Electronic Notes in Theoretical Computer Science 13 (1998)
URL: http://www.elsevier.nl/locate/entcs/volume13.html

A Fully Abstract Metric-Space Denotational Semantics for Reactive Probabilistic Processes

M.Z. Kwiatkowska and G.J. Norman

School of Computer Science,
University of Birmingham,
Edgbaston, Birmingham B15 2TT, UK

Abstract

We consider the calculus of Communicating Sequential Processes (CSP) [8] extended with action-guarded probabilistic choice and provide it with an operational semantics in terms of a suitable extension of Larsen and Skou's [14] reactive probabilistic transition systems. We show that a testing equivalence which identifies two processes if they pass all tests with the same probability is a congruence for a subcalculus of CSP including external and internal choice and the synchronous parallel. Using the methodology of de Bakker and Zucker [3] introduced for classical process calculi, we derive a metric-space semantic model for the calculus and show it is fully abstract.

1 Introduction

When specifying concurrent probabilistic systems, for example fault-tolerant systems, probabilistic protocols and randomized algorithms, it is convenient to use a process calculus which allows compositional specifications: components of the system are specified first, and then combined into larger specifications by means of process operators such as the parallel composition or non-deterministic choice. An important issue that arises when deriving such a calculus is which *process equivalence* to choose, and, having chosen an equivalence, which process operators are preserved under all contexts, or, in other words, is the chosen equivalence a *congruence* for the process operators? The choice of the equivalence depends on the power of discriminating between computations that is necessary for the applications at hand, and can be linear-time, branching-time, or a suitable variant. The congruence property allows to 'collapse' all equivalent processes into a single object, which can prove useful when e.g. constructing data structures for automatic verification (as in e.g. the model checker `fdr2` [21]). It is also a prerequisite when constructing a denotational model for the calculus which is *fully abstract*, i.e. the denotations of two processes are equal precisely when their operational meanings are equivalent.

Many probabilistic extensions of process calculi have been proposed to date, based on CCS [17], CSP [5] and ACP [4] and including amongst others [6,7,16,19,23]. Likewise, several probabilistic equivalences have been introduced, for example: probabilistic bisimulation, defined by Larsen and Skou [14] for reactive systems and extended with non-determinism by Hansson [7]; probabilistic equivalences of Jou and Smolka [11]; probabilistic simulation of Segala and Lynch [22]; Wang Yi and Larsen's testing equivalence [24]; and CSP equivalences of Morgan et al. [19], Lowe [16] and Seidel [23]. The above equivalences differ in their discriminating power, and also in how they interact with process operators [11]. Generally, if one works with a fine (or strong) equivalence such as probabilistic bisimulation then almost all CCS or CSP operators can be adapted to the probabilistic setting. For example, van Glabbeek et al. [6] show that probabilistic bisimulation is a congruence over their calculus PCCS (which contains all the usual SCCS operators) and Baier and Kwiatkowska [2] show congruence properties of full CCS extended with action-guarded probabilistic choice. However, there are cases when probabilistic bisimulation is too fine, as it discriminates between processes that *cannot* be distinguished under a realistic testing scenario.

One alternative is to work with a weaker (or coarser) equivalence, for example extensions of the traces and failures CSP equivalences [5], which are essentially testing equivalences, and hence will only distinguish processes that can be distinguished under a realistic testing scenario. The difficulty with this approach 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 such difficulties include Jou and Smolka [11], where even restriction forces both trace and failure equivalence to fail to be congruences, and [23] and [16], where hiding cannot be defined.

A further complication is that in some process calculi, such as those that derive from CSP, there is a distinction between a *process* (the software behind the black box) and an *environment* (the user that interacts with the black box by means of pressing buttons that cause it to perform actions), which is reflected in the presence of *two* choice operators: internal (determined by the process) and external (determined by the environment). Each choice operator satisfies a set of intuitive axioms which must be preserved when enriching CSP with probabilistic choice. We stress that it would be inappropriate to replace non-deterministic choice with probabilistic choice, as both arise naturally in, and are therefore needed to model, randomized distributed systems: probabilistic choice is made internally according to a probability distribution, whereas non-deterministic choice is made by a scheduler (or a demon) that decides which independently acting component of a distributed system should make a move next.

The aim of this paper is to derive an appropriate process equivalence for the CSP calculus extended with action-guarded probabilistic choice which is a congruence for a large subset of the CSP process operators. The probabilistic choice we consider is *internal*, i.e. made neither by the environment nor by the process but according to a given probability distribution. As a result, our equivalence is applicable when the outcome of a probability distribution is not affected by actions or environment choices, as e.g. in the example of scratch cards [19], but would have to be extended to handle external probabilistic choices. The choice of CSP means that we have to reject fully branching-type equivalences such as probabilistic bisimulation, and instead derive an equivalence based on *testing*. We use Larsen and Skou's reactive transition systems suitably generalised to take account of the three kinds of choice: non-deterministic, deterministic and probabilistic. Milner's button pushing experiments scenario is extended with random experiments, and the testing equivalence defined so that two processes are identified precisely if they agree on the outcome of all the experiments.

We show that thus defined equivalence is a congruence for most of the CSP operators (we are not able to deal with hiding and asynchronous parallel). We then formulate a metric-space denotational semantics based on the constructions of de Bakker and Zucker [3] and show it is fully abstract, in the sense that it maps equivalent processes on to the same denotation. In [13,20] the equivalence considered here is endowed with a logical characterization in terms of the quantitative variant of the Hennessy-Milner Logic introduced in [9]. This completes the work started in [9] by characterizing the equivalence induced by (a variant of) the quantitative `HML`.

Related research concerning probabilistic extensions of CSP includes the work of Seidel [23], where the difference from the standard CSP is that an internal probabilistic choice operator replaces the internal (non-deterministic) choice operator, and so the model constructed is fully deterministic. Similarly, in Lowe [15] non-deterministic 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 [16] has since considered a model which includes internal probabilistic choice, external choice and internal choice, but unfortunately the equivalences considered fail to be congruences. Similarly to [16], Morgan et al. [19] 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 [10] (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. There are, however, problems with the behaviour of certain operators in their model, for example internal choice fails to be idempotent. Solutions to these problems have been investigated in [18].

As far as metric-space denotational models are concerned, we should mention the metric model of [12] where a deterministic subcalculus of CCS extended with action-guarded probabilistic choice was considered, and that of Baier and Kwiatkowska [2] for full CCS extended with action-guarded probabilistic choice.

2 The Model and Testing Equivalence

In this section we overview the definitions necessary for the technical development included in the remainder of this paper; for detailed justification of the constructions see [13,20]. First, we recall the definition of our model, called *reactive probabilistic transition systems*, which extend Larsen and Skou's probabilistic labelled transition systems [14] by allowing processes of the system to exhibit three types of choice: (internal action-guarded) probabilistic, external (deterministic) and internal (non-deterministic). Next we define the testing equivalence [13,20] over reactive probabilistic transition systems which will distinguish two processes only if they can be differentiated by means of experiments.

A (discrete) *probability distribution* on a set D is a function $\pi : D \longrightarrow [0,1]$ such that $\sum_{d \in D} \pi(d) = 1$. We use $\mu(D)$ to denote the set of discrete probability distributions on D. A subset X of the cartesian product $A \times S$ of sets A and S is said to satisfy the *reactiveness condition* if, for any distinct $(a_1, s_1), (a_2, s_2) \in X$: $a_1 \neq a_2$. We let $\mathcal{P}_{\mathrm{fr}}(\cdot \times \cdot)$ denote the powerset operator restricted to only finite reactive subsets of cartesian products satisfying the reactiveness condition.

Definition 2.1 [13,20] 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

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

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

The elements $E \in \mathcal{R}$ of a reactive probabilistic transition system exhibit: *non-deterministic* choice between reactive sets associated with E via the transition relation $\rightarrow$, with each such set $S = \{(a_1, \pi_1), \ldots, (a_m, \pi_m)\}$ modelling a process, deterministic on its first step, that offers a menu $a_1, \ldots, a_m$ of actions to the environment; *deterministic* choice between the actions of the menu made by the environment; and *action-guarded probabilistic* choice made according to the unique distribution π_i following a selection of action a_i from the menu. The models of [14] correspond to the class of deterministic reactive probabilistic transition systems.

We now define the testing preorder and equivalence for reactive probabilistic transition systems as introduced in [13,20]. We extend Milner's button pushing experiments [17] for transition systems with *random experiments*, that is, tests which have as outcome the *probability* of the process passing the given test [1]. Two experiments are said to be *independent* if they are associated with pressing different buttons in the first step. To capture the three types of choice exhibited by processes of a reactive probabilistic transition system, we introduce the following three respective experiments:

(i) $a.t$, where $a \in \mathcal{A}ct$: push the a-button and then, if the button goes down, perform the experiment t.

(ii) $(t_1, \ldots, t_m)$, where for all $1 \leq i \neq j \leq m$ the experiments t_i and t_j are *independent*: make m copies of the process being tested and then perform the experiment t_i on *one* of the copies for all $1 \leq i \leq m$.

(iii) $(\!|t|\!)$: make sufficiently many copies of the process being tested, so that any non-deterministic choice the process can make will occur on at least one of the copies made, and then perform the experiment t on *each* of the copies.

Intuitively, the success or failure of a process passing an experiment corresponds to the success or failure of *one run* (or execution) of the process being experimented on, under different conditions: $(t_1, \ldots, t_m)$ corresponds to the changes in the *environment* (e.g. users selecting actions from menus), whereas $(\!|t|\!)$ corresponds to the changes the *demons* introduce to influence the non-deterministic choices that the processes make.

Formally, the testing language $\mathtt{T}_\omega$ is given as follows, where we use $[t, \ldots, t]$ to distinguish the different types of tests and apply the same restriction to this construct as to $(t, \ldots, t)$. Let $\mathtt{T}$ and $\mathtt{T}_\omega$, with elements t and T respectively, be the testing languages defined inductively by:

$$r ::= \omega \mid [a.T, \ldots, a.T]$$

$$t ::= (\!|r|\!)$$

$$T ::= (t, \ldots, t)$$

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

The outcome of a random experiment is captured by a pair of maps $\mathsf{R}_{\mathbf{glb}}$ and $\mathsf{R}_{\mathbf{lub}}$ from $\mathcal{R}$ and $\mathtt{T}_\omega$ to the unit interval which, for any process $E \in \mathcal{R}$ and test $(\!|r|\!) \in \mathtt{T}$, yield the greatest lower bound and the least upper bound on *the probability of E passing the test* r respectively. This is because in the presence of non-determinism we are unable to calculate the *exact* probability of processes passing the tests, and instead choose to estimate the *worst case* and the *best case* outcome, which in turn yields an *interval* of probabilities. This is the only realistic option since we cannot establish the frequency of non-

[1] Our testing scenario differs from that of Larsen and Skou's in that we attach a different meaning to the phrase "the probability of the process passing a test [13,20]".

deterministic choices, and thus there is no way of calculating any meaningful average. We mention that intervals were also used in [24].

Definition 2.2 [13,20] Let $\mathsf{R}_{\mathbf{glb}}, \mathsf{R}_{\mathbf{lub}} : \mathcal{R} \longrightarrow (\mathtt{T}_\omega \longrightarrow [0,1])$ 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:

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

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

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

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

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

With the help of the above maps, we are now in a position to define our operational order and subsequent equivalence on all reactive probabilistic transition systems. We simply require that the process higher up the order must pass all tests with probability *at least as high* as those below. It turns out that we need only consider the tests $\mathtt{T}$, as opposed to the (larger) set of tests $\mathtt{T}_\omega$.

Definition 2.3 [13,20] 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 $F \sqsubseteq^{\mathsf{R}} E$.

Thus, the order $\sqsubseteq^{\mathsf{R}}$ is an *intersection* of orders $\sqsubseteq^{\mathbf{glb}}$ and $\sqsubseteq^{\mathbf{lub}}$. The equivalence $\overset{\mathsf{R}}{\sim}$ is coarser than probabilistic bisimulation [14], and yet non-probabilistic branching time. It is finer than the CSP equivalences of [16,23] but incomparable to that of [19].

3 The Process Calculus

In this section, we present the process calculus for reactive probabilistic processes RP, based on CSP [5,8,21], in which prefixing is replaced with action-guarded probabilistic choice. We begin by introducing the notation necessary to derive our calculus and investigate its properties.

Definition 3.1 (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 B is any subset of $\mathcal{A}ct$.
- $\{\mu_i \,|\, i \in I\}$ is any countable indexed subset of $(0,1]$ such that $\sum_{i \in I} \mu_i = 1$.

- $\mathcal{X}$ 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.

The following notation pertains to our testing scenario. We write $a \in t$ (a occurs in the test t) if t's corresponding button-pushing experiment involves, at some stage, pressing the a–button. Formally, we can define this by induction on tests: for any $a \in \mathcal{A}ct$: $a \notin (\!|\omega|\!)$, $a \in (\!|[a_1, T_1, \ldots, a_m.T_m]|\!)$ if either $a = a_i$, or $a \in T_i$ for some $1 \leq i \leq m$, and $a \in (t_i, \ldots, t_m)$ if $a \in t_i$ for some $1 \leq i \leq m$. We also need to extend any relabelling function $\lambda : \mathcal{A}ct \to \mathcal{A}ct$ to a function on our testing language $\mathtt{T}$. Again, this can be done by induction on tests as follows: we define the extended map $\lambda : \mathtt{T} \to \mathtt{T}$ by putting: $\lambda(\omega) \stackrel{\text{def}}{=} \omega$ and $\lambda([a.T, \ldots, a.T]) \stackrel{\text{def}}{=} [\lambda(a).\lambda(T), \ldots, \lambda(a).\lambda(T)]$, $\lambda((\!|r|\!)) \stackrel{\text{def}}{=} (\!|\lambda(r)|\!)$ and $\lambda((t, \ldots, t)) \stackrel{\text{def}}{=} (\lambda(t), \ldots, \lambda(t))$.

The calculus RP, which derives its syntax from that of CSP, is given below.

Definition 3.2 The set of RP expressions is given by the syntax:

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

As usual, $\mathbf{0}$ denotes the inactive process, $F_1 \sqcap F_2$ internal choice, $F_1 \,\Box\, F_2$ external choice, $F_1 \parallel F_2$ (synchronous) parallel composition, $F \lceil B$ restriction, $F\,[\lambda]$ relabelling and $\mathit{fix}_x.F$ recursion. Action-guarded probabilistic choice is denoted by $a.\sum_{i \in I} \mu_i.F_i$. 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.

As is customary, since the above syntax allows variables to occur freely in expressions, we will only consider guarded and closed expressions as terms of our calculus, denoting the set of guarded expressions of RP by $\mathcal{G}$ and the set of *processes* (expressions without free or unguarded variables) by Pr.

3.1 Operational Semantics

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

(i) $\mathcal{O}[\![\mathbf{0}]\!] \to \emptyset$.

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

(iii) $\mathcal{O}[\![E_1 \sqcap E_2]\!] \to S$, if $\mathcal{O}[\![E_1]\!] \to S$ or $\mathcal{O}[\![E_2]\!] \to S$.

(iv) $\mathcal{O}[\![E_1 \,\Box\, E_2]\!] \to S$, if $\mathcal{O}[\![E_1]\!] \to S_1$ and $\mathcal{O}[\![E_2]\!] \to S_2$ such that S is a maximal reactive subset of $S_1 \cup S_2$.

(v) $\mathcal{O}[\![E_1 \parallel E_2]\!] \to S$, if $\mathcal{O}[\![E_1]\!] \to S_1$ and $\mathcal{O}[\![E_2]\!] \to S_2$ 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 $F \in \mathrm{Pr}$:

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

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

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

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

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

(viii) $\mathcal{O}[\![\mathit{fix}_x.E]\!] \to S$, if $\mathcal{O}[\![E\{\mathit{fix}_x.E/x\}]\!] \to S$, 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.

With the exception of the rule for $\Box$, all the above transition rules are as expected. The rule for $\Box$ ensures that deterministic choice is made between distinct initial actions of the subprocesses, which degenerates to a *non-deterministic* choice between the corresponding distributions when subprocesses can perform the same action as their initial move. To see this consider the following examples. First, if $\mathcal{O}[\![E_1]\!] \to \{(a, \pi)\}$ and $\mathcal{O}[\![E_2]\!] \to \{(b, \pi')\}$ where $a \neq b$, then from the transition rules we have $\mathcal{O}[\![E_1 \Box E_2]\!] \to \{(a, \pi), (b, \pi')\}$, and hence $E_1 \Box E_2$ makes a deterministic choice between the actions a and b. A a second example, suppose $\mathcal{O}[\![E_1]\!] \to \{(a, \pi), (c, \pi_1)\}$ and $\mathcal{O}[\![E_2]\!] \to \{(b, \pi'), (c, \pi_2)\}$ for some distinct actions a, b and c, then $\mathcal{O}[\![E_1 \Box E_2]\!] \to \{(a, \pi), (b, \pi'), (c, \pi_i)\}$ for $i \in \{1, 2\}$, and thus $E_1 \Box E_2$ makes a deterministic choice between the actions a, b and c, but there is a *non-deterministic* choice between the distributions π_1 and π_2 when performing the action c.

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

Proposition 3.3 *If $E \in \mathrm{Pr}$ and $\mathcal{O}[\![E]\!] \to S$, then $S \in \mathcal{P}_{\mathrm{fr}}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$.*

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

3.2 RP *and the testing order* $\sqsubseteq^{\mathsf{R}}$

Using the operational semantics defined above, we now relate the order $\sqsubseteq^{\mathsf{R}}$ to RP. First, it follows from Proposition 3.3 that we can calculate $\mathsf{R}_{\mathbf{glb}}(\mathcal{O}[\![E]\!])(t)$

and $\mathsf{R}_{\mathbf{lub}}(\mathcal{O}[\![E]\!])(t)$ for all $E \in \mathrm{Pr}$ and $t \in \mathtt{T}$, and hence the order $\sqsubseteq^{\mathsf{R}}$ is well-defined on the set $\{\mathcal{O}[\![E]\!] \mid E \in \mathrm{Pr}\}$. We therefore begin by investigating the properties of the maps $\mathsf{R}_{\mathbf{glb}}$ and $\mathsf{R}_{\mathbf{lub}}$ with respect to the processes Pr and semantic operators of RP. As usual, we extend the order $\sqsubseteq^{\mathsf{R}}$ to all guarded expressions by means of the following definition.

Definition 3.4 For all $F, G \in \mathcal{G}$, $\mathcal{O}[\![F]\!] \sqsubseteq^{\mathsf{R}} \mathcal{O}[\![G]\!]$ if and only if $\mathcal{O}[\![F\{\tilde{E}/\tilde{x}\}]\!] \sqsubseteq^{\mathsf{R}} \mathcal{O}[\![G\{\tilde{E}/\tilde{x}\}]\!]$ for all $\tilde{E} \subseteq \mathrm{Pr}$, 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 will also hold for the guarded terms of RP, and hence for the remainder of this section we will only prove results with respect to processes. Furthermore, to ease notation, let R_* denote either $\mathsf{R}_{\mathbf{glb}}$ or $\mathsf{R}_{\mathbf{lub}}$ and for any $E \in \mathrm{Pr}$ and $t \in \mathtt{T}$ we will denote $\mathsf{R}_*(\mathcal{O}[\![E]\!])(t)$ by $\mathsf{R}_*(E)(t)$.

Lemma 3.5 *For all $E_1, E_2, E \in \mathrm{Pr}$, $t \in \mathtt{T}$, $B \subseteq \mathcal{A}ct$ and relabelling function λ:*

$$(a)\ \mathsf{R}_{\mathbf{glb}}(E_1 \sqcap E_2)(t) = \min\{\mathsf{R}_{\mathbf{glb}}(E_1)(t),\ \mathsf{R}_{\mathbf{glb}}(E_2)(t)\}$$

$$(b)\ \mathsf{R}_{\mathbf{lub}}(E_1 \sqcap E_2)(t) = \max\{\mathsf{R}_{\mathbf{lub}}(E_1)(t),\ \mathsf{R}_{\mathbf{lub}}(E_2)(t)\}$$

$$(c)\quad \mathsf{R}_*(E_1 \parallel E_2)(t) = \mathsf{R}_*(E_1)(t) \cdot \mathsf{R}_*(E_2)(t)$$

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

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

Proof. The proofs of (a) and (b) follow by Definition 2.2 and the transition rules, and the remaining cases follow by induction on $(\!|r|\!) \in \mathtt{T}$. We only consider the case for $\mathsf{R}_{\mathbf{glb}}$ and $\parallel$, the other cases follow similarly. If $r = \omega$, then by definition of $\mathsf{R}_{\mathbf{glb}}$ for any $E_1, E_2 \in \mathrm{Pr}$: $\mathsf{R}_{\mathbf{glb}}(E_1 \parallel E_2)((\!|r|\!)) = 1 = 1 \cdot 1 = \mathsf{R}_{\mathbf{glb}}(E_1)((\!|r|\!)) \cdot \mathsf{R}_{\mathbf{glb}}(E_2)((\!|r|\!))$.

If $r = [a_1.T_1, \ldots, a_m.T_m]$, then T_i is of the form $(t^i_1, \ldots, t^i_{m_i})$ where $t^i_j \in \mathtt{T}$ for all $1 \leq j \leq m_i$ and $1 \leq i \leq m$. Therefore, for any $E_1, E_2 \in \mathrm{Pr}$ and $1 \leq i \leq m$:

$$(1)\qquad \mathsf{R}_{\mathbf{glb}}(E_1 \parallel E_2)(T_i) = \mathsf{R}_{\mathbf{glb}}(E_1)(T_i) \cdot \mathsf{R}_{\mathbf{glb}}(E_2)(T_i).$$

by induction and the definition of $\mathsf{R}_{\mathbf{glb}}$. Next consider any $S \in \mathcal{P}_{\mathrm{fr}}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ such that $\mathcal{O}[\![E_1 \parallel E_2]\!] \to S$, then by definition of the transition rules there exists associated $S_1, S_2 \in \mathcal{P}_{\mathrm{fr}}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ such that $\mathcal{O}[\![E_1]\!] \to S_1$ and $\mathcal{O}[\![E_2]\!] \to S_2$, and hence to ease notation we will denote S by $S_1 \parallel S_2$. If we now consider any $1 \leq i \leq m$ we have the following two possibilities:

(i) $(a_i, \pi) \notin S_1 \parallel S_2$ for any $\pi \in \mu(\mathrm{Pr})$, then without loss of generality we can suppose $(a_i, \pi) \notin S_1$ for any $\pi \in \mu(\mathrm{Pr})$, and therefore:

$$\mathsf{R}_{\mathbf{glb}}(S_1 \parallel S_2)(a_i.T_i) = \mathsf{R}_{\mathbf{glb}}(S_1)(a_i.T_i) \cdot \mathsf{R}_{\mathbf{glb}}(S_2)(a_i.T_i)$$

by definition of $\mathsf{R}_{\mathbf{glb}}$.

(ii) $(a_i, \pi) \in S_1 \,\|\, S_2$ for some $\pi \in \mu(\mathrm{Pr})$, then $(a_i, \pi_1) \in S_1$ and $(a_i, \pi_2) \in S_2$ for some $\pi_1, \pi_2 \in \mu(\mathrm{Pr})$ by definition of the transition rules, and hence by definition of $\mathsf{R}_{\mathbf{glb}}$ and the transition rules $\mathsf{R}_{\mathbf{glb}}(S_1 \,\|\, S_2)(a_i.T_i)$ equals:

$$
\begin{aligned}
&= \sum_{F_1\|F_2 \in \mathrm{Pr}} \Big(\pi_1(F_1)\cdot\pi_2(F_2)\Big)\cdot \mathsf{R}_{\mathbf{glb}}(F_1 \,\|\, F_2)(T_i) \\
&= \sum_{F_1\|F_2 \in \mathrm{Pr}} \Big(\pi_1(F_1)\cdot\pi_2(F_2)\Big)\cdot \Big(\mathsf{R}_{\mathbf{glb}}(F_1)(T_i)\cdot \mathsf{R}_{\mathbf{glb}}(F_2)(T_i)\Big) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{by (1)} \\
&= \Big(\sum_{F_1 \in \mathrm{Pr}} \pi_1(F_1)\cdot \mathsf{R}_{\mathbf{glb}}(F_1)(T_i)\Big)\cdot\Big(\sum_{F_2 \in \mathrm{Pr}} \pi_2(F_2)\cdot \mathsf{R}_{\mathbf{glb}}(F_2)(T_i)\Big) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{rearranging} \\
&= \mathsf{R}_{\mathbf{glb}}(S_1)(a_i.T_i)\cdot \mathsf{R}_{\mathbf{glb}}(S_2)(a_i.T_i) \qquad\qquad \text{by Definition 2.2.}
\end{aligned}
$$

Since these are the only possible cases and this was for arbitrary $1 \le i \le m$ and $S_1, S_2 \in \mathcal{P}_{\mathrm{fr}}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ such that $\mathcal{O}[\![E_1]\!] \to S_1$ and $\mathcal{O}[\![E_2]\!] \to S_2$, by definition of $\mathsf{R}_{\mathbf{glb}}$ it follows that:

$$
\mathsf{R}_{\mathbf{glb}}(S_1 \,\|\, S_2)(r) = \mathsf{R}_{\mathbf{glb}}(S_1)(r)\cdot \mathsf{R}_{\mathbf{glb}}(S_2)(r) \tag{2}
$$

for all $S_1, S_2 \in \mathcal{P}_{\mathrm{fr}}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ such that $\mathcal{O}[\![E_1]\!] \to S_1$ and $\mathcal{O}[\![E_2]\!] \to S_2$. Finally, by definition of $\mathsf{R}_{\mathbf{glb}}$ and using the notation above we have $\mathsf{R}_{\mathbf{glb}}(E_1 \,\|\, E_2)((\!|r|\!))$ is equal to:

$$
\begin{aligned}
&= \min\{\mathsf{R}_{\mathbf{glb}}(S_1 \,\|\, S_2)(r) \mid \mathcal{O}[\![E_1]\!] \to S_1 \;\&\; \mathcal{O}[\![E_2]\!] \to S_2\} \\
&= \min\{\mathsf{R}_{\mathbf{glb}}(S_1)(r)\cdot \mathsf{R}_{\mathbf{glb}}(S_2)(r) \mid \mathcal{O}[\![E_1]\!] \to S_1 \;\&\; \mathcal{O}[\![E_2]\!] \to S_2\} \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{by (2)} \\
&= (\min\{\mathsf{R}_{\mathbf{glb}}(S_1)(r) \mid \mathcal{O}[\![E_1]\!] \to S_1\})\cdot(\min\{\mathsf{R}_{\mathbf{glb}}(S_2)(r) \mid \mathcal{O}[\![E_2]\!] \to S_2\}) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{rearranging} \\
&= \mathsf{R}_{\mathbf{glb}}(E_1)(r)\cdot \mathsf{R}_{\mathbf{glb}}(E_2)(r) \qquad\qquad\qquad \text{by Definition 2.2}
\end{aligned}
$$

and hence the lemma holds for $\mathsf{R}_{\mathbf{glb}}$ and $\|$ by induction on $t \in \mathtt{T}$. □

The next two lemmas establish connections between the orders $\sqsubseteq^{\mathbf{glb}}$ and $\sqsubseteq^{\mathbf{lub}}$ on processes and the maps $\mathsf{R}_{\mathbf{glb}}$ and $\mathsf{R}_{\mathbf{lub}}$ which record the outcomes of random experiments.

Lemma 3.6 *For all $E, F \in \mathrm{Pr}$, $\mathcal{O}[\![E]\!] \sqsubseteq^{\mathbf{glb}} \mathcal{O}[\![F]\!]$ if and only if for any $(\!|r|\!) \in \mathtt{T}$ and $S' \in \mathcal{P}_{\mathrm{fr}}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ such that $\mathcal{O}[\![F]\!] \to S'$ there exists $S'' \in \mathcal{P}_{\mathrm{fr}}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ such that $\mathcal{O}[\![E]\!] \to S''$ and $\mathsf{R}_{\mathbf{glb}}(S')(r) \ge \mathsf{R}_{\mathbf{glb}}(S'')(r)$.*

Proof. First, if $E, F \in \mathrm{Pr}$ and $\mathcal{O}[\![E]\!] \sqsubseteq^{\mathbf{glb}} \mathcal{O}[\![F]\!]$, then for any $(\!|r|\!) \in \mathtt{T}$ and

$S' \in \mathcal{P}_{\mathrm{fr}}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ such that $\mathcal{O}[\![F]\!] \to S'$:

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

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

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

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

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

Lemma 3.7 *For all $E, F \in \mathrm{Pr}$, $\mathcal{O}[\![E]\!] \sqsubseteq^{\mathbf{lub}} \mathcal{O}[\![F]\!]$ if and only if for any $(\!|r|\!) \in \mathtt{T}$ and $S' \in \mathcal{P}_{\mathrm{fr}}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ such that $\mathcal{O}[\![E]\!] \to S'$ there exists $S'' \in \mathcal{P}_{\mathrm{fr}}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ such that $\mathcal{O}[\![F]\!] \to S''$ and $\mathsf{R}_{\mathbf{lub}}(S')(r) \leq \mathsf{R}_{\mathbf{lub}}(S'')(r)$.*

Proof. The proof is the dual of Lemma 3.6 above. □

The next two lemmas demonstrate that the operational semantics is well-behaved on guarded terms with respect to substitution of free variables.

Lemma 3.8 *If $G \in \mathcal{G}$ such that $G\{E/x\} \in \mathrm{Pr}$ for all $E \in \mathrm{Pr}$, then there exists a set $\mathbf{S}_G \subseteq \mathcal{P}_{\mathrm{fr}}(\mathcal{A}ct \times \mu(\mathrm{RP}))$ such that for any $E \in \mathrm{Pr}$, $\mathcal{O}[\![G\{E/x\}]\!] \to S_E$ if and only if there exists $S_G \in \mathbf{S}_G$ where $(a, \pi_E) \in S_E$ if and only if $(a, \pi_G) \in S_G$ and for any $F \in \mathrm{Pr}$:*

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

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

Lemma 3.9 *For any $H \in$ RP and $F, F' \in$ Pr such that $H\{E/x\} \in$ Pr for all $E \in$ Pr and $\mathsf{R}_*(F)(t) \leq \mathsf{R}_*(F')(t)$ for all $t \in \mathtt{T}$ then:*

$$\mathsf{R}_*(H\{F/x\})(t) \leq \mathsf{R}_*(H\{F'/x\})(t) \ \ \textit{for all } t \in \mathtt{T}.$$

Proof. Consider any $H \in$ RP and $F, F' \in$ Pr such that $H\{E/x\} \in$ Pr for any $E \in$ Pr and $\mathsf{R}_*(F)(t) \leq \mathsf{R}_*(F')(t)$ for all $t \in \mathtt{T}$. We prove the lemma by induction on the structure of $H \in$ RP.

(i) If $H \in \mathcal{X}$, then by the hypothesis $H = x$ and for any $t \in \mathtt{T}$:

$$\mathsf{R}_*(H\{F/x\})(t) = \mathsf{R}_*(F)(t) \leq \mathsf{R}_*(F')(t) = \mathsf{R}_*(H\{F'/x\})(t).$$

(ii) If $H = a.\sum_{i\in I} \mu_i.H_i$ and $t \in \mathtt{T}$, then we have the following three cases to consider.

(a) $t = (\!|\omega|\!)$, then $\mathsf{R}_*(H\{F/x\})(t) = 1 = \mathsf{R}_*(H\{F'/x\})(t)$ by Definition 2.2.

(b) $t \neq (\!|\omega|\!)$ and $t \neq (\!|[a.T]|\!)$ for any $T \in \mathtt{T}_\omega$, then $\mathsf{R}_*(H\{F/x\})(t) = 0 = \mathsf{R}_*(H\{F'/x\})(t)$ by Definition 2.2 and the transition rules.

(c) $t = (\!|[a.T]|\!)$ for some $T \in \mathtt{T}_\omega$, then $T = (t_1, \dots, t_m)$ where $t_i \in \mathtt{T}$ for all $1 \leq i \leq m$, and hence by induction and Definition 2.2 we have:

(3) $$\mathsf{R}(H_i\{F/x\})(T) \leq \mathsf{R}(H_i\{F'/x\})(T) \quad \text{for all } i \in I.$$

Furthermore, by Definition 2.2 and the transition rules:

$$\begin{aligned}\mathsf{R}_*(H\{F/x\})((\!|[a.T]|\!)) &= \sum_{i\in I} \mu_i \cdot \mathsf{R}_*(H_i\{F/x\})(T) \\ &\leq \sum_{i\in I} \mu_i \cdot \mathsf{R}_*(H_i\{F'/x\})(T) \text{ by (3)} \\ &= \mathsf{R}_*(H\{F'/x\})((\!|[a.T]|\!)).\end{aligned}$$

(iii) If $H = H_1 \sqcap H_2$, $H = H_1 \,\Box\, H_2$, $H = H_1 \parallel H_2$, $H = H' \lceil B$ or $H = H'\,[\lambda]$, the result follows using induction and Lemma 3.5.

(iv) If $H = \mathit{fix}_y.H'$, then either $x = y$ in which case x is not free in H, therefore $H\{F/x\} = H\{F'/x\} = H$, and hence the lemma holds in this case, or $y \neq x$ in which case for any $t \in \mathtt{T}$ and $E \in$ Pr since $x \neq y$ by definition of the transition rules we can show:

(4) $$\mathsf{R}_*(H\{E/x\})(t) = \mathsf{R}_*(H'\{H/y\}\{E/x\})(t).$$

Therefore, for any $t \in \mathtt{T}$:

$$\begin{aligned}\mathsf{R}_*(H\{F/x\})(t) &= \mathsf{R}_*(H'\{H/y\}\{F/x\})(t) \\ &\leq \mathsf{R}_*(H'\{H/y\}\{F'/x\})(t) \text{ by induction on } H'\{H/y\} \\ &= \mathsf{R}_*(H\{F'/x\})(t) \qquad \text{by (4)}\end{aligned}$$

and hence the lemma holds in this case.

□

Using the lemmas above we can now show that $\overset{\mathsf{R}}{\sim}$ is a congruence over RP.

Proposition 3.10 (Congruence) *The pre-order* $\sqsubseteq^{\mathsf{R}}$ *is preserved by all contexts in the language* RP*. Formally, if we have that* $\mathcal{O}[\![E_i]\!] \sqsubseteq^{\mathsf{R}} \mathcal{O}[\![F_i]\!]$ *for all* $i \in I$ *and* $\mathcal{O}[\![E]\!] \sqsubseteq^{\mathsf{R}} \mathcal{O}[\![F]\!]$*, then:*

$$\mathcal{O}[\![a.\textstyle\sum_{i\in I} \mu_i.E_i]\!] \sqsubseteq^{\mathsf{R}} \mathcal{O}[\![a.\textstyle\sum_{i\in I} \mu_i.F_i]\!]$$

$$\mathcal{O}[\![E \,\Box\, G]\!] \sqsubseteq^{\mathsf{R}} \mathcal{O}[\![F \,\Box\, G]\!]$$

$$\mathcal{O}[\![E \sqcap G]\!] \sqsubseteq^{\mathsf{R}} \mathcal{O}[\![F \sqcap G]\!]$$

$$\mathcal{O}[\![E \,\|\, G]\!] \sqsubseteq^{\mathsf{R}} \mathcal{O}[\![F \,\|\, G]\!]$$

$$\mathcal{O}[\![E \upharpoonright B]\!] \sqsubseteq^{\mathsf{R}} \mathcal{O}[\![F \upharpoonright B]\!]$$

$$\mathcal{O}[\![E\,[\lambda]]\!] \sqsubseteq^{\mathsf{R}} \mathcal{O}[\![F\,[\lambda]]\!]$$

$$\mathcal{O}[\![\mathit{fix}_x.E]\!] \sqsubseteq^{\mathsf{R}} \mathcal{O}[\![\mathit{fix}_x.F]\!].$$

Proof. The proof follows straightforwardly from Lemma 3.5, except in the cases of $\Box$ and *fix* which we now prove.

In the case for $\Box$, suppose $E, F, G \in \mathrm{Pr}$ and $\mathcal{O}[\![E]\!] \sqsubseteq^{\mathsf{R}} \mathcal{O}[\![F]\!]$. If $S' \in \mathcal{P}_{\mathrm{fr}}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ and $\mathcal{O}[\![F \,\Box\, G]\!] \to S'$, then by definition of the transition rules there exist $S_1, S_2 \in \mathcal{P}_{\mathrm{fr}}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ such that $\mathcal{O}[\![F]\!] \to S_1$, $\mathcal{O}[\![G]\!] \to S_2$ and S' is a maximal reactive subset of $S_1 \cup S_2$. Now, considering any $(\!|r|\!) \in \mathtt{T}$, either $r = \omega$, in which case since by construction $\mathcal{O}[\![E \,\Box\, G]\!] \to S''$ for some $S'' \in \mathcal{P}_{\mathrm{fr}}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$, by definition of $\mathsf{R}_{\mathbf{glb}}$: $\mathsf{R}_{\mathbf{glb}}(S')(\omega) = 1 = \mathsf{R}_{\mathbf{glb}}(S'')(\omega)$, 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 $(a_i, \pi) \in S' \cap S_2$, 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 $\mathsf{R}_{\mathbf{glb}}$ we have:

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

Moreover, since $\mathcal{O}[\![E]\!] \sqsubseteq^{\mathsf{R}} \mathcal{O}[\![F]\!]$, by definition $\mathcal{O}[\![E]\!] \sqsubseteq^{\mathbf{glb}} \mathcal{O}[\![F]\!]$ and since $\mathcal{O}[\![F]\!] \to S_1$, Lemma 3.6 implies there exists $S'_1 \in \mathcal{P}_{\mathrm{fr}}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ such that $\mathsf{R}_{\mathbf{glb}}(S'_1)(r_1) \leq \mathsf{R}_{\mathbf{glb}}(S_1)(r_1)$ and $\mathcal{O}[\![E]\!] \to S'_1$. Furthermore, it follows by definition of the transition rules that there exists $S'' \in \mathcal{P}_{\mathrm{fr}}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ such that $\mathcal{O}[\![E \,\Box\, G]\!] \to S''$ and

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

Combining the above, we have $\mathsf{R}_{\mathbf{glb}}(S')(r) \geq \mathsf{R}_{\mathbf{glb}}(S'')(r)$, and since this was for any $(\!|r|\!) \in \mathtt{T}$ and $S' \in \mathcal{P}_{\mathrm{fr}}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ such that $\mathcal{O}[\![F \,\Box\, G]\!] \to S'$, Lemma 3.6 implies $\mathcal{O}[\![E \,\Box\, G]\!] \sqsubseteq^{\mathbf{glb}} \mathcal{O}[\![F \,\Box\, G]\!]$.

Similarly, using Lemma 3.7 instead of Lemma 3.6 and considering any $S' \in \mathcal{P}_{\mathrm{fr}}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ such that $\mathcal{O}[\![E \,\Box\, G]\!] \to S'$, we can show $\mathcal{O}[\![E \,\Box\, F]\!] \sqsubseteq^{\mathbf{lub}}$

$\mathcal{O}[\![F \Box G]\!]$, and thus, since $\sqsubseteq^{\mathsf{R}}$ is the intersection of the orderings $\sqsubseteq^{\mathbf{glb}}$ and $\sqsubseteq^{\mathbf{lub}}$, $\mathcal{O}[\![E \Box G]\!] \sqsubseteq^{\mathsf{R}} \mathcal{O}[\![F \Box G]\!]$ as required.

In the case for *fix*, to simplify the proof we only consider the case when E and F have at most x as a free variable. Then by definition $\mathit{fix}_x.E, \mathit{fix}_x.F \in \mathrm{Pr}$ and $E\{G/x\}, F\{G/x\} \in \mathrm{Pr}$ for all $G \in \mathrm{Pr}$. Furthermore, since by hypothesis $\mathcal{O}[\![E]\!] \sqsubseteq^{\mathsf{R}} \mathcal{O}[\![F]\!]$, we have $\mathcal{O}[\![E\{G/x\}]\!] \sqsubseteq^{\mathsf{R}} \mathcal{O}[\![F\{G/x\}]\!]$ for all $G \in \mathrm{Pr}$ by Definition 3.4, and hence:

$$\mathsf{R}_*(E\{G/x\})(t) \leq \mathsf{R}_*(F\{G/x\})(t) \text{ for all } G \in \mathrm{Pr} \text{ and } t \in \mathtt{T}. \tag{5}$$

To prove $\mathcal{O}[\![\mathit{fix}_x.E]\!] \sqsubseteq^{\mathsf{R}} \mathcal{O}[\![\mathit{fix}_x.F]\!]$ by definition of $\sqsubseteq^{\mathsf{R}}$, it is sufficient to show:

$$\mathsf{R}_*(\mathit{fix}_x.E)((\!|r|\!)) \leq \mathsf{R}_*(\mathit{fix}_x.F)((\!|r|\!)) \text{ for all } (\!|r|\!) \in \mathtt{T} \tag{6}$$

which we now prove by induction on $(\!|r|\!) \in \mathtt{T}$, where to ease notation we let $E' = \mathit{fix}_x.E$ and $F' = \mathit{fix}_x.F$. If $r = \omega$, then (6) holds by Definition 2.2.

If r is of the form $[a_1, T_1, \ldots, a_m.T_m]$, we first consider the test T_i for any $1 \leq i \leq m$. By definition of the testing language $\mathtt{T}$, T_i is of the form $((\!|r^i_1|\!), \ldots, (\!|r^i_{m_i}|\!))$, and hence by Definition 2.2:

$$\begin{aligned} \mathsf{R}_*(E')(T_i) &= \prod_{j=1}^{m_i} \mathsf{R}_*(E')((\!|r^i_j|\!)) \\ &\leq \prod_{j=1}^{m_i} \mathsf{R}_*(F')((\!|r^i_j|\!)) && \text{by induction} \\ &= \mathsf{R}_*(F')(T_i) && \text{by Definition 2.2.} \end{aligned}$$

Therefore, by Lemma 3.9 we have:

$$\mathsf{R}_*(H\{E'/x\})(T_i) \leq \mathsf{R}_*(H\{F'/x\})(T_i) \tag{7}$$

for any $H \in \mathrm{RP}$ such that $H\{G/x\} \in \mathrm{Pr}$ for all $G \in \mathrm{Pr}$.

Next, since by hypothesis $F\{G/x\} \in \mathrm{Pr}$ for all $G \in \mathrm{Pr}$, using Lemma 3.8 we infer that for any $S_{E'} \in \mathcal{P}_{\mathrm{fr}}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ such that $\mathcal{O}[\![F\{E'/x\}]\!] \to S_{E'}$ there exists $S_{F'} \in \mathcal{P}_{\mathrm{fr}}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ where $\mathcal{O}[\![F\{F'/x\}]\!] \to S_{F'}$, $(a, \pi_{E'}) \in S_{E'}$ if and only if $(a, \pi_{F'}) \in S_{F'}$ and for any $G \in \mathrm{Pr}$:

$$\pi_{E'}(G) = \begin{cases} \pi_F(H) & \text{if } G = H\{E'/x\} \text{ for some } H \in \mathrm{RP} \\ 0 & \text{otherwise} \end{cases} \tag{8}$$

and

$$\pi_{F'}(G) = \begin{cases} \pi_F(H) & \text{if } G = H\{F'/x\} \text{ for some } H \in \mathrm{RP} \\ 0 & \text{otherwise} \end{cases} \tag{9}$$

for some $\pi_F \in \mu(\mathrm{RP})$.

Then, considering the test $a_i.T_i$ we have the following two cases:

(i) $(a, \pi) \notin S_{E'}$ for any $\pi \in \mu(\mathrm{Pr})$ then $(a, \pi) \notin S_{F'}$ for any $\pi \in \mu(\mathrm{Pr})$, and hence $\mathsf{R}_*(S_{E'})(a_i.T_i) = 0 = \mathsf{R}_*(S')(a_i.T_i)$ by Definition 2.2.

(ii) $(a, \pi_{E'}) \in S_{E'}$ for some $\pi_{E'} \in \mu(\mathrm{Pr})$, then by Definition 2.2 and (8),

$\mathsf{R}_*(S_{E'})(a_i.T_i)$ equals:

$$
\begin{aligned}
&= \sum_{H\in\mathrm{RP}} \pi_F(H)\cdot \mathsf{R}_*(H\{E'/x\})(T_i) && \text{for some } \pi_F \in \mu(\mathrm{RP})\\
&\leq \sum_{H\in\mathrm{RP}} \pi_{F'}(H)\cdot \mathsf{R}_*(H\{F'/x\})(T_i) && \text{by (7)}\\
&= \mathsf{R}_*(S_{F'})(a_i.T_i) && \text{by Definition 2.2 and (9).}
\end{aligned}
$$

Now, since these are all the possible cases and this was for arbitrary $1 \leq i \leq m$, we have $\mathsf{R}_*(S_{E'})(r) \leq \mathsf{R}_*(S_{F'})(r)$ by Definition 2.2. Furthermore, since $S_{E'} \in \mathcal{P}_{\mathrm{fr}}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ was arbitrary, for any $S_{E'} \in \mathcal{P}_{\mathrm{fr}}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ such that $\mathcal{O}[\![F\{E'/x\}]\!] \to S_{E'}$ there exists $S_{F'} \in \mathcal{P}_{\mathrm{fr}}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ such that $\mathcal{O}[\![F\{F'/x\}]\!] \to S_{F'}$ and $\mathsf{R}_{\mathbf{lub}}(S_{E'})(r) \leq \mathsf{R}_{\mathbf{lub}}(S_{F'})(r)$. Furthermore, by symmetry for any $S_{F'} \in \mathcal{P}_{\mathrm{fr}}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ such that $\mathcal{O}[\![F\{F'/x\}]\!] \to S_{F'}$ there exists $S_{E'} \in \mathcal{P}_{\mathrm{fr}}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$ such that $\mathcal{O}[\![F\{E'/x\}]\!] \to S_{E'}$ and $\mathsf{R}_{\mathbf{lub}}(S_{E'})(r) \leq \mathsf{R}_{\mathbf{lub}}(S_{F'})(r)$. Putting this together, by Definition 2.2 we have

$$
\begin{aligned}
&\mathsf{R}_*(F\{E'/x\})((\!|r|\!)) \leq \mathsf{R}_*(F\{F'/x\})((\!|r|\!))\\
&\quad\Rightarrow \mathsf{R}_*(E\{E'/x\})((\!|r|\!)) \leq \mathsf{R}_*(F\{F'/x\})((\!|r|\!)) && \text{by (5)}\\
&\quad\Rightarrow \mathsf{R}_*(E')((\!|r|\!)) \leq \mathsf{R}_*(F')((\!|r|\!)) && \text{by the transition rules}
\end{aligned}
$$

and hence (6) holds by induction as required. □

3.3 Equational Laws

In this section, we investigate equational laws for RP. We first define the following "equality" and "order" relations co-inductively over the set of processes of RP.

Definition 3.11 A relation $\equiv^{\mathrm{e}} \subseteq \mathrm{Pr}\times\mathrm{Pr}$ is an "equality" relation if whenever $E \equiv^{\mathrm{e}} F$:

(*i*) if $\mathcal{O}[\![E]\!] \to S'$ then $\mathcal{O}[\![F]\!] \to S''$ such that $S' \equiv^{\mathrm{e}} S''$
(*ii*) if $\mathcal{O}[\![F]\!] \to S''$ then $\mathcal{O}[\![E]\!] \to S'$ such that $S'' \equiv^{\mathrm{e}} S'$

where for any $S', S'' \in \mathcal{P}_{\mathrm{fr}}(\mathcal{A}ct\times\mu(\mathrm{RP}))$, $S' \equiv^{\mathrm{e}} S''$ 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 an "order" relation if whenever $E \sqsubseteq^{\mathrm{e}} F$:

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

where for any $S', S'' \in \mathcal{P}_{\mathrm{fr}}(\mathcal{A}ct \times \mu(\mathrm{RP}))$, $S' \sqsubseteq^{\mathrm{e}} S''$ 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 "order" relations as our equality and order over RP.

Definition 3.12 Let $\equiv$ and $\sqsubseteq$ be the maximum "equality" relation and "order" relation respectively.

We now list some of the equational laws of RP in Figure 1 below, where we assume $a, b \in \mathcal{A}ct$ are distinct.

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

Fig. 1. Equational Laws of RP.

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 $\parallel$ 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 laws 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 2 below.

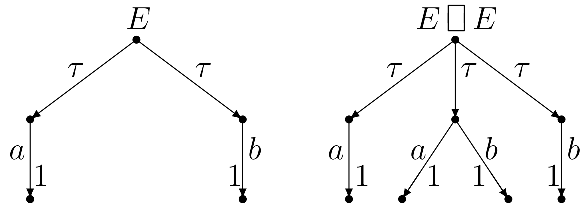


Fig. 2. Example to show external choice is not idempotent.

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

4 Denotational Semantics

In this section we present denotational semantics for our probabilistic calculus RP, based on de Bakker and Zucker's metric-space construction of denotational semantics for non-probabilistic process calculi [3]. The reader should note though that through the addition of probabilistic behaviour our setting becomes more complex, and as a result several of the techniques of de Bakker and Zucker and the more general metric constructions of America and Rutten [1] could not be used. For example, we were unable to inductively define a metric and use the categorical techniques of [1] to derive a domain equation for reactive probabilistic processes. Instead, we use a metric simultaneously based on both the *tree-like "paths"* that processes can perform and *truncations*, and construct a complete metric space of reactive probabilistic processes via the standard completion of the finite processes. For a more detailed account of our construction and the problems encountered see [20].

We proceed by applying the techniques of [3] to derive an inductively defined collection of carrier sets $(R_n)_{n \in \mathbb{N}}$, where the elements of the spaces model *finite* reactive probabilistic processes. Intuitively, for any $n \in \mathbb{N}$, R_n models the reactive probabilistic processes capable of performing transitions up to the *depth* n. First, however, we require the following definition.

Definition 4.1 For any sets A and R, let $A \rightharpoonup R$ denote the set of *partial maps* from A to R. Furthermore, for any $f \in A \rightharpoonup S$, let $dom(f)$ denote the subset of A on which f is defined, and let $\perp \in A \rightharpoonup R$ be the totally undefined function, that is, $\perp$ is the partial map such that $dom(\perp) = \emptyset$.

Formally, we define the carrier sets $(R_n)_{n \in \mathbb{N}}$ as follows, where $\mathcal{P}_{\mathrm{fn}}(\cdot)$ denotes the powerset operator restricted to finite nonempty subsets.

Definition 4.2 (Finite reactive probabilistic processes) Let R_n, $n \in \mathbb{N}$, be a collection of carrier sets defined inductively by:

$$R_0 = \{\perp\} \ \text{ and } \ R_{n+1} = \mathcal{P}_{\mathrm{fn}}(A \rightharpoonup \mu(R_n)).$$

Furthermore, let $R_\omega = \cup_n R_n$ denote the set of reactive probabilistic processes of bounded depth.

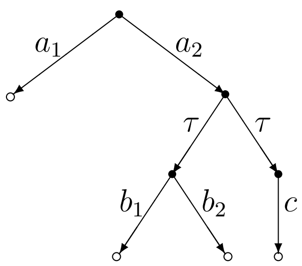
As mentioned above, the metric we introduce is based on the tree-like "paths" that processes can perform and truncations, which we now introduce. First, the set of "paths" that processes can perform, A^*_{r}, is defined as follows, where $\mathcal{P}_{\mathrm{fnr}}(\cdot \times \cdot)$ denotes the powerset operator restricted to finite nonempty subsets of cartesian products satisfying the reactiveness condition.

Definition 4.3 Let A^n_{r}, $n \in \mathbb{N}$, be the sets inductively defined as follows. Put:

$$A^0_{\mathrm{r}} = \mathcal{P}_{\mathrm{fnr}}(A) \ \text{ and } \ A^{n+1}_{\mathrm{r}} = \mathcal{P}_{\mathrm{fnr}}\Big((A \times \mathcal{P}_{\mathrm{fnr}}(A^n_{\mathrm{r}})) \cup A\Big).$$

Furthermore, let $A^*_{\mathrm{r}} = \cup_n A^n_{\mathrm{r}}$.

The elements of A^*_{r} can be thought of graphically as tree-like computation paths. For example, $\{a_1, (a_2, \{\{b_1, b_2\}, \{c\}\})\} \in A^1_{\mathrm{r}}$ can be represented as follows:



Next we introduce the map $\mathcal{V}$ which calculates *the probability of processes performing "paths" in A^*_{r}*. As already stated earlier, since processes can perform non-deterministic choices we will be unable to calculate the exact probabilities. To overcome this we let $\mathcal{V}$ take values in the set of closed *intervals* (subsets) of $[0,1]$, denoted by the set $\mathcal{I}$, which we endow with a distance $d_{\mathcal{I}}$. Therefore, before we introduce the map $\mathcal{V}$, we formally define $\mathcal{I}$ and introduce the operators on $\mathcal{I}$ required in the definition of $\mathcal{V}$, and also the definitions pertaining to $\mathcal{I}$ that we will require later on in this section.

Definition 4.4 (Intervals) Let $\mathcal{I} = \{[a,b] \,|\, 0 \leq a \leq b \leq 1\}$. We now define addition, multiplication, union and scalar multiplication on $\mathcal{I}$ as follows. For all $[a,b], [c,d] \in \mathcal{I}$ and $e \in [0,1]$:

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

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

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

Proposition 4.5 *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*

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

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

Definition 4.6 Let $d_{\mathcal{I}}:\mathcal{I}\times\mathcal{I}\longrightarrow[0,1]$ 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 4.7 *The mapping $d_{\mathcal{I}}$ is a metric on $\mathcal{I}$.*

Lemma 4.8 *For all $[a,b],[c,d]\in\mathcal{I}$, $0\leq d_{\mathcal{I}}([a,b],[c,d])\leq 1$.*

Proposition 4.9 *For all $[a_1,b_1]$, $[a_2,b_2]$ and $[c,d]\in\mathcal{I}$:*

$$(a)\ d_{\mathcal{I}}([a_1,b_1]\cdot[c,d],[a_2,b_2]\cdot[c,d])\leq d_{\mathcal{I}}([a_1,b_1],[a_2,b_2])$$

$$(b)\ d_{\mathcal{I}}([a_1,b_1]\sqcup[c,d],[a_2,b_2]\sqcup[c,d])\leq d_{\mathcal{I}}([a_1,b_1],[a_2,b_2]).$$

Proposition 4.10 *If $n\geq 1$ and $\{[a_i,b_i]\,|\,i\in\{1,\ldots,n\}\}$ and $\{[c_i,d_i]\,|\,i\in\{1,\ldots,n\}\}$ are subsets of $\mathcal{I}$, then there exists $j\in\{1,\ldots,n\}$ such that:*

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

We are now in a position to define $\mathcal{V}$ as follows. Given a "path" V in A_{r}^* and a process p in R_ω, the map $\mathcal{V}$ calculates the *interval of probabilities* to which the probability of the process p performing V belongs.

Definition 4.11 Let $\mathcal{V}:(A_{\text{r}}^*\times R_\omega)\longrightarrow\mathcal{I}$ be the mapping defined inductively on A_{r}^n as follows. For any $f\in A\rightharpoonup\mu(R_\omega)$, $a\in A$, $V\in A_{\text{r}}^n$ and $\mathbf{V}\in\mathcal{P}_{\text{fnr}}(A_{\text{r}}^n)$ put:

$$\mathcal{V}(a,f)=\begin{cases}[1,1] \text{ if } a\in dom(f)\\ [0,0] \text{ otherwise}\end{cases}$$

$$\mathcal{V}(a\mathbf{V},f)=\begin{cases}\sum_{q\in R_\omega} f(a)(q)\cdot\mathcal{V}(\mathbf{V},q) \text{ if } a\in dom(f)\\ [0,0] \qquad\qquad \text{otherwise}\end{cases}$$

$$\mathcal{V}(V,f) = \prod_{v \in V} \mathcal{V}(v,f)$$

and furthermore for all $p \in R_\omega$ put:

$$\mathcal{V}(\mathbf{V},p) = \prod_{V \in \mathbf{V}} \mathcal{V}(V,p) \quad \text{and} \quad \mathcal{V}(V,p) = \bigsqcup_{f \in p} \mathcal{V}(V,f).$$

To show the well-definedness of the above map we use the following lemma.

Lemma 4.12 *For all $p \in R_\omega$ and $V \in A_{\mathrm{r}}^* : \mathcal{V}(V,p) \in \mathcal{I}$.*

Using the map $\mathcal{V}$ and metric $d_{\mathcal{I}}$ defined above we can introduce a metric on processes in R_ω given below. For a pair of processes p, q we first calculate, for each "path" V, the interval of probabilities of p performing V, and q performing V respectively, and then take the max norm over the "paths" V of the distance $d_{\mathcal{I}}$ between thus computed intervals. Thus, the closer the intervals of probabilities, the closer the processes are. Summation could not be used in place of max since it is unbounded.

Proposition 4.13 *R_ω (and R_n for any $n \in \mathbb{N}$) is a pseudo-metric space with respect to the metric:*

$$d_{\mathcal{V}}(p,q) = \max_{V \in A_{\mathrm{r}}^*} d_{\mathcal{I}}(\mathcal{V}(V,p), \mathcal{V}(V,q)).$$

Furthermore, $0 \leq d_{\mathcal{V}}(p,q) \leq 1$ for all $p, q \in R_\omega$.

Intuitively, the metric $d_{\mathcal{V}}$ over R_ω gives us the correct notion of convergence of Cauchy sequences. If we consider the sequence of processes $\langle E_n \rangle_n$ of RP where $E_n = a.(2^{-n}).b.1.\mathbf{0} + a.(1-2^{-n}).\mathbf{0}$ then, as $n \to \infty$, the probability of E_n performing the trace ab becomes more and more insignificant, that is, the operational behaviour of E_n *converges* to the process $a.1.\mathbf{0}$, and hence we would expect the sequence $\langle E_n \rangle_n$ to be Cauchy. Now, for any $n \in \mathbb{N}$ the distance between the denotations of E_n and E_{n+1} with respect to the metric $d_{\mathcal{V}}$ would be $2^{-(n+1)}$, and thus $\langle E_n \rangle_n$ is Cauchy as required. In contrast, with respect to the classically derived ultra-metric of [2], the distance between E_n and E_{n+1} would be $\frac{1}{2}$, and so this convergence property would be lost.

Unfortunately, the pseudo-metric $d_{\mathcal{V}}$ does not give us the Cauchy sequences we would expect to model recursive reactive probabilistic processes. For example, we would expect the sequence $\langle F_n \rangle_n$ where

$$F_n = \overbrace{a.1.\ldots a.1.}^{n \text{ times}}\mathbf{0}$$

for all $n \in \mathbb{N}$ to be Cauchy so that the limit can then be used to model the recursive process $\mathit{fix}_x.a.1.x$. However, the distance between F_n and F_m for any $n \neq m$ with respect to the metric $d_{\mathcal{V}}$ is 1, and thus $\langle F_n \rangle_n$ is not a Cauchy sequence with respect to $d_{\mathcal{V}}$. To solve this problem we introduce *truncations* of processes to the finite depth $k \in \mathbb{N}$ as follows.

Definition 4.14 (Truncations) Let $f \in A \rightharpoonup \mu(R_\omega)$. For $k \in \mathbb{N}$ define the kth *truncation* of f, $f[k] \in A \rightharpoonup \mu(R_\omega)$ by induction on $k \in \mathbb{N}$ by putting:

$f[0] = \perp$ and for any $k \in \mathbb{N}$, $dom(f[k+1]) = dom(f)$ and for any $a \in dom(f[k+1])$ and $p \in R_\omega$,

$$f[k+1](a)(p) = \sum_{\substack{q \in R_\omega \\ \& \, q[k]=p}} f(a)(q)$$

where for any $q \in R_\omega$ and $k \in \mathbb{N}$: $q[k] = \{g[k] \mid g \in q\}$.

The truncations of processes satisfy the properties given below, useful in the proofs included in the remainder of this section.

Proposition 4.15 *For all $p, q \in R_\omega$ and $k, m \in \mathbb{N}$:*

(a) *if $p \in R_m$, then $p[k] \in R_k$ 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) $d_\mathcal{V}(p[k], q[k]) \leq d_\mathcal{V}(p, q)$.

Lemma 4.16 *For all $p \in R_\omega$, $V \in A_\mathrm{r}^*$ and $k \in \mathbb{N}$: $\mathcal{V}(V, p[0]) = [0, 0]$ and*

$$\mathcal{V}(V, p[k+1]) = \begin{cases} \mathcal{V}(V, p) & \text{if } V \in A_\mathrm{r}^k \\ [0, 0] & \text{otherwise.} \end{cases}$$

Proof. The proof follows by induction on $k \in \mathbb{N}$. □

Now, using the metric $d_\mathcal{V}$ together with truncations, we reach the following metric on R_ω, where the distance is set to an infinite sum of distances between the truncations of the two processes with respect to the metric $d_\mathcal{V}$, with each summand weighted by the depth of the truncation in inverse proportion.

Definition 4.17 For all $p, q \in R_\omega$, we define $d_\omega : R_\omega \times R_\omega \longrightarrow [0, 1]$ as follows:

$$d_\omega(p, q) = \sum_{k=1}^{\infty} 2^{-k} \cdot d_\mathcal{V}(p[k], q[k]).$$

Proposition 4.18 (R_ω, d_ω) *(and (R_n, d_ω) for any $n \in \mathbb{N}$) is a pseudo-metric space. Furthermore, $0 \leq d_\omega(p, q) \leq 1$ for all $p, q \in R_\omega$.*

We now apply the standard metric completion technique to derive the metric space (R, d) of (finite and infinite) reactive probabilistic processes.

Definition 4.19 Define the space (R, d) of *reactive probabilistic processes* as the metric completion of (R_ω, d_ω).

Since we have applied standard completion techniques, R consists of the set of equivalence classes of Cauchy sequences of R_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 [1] have not been used to derive a domain equation for reactive 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 R_ω.

Lemma 4.20 *For all $p \in R_\omega$, $\langle p[n] \rangle_n$ is a Cauchy sequence.*

Lemma 4.21 *If $\langle p_n \rangle_{n\in\mathbb{N}}$ is a sequence in R_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 $n \in \mathbb{N}$.*

4.1 Modelling Semantic Operators of RP

Having obtained the complete metric space (R, d) (assuming $A = \mathcal{A}ct$), we can now give denotational semantics for our language RP. The first step is the introduction of the semantic operators: union (for non-deterministic choice), deterministic choice, synchronous parallel, restriction and relabelling. We have to verify that each operator is well-defined and continuous.

Definition 4.22 (Union) For any $p, q \in R_\omega$, let $p \cup q$ be set-theoretic union.

Lemma 4.23 *For all $p, q \in R_\omega$ and $n \in \mathbb{N}$: $(p \cup q)[n] = p[n] \cup q[n]$.*

Proposition 4.24 *$\cup$ is continuous and well-defined on (R_ω, d_ω).*

Proof. Consider any $p, q, r \in R_\omega$, $V' \in A_{\mathrm{r}}^*$ and $n \in \mathbb{N}$. Then by Lemma 4.23 and the definition of $\mathcal{V}$, $d_\mathcal{I}(\mathcal{V}(V', (p \cup r)[n]), \mathcal{V}(V', (q \cup r)[n])$ equals:

$$\begin{aligned}
&= d_\mathcal{I}(\mathcal{V}(V', p[n]) \sqcup \mathcal{V}(V', r[n]), \mathcal{V}(V', q[n]) \sqcup \mathcal{V}(V', r[n])) \\
&\leq d_\mathcal{I}(\mathcal{V}(V', p[n]), \mathcal{V}(V', q[n])) && \text{by Proposition 4.7}(b) \\
&\leq \max\nolimits_{V \in A_{\mathrm{r}}^*} d_\mathcal{I}(\mathcal{V}(V, p[n]), \mathcal{V}(V, q[n])) && \text{since } V' \in A_{\mathrm{r}}^* \\
&= d_\mathcal{V}(p[n], q[n]) && \text{by definition of } d_\mathcal{V}.
\end{aligned}$$

Then, since this was for arbitrary $V' \in A_{\mathrm{r}}^*$ and $n \in \mathbb{N}$, it follows by definition of d and $d_\mathcal{V}$ that $d_\omega(p \cup r, q \cup r) \leq d_\omega(p, q)$, and hence $\cup$ is continuous.

To complete the proof we show $p \cup q \in R_\omega$ for all $p, q \in R_\omega$ which follows by definition of R_ω. $\square$

Definition 4.25 (External Choice Operator) For any $p, q \in R_\omega$, let

$$p \,\Box\, q = \{h \mid h \in f \,\Box\, g,\ f \in p \text{ and } g \in q\}$$

where $f \Box g$ is the subset of $A \rightharpoonup \mu(R_\omega)$ such that $h \in f \Box g$ if and only if $dom(h) = dom(f) \cup dom(g)$ and for any $a \in dom(h)$: $h(a) = f(a)$ if $a \notin dom(g)$, $h(a) = g(a)$ if $a \notin dom(f)$ and either $h(a) = f(a)$ or $h(a) = g(a)$ otherwise.

Lemma 4.26 *For all* $p, q \in R_\omega$ *and* $V \in A_{\mathrm{r}}^*$:

$$\mathcal{V}(V, p \Box q) = \bigsqcup_{\substack{V_1 \cup V_2 = V \\ \& \, V_1 \cap V_2 = \emptyset}} \mathcal{V}(V_1, p) \cdot \mathcal{V}(V_2, q)$$

where $V_1, V_2 \in A_{\mathrm{r}}^* \cup \{\emptyset\}$ *and* $\mathcal{V}(\emptyset, r) \stackrel{\mathrm{def}}{=} [1,1]$ *for any* $r \in R_\omega$.

Proof. Consider any $p, q \in R_\omega$ and $V \in A_{\mathrm{r}}^*$, then by definition of $\mathcal{V}$ and Proposition 4.5, it is sufficient to prove that:

$$\min_{\substack{V_1 \cup V_2 = V \\ \& \, V_1 \cap V_2 = \emptyset}} \mathcal{V}(V_1, p) \cdot \mathcal{V}(V_2, q) =_{\mathrm{left}} \min_{h \in X \Box Y} \mathcal{V}(V, h)$$

and

$$\max_{\substack{V_1 \cup V_2 = V \\ \& \, V_1 \cap V_2 = \emptyset}} \mathcal{V}(V_1, p) \cdot \mathcal{V}(V_2, q) =_{\mathrm{right}} \max_{h \in X \Box Y} \mathcal{V}(V, h).$$

We only prove the case for max as the case for min follows similarly. First, consider any $h' \in p \Box q$. By definition of $\Box$, there exists $f' \in p$ and $g' \in q$ such that $h' \in f' \Box g'$. If we set:

$$V_1' = \{v \mid v = a \in V \text{ or } v = a\mathbf{V} \in V \text{ and } h'(a) = f'(a)\} \ \text{ and } \ V_2' = V \setminus V_1'$$

then $V_1' \cup V_2' = V$, $V_1' \cap V_2' = \emptyset$ and by definition of $\mathcal{V}$ we have:

$$\begin{aligned}
\mathcal{V}(V, h') &= \mathcal{V}(V_1', f') \cdot \mathcal{V}(V_2', g') \\
&\leq_{\mathrm{right}} \max_{f \in p} \mathcal{V}(V_1', f) \cdot \max_{g \in q} \mathcal{V}(V_2', g) && \text{since } f' \in p \text{ and } g' \in q \\
&=_{\mathrm{right}} \mathcal{V}(V_1', p) \cdot \mathcal{V}(V_2', q) && \text{by definition of } \mathcal{V} \\
&\leq_{\mathrm{right}} \max_{\substack{V_1 \cup V_2 = V \\ \& \, V_1 \cap V_2 = \emptyset}} \mathcal{V}(V_1, p) \cdot \mathcal{V}(V_2, q) && \text{since } V_1' \cup V_2' = V \text{ and } V_1' \cap V_2' = \emptyset.
\end{aligned}$$

Thus, since this was for arbitrary $h' \in p \Box q$ we infer:

$$\max_{h \in p \Box q} \mathcal{V}(V, h) \leq_{\mathrm{right}} \max_{\substack{V_1 \cup V_2 = V \\ \& \, V_1 \cap V_2 = \emptyset}} \mathcal{V}(V_1, p) \cdot \mathcal{V}(V_2, q). \tag{10}$$

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 $V_1' \cap V_2' = \emptyset$, by definition of $\mathcal{V}$ there exists $f' \in p$ and $g' \in q$ such that $\mathcal{V}(V_1', p) =_{\mathrm{right}} \mathcal{V}(V_1', f')$ and $\mathcal{V}(V_2', q) =_{\mathrm{right}} \mathcal{V}(V_2', g')$. Now letting $h' \in A \rightharpoonup \mu(R)$ be a partial map satisfying the following conditions: $dom(h') = dom(f') \cup dom(g')$ and for any $a \in dom(h')$:

- $h'(a) = f'(a)$ if $a \in V_1'$ or $a\mathbf{V} \in V_1'$ for some $\mathbf{V} \in \mathcal{P}_{\mathrm{fnr}}(A_{\mathrm{r}}^*)$
- $h'(a) = g'(a)$ if $a \in V_2'$ or $a\mathbf{V} \in V_2'$ for some $\mathbf{V} \in \mathcal{P}_{\mathrm{fnr}}(A_{\mathrm{r}}^*)$
- $h'(a) = f'(a)$ or $h(a) = g(a)$ if $a \notin V$ and $a\mathbf{V} \notin V$ for all $\mathbf{V} \in \mathcal{P}_{\mathrm{fnr}}(A_{\mathrm{r}}^*)$.

then by Definition 4.25 we have $h' \in p \Box q$. Then similarly to the first part of the lemma we have:

$$\mathcal{V}(V_1', f') \cdot \mathcal{V}(V_2', g') = \mathcal{V}(V, h') \leq_{\mathrm{right}} \max_{h \in p \Box q} \mathcal{V}(V, h).$$

Since this was for any $V_1', V_2' \in A_{\mathrm{r}}^* \cup \{\emptyset\}$ with $V_1' \cup V_2' = V$ and $V_1' \cap V_2' = \emptyset$, by construction of f' and g' we obtain:

$$\max_{\substack{V_1 \cup V_2 = V \\ \& \, V_1 \cap V_2 = \emptyset}} \mathcal{V}(V_1, p) \cdot \mathcal{V}(V_2, q) \leq_{\mathrm{right}} \max_{h \in p \Box q} \mathcal{V}(V, h). \tag{11}$$

Putting (10) and (11) together we have:

$$\max_{\substack{V_1 \cup V_2 = V \\ \& \, V_1 \cap V_2 = \emptyset}} \mathcal{V}(V_1, p) \cdot \mathcal{V}(V_2, q) =_{\mathrm{right}} \max_{h \in p \Box q} \mathcal{V}(V, h)$$

as required. □

Lemma 4.27 *For all $p, q \in R_\omega$ and $n \in \mathbb{N}$: $(p \Box q)[n] = p[n] \Box q[n]$.*

Proposition 4.28 *$\Box$ is continuous and well-defined on (R_ω, d_ω).*

Proof. Consider any $p, q, r \in R_\omega$, $V' \in A_{\mathrm{r}}^*$ and $n \in \mathbb{N}$. Then by Lemma 4.27, $d_{\mathcal{I}}(\mathcal{V}(V', (p \Box r)[n]), \mathcal{V}(V', (q \Box r)[n])$ equals:

$$\begin{aligned} &= d_{\mathcal{I}}(\mathcal{V}(V', p[n] \Box r[n]), \mathcal{V}(V', q[n] \Box r[n])) \\ &\leq d_{\mathcal{I}}(\mathcal{V}(V_1, p[n]) \cdot \mathcal{V}(V_2, r[n]), \mathcal{V}(V_1, q[n]) \cdot \mathcal{V}(V_2, r[n])) \end{aligned}$$

for some $V_1, V_2 \in A_{\mathrm{r}}^* \cup \{\emptyset\}$ such that $V_1 \cup V_2 = V'$ and $V_1 \cap V_2 = \emptyset$ by Lemma 4.26 and Proposition 4.10. Considering the possible forms of V_1, then either $V_1 = \emptyset$ and since $\mathcal{V}(\emptyset, r') \stackrel{\mathrm{def}}{=} [1, 1]$ for any $r' \in R_\omega$:

$$\begin{aligned} & d_{\mathcal{I}}(\mathcal{V}(V', (p \Box r)[n]), \mathcal{V}(V', (q \Box r)[n])) \\ & \qquad \leq d_{\mathcal{I}}([1, 1] \cdot \mathcal{V}(V_2, r[n]), [1, 1] \cdot \mathcal{V}(V_2, r[n])) \\ & \qquad = 0 \qquad\qquad \text{since } d_{\mathcal{I}} \text{ is a metric} \\ & \qquad \leq d_{\mathcal{V}}(p[n], q[n]) \text{ by Proposition 4.13} \end{aligned}$$

or $V_1 \in A_{\mathrm{r}}^*$ and in this case by Proposition 4.9(a):

$$\begin{aligned} d_{\mathcal{I}}(\mathcal{V}(V', (p \Box r)[n]), \mathcal{V}(V', (q \Box r)[n]) &\leq d_{\mathcal{I}}(\mathcal{V}(V_1, p[n]), \mathcal{V}(V_1, q[n])) \\ &\leq \max\nolimits_{V \in A_{\mathrm{r}}^*} d_{\mathcal{I}}(\mathcal{V}(V, p[n]), \mathcal{V}(V, q[n])) \quad \text{since } V_1 \in A_{\mathrm{r}}^* \\ &= d_{\mathcal{V}}(p[n], q[n]) \qquad\qquad \text{by definition of } d_{\mathcal{V}}. \end{aligned}$$

The remainder of the proof follows similarly to Proposition 4.24 above. □

Before we can introduce the remaining semantic operators, we need the following definition.

Definition 4.29 The *degree* of a process $p \in R_\omega$ is defined inductively by putting: $deg(p) = 0$ if $p = \{\bot\}$, $deg(p) = n + 1$ if $p \in R_{n+1} \setminus R_n$ for some $n \in \mathbb{N}$.

Using this we can now define the remaining operators by induction on the degree.

Definition 4.30 (Synchronous Parallel Operator) For any $p, q \in R_\omega$ of non-zero degree, let $\{\bot\} \,\|\, \{\bot\} = \{\bot\}$, $\{\bot\} \,\| p = p \,\|\, \{\bot\} = \{\bot\}$ and $p \| q = \{f \| g \mid f \in p \text{ and } g \in q\}$ where for any $f, g \in A \rightharpoonup \mu(R_\omega)$: $dom(f \| g) = dom(f) \cap dom(g)$ and for any $a \in dom(f \| g)$ and $r \in R_\omega$:

$$(f||g)(a)(r) = \sum_{\substack{r_1, r_2 \in R_\omega \\ \& \, r_1 \| r_2 = r}} f(a)(r_1) \cdot g(a)(r_2).$$

Lemma 4.31 *For all $p, q \in R_\omega$ and $V \in A_{\mathrm{r}}^*$ and $n \in \mathbb{N}$: $\mathcal{V}(V, p \,\|\, q) = \mathcal{V}(V, p) \cdot \mathcal{V}(V, q)$ and $(p \,\|\, q)[n] = p[n] \,\|\, q[n]$.*

Proposition 4.32 $\|$ *is continuous and well-defined on (R_ω, d_ω).*

Proof. The proof follows similarly to Proposition 4.24 using Lemma 4.8(a) and Lemma 4.31. □

Definition 4.33 (Restriction Operator) For any $p \in R_\omega$ with non-zero degree and $B \subseteq A$ let $\{\bot\} \lceil B = \{\bot\}$ and $p \lceil B = \{f \lceil B \mid f \in p\}$ where for any $f \in A \rightharpoonup \mu(R_\omega)$, $dom(f \lceil B) = dom(f) \cap B$ and for any $a \in dom(f \lceil B)$ and $q \in R_\omega$:

$$(f \lceil B)(a)(q) = \sum_{\substack{r \in R_\omega \, \& \\ r \lceil B = q}} f(a)(r).$$

Lemma 4.34 *For all $p \in R_\omega$, $V \in A_{\mathrm{r}}^*$, $B \subseteq A$ and $n \in \mathbb{N}$:*

$$\mathcal{V}(V, p \lceil B) = \begin{cases} [0,0] & \text{if } a \in V \text{ for some } a \in A \setminus B \\ \mathcal{V}(V, p) & \text{otherwise} \end{cases}$$

and $(p \lceil B)[n] = p[n] \lceil B$.

Proposition 4.35 *For all $B \subseteq A$, $\lceil B$ is continuous and well-defined on (R_ω, d_ω).*

Definition 4.36 (Relabelling Operator) For any $p \in R_\omega$ with non-zero degree and $\lambda : A \to A$ let $\{\bot\}[\lambda] = \{\bot\}$ and $p[\lambda] = \{f[\lambda] \mid f \in p\}$ where for any $f \in A \rightharpoonup \mu(R_\omega)$, $dom(f[\lambda]) = \{\lambda(a) \mid a \in dom(f)\}$, and for any $a \in dom(f\,[\lambda])$ and $q \in R_\omega$:

$$f(a)\,[\lambda](q) = \sum_{\substack{r \in R_\omega \, \& \\ r\,[\lambda] = q}} f(a)(r).$$

Lemma 4.37 *For all $p \in R_\omega$, $V \in A_{\mathrm{r}}^*$, $\lambda : A \to A$ and $n \in \mathbb{N}$: $\mathcal{V}(V, p\,[\lambda]) = \mathcal{V}(\lambda^{-1}(V), p)$ and $(p\,[\lambda])[n] = (p[n])\,[\lambda]$.*

Proposition 4.38 *For all $\lambda : A \to A$, $[\lambda]$ is continuous and well-defined on (R_ω, d_ω).*

4.2 Denotational Semantics for RP

We are now in a position to give denotational semantics to the guarded expressions $\mathcal{G}$ of RP. We accomplish this by defining a map $\mathcal{D}$ from RP to R, but only consider properties of this map over guarded terms. By construction, the elements of R are the equivalence classes of the Cauchy sequences of (R_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 RP to R_ω such that $\langle\mathcal{D}[\![E]\!]\rangle_{n\in\mathbb{N}}$ is Cauchy for any $E \in \mathcal{G}$, and then set $\mathcal{D}[\![E]\!] = [\langle\mathcal{D}[\![E]\!]\rangle_{n\in\mathbb{N}}]_\sim$ for any $E \in \mathcal{G}$.

As usual, in order to handle the variables x in the expressions RP, we introduce environments Env, ranged over by ρ, defined by Env$= \mathcal{X} \to R$. Similarly to the above discussion, for any $\rho \in$ Env we can suppose that there exists a sequence of maps $(\rho_n)_{n\in\mathbb{N}}$ such that $\rho_n : \mathcal{X} \to R_\omega$ for all $n \in \mathbb{N}$, $\langle\rho_n(x)\rangle_{n\in\mathbb{N}}$ is Cauchy in (R_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 4.39 For any set R, $a \in A$ and family $\langle\mu_i, p_i\rangle_{i\in I}$ where $\langle\mu_i, p_i\rangle \in (0,1] \times R$ for all $i \in I$ and $q \in R$, let:

$$dom(\Phi_R(a, \langle\mu_i, p_i\rangle_{i\in I})) = \{a\} \ \text{ and } \ \Phi_R(a, \langle\mu_i, p_i\rangle_{i\in I})(a)(q) = \sum_{\substack{i\in I\,\&\\ q=p_i}} \mu_i.$$

Lemma 4.40 *If* $\sum_{i\in I}\mu_i = 1$*, then* $\Phi_R(a, \langle\mu_i, p_i\rangle_{i\in I}) \in A \rightharpoonup \mu(R)$*.*

We can now define denotational metric-space semantics for RP.

Definition 4.41 (Denotational Semantics) Let $\mathcal{D}_n : \text{RP} \to (\text{Env} \to R_\omega)$, $n \in \mathbb{N}$, be the collection of maps defined inductively as follows. Put $\mathcal{D}_0[\![E]\!] = \{\bot\}$ for all $E \in$ RP, and $\mathcal{D}_{n+1}$ be defined inductively on the structure of elements of RP as follows:

$$\begin{aligned}
\mathcal{D}_{n+1}[\![x]\!](\rho) &= \rho_{n+1}(x)\\
\mathcal{D}_{n+1}[\![\mathbf{0}]\!](\rho) &= \{\bot\}\\
\mathcal{D}_{n+1}[\![\textstyle\sum_{i\in I} a_{\mu_i}.E_i]\!](\rho) &= \{\Phi_{R_\omega}(a, \langle\mu_i, \mathcal{D}_n[\![E_i]\!](\rho)\rangle_{i\in I})\}\\
\mathcal{D}_{n+1}[\![E_1 \sqcap E_2]\!](\rho) &= \mathcal{D}_{n+1}[\![E_1]\!](\rho) \cup \mathcal{D}_{n+1}[\![E_2]\!](\rho)\\
\mathcal{D}_{n+1}[\![E_1 \,\square\, E_2]\!](\rho) &= \mathcal{D}_{n+1}[\![E_1]\!](\rho) \,\square\, \mathcal{D}_{n+1}[\![E_2]\!](\rho)\\
\mathcal{D}_{n+1}[\![E_1 \parallel E_2]\!](\rho) &= \mathcal{D}_{n+1}[\![E_1]\!](\rho) \parallel \mathcal{D}_{n+1}[\![E_2]\!](\rho)\\
\mathcal{D}_{n+1}[\![E \upharpoonright B]\!](\rho) &= \mathcal{D}_{n+1}[\![E]\!](\rho) \upharpoonright B\\
\mathcal{D}_{n+1}[\![E\,[\lambda]]\!](\rho) &= \mathcal{D}_{n+1}[\![E]\!](\rho)\,[\lambda]\\
\mathcal{D}_{n+1}[\![\mathit{fix}_x.E]\!](\rho) &= \mathcal{D}_{n+1}[\![E]\!](\rho\{\mathcal{D}_n[\![\mathit{fix}_x.E]\!](\rho)/x\}).
\end{aligned}$$

Furthermore, let $\mathcal{D} : \text{RP} \to (\text{Env} \to R)$ be the map defined as follows: for any $E \in$ 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 we shall require the following technical lemma.

Lemma 4.42 *For all* $E \in \mathrm{RP}$*,* $G \in \mathcal{G}$*,* $F \in \mathrm{Pr}$*,* $\rho \in \mathrm{Env}$ *and* $n \in \mathbb{N}$:

(*a*) $\mathcal{D}_{n+1}[\![G]\!](\rho)[n] = \mathcal{D}_n[\![G]\!](\rho)[n]$

(*b*) $\mathcal{D}_n[\![E\{F/x\}]\!](\rho)[n] = \mathcal{D}_n[\![E]\!](\rho\{D_n[\![F]\!]/x\})[n]$

(*c*) $\mathcal{D}_{n+1}[\![G\{F/x\}]\!](\rho)[n+1] = \mathcal{D}_{n+1}[\![G]\!](\rho\{D_n[\![F]\!]/x\})[n+1]$.

Proof. The lemma follows by induction on the structure of $E \in \mathrm{RP}$ and $G \in \mathcal{G}$. □

Proposition 4.43 $\mathcal{D}$ *is well-defined on the guarded expressions of* RP*.*

Proof. First, we prove that $\mathcal{D}_n[\![E]\!](\rho) \in R_\omega$ for all $E \in \mathcal{G}$ and $n \in \mathbb{N}$ by induction on n. The case for $n = 0$ is trivial.

Now suppose $\mathcal{D}_n[\![E]\!](\rho) \in R_\omega$ for all $E \in \mathcal{G}$ and some $n \in \mathbb{N}$, we prove the case for $n+1$ by induction on the structure of $E \in \mathcal{G}$.

(i) If $E = \mathbf{0}$, then by definition $\mathcal{D}_{n+1}[\![\mathbf{0}]\!](\rho) = \{\perp\} \in R_\omega$.

(ii) If $E = a.\sum_{i\in I}\mu_i.E_i$, then by induction $\mathcal{D}_n[\![E_i]\!](\rho) \in R_\omega$ for all $i \in I$, and since by construction $\sum_{i\in I}\mu_i = 1$, using Lemma 4.40 we have:

$$\Phi_{R_\omega}(a, \langle \mu_i, \mathcal{D}_n[\![E_i]\!](\rho)\,\rangle_{i\in I}) \in A \rightharpoonup \mu(R_\omega)$$

and therefore, $\mathcal{D}_{n+1}[\![E]\!](\rho) \in R_\omega$ by definition of $\mathcal{D}_{n+1}$.

(iii) If $E = E_1 \sqcap E_2$, $E = E_1 \,\Box\, E_2$, $E = E_1 \parallel E_2$, $E = E' \lceil B$ or $E = E'\,[\lambda]$, the proposition holds by definition of $\mathcal{D}_{n+1}$, the well-definedness of the semantic operators and induction.

(iv) If $E = \mathit{fix}_x.E'$, then $\mathcal{D}_{n+1}[\![E']\!](\rho) \in R_\omega$ and $\mathcal{D}_n[\![E]\!](\rho) \in R_\omega$ by induction on E' and $n \in \mathbb{N}$ 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 $E \in \mathcal{G}$ the sequence $\langle D_n[\![E]\!]\rangle_{n\in\mathbb{N}}$ is Cauchy in (R_ω, d_ω), which follows from the continuity of the semantic operators, Lemma 4.21 and Lemma 4.42. □

4.2.1 Full Abstraction

In this section we show that the above denotational model is fully abstract, that is, two RP expressions are equivalent with respect to $\overset{\mathsf{R}}{\sim}$ if and only if their denotations (under the semantic map $\mathcal{D}$) have distance zero. By definition, the operational equivalence $\overset{\mathsf{R}}{\sim}$ is based on the maps $\mathsf{R}_{\mathbf{glb}}$ and $\mathsf{R}_{\mathbf{lub}}$ where

$$\mathsf{R}_{\mathbf{glb}}, \mathsf{R}_{\mathbf{lub}} : \{\mathcal{O}[\![E]\!] \mid E \in \mathrm{Pr}\} \longrightarrow (\mathtt{T} \longrightarrow [0,1])$$

and the metric d is based on the map $\mathcal{V}$, where

$$\mathcal{V} : \Big(A_{\mathrm{r}}^* \times \{\mathcal{D}_n[\![E]\!] \mid E \in \mathcal{G}\}\Big) \longrightarrow \mathcal{I}$$

for all $n \in \mathbb{N}$. Therefore, to obtain a full abstraction result, we must first relate the semantic maps $\mathcal{O}$ and $\mathcal{D}$ and our testing language $\mathtt{T}$ and the set of trees A^*_{r}, and then, using these results, the maps $\mathsf{R}_{\mathbf{glb}}$, $\mathsf{R}_{\mathbf{lub}}$ and $\mathcal{V}$. This leads to a connection between $\overset{\mathsf{R}}{\sim}$ and the metric d_ω, and hence the full abstraction result. Formally, we have the following lemmas and definition.

Lemma 4.44 *For all $E \in \mathrm{Pr}$, $\rho \in \mathrm{Env}$ and $S \in \mathcal{P}_{\mathrm{fr}}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$, we have $\mathcal{O}[\![E]\!] \to S$ if and only if $f^S_{n+1} \in \mathcal{D}_{n+1}[\![E]\!](\rho)$ for all $n \in \mathbb{N}$ such that if $S = \emptyset$ then $f^S_{n+1} = \perp$, and if $S = \{(a_1, \pi_1), \ldots (a_m, \pi_m)\}$ then $dom(f^S_{n+1}) = \{a_1, \ldots, a_m\}$, and for any $1 \leq i \leq m$ and $Y \in R$:*

$$f^S_{n+1}(a_i)[n+1](Y) = \sum_{\substack{F \in \mathrm{RP}\ \& \\ \mathcal{D}_n[\![F]\!](\rho)[n]=Y}} \pi_i(F).$$

Definition 4.45 Let $\xi : A^*_{\mathrm{r}} \to \mathtt{T} \setminus \{(\!| \perp |\!)\}$ be the mapping defined inductively as follows:

$$\begin{aligned} \xi(\{a_1, \ldots, a_m\}) &= (\!|[a_1.(\!| \perp |\!), \ldots, a_m.(\!| \perp |\!)]|\!) \\ \xi(\{V_1, \ldots, V_m\}) &= (\xi(V_1), \ldots, \xi(V_{m'})) \\ \xi(\{a_1\mathbf{V}_1, \ldots, a_m\mathbf{V}_m\}) &= (\!|[a_1.\xi(\mathbf{V}_1), \ldots a_m.\xi(\mathbf{V}_m)]|\!). \end{aligned}$$

Lemma 4.46 *The mapping ξ is bijective.*

Lemma 4.47 *For all $E \in \mathrm{Pr}$, $\rho \in \mathrm{Env}$, $V \in A^n_{\mathrm{r}}$ and $n \in \mathbb{N}$:*

$$\mathcal{V}(V, \mathcal{D}_{n+1}[\![E]\!](\rho)[n+1]) = [\mathsf{R}_{\mathbf{glb}}(E)(\xi(V)), \mathsf{R}_{\mathbf{lub}}(E)(\xi(V))].$$

Proof. The proof is by induction on $n \in \mathbb{N}$. If $V \in A^0_{\mathrm{r}}$, then $V = \{a_1, \ldots, a_m\}$ for some $\{a_1, \ldots, a_m\} \subseteq A$ and by Definition 4.45 we have $\xi(\{a_1, \ldots, a_m\}) = (\!|[a_1.(\!| \perp |\!), \ldots, a_m.(\!| \perp |\!)]|\!)$. Now, considering any $S \in (\mathcal{A}ct \times \mu(\mathrm{Pr}))$ and letting $r = [a_1.(\!| \perp |\!), \ldots, a_m.(\!| \perp |\!)]$:

$$\text{(12)} \quad \mathsf{R}_*(S)(r) = \begin{cases} 1 \text{ if } \{(a_1, \pi_1), \ldots, (a_m, \pi_m)\} \subseteq S \ \& \ \{\pi_1, \ldots, \pi_m\} \subseteq \mu(\mathrm{Pr}) \\ 0 \text{ otherwise} \end{cases}$$

by Definition 2.2. Furthermore, using the notation of Lemma 4.44 above we have:

$$\begin{aligned} \mathcal{V}(V, f^S_1[1]) &= \begin{cases} [1,1] \text{ if } \{a_1, \ldots, a_m\} \subseteq dom(f^S_1[1]) \\ [0,0] \text{ otherwise} \end{cases} \\ &= \begin{cases} [1,1] \text{ if } \{a_1, \ldots, a_m\} \subseteq dom(f^S_1) \\ [0,0] \text{ otherwise} \end{cases} && \text{by Definition 4.14} \\ \text{(13)} \qquad &= [\mathsf{R}_{\mathbf{glb}}(S)(r), \mathsf{R}_{\mathbf{lub}}(S)(r)] && \text{by Lemma 4.44 and (12).} \end{aligned}$$

Then for any $E \in \mathrm{Pr}$ by Lemma 4.44:

$$\begin{aligned}
\mathcal{V}(V, \mathcal{D}_1[\![E]\!][1]) &= \sqcup\{\mathcal{V}(V, f_1^S[1]) \mid \mathcal{O}[\![E]\!] \to S\} \\
&= \left[\min_{\mathcal{O}[\![E]\!]\to S} \mathcal{V}(V, f_1^S[1]), \max_{\mathcal{O}[\![E]\!]\to S} \mathcal{V}(v, f_1^S[1])\right] && \text{by Definition 4.4} \\
&= \left[\min_{\mathcal{O}[\![E]\!]\to S} \mathsf{R}_{\mathbf{glb}}(S)(r), \max_{\mathcal{O}[\![E]\!]\to S} \mathsf{R}_{\mathbf{lub}}(S)(r)\right] && \text{by (13)} \\
&= [\mathsf{R}_{\mathbf{glb}}(E)((\!|r|\!)), \mathsf{R}_{\mathbf{lub}}(E)((\!|r|\!))] && \text{by Definition 2.2} \\
&= [\mathsf{R}_{\mathbf{glb}}(E)(\xi(V)), \mathsf{R}_{\mathbf{lub}}(E)(\xi(V))] && \text{by definition of } r
\end{aligned}$$

and thus the lemma holds for $n = 0$.

Now suppose the lemma holds for some $n \in \mathbb{N}$ and consider any $\mathbf{V} \in \mathcal{P}_{\mathrm{fnr}}(A_{\mathrm{r}}^n)$, then $\mathbf{V} = \{V_1, \ldots, V_m\}$ for some $m \geq 1$ and by definition of $\mathcal{V}$:

$$\begin{aligned}
\mathcal{V}(\mathbf{V}, \mathcal{D}_{n+1}[\![E]\!][n+1]) &= \prod_{i=1}^{m} \mathcal{V}(V_i, \mathcal{D}_{n+1}[\![E]\!][n+1]) \\
&= \prod_{i=1}^{m} [\mathsf{R}_{\mathbf{glb}}(E)(\xi(V_i)), \mathsf{R}_{\mathbf{lub}}(E)(\xi(V_i))] && \text{by induction} \\
&= \left[\prod_{i=1}^{m} \mathsf{R}_{\mathbf{glb}}(E)(\xi(V_i)), \prod_{i=1}^{m} \mathsf{R}_{\mathbf{lub}}(E)(\xi(V_i))\right] && \text{by Definition 4.4} \\
&= [\mathsf{R}_{\mathbf{glb}}(E)(\xi(\mathbf{V})), \mathsf{R}_{\mathbf{lub}}(E)(\xi(\mathbf{V}))] && \text{by definition of } \xi.
\end{aligned}$$

Next consider any $v \in (A \times A_{\mathrm{r}}^n) \cup A$ and $S \in \mathcal{P}_{\mathrm{fr}}(\mathcal{A}ct \times \mu(\mathrm{Pr}))$, then either $v \in A$ and similarly to the case when $n = 0$ we can show:

$$\mathcal{V}(v, f_{n+2}^S[n+2]) = [\mathsf{R}_{\mathbf{glb}}(S)(\xi(v)), \mathsf{R}_{\mathbf{lub}}(S)(\xi(v))]$$

or $v = a\mathbf{V}$ for some $a \in \mathcal{A}ct$ and $\mathbf{V} \in \mathcal{P}_{\mathrm{fnr}}(A_{\mathrm{r}}^n)$ in which case we have the following two possibilities:

(i) $(a, \pi) \in S$ for some $\pi \in \mu(\mathrm{Pr})$, in which case using Lemma 4.44 $a \in dom(f_{n+2}^S)$, and therefore by definition of $\mathcal{V}$:

$$\begin{aligned}
\mathcal{V}(v, f_{n+2}^S[n+2]) &= \sum_{q \in R_\omega} f_{n+2}^S(a)[n+2](q) \cdot \mathcal{V}(\mathbf{V}, q) \\
&= \sum_{q \in R_\omega} \left(\sum_{\substack{F \in \mathrm{Pr}\,\& \\ \mathcal{D}_{n+1}[\![F]\!][n+1] = q}} \pi(F) \right) \cdot \mathcal{V}(\mathbf{V}, q) && \text{by Lemma 4.44} \\
&= \sum_{F \in \mathrm{Pr}} \pi(F) \cdot \mathcal{V}(\mathbf{V}, \mathcal{D}_{n+1}[\![F]\!][n+1]) && \text{rearranging} \\
&= \sum_{F \in \mathrm{Pr}} \pi(F) \cdot [\mathsf{R}_{\mathbf{glb}}(F)(\xi(\mathbf{V})), \mathsf{R}_{\mathbf{lub}}(F)(\xi(\mathbf{V}))] && \text{from above} \\
&= \left[\sum_{F \in \mathrm{Pr}} \pi(F) \cdot \mathsf{R}_{\mathbf{glb}}(F)(\xi(\mathbf{V})), \sum_{F \in \mathrm{Pr}} \pi(F) \cdot \mathsf{R}_{\mathbf{lub}}(F)(\xi(\mathbf{V}))\right] \\
& && \text{by Definition 4.4} \\
&= [\mathsf{R}_{\mathbf{glb}}(S)(\xi(v)), \mathsf{R}_{\mathbf{lub}}(S)(\xi(v))] && \text{by Definition 2.2.}
\end{aligned}$$

(ii) $(a, \pi) \notin S$ for any $\pi \in \mu(\text{Pr})$, and hence by Definition 2.2, $\mathcal{V}$ and Lemma 4.44:

$$\mathcal{V}(v, f^S_{n+2}[n+2]) = [0,0] = [\mathsf{R}_{\mathbf{glb}}(S)(\xi(v)), \mathsf{R}_{\mathbf{lub}}(S)(\xi(v))].$$

Then since these are all the possible cases and $v \in (A \times A^n_{\mathrm{r}}) \cup A$ was arbitrary:

$$\mathcal{V}(v, f^S_{n+2}[n+2]) = [\mathsf{R}_{\mathbf{glb}}(S)(\xi(v)), \mathsf{R}_{\mathbf{lub}}(S)(\xi(v))] \tag{14}$$

for all $v \in (A \times A^n_{\mathrm{r}}) \cup A$.

Now considering any $V \in A^{n+1}_{\mathrm{r}}$, by definition $V = \{v_1, \ldots, v_m\}$ for some $m \in \mathbb{N}$ where $v_i \in (A \times A^n_{\mathrm{r}}) \cup A$ for all $1 \leq i \leq m$, and hence by definition of $\mathcal{V}$:

$$\begin{aligned}
\mathcal{V}(V, f^S_{n+2}[n+2]) &= \prod_{i=1}^{m} \mathcal{V}(v_i, f^S_{n+2}[n+2]) \\
&= \prod_{i=1}^{m} [\mathsf{R}_{\mathbf{glb}}(S)(\xi(v_i)), \mathsf{R}_{\mathbf{lub}}(S)(\xi(v_i))] && \text{by (14)} \\
&= \left[\prod_{i=1}^{m} \mathsf{R}_{\mathbf{glb}}(S)(\xi(v_i)) \prod_{i=1}^{m} \mathsf{R}_{\mathbf{lub}}(S)(v_i)) \right] && \text{by Definition 4.4} \\
&= [\mathsf{R}_{\mathbf{glb}}(S)(\xi(V)), \mathsf{R}_{\mathbf{lub}}(S)(\xi(V))] && \text{by Definition 4.45.}
\end{aligned}$$

The remainder of the proof follows as for the case when $n = 0$. □

Theorem 4.48 (Full abstraction) *For all $E, F \in \mathcal{G}$:*

$$\mathcal{O}[\![E]\!] \overset{\mathsf{R}}{\sim} \mathcal{O}[\![F]\!] \textit{ if and only if } \mathcal{D}[\![E]\!](\rho) = \mathcal{D}[\![F]\!](\rho) \textit{ for all } \rho \in \text{Env}.$$

Proof. We only consider the case for $E, F \in \text{Pr}$, as the case for $E, F \in \mathcal{G} \setminus \text{Pr}$ follows by definition of $\overset{\mathsf{R}}{\sim}$ and we remove ρ for simplicity. First, consider any $E, F \in \text{Pr}$ such that $\mathcal{D}[\![E]\!] = \mathcal{D}[\![F]\!]$. Then $d_\omega(\mathcal{D}_n[\![E]\!][n], \mathcal{D}_n[\![F]\!][n]) = 0$ for all $n \in \mathbb{N}$ by Lemma 4.21 and Lemma 4.42, and hence by definition of d and $d_{\mathcal{V}}$:

$$\begin{aligned}
&\mathcal{V}(V, \mathcal{D}_{n+1}[\![E]\!][n+1]) = \mathcal{V}(V, \mathcal{D}_{n+1}[\![F]\!][n+1]) \text{ for all } V \in A^n_{\mathrm{r}} \;\&\; n \in \mathbb{N} \\
&\quad \Rightarrow \mathsf{R}_*(E)(\xi(V)) = \mathsf{R}_*(F)(\xi(V)) \text{ for all } V \in A^*_{\mathrm{r}} && \text{by Lemma 4.47} \\
&\quad \Rightarrow \mathsf{R}_*(E)(t) = \mathsf{R}_*(F)(t) \text{ for all } t \in \mathtt{T} \setminus (\!|\omega|\!) && \text{by Lemma 4.46} \\
&\quad \Rightarrow \mathsf{R}_*(E)(t) = \mathsf{R}_*(F)(t) \text{ for all } t \in \mathtt{T} && \text{by Definition 2.2} \\
&\quad \Rightarrow \mathcal{O}[\![E]\!] \overset{\mathsf{R}}{\sim} \mathcal{O}[\![F]\!] && \text{by definition of } \overset{\mathsf{R}}{\sim}
\end{aligned}$$

as required. □

5 Conclusions

We have considered a process calculus based on CSP [5,8,21] extended with internal action-guarded probabilistic choice. A testing equivalence, coarser than probabilistic bisimulation [14], has been defined for this calculus and shown to be a congruence for the main CSP process operators, including external (deterministic) and internal (non-deterministic) choice and synchronous parallel. A logical characterization of the equivalence can be found in [13,20]. We were unable to model the hiding and asynchronous parallel operators which is related to our model containing action-guarded probabilistic choice. If we were to add the hiding operator, for example, then there will exist probabilistic transitions which are hidden, and it would be problematic to establish the probability of such hidden moves through testing. The inability to model hiding is unfortunate since the model checker `fdr2` [21] uses it in an essential way. Asynchronous parallel is not so crucial for verification, but is needed for compositional specification of e.g. distributed probabilistic protocols. It would be worthwhile to formulate a testing equivalence which is a congruence for the full calculus of CSP, including hiding, extended with internal probabilistic choice; a preliminary proposal for how this might be achieved has been made in [20].

Using de Bakker and Zucker's construction for classical process calculi [3], we have derived a denotational model for our process calculus 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" fully abstract model constructed by Baier and Kwiatkowska [2] for a CCS-based calculus, in the following sense. 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 [2] gives rise to the discrete topology on [0,1]. The Euclidean metric is intuitively desirable in the continuous setting of probabilities, but this comes at a cost: we only have a pseudo-metric, whereas the metric defined in [2] 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 [1] applicable in the case of the inductive metric of [2].

The above raises important issues that would be worth studying. What should the notion of a probabilistic process be? We have found the transition systems modelling paradigm limiting and in some cases misleading. Could Banach spaces be used instead? What is the correct categorical approach to use here? In particular, can one define an inductive metric satisfying the intuitive properties of our metric?

Acknowledgement

We are grateful to Michael Huth, Achim Jung, Gavin Lowe and Bill Roscoe for comments on earlier versions of this work.

References

[1] 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.*

[2] C. Baier and M.Z. Kwiatkowska. Domain equations for probabilistic processes (Extended Abstract). *In C. Palamidessi and J. Parrow , editors, Proc. EXPRESS'97, volume 7, Electronic Notes in Theoretical Computer Science, Elsevier, 1997.*

[3] J.W. de Bakker and J.I. Zucker. Processes and the denotational semantics of concurrency. *Information and Control, 54(1/2):70-120, 1982.*

[4] J.A. Bergstra and J.W. Klop. Process algebra for synchronous communication. *Information and Computation, 60:109-134, 1984.*

[5] 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.*

[6] 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.*

[7] H.A. Hansson. Time and probability in the formal design of distributed systems. *Volume 1 of Real-Time Safety Critical Systems, Elsevier, 1994.*

[8] C.A.R. Hoare. Communicating sequential processes, *Prentice Hall, 1985.*

[9] 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.*

[10] 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.*

[11] 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, CONCUR'90, volume 458 of Lecture Notes in Computer Science, pages 367-383, Springer Verlag, 1990.*

[12] 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.*

[13] M.Z. Kwiatkowska and G.J. Norman. A testing equivalence for reactive probabilistic processes. *To appear in Proc. EXPRESS'98, Electronic Notes in Theoretical Computer Science, Elsevier, September 1998.*

[14] K.G. Larsen and A. Skou. Bisimulation through probabilistic testing. *Information and Computation, 94(1):1-28, 1991.*

[15] G. Lowe. Probabilistic and Prioritized Models of Timed CSP. *Theoretical Computer Science, 138:315-352, 1995.*

[16] G. Lowe. Representing nondeterministic and probabilistic behaviour in reactive processes. *Technical Report, 1993.* Available at `http://www.mcs.le.ac.uk/~glowe/Publications.html`.

[17] R. Milner. Communication and concurrency. *Prentice Hall, 1989.*

[18] C. Morgan, A. McIver, K. Seidel and J.W. Sanders. Argument duplication in probabilistic CSP. *Technical Report PRG-TR-95, Oxford University Computing Laboratory, 1995.*

[19] C. Morgan, A. McIver, K. Seidel and J.W. Sanders. Refinement-oriented probability for CSP. *Formal Aspects of Computing, 8(6):617-647, 1996.*

[20] G.J. Norman. Metric semantics for reactive probabilistic processes. *Ph.D Thesis, School of Computer Science, the University of Birmingham, November 1997.*

[21] A.W. Roscoe. The theory and practice of concurrency. *Prentice Hall International Series in Computer Science, 1997.*

[22] 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.*

[23] K. Seidel. Probabilistic communicating processes. *Theoretical Computer Science, 152:219-249, 1995.*

[24] Wang Yi and K.G. Larsen. Testing probabilistic and non-deterministic processes. *Protocol Specification, Testing and Verification XII:47-61, Florida, USA, 1992.*