\mathbf{lub}}(E)(T_{\theta\{\phi_x^{n}/x\}}) & \text{by definition of } \mathsf{R}_{\mathbf{lub}}. \end{array}$$

2. If $\theta = \theta_1 \wedge \theta_2$ for some $\theta_1, \theta_2 \in \mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$ of height less than or equal to k, then for all $n \in \mathbb{N}$ by Definition 7.6.1 we reach:

$$r_{\theta\{\phi_x^n/x\}} = r_{\theta_1\{\phi_x^n/x\}} \,\|\, r_{\theta_2\{\phi_x^n/x\}}. \tag{7.3}$$

Therefore, for any $S \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathcal{R}))$ and $n \in \mathbb{N}$, by (7.3) and Lemma 4.5.10:

$$\begin{array}{rll} \mathsf{R}_{\mathbf{lub}}(S)(r_{\theta\{\phi_x^{n+1}/x\}}) = & \mathsf{R}_{\mathbf{lub}}(S)(r_{\theta_1\{\phi_x^{n+1}/x\}}) \cdot \mathsf{R}_{\mathbf{lub}}(S)(r_{\theta_2\{\phi_x^{n+1}/x\}}) & \\ \leq & \mathsf{R}_{\mathbf{lub}}(S)(r_{\theta_1\{\phi_x^{n}/x\}}) \cdot \mathsf{R}_{\mathbf{lub}}(S)(r_{\theta_2\{\phi_x^{n}/x\}}) & \text{by induction} \\ = & \mathsf{R}_{\mathbf{lub}}(S)(r_{\theta_1\{\phi_x^{n}/x\}} \,\|\, r_{\theta_2\{\phi_x^{n}/x\}}) & \text{by Lemma 4.5.10} \\ = & \mathsf{R}_{\mathbf{lub}}(S)(r_{\theta\{\phi_x^{n}/x\}}) & \text{by (7.3).} \end{array}$$

Furthermore, similarly to the above using Lemma 4.5.11 instead of Lemma 4.5.10, for any $E \in \mathcal{R}$:

$$\mathsf{R}_{\mathbf{lub}}(E)(T_{\theta\{\phi_x^{n+1}/x\}}) \leq \mathsf{R}_{\mathbf{lub}}(E)(T_{\theta\{\phi_x^{n}/x\}}).$$

3. If $\theta = \langle\varepsilon\rangle(\theta_1 \wedge \theta_2)$, then for any $S \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathcal{R}))$ by Definition 7.6.1 similarly to case 2. we can show that for all $n \in \mathbb{N}$:

$$\mathsf{R}_{\mathbf{lub}}(S)(r_{\theta\{\phi_x^{n+1}/x\}}) \leq \mathsf{R}_{\mathbf{lub}}(S)(r_{\theta\{\phi_x^{n}/x\}}).$$

Then since this was for any $S \in \mathcal{P}_{fr}(\mathcal{A}ct \times \mu(\mathcal{R}))$ and $T_{\theta\{\phi_x^{n+1}/x\}} = (\!|r_{\theta\{\phi_x^{n+1}/x\}}|\!)$ by Definition 7.6.1, we have for any $E \in \mathcal{R}$:

$$\mathsf{R}_{\mathbf{lub}}(E)(T_{\theta\{\phi_x^{n+1}/x\}}) \leq \mathsf{R}_{\mathbf{lub}}(E)(T_{\theta\{\phi_x^{n}/x\}})$$

similarly to the first case.

Since these are all the possible cases the lemma holds by induction on the height of formulae of $\mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$. $\square$

Corollary 7.6.5 *For all $\phi \in \mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$, $x \in \mathtt{Var}$ and $E \in \mathcal{R}$, the limit $\lim_{n\to\infty} \mathsf{R}_{\mathbf{lub}}(E)(T^n_{\phi_x})$ exists and is in the interval* $[0,1]$.

Proof. If we consider any $\phi \in \mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$, then using Proposition 7.6.4 letting $\theta = \phi$, we have $\langle \mathsf{R}_{\mathbf{lub}}(E)(T^n_{\phi_x})\rangle_{n\in\mathbb{N}}$ is a decreasing sequence in the interval $[0,1]$, and hence the (unique) limit exists and is in the interval $[0,1]$. □

Using Corollary 7.6.5 and Huth and Kwiatkowska's interpretation of the greatest fixed point operator, in fact the value of $\lim_{n\to\infty} \mathsf{R}(E)(T^n_{\phi_x})$ corresponds to that of the greatest fixed point operator, that is, for any $\phi \in \mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$ and $E \in \mathcal{R}$:

$$[\![\nu x.\phi]\!]E = \lim_{n\to\infty} \mathsf{R}_{\mathbf{lub}}(E)(T^n_{\phi_x}).$$

The connection with the greatest, as opposed to the least, fixed point operator arises from the fact that there is no test representing `false` in our testing language $\mathtt{T}$, and hence we must begin all iterations from `true` (that is, $(\!|\bot|\!)$), and since $\mathsf{R}_{\mathbf{lub}}(E)(T) \leq 1$ for all $E \in \mathcal{R}$ and $T \in \mathtt{T}_\omega$, any monotone sequence we construct will either be constant at 1 or *decreasing*. Hence, the limit corresponds with the greatest fixed point. To give an example of the values of $[\![\nu x.\phi]\!]E$ consider the recursive probabilistic processes given in Figure 7.1 below.

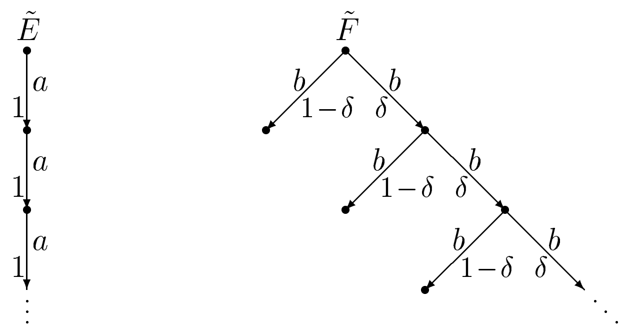


Figure 7.1: Examples of recursive probabilistic processes.

Then, by simple calculations we have:

$$[\![\nu x.\langle\varepsilon\rangle\langle a\rangle x]\!]\tilde{E} = [\![\nu x.[\varepsilon]\langle a\rangle x]\!]\tilde{E} = 1 \quad \text{and}$$

$$[\![\nu x.\langle\varepsilon\rangle\langle b\rangle x]\!]\tilde{F} = [\![\nu x.[\varepsilon]\langle b\rangle x]\!]\tilde{F} = \lim_{n\to\infty} \delta^n = \begin{cases} 1 & \text{if } \delta = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Unlike the above, the values of the greatest fixed point operator with respect to the formulae of $\mathtt{HML}_{\mathrm{r}}^{\langle\varepsilon\rangle}$ and $\mathtt{HML}_{\mathrm{r}}^{[\varepsilon]}$ may differ in the case of processes with non-deterministic behaviour. Suppose that $\tilde{G}$ is the process that makes an internal choice between behaving as $\tilde{E}$ and $\tilde{F}$ in Figure 7.1. If $a \neq b$, then we have:

$$[\![\nu x.\langle\varepsilon\rangle\langle a\rangle x]\!]\tilde{G} = 1, \quad [\![\nu x.\langle\varepsilon\rangle\langle b\rangle x]\!]\tilde{G} = \begin{cases} 1 & \text{if } \delta = 1 \\ 0 & \text{otherwise.} \end{cases}$$

$$\text{and} \quad [\![\nu x.[\varepsilon]\langle a\rangle x]\!]\tilde{G} = [\![\nu x.[\varepsilon]\langle b\rangle x]\!]\tilde{G} = 0.$$

On the other hand, if $a = b$ then:

$$[\![\nu x.\langle\varepsilon\rangle\langle a\rangle x]\!]\tilde{G} = 1 \text{ and } [\![\nu x.[\varepsilon]\langle a\rangle x]\!]\tilde{G} = \begin{cases} 1 & \text{if } \delta = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Comparing this with the classical interpretation of $\nu x.\langle a\rangle x$, which means there exists an infinite path of a actions, intuitively the pair of values

$$\left[[\![\nu x.[\varepsilon]\langle a\rangle]\!]\tilde{G}, [\![\nu x.\langle\varepsilon\rangle\langle a\rangle]\!]\tilde{G}\right]$$

corresponds to the interval containing the probability that $\tilde{G}$ will perform an infinite path of a actions.

We conclude this chapter by noting a result of some interest: if we restrict ourselves to any deterministic probabilistic transition system $(\mathcal{R}^{\mathrm{d}}, \mathcal{A}ct, \rightarrow)$, then adding negation to the logic $\mathtt{HML}_{\mathrm{d}}$ to form $\mathtt{HML}_{\mathrm{d}}^{\neg}$ does not influence the equivalence induced from the logic, in the sense that the obtained equivalence will still correspond to our equivalence $\overset{\mathsf{d}}{\sim}$ over deterministic probabilistic transition systems, and also over any purely probabilistic transition system. The proof of this follows by Proposition 7.3.2 and replacing Proposition 7.3.3 by the following proposition, which is proved by induction on the height of formulae of $\mathtt{HML}_{\mathrm{d}}^{\neg}$.

Proposition 7.6.6 *If $\phi \in \mathtt{HML}_{\mathrm{d}}^{\neg}$ then there exists $\mathbf{T} \subseteq \mathtt{T}_{\omega}^{\mathrm{d}}$ and $\Delta_\phi : \mathbf{T} \rightarrow \{-1, +1\}$ such that:*

$$\textit{either} \quad [\![\phi]\!]E = \sum_{T \in \mathbf{T}} \Delta_\phi(T) \cdot \mathsf{D}(E)(T) \qquad \textit{for all } E \in \mathcal{R}^{\mathrm{d}}$$

$$\textit{or} \quad [\![\phi]\!]E = 1 - \sum_{T \in \mathbf{T}} \Delta_\phi(T) \cdot \mathsf{D}(E)(T) \quad \textit{for all } E \in \mathcal{R}^{\mathrm{d}}.$$

Chapter 8

Conclusions

In this thesis we first presented an equivalence for reactive probabilistic processes based on testing which aims only to distinguish processes with observably different behaviour. This equivalence does not distinguish between when probabilistic choices occur, which as discussed in Section 2.4 we feel is unimportant as neither processes nor the environment can influence the choice made. On the other hand, our equivalence does capture the difference in the behaviour of processes with respect to other forms of choice, that is external and internal choices, which we feel is important since these can be influenced by both processes and the environment. To some users, the time at which internal choices are made is unimportant since the environment has no control over which alternative is chosen. Our equivalence is intended to be the "finest" equivalence which can realistically be based on the observable behaviour of processes, that is, one based only on the outcome of *single* runs of processes potentially under different conditions (for example, changes in the environment or different internal choices made) but by varying the test language we can also derive other equivalences. For example, by weakening our testing language we can construct an equivalence which will abstract away from the time at which internal choices are made (in fact, we have already given a definition of the functions that will induce such an equivalence, namely $\mathsf{D}_{\mathsf{glb}}$ and $\mathsf{D}_{\mathsf{lub}}$ as given in Section 4.5). Furthermore, by placing suitable restrictions on the construction of composite tests, that is, those of the form $(t, \ldots, t)$ in our testing language, we will derive both a "trace" equivalence (by removing all occurrences of the construct) and a "failure/ready" equivalence (by only allowing this construct at the final step).

Next we constructed a process calculus for reactive probabilistic processes for which we have shown that our equivalence is a congruence. Returning to the discussion above, if we consider the weaker equivalences induced from the mappings $\mathsf{D}_{\mathsf{glb}}$ and $\mathsf{D}_{\mathsf{lub}}$ (the trace and failure/ready equivalences) then we can show them to be congruences for our process calculus.

As discussed in Section 2.4, we are unable to add certain syntactic operators without losing the congruence property of our equivalence (for example, asynchronous parallel), assuming our equivalence is based only on differences in "observable behaviour". However, as mentioned in Section 5.7, we have proposed a solution to this by considering a process calculus with a separate probabilistic choice operator.

Following this, we have presented a denotational model for our process calculus based on de Bakker and Zucker's construction for classical process calculi, which we have shown is fully abstract with respect to our operational model. The denotational semantics we have constructed is "smooth" as opposed to the "discrete" model constructed by Baier and Kwiatkowska [BK97]. To elaborate on this, consider the space of probability distributions over a two point set. With the metric presented here it is isomorphic to the Euclidean metric over [0,1], whereas the ultra-metric of [BK97] gives rise to the discrete topology on [0,1]. This, however, comes at a cost: we have constructed a pseudo-metric, whereas the metric constructed in [BK97] is an ultra-metric. Also, our metric is not inductive, and as a result we cannot use America and Rutten's general framework for metric semantics [AR89], whereas the metric constructed in [BK97] is inductive and therefore the framework of [AR89] can be used.

We have also considered a logical characterisation of our process equivalence by means of a quantitative interpretation of the logic `HML`, and since we have only considered a positive sub-logic the connection still holds when we add the greatest fixed point operator to our logic.

8.1 Future Work

As already discussed, a possible future continuation of this work would be to give semantics to a process calculus containing a separate probabilistic choice operator, which may allow the addition of syntactic operators such as asynchronous parallel and hiding without losing the congruence property of an equivalence based only on the observable behaviour of processes. Other possible future topics include:

- A sound and complete axiomatisation of RP.
- Formulating a domain-theoretic denotational semantics for RP, since domain-theoretic models have been constructed for CSP based on both failure and ready sets, and our equivalence can intuitively be thought of as an "extension" of failure and ready sets to include more of the branching information of processes.

- Developing a (metric) denotational model for the generative and stratified models of van Glabbeek et al. [GSST90].

- Constructing a denotational model for stochastic process calculi; we have already derived a metric model for a subset of the stochastic process calculus called Performance Evaluation Process Algebra (PEPA) [Hil96] in [KN96a] (joint with M.Kwiatkowska), and to give a complete metric model for the full calculus we will need to add probabilistic behaviour, which may involve combining the work of this thesis and that of [KN96a].

- Generalising the logical framework by removing the rather strong syntactic conditions on the logics considered. This may have to involve a more complicated interpretation since, by removing the conditions we impose on constructs of the form $\phi \wedge \psi$, the values of $[\![\phi]\!]E$ and $[\![\psi]\!]E$, for certain probabilistic processes E, will no longer be independent and we will therefore be unable to use multiplication in the definition of $[\![\phi \wedge \psi]\!]$. To formulate a probabilistically sound definition we will have to consider conditional probabilities, since for dependent events the probability of both events occurring is given in terms of the conditional probabilities of each event occurring given the other has occurred. This research would also consider adding negation, which as already mentioned earlier, has no effect on the equivalence induced from the interpretaion of the logics in the cases when processes do not exhibit any non-deterministic behaviour. One of the main results of this, in the case when process can make internal choices, would be the introduction of formulae containing both the operators $\langle\varepsilon\rangle$ and $[\varepsilon]$ which by the syntactic restrictions imposed have so far been excluded.

Bibliography

[Abr87] S. Abramsky. Observational equivalence as a testing equivalence. *Theoretical Computer Science, 53:225-241, 1987.*

[Abr91a] S. Abramsky. A domain equation for bisimulation. *Information and Computation, 92:161-218, 1991.*

[Abr91b] S. Abramsky. Domain theory in logical form. *Annals of Pure and Applied Logic, 51:1-77, 1991.*

[AJ94] S. Abramsky and A. Jung. Domain theory. *In S. Abramsky, D.M. Gabbay and T.S.E. Maibaum, editors, volume 3 of Handbook of Logic in Computer Science, pages 1-168, Clarendon Press, 1994.*

[AR89] P.H.M. America and J.J.M.M. Rutten. Solving reflexive domain equations in a category of complete metric spaces. *Journal of Computer and System Science, 39(3):343-375, 1989.*

[BBS92] J.C.M. Baeten, J.A. Bergstra and S.A. Smolka. Axiomatising probabilistic processes ACP with generative probability. *In R. Cleaveland, editor, Proc. CONCUR'92: 3rd Conference on Concurrency Theory, volume 630 of Lecture Notes in Computer Science, pages 472-485, Springer Verlag, 1992.*

[BCHKR97] C. Baier, E. Clarke, V. Hartonas-Garmhausen, M.Z. Kwiatkowska and M.D. Ryan. Symbolic model checking for probabilistic processes. *In Proc. 24th Int. Coll. on Automata, Languages and Programming (ICALP), volume 1256 of Lecture Notes in Computer Science, pages 430-440, Springer Verlag, 1997.*

[BK97] C. Baier and M.Z. Kwiatkowska. Domain equations for probabilistic processes (Extended Abstract). *In Proc. EXPRESS Workshop, volume 7, Electronic Notes in Theoretical Computer Science, Elsevier, 1997.*

[BZ82] J.W. de Bakker and J.I. Zucker. Processes and the denotational semantics of concurrency. *Information and Control, 54(1/2):70-120, 1982.*

[BK84] J.A. Bergstra and J.W. Klop. Process algebra for synchronous communication. *Information and Computation, 60:109-134, 1984.*

[BKO88] J.A. Bergstra, J.W. Klop and E.R. Olderog. Readies and failures in the algebra of communicating processes. *SIAM Journal of Computing, 17(6):1134-1177, 1988.*

[BM89] B. Bloom and A.R. Meyer. A remark on bisimulation between probabilistic processes. *In A.R. Meyer and M.A. Taitslin, editors, Symp. on Logical Foundations of Computer Science (Logic at Botik), volume 363 of Lecture Notes in Computer Science, pages 26-40, Springer Verlag, 1989.*

[Bre94] F. van Breugel. Topological models in comparative semantics. *PhD Thesis, Vrije Universiteit, 1994.*

[Bro83] S.D. Brookes. On the relationship of CCS and CSP. *In J. Diáz, editor, Proc. 10th Int. Coll. on Automata Languages and Programming (ICALP), volume 154 of Lecture Notes in Computer Science, pages 83-96, Springer Verlag, 1983.* .W.

[BHR84] S.D. Brookes, C.A.R. Hoare and A.W. Roscoe. A theory of communicating sequential processes. *Journal of the ACM, 31(3):560-599, 1984.*

[Chr90] I. Christoff. Testing equivalences and fully abstract models for probabilistic processes. *In J.C.M. Baeten and J.W. Klop, editors, Proc. CONCUR'90: Theories of Concurrency: Unification and Extension, volume 458 of Lecture Notes in Computer Science, pages 126-140, Springer Verlag, 1990.*

[Chr93] L. Christoff. Specification and verification methods for probabilistic processes. *PhD Thesis, Department of Computer Science, Uppsala University, Sweden.* Available as report DoCS 93/37.

[CES83] E.M. Clarke, E.A. Emerson and A.P. Sistla. Automatic verification of finite-state concurrent systems using temporal logics. *In Proc. 10th ACM Symp. on Principles of Programming Languages, pages 117-126, 1983.*

[CSZ92] R. Cleaveland, S.A. Smolka and A.E. Zwarico. Testing preorders for probabilistic processes. *In Proc. 19th Int. Coll. on Automata, Languages and Programming (ICALP), volume 623 of Lecture Notes in Computer Science, pages 708-719, Springer Verlag, 1992.*

[EH] A. Edalat and R. Heckmann. A computational model for metric spaces. *Theoretical Computer Science (to appear).* Available at `http://theory.doc.ic.ac.uk/people/Edalat`.

[GJS90] A. Giacalone, C-C. Jou and S.A. Smolka. Algebraic reasoning for probabilistic concurrent systems. *In M. Broy and C.B. Jones, editors, Proc. IFIP TC2 Working Conference on Programming Concepts and Methods, Sea of Galilee, Israel, pages 443-458, 1990.*

[Gla90] R.J. van Glabbeek. The linear time-branching time spectrum. *In J.C.M. Beaten and J.W. Klop editors, Proc. CONCUR'90: Theories of Concurrency: Unification and Extension, volume 458 of Lecture Notes in Computer Science, pages 278-297, Springer Verlag, 1990.*

[GSST90] R.J. van Glabbeek, S.A. Smolka, B. Steffen and C.M.N. Tofts. Reactive, generative and stratified models of probabilistic processes. *In Proc. 5th IEEE Int. Symp. on Logic in Computer Science (LICS), pages 130-141, 1990.*

[Gla93] R.J. van Glabbeek. The linear time-branching time spectrum II. *In E. Best, editor, Proc. CONCUR'93: 4th Int. Conference on Concurrency Theory, volume 715 of Lecture Notes in Computer Science, pages 66-81, Springer Verlag, 1993.*

[GW86] G. Grimmett and D. Welsh. Probability: an introduction. *Oxford University Press, 1986.*

[GH90] M. Große-Rhode and H. Ehrig. Transformation of combined data type and process specifications using projection algebras. *In J.W. de Bakker, W.P. de Roever and G. Rozenberg, editors, REX Workshop on Stepwise Refinement of Distributed Systems: Models, Formalisms, Correctness, volume 430 of Lecture Notes in Computer Science, pages 301-339, Springer Verlag, 1990.*

[FH82] Y.A. Feldman and D. Harel. A probabilistic dynamic logic. *Journal of Computer and System Sciences, 28:193:215, 1982.*

[FL79] M.J. Fischer and R.E. Ladner. Propositional Dynamic Logic of regular programs. *Journal of Computer System Science, 18(2):194-211, 1979.*

[HJ90] H.A. Hansson. and B. Jonsson. A calculus for communicating systems with time and probability. *In Proc. 11th IEEE Real-Time Systems Symp., pages 278-287, 1990.*

[HJ94] H.A. Hansson. and B. Jonsson. A logic for reasoning about time and reliability. *Formal Aspects of Computing, International Journal of Formal Methods, 6(5):512-535, 1994.*

[Han94] H.A. Hansson. Time and probability in the formal design of distributed systems. *Volume 1 of Real-Time Safety Critical Systems, Elsevier, 1994.*

[Har79] D. Harel. First order dynamic logic. *Volume 68 of Lecture Notes in Computer Science, Springer Verlag, 1979.*

[Hen85] M.C.B. Hennessy. Acceptance trees. *Journal of the Association for Computing Machinery, 32(4):896-928, 1985.*

[HM85] M.C.B. Hennessy and R. Milner. Algebraic laws for nondeterminism and concurrency. *Journal of the Association for Computing Machinery, 32(1):137-161, 1985.*

[Her90] T. Herman. Probabilistic self stabilisation. *Information Processing Letters, 35(2):63-67, 1990.*

[Hil96] J. Hillston. A compositional approach to performance modelling. *Distinguished Dissertation Series, Cambridge University Press, 1996.*

[Hoa85] C.A.R. Hoare. Communicating sequential processes, *Prentice Hall, 1985.*

[HK97] M. Huth and M.Z. Kwiatkowska. Quantitative analysis and model checking. *In Proc. 12th IEEE Int. Symp. on Logic in Computer Science (LICS), pages 111-122, 1997.*

[JP89] C. Jones and G.D. Plotkin. A probabilistic powerdomain of evaluations. *In Proc. 4th IEEE Int. Symp. on Logic in Computer Science (LICS), pages 186-195, 1989.*

[Jon90] C. Jones. Probabilistic non-determinism. *PhD Thesis, University of Edinburgh, 1990.* Available as report ECS-LFCS-90-105.

[JL91] B. Jonsson and K.G. Larsen. Specification and refinement of probabilistic processes. *In Proc. 6th IEEE Int. Symp. on Logic in Computer Science (LICS), pages 266-277, 1991.*

[JY95] B. Jonsson and Wang Yi. Compositional testing preorders for probabilistic processes. *In Proc. 10th IEEE Int. Symp. on Logic in Computer Science (LICS), 1995.*

[JS90] C-C. Jou and S.A. Smolka. Equivalences, congruences and complete axiomatisations for probabilistic processes. *In J.C.M. Baeten and J.W. Klop, editors, Proc. CONCUR'90: Theories of Concurrency: Unification and Extension, volume 458 of Lecture Notes in Computer Science, pages 367-383, Springer Verlag, 1990.*

[Koz81] D. Kozen. Semantics of probabilistic programs. *Journal of Computer System Science, 22:328-350, 1981.*

[Koz83a] D. Kozen. Probabilistic PDL. *In Proc. 15th ACM Symp. on the Theory of Computing, pages 291-297, 1983.*

[Koz83b] D. Kozen. Results on the propositional μ-calculus. *Theoretical Computer Science, 27:333-354, 1983.*

[KN96a] M.Z. Kwiatkowska and G. Norman. Metric denotational semantics for PEPA. *In M. Ribaudo, editor, Proc. 4th Process Algebra and Performance Modelling Workshop, pages 120-138, CLUT, 1996.*

[KN96b] M.Z. Kwiatkowska and G. Norman. Probabilistic metric semantics for a simple language with recursion. *In W. Penczek and A. Szalas, editors, Proc. Mathematical Foundations of Computer Science (MFCS), volume 1113 of Lecture Notes in Computer Science, pages 419-430, Springer Verlag, 1996.*

[Lam89] L. Lamport. A simple approach to specifying concurrent systems. *Communications of the ACM, 32(1):32-45, 1989.*

[LS91] K.G. Larsen and A. Skou. Bisimulation through probabilistic testing. *Information and Computation, 94(1):1-28, 1991.* Preliminary version of this paper appeared in *Proc. 16th Annual ACM Symposium on Principles of Programming Languages, pages 134-352, 1989.*

[LS92] K.G. Larsen and A. Skou. Compositional verification of probabilistic processes. *In R. Cleaveland, editor, Proc. CONCUR'92: 3rd Int. Conference on Concurrency Theory, in volume 630 of Lecture Notes in Computer Science, pages 456-471, Springer Verlag, 1992.*

[LR81] D. Lehmann and M.O. Rabin. On the advantage of free choice: a symmetric and fully distributed solution to the dining philosophers problem. *In Proc. 8th Annual ACM Symp. on Principles of Programming Languages, pages 133-138, 1981.*

[Low93] G. Lowe. Probabilities and priorities in timed CSP. *PhD Thesis, Oxford University Computing Laboratory, 1993.* Available as report PRG-111.

[Low] G. Lowe. Representing nondeterministic and probabilistic behaviour in reactive processes. *Submitted for publication.* Available at `http://www.mcs.le.ac.uk/~glowe/Publications.html`.

[Mil83] R. Milner. Calculi for synchrony and asynchrony. *Theoretical Computer Science, 25(3):267-310, 1983.*

[Mil89] R. Milner. Communication and concurrency. *Prentice Hall, 1989.*

[Mis91] M.W. Mislove. Algebraic posets, algebraic cpos and models for concurrency. *In G.M. Reed, A.W. Roscoe and R.F. Wachter, editors, Topology and Category Theory in Computer Science, pages 75-111, Oxford University Press, 1991.*

[MMSS95] C. Morgan, A. Mclver, K. Seidel and J.W. Sanders. Argument duplication in probabilistic CSP. *Technical Report PRG-TR-95, Oxford University Computing Laboratory, 1995.* Available from [PSG].

[MMSS96] C. Morgan, A. Mclver, K. Seidel and J.W. Sanders. Refinement-oriented probability for CSP. *Formal Aspects of Computing, 8(6):617-647, 1996.* Also available from [PSG].

[MM] C. Morgan and A. Mclver. An expectation-transformer model for probabilistic temporal logic. *Submitted for publication.* Available from [PSG].

[NH84] R. de Nicola and M.C.B. Hennessy. Testing equivalences for processes. *Theoretical Computer Science, 34:83-133, 1984.*

[Niv79] M. Nivat. Infinite words, infinite trees, infinite computations. *In J.W. de Bakker and J. van Leeuwen, editors, Foundations of Computer Science III, part 2: Languages, Logics, Semantics, volume 109 of Mathematical Centre Tracts, pages 3-52, Mathematical Centre, Amsterdam, 1979.*

[PSG] Probabilistic Systems Group, Oxford University. Collected reports. Available at `http://www.comlab.ox.ax.uk/oucl/groups/probs/bibliography.html`.

[Par81] D.M.R. Park. Concurrency and automata on infinite sequences. *In P. Dussen, editor, Proc. 5th GI Conference, volume 104 of Lecture Notes in Computer Science, pages 167-183, Springer Verlag, 1981.*

[Plo81] G.D. Plotkin. A structural approach to operational semantics. *Report DAIMI FN-19, Aarhus University, 1981.*

[Plo81] G.D. Plotkin. Post-graduate lecture notes in advanced domain theory. *Department of Computer Science, University of Edinburgh, 1981.*

[Pnu77] A. Pnueli. The temporal logics of programs. *In Proc. 18th IEEE Int. Symp. on Foundations in Computer Science, pages 46-57, 1977.*

[Pug90] W. Pugh. Skip lists: a probabilistic alternative to balanced trees. *Communications of the ACM, (33):668-676, 1990.*

[PS87] S. Purushothaman and P.A. Subrahmanyam. Reasoning about probabilistic behaviour in concurrent systems. *In IEEE Transactions on Software Engineering, SE-13(6):740-745, 1987.*

[Rab63] M.O. Rabin. Probabilistic automata. *Information and Control, 6:230-245, 1963.*

[SL94] R. Segala and N. Lynch. Probabilistic simulations for probabilistic processes. *In B. Jonsson and J. Parrow, editors, Proc. CONCUR'94: volume 836 of Lecture Notes in Computer Science, pages 481-496, Springer, 1994.*

[SPH84] M. Sharir, A. Pnueli and S. Hart. Verification of probabilistic programs. *SIAM Journal on Computing, 13(2):292-314, 1984.*

[Sei92] K. Seidel. Probabilistic communicating processes. *PhD Thesis, Oxford University Computing Laboratory, 1992.* Available as report PRG-102.

[Sto77] J. Stoy. Denotational semantics, the Scott Strachey approach to program language theory. *MIT Press, Cambridge, 1977.*

[Sut77] W.A. Sutherland. Introduction to metric and topological spaces. *Oxford University Press, 1977.*

[Tof90] C.M.N. Tofts. A synchronous calculus of relative frequency. *In J.C.M. Baeten and J.W. Klop editors, Proc. CONCUR'90: Theories of Concurrency: Unification and Extension, volume 458 of Lecture Notes in Computer Science, pages 467-480, Springer Verlag, 1990.*

[YL92] Wang Yi and K.G. Larsen. Testing probabilistic and non-deterministic processes. *Protocol Specification, Testing and Verification XII:47-61, Florida, USA, 1992.*

[YCDS94] S. Yuen, R. Cleaveland, Z. Dayar and S.A. Smolka. Fully abstract characterisations of testing preorders for probabilistic processes. *In B. Jonsson and J. Parrow, editors, Proc. CONCUR'94: 5th Int. Conference on Concurrency Theory, volume 836 of Lecture Notes in Computer Science, pages 497-512, Springer Verlag, 1994.*