Electronic Notes in Theoretical Computer Science 40 (2001)
URL: http://www.elsevier.nl/locate/entcs/volume40.html 28 pages

Metric Semantics and Full Abstractness for Action Refinement and Probabilistic Choice

J.I. den Hartog [a], E.P. de Vink [b,c] and J.W. de Bakker [a]

[a] *Department of Software Engineering, CWI, P.O. Box 94079, 1090 GB Amsterdam, The Netherlands*

[b] *Faculty of Mathematics and Computer Science, Technical University Eindhoven, P.O. Box 513, 5600 MB Eindhoven, The Netherlands*

[c] *LIACS, Leiden University, P.O. Box 9512, 2300 RA Leiden, The Netherlands*

Abstract

This paper provides a case-study in the field of metric semantics for probabilistic programming. Both an operational and a denotational semantics are presented for an abstract process language $\mathcal{L}_{pr}$, which features action refinement and probabilistic choice. The two models are constructed in the setting of complete ultrametric spaces, here based on probability measures of compact support over sequences of actions. It is shown that the standard toolkit for metric semantics works well in the probabilistic context of $\mathcal{L}_{pr}$, e.g. in establishing the correctness of the denotational semantics with respect to the operational one. In addition, it is shown how the method of proving full abstraction —as proposed recently by the authors for a nondeterministic language with action refinement— can be adapted to deal with the probabilistic language $\mathcal{L}_{pr}$ as well.

1 Introduction

In this paper we study the applicability of metric techniques for the development of an operational and a denotational semantics for a nontrivial language, and for their comparison in a probabilistic setting. We have chosen to mix discrete probabilistic choice with the construct of action refinement. In [HVB99] we have indicated how, in a nondeterministic setting, an operational and a denotational semantics can be constructed, the correctness of the denotational model with respect to the operational one can be established, and, moreover, how a full abstractness result can be obtained, all using metric methods. The aim of this paper is to investigate the flexibility of the metric machinery by combination and adaptation of earlier results. It turns out that indeed the various techniques are orthogonal: replacing nondeterminacy by probability does not affect the proof methods.

There exist only a few metric models for probabilistic process languages. In [KN98], extending the earlier [KN96], action guarded probabilistic choice is added to a subset of CSP. A full abstractness result is obtained for a metric denotational model with respect to a variant of probabilistic bisimulation as proposed by [LS91]. The semantical interpretation of probability in [KN98] is based on a different quantitative paradigm than the one of the present paper, namely worst-case best-case intervals. Moreover, the denotational semantics is developed in situ and does not appeal to a general methodology of constructing operational and denotational semantics. A model logic approach to quantitative process equivalences is reported in [DGJP99]. Van Breugel and Worrel [BW01] have developed a quantitative comparison of probabilistic systems based on the Hutchinson metric exploiting the existence of a final co-algebra in the category of pseudo-metric spaces. In this approach two systems are close if they assign approximately the same probabilities to similar processes. This is different from the approach in this paper were two systems are considered close if they assign exactly the same probability to processes which are close to each other. As far as the probabilistic information is concerned, the approach of this paper is qualitative; one can check whether or not two probabilities are the same, but not how far apart two probabilities are. In [BK97] a metric denotational semantics for an extension of CCS with action guarded probabilistic choice is shown to be fully abstract with respect to probabilistic bisimulation. The present paper establishes full abstraction with respect to an operational model. Identification of bisimilar processes (here for probabilistic bisimulation à la Larsen and Skou) is automatic when working with metric domains obtained as final coalgebras of contracting functors (cf. [RT94,VR99,HV99b]). The work of Seidel [Sei95] exploits the measure theoretical apparatus of stochastic kernels for the modeling of CSP-style operators. Apart from the important papers [GSS95,LS91] for probabilistic bisimulation we mention [Chr90,NFL95,GRN98] as fully abstract models for probabilistic choice in the setting of testing semantics.

The construct of action refinement has been studied by several authors in different settings, mostly in the true concurrency framework. An early full abstraction result is [NEL88] where series-parallel pomsets are used for the modeling. Work in the area of Petri-nets includes the approach of Vogler using interval semi-words (cf. [Vog91,Vog92]). A process algebra for action refinement is proposed in [Ace90,AH93]. Gorrieri and co-workers base their semantics [Gor91,DG95,GGR96] on the causal trees of [DD89,DD93]. Other work on the semantics of action refinement includes [CS95,Ren93]. A metric interleaving semantics is presented in [BV94].

The paper [HVB99] studies a process language $\mathcal{L}_{ref}$ with action refinement and nondeterministic and parallel composition in a metric setting. The domain of meanings consists of compact sets of sequences of actions. It is shown that the denotational semantics given for $\mathcal{L}_{ref}$ is fully abstract with respect to the operational semantics presented there. The present paper, devoted to the process language $\mathcal{L}_{pr}$, seeks to adapt the result of [HVB99] from a nondeterministic framework to a probabilistic one. The nondeterministic constructs of nondeterministic and parallel composition of $\mathcal{L}_{ref}$ are removed and the construct of probabilistic choice is added in $\mathcal{L}_{pr}$. Although probability measures of compact support over sequences of actions are used as semantical objects in this paper, our case-study shows that essentially the metrical instruments from [HVB99] remain the same: Banach's Fixed Point Theorem and the '$\varepsilon \leq \frac{1}{2}\varepsilon$-principle' as general techniques (see, e.g., [BV96]) and the method of proving full abstraction. Moreover, our analysis illustrates that the techniques to deal with action refinement, as introduced in [HVB99], is eligible to be mixed with other elements of the metric approach.

There are no nondeterministic constructs in the language $\mathcal{L}_{pr}$ because the presence of both nondeterminism and probability in the same language creates several modeling issues (see, e.g., [Har98,HV99a,Mis00]). The presence of action refinement does not seem to influence the extension of a probabilistic language to a language containing both nondeterminism and probability. The approach of [Har98] can likely also be used to extend the language $\mathcal{L}_{pr}$ with nondeterministic choice and parallel composition. Full abstractness, however, is not dealt with in [Har98]. To obtain full abstractness for parallel composition with synchronization a more complex approach using failure sets, also exploited in [HVB99], should be used. At present, it is an open question whether failure sets can be easily combined with the probabilistic concepts used in this paper.

The method of proving full abstraction for a denotational semantics $\mathcal{D}$ with respect to an operational semantics $\mathcal{O}$ is outlined as follows. The denotational semantics $\mathcal{D}$ for $\mathcal{L}_{pr}$ has functionality $\mathcal{D}\colon \mathcal{L}_{pr} \to \mathit{SemRef} \to \mathbb{P}$ where *SemRef*, the collection of semantical refinements, is given by $\mathit{SemRef} = \mathit{Act} \to \mathbb{P}$, *Act* is a given set of atomic actions and $\mathbb{P}$ is the complete ultrametric space of probability measures of compact support of finite and infinite sequences of actions from *Act*. The main hurdle to be taken is the proof of completeness for $\mathcal{D}$, i.e., to prove the implication

$$\mathcal{O}[\![C[s']]\!] = \mathcal{O}[\![C[s'']]\!] \text{ for all contexts } C[\cdot] \;\Rightarrow\; \mathcal{D}(s') = \mathcal{D}(s'') \tag{1.1}$$

for any two statements $s', s'' \in \mathcal{L}_{pr}$. Instead of proving (1.1) directly we focus on its contraposition

$$\mathcal{D}(s') \neq \mathcal{D}(s'') \;\Rightarrow\; \mathcal{O}[\![C[s']]\!] \neq \mathcal{O}[\![C[s'']]\!] \text{ for some context } C[\cdot]. \tag{1.2}$$

So we assume $\mathcal{D}(s') \neq \mathcal{D}(s'')$ for two statements $s', s'' \in \mathcal{L}_{pr}$. Hence, for some semantical refinement $\eta \in \mathit{SemRef}$ we have that $\mathcal{D}(s')(\eta)$ and $\mathcal{D}(s'')(\eta)$ are not equal, and that they have therefore a positive distance. Due to the structure of $\mathbb{P}$ we then have that $d(\mathcal{D}(s')(\eta), \mathcal{D}(s'')(\eta)) = 2^{-n}$ for some $n \geq 0$. We subsequently choose a so-called finitary semantical refinement $\eta' \in \mathit{SemRef}$ for which $d(\mathcal{D}(s')(\eta'), \mathcal{D}(s'')(\eta')) = 2^{-n}$ as well. Thus, we can restrict our attention to finitary η' only, without altering the distance of $\mathcal{D}(s')$ and $\mathcal{D}(s'')$. The crucial property of finitary semantical refinements, such as η', is that in the setting of $\mathcal{L}_{pr}$ they can be represented by a finite sequences $\langle a_i \rightsquigarrow s_i\rangle_{i=1}^n$ of action refinements. More precisely, we can find actions $a_1, \ldots, a_n$ and statements $s_1, \ldots, s_n$ such that $\mathcal{D}(s)(\eta') = \mathcal{D}(s\langle a_i \rightsquigarrow s_i\rangle_{i=1}^n)(\eta_{id})$ for any statement $s \in \mathcal{L}_{pr}$ (where η_{id} is the so-called empty semantical refinement which essentially does not alter the meaning of any action s). We thus obtain $d(\mathcal{D}(s'\langle a_i \rightsquigarrow s_i\rangle_{i=1}^n)(\eta_{id}), \mathcal{D}(s''\langle a_i \rightsquigarrow s_i\rangle_{i=1}^n)(\eta_{id})) = 2^{-n}$. The correctness result for the denotational semantics yields, for any statement s, that $\mathcal{D}(s)(\eta_{id}) = \mathcal{O}[\![s]\!]$. So, we derive, putting $C[\cdot] = (\cdot)\langle a_i \rightsquigarrow s_i\rangle_{i=1}^n$, that $d(\mathcal{O}[\![C[s']]\!], \mathcal{O}[\![C[s'']]\!]) = 2^{-n}$ and therefore $\mathcal{O}[\![C[s']]\!] \neq \mathcal{O}[\![C[s'']]\!]$ as was required for proving (1.2).

The remainder of this paper is organized as follows. Section 2 presents some mathematical preliminaries and some notation. The language $\mathcal{L}_{pr}$ and its operational semantics is introduced in Section 3, while Section 4 is devoted to the denotational semantics $\mathcal{D}$ for $\mathcal{L}_{pr}$. The correctness of the model $\mathcal{D}$ with respect to the semantics $\mathcal{O}$ is subject of Section 5, whereas the full abstraction result is discussed in Section 6. Finally, Section 7 addresses some concluding remarks.

2 Mathematical preliminaries

We assume a basic understanding of elementary metric topology and basic measure theory, in particular the notions of complete metric space, closed and compact subset, and σ-algebra and Borel probability measure. We refer to [BV96] or standard textbooks on general topology such as [Dug76,Eng89] for more details on the former topic, and to [Rud66,Hal74] for more information on the latter.

A metric space X is said to be an ultrametric space if, for all $x, y, z \in X$, it holds that $d(x,z) \leq \max\{\, d(x,y), d(y,z) \,\}$. We use $B_\varepsilon(x)$ with $\varepsilon > 0$ and some element x in a metric space (X,d) to denote the open ball of radius ε and center x. Often the metric d is left implicit. We call a function $f: X_1 \to X_2$ between metric spaces (X_1, d_1) and (X_2, d_2) nonexpansive if $d_2(f(x), f(y)) \leq d_1(x,y)$ for all $x, y \in X_1$. The mapping f is called a contraction if there exists a real number α, $0 \leq \alpha < 1$ such that $d_2(f(x), f(y)) \leq \alpha \cdot d_1(x,y)$ for all $x, y \in X_1$. In the latter situation we also refer to f as an α-contraction.

The following version of Banach's Fixed Point Theorem will be frequently applied in the sequel.

Theorem 2.1 *A contraction $f: X \to X$ on a complete metric space (X,d) has a unique fixed pont $\mathrm{fix}(f)$ in X. Moreover, if $X_0 \subseteq X$ is a nonempty and closed subset such that $f(x) \in X_0$ when $x \in X_0$, then it holds that $\mathrm{fix}(f) \in X_0$.*

The semantical models discussed in this paper are based on the collection Act^∞ of finite and infinite sequences or words over the alphabet Act and on Borel probability measures on Act^∞. We endow the set Act^∞ with the so-called

Baire metric d_B given by

$$d_B(w, v) = 2^{-\sup\{\, n | w[n]=v[n] \,\}}$$

where $w[n], v[n]$ denote the prefixes of w, v of length n. As a consequence we have $d_B(a \cdot w, a \cdot v) = \frac{1}{2} d_B(w, v)$ and $d_B(a \cdot w, b \cdot v) = 1$ for $a \neq b$. It holds that (Act^∞, d_B) is a complete ultrametric space.

A Borel probability measure p on Act^∞ is said to be of compact support if there exists a compact set $K \subseteq Act^\infty$ such that $p(O) = 0$ iff $O \cap K = \emptyset$ for every open $O \subseteq Act^\infty$. The collection $\mathcal{M}(Act^\infty)$ of Borel probability measures of compact support comes equipped with the Hutchinson-metric

$$d_H(p, p') = \inf\{\, \varepsilon \mid p(B_\varepsilon(w)) = p'(B_\varepsilon(w)) \,\}.$$

It holds that $\mathcal{M}(Act^\infty)$ is a complete ultrametric space (cf. [VR99]). For $a \in Act$ and $p \in \mathcal{M}(Act^\infty)$ the Borel probability measure $a \cdot p$ is given by $(a \cdot p)(B) = p(B/a)$ for Borel-sets $B \subseteq Act^\infty$ where $B/a \overset{df}{=} \{\, w \mid a \cdot w \in B \,\}$. In fact $a \cdot p$ is the measure p along pref_a, i.e. $a \cdot p = p \circ \mathit{pref}_a^{-1}$, with $\mathit{pref}_a\colon Act^\infty \to Act^\infty$, $\mathit{pref}_a(w) = a \cdot w$. We have that

$$d_H(a \cdot p, a \cdot p') = \tfrac{1}{2} d_H(p, p'). \tag{2.1}$$

For $w \in Act^\infty$ the Dirac-measure $\mathit{Dir}(w)$ is defined as $w(B) = 1$ if $w \in B$, $w(B) = 0$ otherwise for any Borel set $B \subseteq Act^\infty$. For $m \geq 1$, $0 \leq \rho_1, \ldots, \rho_m \leq 1$ such that $\rho_1 + \cdots + \rho_m = 1$ and $p_1, \ldots, p_m \in \mathcal{M}(Act^\infty)$, the convex combination $\bigoplus_{i=1}^m \rho_i * p_i$ is given by $(\bigoplus_{i=1}^m \rho_i * p_i)(B) = \sum_{i=1}^m \rho_i \cdot p_i(B)$ for any Borel set $B \subseteq Act^\infty$. We have the following basic property:

$$d_H\Big(\bigoplus_{i=1}^m \rho_i * p_i, \bigoplus_{i=1}^m \rho_i * p'_i\Big) \leq \max\{\, d_H(p_i, p'_i) \mid 1 \leq i \leq m \,\} \tag{2.2}$$

for arbitrary $p_i, p'_i \in \mathcal{M}(Act^\infty)$.

For a nonempty set V and a metric space X let $V \to X$ denote the collection of all functions from V to X. The set $V \to X$ is endowed with the distance of pointwise convergence inherited from X, i.e., $d(f, g) = \sup\{\, d(f(v), g(v)) \mid v \in V \,\}$ for $f, g\colon V \to X$. If X is a complete ultrametric space, then $V \to X$ is a complete ultrametric space as well. For metric spaces X and Y we denote by $X \to_1 Y$ the collection of all nonexpansive mappings from X to Y. We consider $X \to_1 Y$ to be a subspace of $X \to Y$. We have that completeness of Y implies completeness of $X \to_1 Y$.

3 Operational semantics

In this section we introduce the process language $\mathcal{L}_{pr}$ and present its operational semantics $\mathcal{O}$. The model $\mathcal{O}$ will serve as a point of reference for our understanding of $\mathcal{L}_{pr}$ and for the semantical considerations in later sections. We start off with the syntax for $\mathcal{L}_{pr}$.

Definition 3.1 Let *Act* and *PVar* be given syntactical classes of countably infinite many *actions* and *procedure variables,* respectively. The language $\mathcal{L}_{pr}$, ranged over by s, is then given by

$$s ::= a \mid s; s \mid s \oplus_\pi s \mid s\langle a \rightsquigarrow s\rangle \mid x,$$

where a and x range over Act and $PVar$ and $0 < \pi < 1$.

Elements of $\mathcal{L}_{pr}$ are referred to as statements. The language $\mathcal{L}_{pr}$ contains the usual ingredients of abstract, uninterpreted actions a, sequential composition $s_1; s_2$ and recursion via procedure variables. More specific constructions in $\mathcal{L}_{pr}$ are the construction of probabilistic choice $s_1 \oplus_\pi s_2$ and of action refinement $s_1\langle a \rightsquigarrow s_2\rangle$.

The intuition behind the construct $s_1 \oplus_\pi s_2$ is that upon its execution, with probability π the alternative s_1 is taken, and with the complementary probability $1 - \pi$ the alternative s_2 is executed. The idea underlying action refinement is that in $s_1\langle a \rightsquigarrow s_2\rangle$ the actions of s_1 are performed, but with the execution of s_2 replacing the execution of actions a of s_1. So, for example, $a \oplus_{1/4} (b; c)$ delivers, on the average, in 25% of the cases a and in 75% the sequence bc. Instead $((a \oplus_{1/4} (b; c))\langle a \rightsquigarrow b; d\rangle)\langle c \rightsquigarrow d\rangle$ will have bd for all of its executions.

In order to cater for recursion we assume that some declaration D: $PVar \rightarrow Stat$ is given, such that for $x \in PVar$, the statement $D(x)$ is guarded. (Here we define that each action a is guarded, that $s_1; s_2$ is guarded if s_1 is guarded, and that $s_1 \oplus_\pi s_2$ and $s_1\langle a \rightsquigarrow s_2\rangle$, respectively, are guarded if both s_1 and s_2 are guarded.)

The transition system for $\mathcal{L}_{pr}$ makes use of so-called refinement sequences in order to keep track of the relevant action refinements. As states of the transition system we choose resumptions which typically consist of sequential and probabilistic compositions of pairs of a statement and a refinement sequence.

Definition 3.2

(a) The class *Ref* of *refinement sequences* is given by

$$R ::= \epsilon \mid \langle a \rightsquigarrow s\rangle \cdot R,$$

where ϵ is a fresh symbol representing the empty sequence. *Ref* is ranged over by R.

(b) The class *Res*, the elements of which are called *resumptions* and ranged over by r, is given by

$$r ::= \mathrm{E} \mid s : R \mid r; r \mid r \oplus_\rho r,$$

where E is a fresh symbol and R is a refinement sequence as introduced in part (a).

Below we also employ the notation $\langle a_1 \rightsquigarrow s_1\rangle\langle a_2 \rightsquigarrow s_2\rangle \cdots \langle a_n \rightsquigarrow s_n\rangle$ for arbitrary refinement sequences, and the notion $R \cdot \langle a \rightsquigarrow s\rangle$ for nonempty refinement sequences. We will furthermore identify E; r with the resumption r.

In the transition system as given by Definition 3.3 below, we make use of schemes of the form $r_1 \rightarrow_{D,0} r_2$ which are shorthand for rules of the form

$$\frac{r_1 \xrightarrow{\lambda}_D r}{r_2 \xrightarrow{\lambda}_D r}$$

indicating that if the resumption r_1 makes a λ-transition to the resumption r then so does the resumption r_2. For π such that $0 < \pi < 1$ we use π^c to denote $1 - \pi$.

Definition 3.3 Define the set *Lab*, ranged over by λ, as $Lab = Act \cup (0,1)$. The transition system $\rightarrow \subseteq Res \times Lab \times Res$ is given by the following axioms and rules:

- $$a : \epsilon \xrightarrow{a}_D \mathrm{E} \qquad \text{(Act 1)}$$
  $$a : \langle a' \rightsquigarrow s' \rangle \cdot R \rightarrow_{D,0} s' : R \qquad \text{if } a = a' \qquad \text{(Act 2)}$$
  $$a : \langle a' \rightsquigarrow s' \rangle \cdot R \rightarrow_{D,0} a : R \qquad \text{if } a \neq a' \qquad \text{(Act 3)}$$
- $$x : R \rightarrow_{D,0} D(x) : R \qquad \text{(Rec)}$$
- $$(s_1 * s_2) : R \rightarrow_{D,0} (s_1 : R) * (s_2 : R) \qquad \text{for } * \in \{;\, , \oplus_\rho\} \qquad \text{(Op)}$$
- $$s\langle a' \rightsquigarrow s' \rangle : R \rightarrow_{D,0} s : \langle a' \rightsquigarrow s' \rangle \cdot R \qquad \text{(Ref)}$$
- $$\frac{r_1 \xrightarrow{\lambda}_D r_1'}{r_1 ; r_2 \xrightarrow{\lambda}_D r_1' ; r_2} \qquad \text{(Seq)}$$
- $$r_1 \oplus_\pi r_2 \xrightarrow{\pi}_D r_1 \qquad r_1 \oplus_\pi r_2 \xrightarrow{\pi^c}_D r_2 \qquad \text{(PChoice 1,2)}$$

The axiom (Act 1) and rules (Act 2) and (Act 3) reflect the stack-like book-keeping for action refinement. The leftmost component of a refinement sequence applies, if the action to be refined, viz. a', matches the action in the control part of the resumption, viz. a; otherwise the action refinement is skipped. If no action refinement is left on the stack, i.e. the refinement sequence in the resumption is the empty sequence ϵ, the action a itself is executed as indicated by the label $a \in Act \subseteq Lab$ of the axiom (Act 1).

Procedure variables are handled by means of body replacement using the implicitly given declaration D. Sequential and probabilistic composition in the control part of a resumption, i.e. for resumptions of the format $(s_1 * s_2) : R$, distribute over the pair-constructor ':' of resumptions 'yielding' $(s_1 : R) * (s_2 : R)$. Similarly, an action refinement $s\langle a' \rightsquigarrow s' \rangle$ in the control part of a resumption $s\langle a' \rightsquigarrow s' \rangle : R$ amounts to an update of the refinement sequence of the resumption, where the action refinement $\langle a' \rightsquigarrow s' \rangle$ is prefixed to the sequence R. A sequential composition of resumptions is handled as usual.

A probabilistic choice between resumptions is resolved by selection of one of the probabilistic alternatives while delivering its probability as a label π or $1-\pi$ in the open interval $(0,1) \subseteq \mathit{Lab}$. Note that we suppress the issue of multiplicity of transitions. The typical example being the transitions for the statement $a \oplus_{1/2} a$. There are several techniques to handle this, e.g., considering multi-sets of transitions or using a regime of indices.

Examples Consider the resumption $(a \oplus_{1/4} (b;c)) : \epsilon$. Since

$$(a : \epsilon) \oplus_{1/4} ((b;c) : \epsilon) \xrightarrow{\frac{1}{4}}_D (a : \epsilon)$$

by (PChoice 1), we have

$$(a \oplus_{1/4} (b;c)) : \epsilon \xrightarrow{\frac{1}{4}}_D a : \epsilon.$$

Similarly, since

$$(a : \epsilon) \oplus_{1/4} ((b;c) : \epsilon) \xrightarrow{\frac{3}{4}}_D ((b;c) : \epsilon)$$

by (PChoice 2), we have

$$(a \oplus_{1/4} (b;c)) : \epsilon \xrightarrow{\frac{3}{4}}_D (b;c) : \epsilon.$$

For the resumption $(((a \oplus_{1/4} (b;c))\langle a \rightsquigarrow b;d\rangle)\langle c \rightsquigarrow d\rangle) : \epsilon$ we have, applying the shorthand of the $\rightarrow_{D,0}$-notation, for example

$$\begin{aligned}
&(((a \oplus_{1/4} (b;c))\langle a \rightsquigarrow b;d\rangle)\langle c \rightsquigarrow d\rangle) : \epsilon \\
&\rightarrow_{D,0} \;\; ((a \oplus_{1/4} (b;c))\langle a \rightsquigarrow b;d\rangle) : \langle c \rightsquigarrow d\rangle \;\; \text{by (Ref)} \\
&\rightarrow_{D,0} \;\; (a \oplus_{1/4} (b;c)) : \langle a \rightsquigarrow b;d\rangle \cdot \langle c \rightsquigarrow d\rangle \;\; \text{by (Ref)} \\
&\rightarrow_{D,0} \;\; (a : \langle a \rightsquigarrow b;d\rangle \cdot \langle c \rightsquigarrow d\rangle) \oplus_{1/4} ((b;c) : \langle a \rightsquigarrow b;d\rangle \cdot \langle c \rightsquigarrow d\rangle) \;\; \text{by (Op)} \\
&\xrightarrow{\frac{1}{4}}_D \;\; a : \langle a \rightsquigarrow b;d\rangle \cdot \langle c \rightsquigarrow d\rangle \;\; \text{by (PChoice 1)}
\end{aligned}$$

In turn, considering the resumption $a : \langle a \rightsquigarrow b;d\rangle \cdot \langle c \rightsquigarrow d\rangle$ we have

$$\begin{aligned}
&a : \langle a \rightsquigarrow b;d\rangle \cdot \langle c \rightsquigarrow d\rangle \\
&\rightarrow_{D,0} \;\; (b;d) : \langle c \rightsquigarrow d\rangle \;\; \text{by (Act 2)} \\
&\rightarrow_{D,0} \;\; (b : \langle c \rightsquigarrow d\rangle); (d : \langle c \rightsquigarrow d\rangle) \;\; \text{by (Op)} \\
&\rightarrow_{D,0} \;\; (b : \epsilon); (d : \langle c \rightsquigarrow d\rangle) \;\; \text{by (Act 3),(Seq)} \\
&\xrightarrow{b}_D \;\; d : \langle c \rightsquigarrow d\rangle \;\; \text{by (Act 1),(Seq).}
\end{aligned}$$

Often structural induction is not a suitable proof technique in the semantical investigations below, due to the presence of procedure variables in $\mathcal{L}_{pr}$. Instead we call upon so-called *wgt*-induction which is based on the transition system for $\mathcal{L}_{pr}$. In particular, we will directly obtain from the definition of the *wgt*-function on *Res* –to be given in a minute– that $wgt(r') < wgt(r)$ if $r \rightarrow_{D,0} r'$.

Definition 3.4

(a) The function $wgt\colon \mathcal{L}_{ref} \to \mathbb{N}$ is given by

$$\begin{aligned} wgt(a) &= 1 \\ wgt(s_1; s_2) &= wgt(s_1) + 1 \\ wgt(s_1 \oplus_\rho s_2) &= wgt(s_1) + wgt(s_2) + 1 \\ wgt(s_1 \langle a \rightsquigarrow s_2 \rangle) &= wgt(s_1) + wgt(s_2) + 1 \\ wgt(x) &= wgt(D(x)) + 1. \end{aligned}$$

(b) The function $wgt\colon Res \to \mathbb{N}$ is given by

$$\begin{aligned} & wgt(\mathrm{E}) = 0 \\ & wgt(s : \langle a_1 \rightsquigarrow s_1 \rangle \langle a_2 \rightsquigarrow s_2 \rangle \cdots \langle a_n \rightsquigarrow s_n \rangle) \\ & \qquad = wgt(s) + wgt(s_1) + wgt(s_2) + \cdots + wgt(s_n) \\ & wgt(r_1; r_2) = wgt(r_1) + 1 \\ & wgt(r_1 \oplus_\rho r_2) = wgt(r_1) + wgt(r_2) + 1. \end{aligned}$$

Note that the well-definedness of wgt relies on the guardedness of the statements $D(x)$ for $x \in PVar$. We will adopt the notation $r \Rightarrow_D \pi * r_1 \oplus \pi^c * r_2$ in case both $r \xrightarrow{\pi}_D r_1$ and $r \xrightarrow{\pi^c}_D r_2$. Here it is not necessarily the case that r equals $r_1 \oplus_\pi r_2$ (cf. the examples following Definition 3.3).

A first application of the technique of wgt-induction is the following structural property of the transition system.

Lemma 3.5 *For all $r \in Res$ exactly one of the following cases holds:*

- $r = E$
- $r \xrightarrow{a}_D r'$ *for some* $a \in Act$, $r' \in Res$
- $r \Rightarrow_D \pi * r' \oplus \pi^c * r''$ *for some* $r', r'' \in Res$ *and* $\pi \in (0, 1)$.

Proof. *We only consider the cases for a sequential composition of resumptions. The other cases are straightforward. Suppose $r \equiv r_1; r_2$. Note, $r_1 \not\equiv E$ as $E; r_2$ is identified with r_2. As $\mathrm{wgt}(r_1) < \mathrm{wgt}(r)$ we have by the induction hypothesis that either $r_1 \xrightarrow{a}_D r_1'$ or $r_1 \Rightarrow_D \pi * r_1' \oplus \pi^c * r_1''$. Therefore, by (Seq), $r_1; r_2 \xrightarrow{a}_D r_1'; r_2$ or $r_1; r_2 \Rightarrow_D \pi * (r_1'; r_2) \oplus \pi^c * (r_1''; r_2)$. From inspection of the transition system we obtain that, for a resumption of the format of r only rule (Seq) of the transition system applies. Hence, if $r \xrightarrow{\lambda}_D r'$ then there exist r_1, r_2, r_1' such that $r \equiv r_1; r_2$, $r_1 \xrightarrow{\lambda}_D r_1'$ and $r' \equiv r_1'; r_2$ from which it follows that exactly one of the three cases above holds for a sequential composition of resumptions.* $\square$

The lemma above states that a resumption is either a terminating resumption (i.e. $r \equiv \mathrm{E}$), a deterministic resumption (i.e. $\exists a, r'\colon r \xrightarrow{a}_D r'$), or a probabilistic resumption (i.e. $\exists \pi, r', r''\colon r \Rightarrow_D \pi * r' \oplus \pi^c * r''$). This fact will be exploited in the definition of the operational semantics for $\mathcal{L}_{pr}$.

Definition 3.6

(a) The semantical mapping $\mathcal{O}\colon Res \to \mathcal{M}(Act^\infty)$ is given by

$$\begin{aligned} \mathcal{O}(\mathrm{E}) &= \epsilon \\ \mathcal{O}(r) &= a \cdot \mathcal{O}(r') \ \text{ if } r \xrightarrow{a}_D r' \\ \mathcal{O}(r) &= \pi * \mathcal{O}(r') \oplus \pi^c * \mathcal{O}(r'') \ \text{ if } r \Rightarrow_D \pi * r' \oplus \pi^c * r'' \end{aligned}$$

(b) The operational semantics $\mathcal{O}[\![\cdot]\!]\colon Stat \to \mathcal{M}(Act^\infty)$ is given by $\mathcal{O}[\![s]\!] = \mathcal{O}(s : \epsilon)$.

We choose to deliver a probability measure over finite and infinite sequences of actions as the meaning of a statement from $\mathcal{L}_{pr}$. The intuition is that execution of a statement yields, in general, several runs of actions with a certain probability. The distribution assigning the associated probability to a sequence of actions thus reflects the computational essence of the statement. Because infinitely many and infinite sequences may occur as possible computations (e.g. for x where $D(x) = a \oplus_{1/4} (a; x)$ and for y where $D(y) = b; y$), we have to resort to the more general probability measures.

Examples

(1) $\mathcal{O}((a \oplus_{1/4} (b; c)) : \epsilon)$

$= \frac{1}{4} * \mathcal{O}(a : \epsilon) \oplus \frac{3}{4} * \mathcal{O}((b; c) : \epsilon)$

as $(a \oplus_{1/4} (b; c)) : \epsilon \Rightarrow_D \frac{1}{4} * (a : \epsilon) \oplus \frac{3}{4} * ((b; c) : \epsilon)$

$= \frac{1}{4} * a \cdot \mathcal{O}(\mathrm{E}) \oplus \frac{3}{4} * b \cdot \mathcal{O}(c : \epsilon)$ as $a : \epsilon \xrightarrow{a}_D \mathrm{E}$ and $(b; c) : \epsilon \xrightarrow{b}_D c : \epsilon$

$= \frac{1}{4} * a \cdot Dir(\epsilon) \oplus \frac{3}{4} b \cdot c \cdot Dir(\epsilon)$ as $\mathcal{O}(\mathrm{E})$ and $c \xrightarrow{c}_D \mathrm{E}$

$= \frac{1}{4} * Dir(a) \oplus \frac{3}{4} * Dir(bc)$.

(2) $\mathcal{O}((((a \oplus_{1/4} (b; c))\langle a \rightsquigarrow b; d\rangle)\langle c \rightsquigarrow d\rangle) : \epsilon)$

$= \frac{1}{4} * \mathcal{O}(a : \langle a \rightsquigarrow b; d\rangle\langle c \rightsquigarrow d\rangle) \oplus \frac{3}{4} * \mathcal{O}((b; c) : \langle a \rightsquigarrow b; d\rangle\langle c \rightsquigarrow d\rangle)$

as $(a \oplus_{1/4} (b; c))\langle a \rightsquigarrow b; d\rangle\langle c \rightsquigarrow d\rangle \Rightarrow_D$

$\frac{1}{4} * (a : \langle a \rightsquigarrow b; d\rangle\langle c \rightsquigarrow d\rangle) \oplus \frac{3}{4} * ((b; c) : \langle a \rightsquigarrow b; d\rangle\langle c \rightsquigarrow d\rangle)$

$= \frac{1}{4} * b \cdot \mathcal{O}(d : \langle c \rightsquigarrow d\rangle) \oplus \frac{3}{4} \cdot b \cdot \mathcal{O}(c : \langle a \rightsquigarrow b; d\rangle\langle c \rightsquigarrow d\rangle)$

as $a : \langle a \rightsquigarrow b; d\rangle\langle c \rightsquigarrow d\rangle \xrightarrow{b}_D d : \langle c \rightsquigarrow d\rangle$

and $(b; c) : \langle a \rightsquigarrow b; d\rangle\langle c \rightsquigarrow d\rangle \xrightarrow{b}_D c : \langle a \rightsquigarrow b; d\rangle\langle c \rightsquigarrow d\rangle$

$= \frac{1}{4} * b \cdot d \cdot \mathcal{O}(\mathrm{E}) \oplus \frac{3}{4} \cdot b \cdot d \cdot \mathcal{O}(\mathrm{E})$

as $d : \langle c \rightsquigarrow d \rangle \xrightarrow{d}_D \mathrm{E}$ and $c : \langle a \rightsquigarrow b; d \rangle \langle c \rightsquigarrow d \rangle \xrightarrow{d}_D \mathrm{E}$

$= \frac{1}{4} * \mathit{Dir}(bd) \oplus \frac{3}{4} * \mathit{Dir}(bd)$

$= \mathit{Dir}(bd).$

(3) Next we compute $\mathcal{O}(x : \epsilon)$ where $D(x) = a \oplus_{1/2} (a; x)$. For this it turns out to be convenient to exploit the metric foundation of $\mathcal{O}$. On the one hand we have

$$\mathcal{O}(x : \epsilon) = \tfrac{1}{2} * a \cdot \mathcal{O}(\epsilon) \oplus \tfrac{1}{2} * a \cdot \mathcal{O}(x : \epsilon). \tag{3.1}$$

On the other hand we have for the probability measure $p \in \mathcal{M}(Act^\infty)$ given by $p = \frac{1}{2} * \mathit{Dir}(a) \oplus \frac{1}{4} * \mathit{Dir}(aa) \oplus \frac{1}{8} * \mathit{Dir}(aaa) \oplus \cdots = \bigoplus_{n=1}^{\infty} \frac{1}{2}^n * \mathit{Dir}(a^n)$ that p satisfies

$$p = \tfrac{1}{2} * \mathit{Dir}(a) \oplus \tfrac{1}{2} * a \cdot p. \tag{3.2}$$

We claim that $\mathcal{O}(x : \epsilon) = p$. This can be shown by the following metric argument:

$d(\mathcal{O}(x : \epsilon), p)$

$=$ [equations (3.1), (3.2)] $d(\frac{1}{2} * \mathit{Dir}(a) \oplus \frac{1}{2} * a \cdot \mathcal{O}(x : \epsilon), \frac{1}{2} * \mathit{Dir}(a) \oplus \frac{1}{2} * a \cdot p)$

$\leq$ [property (2.2)] $\max\{ d(\mathit{Dir}(a), \mathit{Dir}(a)), d(a \cdot \mathcal{O}(x : \epsilon), a \cdot p) \}$

$=$ [property (2.1)] $\frac{1}{2} d(\mathcal{O}(x : \epsilon), p)$.

We conclude that $d(\mathcal{O}(x : \epsilon), p) = 0$ and hence, since $\mathcal{M}(Act^\infty)$ is a metric space, that $\mathcal{O}(x : \epsilon) = p$.

Although it holds that $\mathit{wgt}(r) > \mathit{wgt}(r_1), \mathit{wgt}(r_2)$ if $r \Rightarrow_D \pi * r_1 \oplus \pi^c * r_2$ there is in general no structural relationship nor a comparison in wgt for r at the right-hand side and r' at the left-hand side of the second clause of Definition 3.6. Therefore the definition of $\mathcal{O}$ needs further justification. We introduce a higher-order transformation $\Phi \colon \mathit{Sem} \to \mathit{Sem}$ and check that Φ is a contraction on a complete metric space. Then, by Banach's Fixedpoint Theorem, there exists a unique fixedpoint of Φ, which must equal $\mathcal{O}$ by its definition.

Lemma 3.7 *Put $\mathit{Sem} = \mathit{Res} \to \mathcal{M}(Act^\infty)$. The higher-order transformation $\Phi \colon \mathit{Sem} \to \mathit{Sem}$ is given by*

$$\Phi(S)(E) = \epsilon$$

$$\Phi(S)(r) = a \cdot S(r') \quad \text{if } r \xrightarrow{a}_D r'$$

$$\Phi(S)(r) = \pi * \Phi(S)(r') \oplus \pi^c * \Phi(S)(r'') \quad \text{if } r \Rightarrow_D \pi * r' \oplus \pi^c * r''$$

for $S \in \mathit{Sem}$. Then Φ is well-defined and $\frac{1}{2}$-contractive.

Proof. *Well-definedness of Φ follows from the fact that $\mathit{wgt}(r'), \mathit{wgt}(r'') <$*

$wgt(r)$ if $r \Rightarrow_D \pi * r' \oplus \pi^c * r''$. In order to show $\frac{1}{2}$-contractiveness of Φ we check

$$d(\Phi(S_1)(r), \Phi(S_2)(r)) \leq \tfrac{1}{2} d(S_1, S_2)$$

for arbitrary $S_1, S_2 \in Sem$ by distinguishing three cases. The case for E is clear.

$$\begin{aligned}
[r \xrightarrow{a}_D r'] \quad & d(\Phi(S_1)(r), \Phi(S_2)(r)) \\
= \; & d(a \cdot S_1(r'), a \cdot S_2(r')) \\
= \; & \text{[property (2.1)]} \; \tfrac{1}{2} d(S_1(r'), S_2(r')) \\
\leq \; & \text{[definition } d \text{ on } Sem] \; \tfrac{1}{2} d(S_1, S_2)
\end{aligned}$$

$$\begin{aligned}
[r \Rightarrow_D \pi * r' \oplus \pi^c * r''] \quad & d(\Phi(S_1)(r), \Phi(S_2)(r)) \\
= \; & d(\pi * \Phi(S_1)(r') \oplus \pi^c * \Phi(S_1)(r''), \pi * \Phi(S_2)(r') \oplus \pi^c * \Phi(S_2)(r'')) \\
= \; & \text{[property (2.2)]} \\
& \max\{\, d(\Phi(S_1)(r'), \Phi(S_2)(r')), d(\Phi(S_1)(r''), \Phi(S_2)(r'')) \,\} \\
\leq \; & \text{[induction hypothesis on } r', r''] \; \tfrac{1}{2} d(S_1, S_2).
\end{aligned}$$

□

4 Denotational semantics

The operational semantics $\mathcal{O}$ is of a step-oriented nature. The model $\mathcal{O}$ reflects the *computational* intuition underlying the process language $\mathcal{L}_{pr}$. In this section we present a denotational semantics $\mathcal{D}$ for $\mathcal{L}_{pr}$. Traditionally, this implies that $\mathcal{D}$ has the following characteristic properties:

- $\mathcal{D}$ maps statements into a mathematical domain (here, a complete ultrametric space)
- compositionality, i.e. the meaning $\mathcal{D}(s_1 * s_2)$ of a composition $s_1 * s_2$ in $\mathcal{L}_{pr}$ is obtained from a composition $\mathcal{D}(s_1) * \mathcal{D}(s_2)$ of the meanings $\mathcal{D}(s_1)$ of s_1 and $\mathcal{D}(s_2)$ of s_2
- recursion is handled via a fixed point construction (here, Banach's Fixed Point Theorem).

First we present our mathematical domain.

Definition 4.1 The domain of denotations $\mathbb{P}$ is given by $\mathbb{P} = \mathcal{M}(\mathbb{Q})$ where $\mathbb{Q} = Act^\infty \setminus \{\epsilon\}$.

The metavariables p and q are used to range over $\mathbb{P}$ and $\mathbb{Q}$, respectively. The restriction to measures over nonempty words is necessary for proving Lemma 4.6 which is in turn crucial in proving the fixed point characterization of $\mathcal{D}$ in Lemma 4.8. We have that every element in $\mathbb{P}$ can be written in one of the following three forms:

- the indicator function $Dir(a)$ for some $a \in Act$
- $a \cdot p$ for some $a \in Act$, $p \in \mathbb{P}$
- $\bigoplus_{i=1}^{m} \rho_i * p_i$ for $\rho_i \in (0,1)$, $p_i = a_i$ or $p_i = a_i \cdot p'_i$ with $a_i \in Act$, $p'_i \in \mathbb{P}$ and $\sum_{i \in I} \rho_i = 1$.

The fact that a finite combination in the third clause for the representation of elements in $\mathbb{P}$ suffices, follows from the observation that in $\mathbb{P}$ only measures of compact support are considered.

Next we provide semantical counterparts of the syntactical construction of the sequential and probabilistic compositions ';' and '$\oplus_\pi$'.

Definition 4.2

(a) The semantical operator ';': $\mathbb{P} \times \mathbb{P} \to \mathbb{P}$ is given by

$$\begin{aligned} Dir(a); p &= a \cdot p \\ (a \cdot p); p' &= a \cdot (p; p') \\ (\textstyle\bigoplus_{i=1}^{m} \rho_i * p_i); p' &= \textstyle\bigoplus_{i=1}^{m} \rho_i * (p_i; p') \end{aligned}$$

(b) The semantical operator '$\oplus_\pi$': $\mathbb{P} \times \mathbb{P} \to \mathbb{P}$, for $\pi \in (0,1)$, is given by

$$p \oplus_\pi p' = (\pi * p) \oplus (\pi^c * p').$$

The definition of the semantical operator ';' needs further comment as ';' occurs also at the right-hand side of Definition 4.2. Again, we introduce a higher-order transformation. Now we consider a mapping $\Omega_;: Op \to Op$ on a complete metric space Op and verify the contractivity of $\Omega_;$.

Lemma 4.3 *Put $Op = \mathbb{P} \times \mathbb{P} \to \mathbb{P}$. Define the higher-order transformation $\Omega_;: Op \to Op$ by*

$$\begin{aligned} \Omega_;(\phi)(Dir(a), p') &= a \cdot p' \\ \Omega_;(\phi)(a \cdot \bar{p}, p') &= a \cdot \phi(\bar{p}, p') \\ \Omega_;(\phi)(\textstyle\bigoplus_{i=1}^{m} \rho_i * p_i, p') &= \textstyle\bigoplus_{i=1}^{m} \rho_i * \Omega_;(\phi)(p_i, p'). \end{aligned}$$

Then $\Omega_;$ is well-defined and $\frac{1}{2}$-contractive.

Proof. *Well-definedness of $\Omega_;$ is clear. In the third clause each p_i is either of the format $p_i = Dir(a_i)$ or $p_i = a_i \cdot \bar{p}_i$, which are covered by the other clauses.*

To show that $\Omega_;$ is contractive we prove, for arbitrary $\phi_1, \phi_2 \in Op$, $p, p' \in \mathbb{P}$,

$$d(\Omega_;(\phi_1)(p, p'), \Omega_;(\phi_2)(p, p')) \leq \tfrac{1}{2} d(\phi_1, \phi_2)$$

from which, by definition of d on Op, it follows that $d(\Omega_;(\phi_1), \Omega_;(\phi_2)) \leq \frac{1}{2} d(\phi_1, \phi_2)$. We distinguish three cases:

$[a]$ $\quad d(\Omega_;(\phi_1)(a, p'), \Omega_;(\phi_2)(a, p')) = d(a \cdot p', a \cdot p') = 0$

$[a \cdot \bar{p}]$ $\quad d(\Omega_;(\phi_1)(a \cdot \bar{p}), \Omega_;(\phi_2)(a \cdot \bar{p}))$

$$= d(a \cdot \phi_1(\bar{p}, p'), a \cdot \phi_2(\bar{p}, p'))$$

$$
\begin{aligned}
&= \textit{[property (2.1)]}\ \tfrac{1}{2}d(\phi_1(\bar{p},p'),\phi_2(\bar{p},p')) \\
&\leq \tfrac{1}{2}d(\phi_1,\phi_2)
\end{aligned}
$$

$[\bigoplus_{i=1}^{m} \rho_i * p_i]$ $\quad d(\Omega_;(\phi_1)(\bigoplus_{i=1}^{m} \rho_i * p_i, p'), \Omega_;(\phi_2)(\bigoplus_{i=1}^{m} \rho_i * p_i, p'))$

$$
\begin{aligned}
&= d(\textstyle\bigoplus_{i=1}^{m} \rho_i * \Omega_;(\phi_1)(p_i,p'), \bigoplus_{i=1}^{m} \rho_i * \Omega_;(\phi_2)(p_i,p')) \\
&\leq \textit{[property (2.2)]}\ \max\{\ d(\Omega_;(\phi_1)(p_i,p'),\Omega_;(\phi_2)(p_i,p') \mid i \in I\ \} \\
&\leq \textit{[previous cases]}\ \tfrac{1}{2}d(\phi_1,\phi_2).
\end{aligned}
$$

□

We next present the denotational semantics $\mathcal{D}$ for $\mathcal{L}_{pr}$. In the context of $\mathcal{D}$ the role of the refinement sequences R as for the operational semantics $\mathcal{O}$, will now be played by so-called semantical refinements as introduced in [HVB99]. The usage of an extra argument for the semantical mapping $\mathcal{D}$ is reminiscent of the deployment of so-called environments to handle recursion (see, e.g., [Sto77]).

Definition 4.4 Let the collection *SemRef* of semantical refinements, ranged over by η, be given by $\mathit{SemRef} = \mathit{Act} \to \mathbb{P}$. In particular we distinguish $\eta_{id} \in \mathit{SemRef}$ such that $\eta_{id}(a) = \mathit{Dir}(a)$ for all $a \in \mathit{Act}$. The semantical mapping $\mathcal{D}\colon \mathcal{L}_{pr} \to \mathit{SemRef} \to \mathbb{P}$ is given by

$$
\begin{aligned}
\mathcal{D}(a)(\eta) &= \eta(a) \\
\mathcal{D}(s;s')(\eta) &= \mathcal{D}(s)(\eta);\mathcal{D}(s')(\eta) \\
\mathcal{D}(s \oplus_\pi s')(\eta) &= \mathcal{D}(s)(\eta) \oplus_\pi \mathcal{D}(s')(\eta) \\
\mathcal{D}(s\langle a \rightsquigarrow s'\rangle)(\eta) &= \mathcal{D}(s)(\eta[\mathcal{D}(s')(\eta)/a]) \\
\mathcal{D}(x)(\eta) &= \mathcal{D}(D(x))(\eta)
\end{aligned}
$$

The denotational semantics $\mathcal{D}[\![\cdot]\!]\colon \mathcal{L}_{pr} \to \mathbb{P}$ is given by $\mathcal{D}[\![s]\!] = \mathcal{D}(s)(\eta_{id})$.

Note that Definition 4.4 does not go by structural induction (cf. the clause for x) nor does it go by *wgt*-induction (cf. the clause for $s;s'$). We first provide some examples of $\mathcal{D}$ before delving into the well-definedness of $\mathcal{D}$.

Examples

(1) $\quad \mathcal{D}(a \oplus_{1/4} (b;c))(\eta_{id})$

$$
\begin{aligned}
&= \mathcal{D}(a)(\eta_{id}) \oplus_{1/4} \mathcal{D}(b;c)(\eta_{id}) \\
&= \tfrac{1}{4} * \eta_{id}(a) \oplus \tfrac{3}{4} * (\mathcal{D}(b)(\eta_{id});\mathcal{D}(c)(\eta_{id})) \\
&= \tfrac{1}{4} * \mathit{Dir}(a) \oplus \tfrac{3}{4} * (\eta_{id}(b);\eta_{id}(c)) \\
&= \tfrac{1}{4} * \mathit{Dir}(a) \oplus \tfrac{3}{4} * (\mathit{Dir}(b);\mathit{Dir}(c)) \\
&= \tfrac{1}{4} * \mathit{Dir}(a) \oplus \tfrac{3}{4} * (\mathit{Dir}(bc))
\end{aligned}
$$

(2) $\mathcal{D}(((a \oplus_{1/4} (b;c))\langle a \rightsquigarrow b;d\rangle)\langle c \rightsquigarrow d\rangle)(\eta_{id})$

$= \mathcal{D}((a \oplus_{1/4} (b;c))\langle a \rightsquigarrow b;d\rangle)(\eta_{id}[\mathcal{D}(d)(\eta_{id})/c])$

$= \mathcal{D}((a \oplus_{1/4} (b;c))\langle a \rightsquigarrow b;d\rangle)(\eta_{id}[\mathit{Dir}(d)/c])$

$= \mathcal{D}((a \oplus_{1/4} (b;c))(\eta_{id}[\mathit{Dir}(d)/c][\mathcal{D}(b;d)(\eta_{id}[\mathit{Dir}(d)/c])/a]))$

$= \ldots$

$= \mathcal{D}(a \oplus_{1/4} (b;c))(\eta_{id}[\mathit{Dir}(d)/c, \mathit{Dir}(bd)/a])$

$= \frac{1}{4} * \mathcal{D}(a)(\eta_{id}[\mathit{Dir}(d)/c, \mathit{Dir}(bd)/a]) \oplus$
$\frac{3}{4} * \mathcal{D}(b;c)(\eta_{id}[\mathit{Dir}(d)/c, \mathit{Dir}(bd)/a])$

$= \ldots$

$= \frac{1}{4} * \mathit{Dir}(bd) \oplus \frac{3}{4} * (\mathit{Dir}(b); \mathit{Dir}(d))$

$= \frac{1}{4} * \mathit{Dir}(bd) \oplus \frac{3}{4} * \mathit{Dir}(bd)$

$= \mathit{Dir}(bd)$

(3) Suppose $D(x) = a \oplus_{1/2} (a;x)$. On the one hand we have
$\mathcal{D}(x)(\eta_{id})$

$= \mathcal{D}(a \oplus_{1/2} (a;x))(\eta_{id})$

$= \frac{1}{2} * \mathcal{D}(a)(\eta) \oplus \frac{1}{2} * (\mathcal{D}(a)(\eta_{id}); \mathcal{D}(x)(\eta_{id}))$

$= \frac{1}{2} * \mathit{Dir}(a) \oplus \frac{1}{2} * (a \cdot \mathcal{D}(x)(\eta_{id}))$

On the other hand we have for $p = \bigoplus_{i=1}^{\infty} \left(\frac{1}{2}\right)^n * \mathit{Dir}(a^n)$ that $p = \frac{1}{2} * \mathit{Dir}(a) \oplus \frac{1}{2} * (a \cdot p)$. Hence, as for the same example in the context of Section 3, we have
$d(\mathcal{D}(x)(\eta_{id}), p)$

$= d(\frac{1}{2} * \mathit{Dir}(a) \oplus \frac{1}{2} * (a \cdot \mathcal{D}(x)(\eta_{id})), \frac{1}{2} * \mathit{Dir}(a) \oplus *(a \cdot p))$

$\leq$ [property (2.2)] $\max\{\, d(\mathit{Dir}(a), \mathit{Dir}(a)), d(a \cdot \mathit{Dir}(x)(\eta_{id}), a \cdot p) \,\}$

$=$ [property (2.1)] $\frac{1}{2} \cdot d(\mathcal{D}(x)(\eta_{id}), p)$.

Therefore, $d(\mathit{Dir}(x)(\eta_{id}), p) = 0$ and $\mathcal{D}(x)(\eta_{id}) = \bigoplus_{i=1}^{\infty} \left(\frac{1}{2}\right)^n * \mathit{Dir}(a^n)$.

We first establish some nonexpansiveness/contractivity properties and distributivity results of the semantical operators that are needed for the justification of the definition of $\mathcal{D}$ in the sequel.

Lemma 4.5 *The semantical operator '$;$' is nonexpansive in its first argument and $\frac{1}{2}$-contractive in its second argument.*

Proof. *Define the subset $Op_0 \subseteq Op$ by $\phi \in Op_0 \iff d(\phi(p,p''), \phi(p',p'')) \leq d(p,p') \wedge d(\phi(p,p'), \phi(p,p'')) \leq \frac{1}{2} d(p',p'')$. Note that $Op_0 \subseteq Op$ is a nonempty* *and closed subset. We check that* $\phi \in Op_0$ *implies* $\Omega_;(\phi) \in Op_0$ *and then apply Theorem 2.1.*

Pick any $\phi \in Op_0$ *and choose arbitrary* $p, p', p'' \in \mathbb{P}$*. We verify the inequality* $d(\Omega_;(\phi)(p,p''), \Omega_;(\phi)(p',p'')) \leq d(p,p')$*. Without loss of generality (leaving the details to the reader) we can assume* $d(p,p') < \frac{1}{2}$*. We distinguish three cases.*

$[p = a, p' = a]$ *Clear.*

$[p = a \cdot \bar{p}, p' = a \cdot \bar{p}']$ *We have that* $d(p,p') = \frac{1}{2} d(\bar{p}, \bar{p}')$*.*

$$
\begin{aligned}
& d(\Omega_;(\phi)(p,p''), \Omega_;(\phi)(p',p'')) \\
= \ & d(a \cdot \phi(\bar{p}, p'), a \cdot \phi(\bar{p}', p'')) \\
= \ & \tfrac{1}{2} d(\phi(\bar{p}, p''), \phi(\bar{p}', p'')) \\
\leq \ & \text{[property } \phi] \ \tfrac{1}{2} d(\bar{p}, \bar{p}') \\
= \ & d(p,p')
\end{aligned}
$$

$[p = \bigoplus_{i=1}^m \rho_i * p_i, p' = \bigoplus_{i=1}^m \rho_i * p'_i]$ *Note that, for* i, $1 \leq i \leq m$, p_i, p'_i *are either both of the format* $p_i = a_i$, $p'_i = a_i$ *or both of the format* $p_i = a_i \cdot \bar{p}_i, p'_i = a_i \cdot \bar{p}'_i$*.*

$$
\begin{aligned}
& d(\Omega_;(\phi)(p,p''), \Omega_;(\phi)(p',p'')) \\
= \ & d(\textstyle\bigoplus_{i=1}^m \rho_i * \Omega_;(\phi)(p_i, p''), \bigoplus_{i=1}^m \rho_i * \Omega_;(\phi)(p'_i, p'')) \\
= \ & \max\{ \, d(\Omega_;(\phi)(p_i, p''), \Omega_;(\phi)(p'_i)) \\
\leq \ & \text{[earlier cases]} \ d(p,p').
\end{aligned}
$$

We conclude that $d(\Omega_;(\phi)(p,p''), \Omega_;(\phi)(p',p'')) \leq d(p,p')$*. Similarly, one can prove that* $d(\Omega_;(\phi)(p,p'), \Omega_;(\phi)(p,p'')) \leq \frac{1}{2} d(p',p'')$*.* □

Nonexpansiveness of the semantical operator '$\oplus_\pi$' is straightforward.

Lemma 4.6 *The semantical operator '*$\oplus_\pi$*' is nonexpansive for all* $\pi \in (0,1)$*.*

Proof. *Immediate by property (2.2).* □

Next we establish that probabilistic composition distributes over sequential composition.

Lemma 4.7 *For all* $p, p', p'' \in \mathbb{P}$ *it holds that* $(p \oplus_\pi p'); p'' = (p; p'') \oplus_\pi (p'; p'')$*.*

Proof. *Suppose* $p = \bigoplus_{i=1}^m \rho_i * p_i$, $p' = \bigoplus_{j=1}^n \sigma_j * p'_j$*. Then, for any* $\pi \in (0,1)$,

$$
\begin{aligned}
& (p \oplus_\pi p'); p'' \\
= \ & ((\textstyle\bigoplus_{i=1}^m (\pi \cdot \rho_i) * p_i) \oplus (\bigoplus_{j=1}^n (\pi^c \cdot \sigma_j) * p'_j)); p'' \\
= \ & (\textstyle\bigoplus_{i=1}^m (\pi \cdot \rho_i) * (p_i; p'')) \oplus ((\pi^c \cdot \sigma_j) * (p'_j; p'')) \\
= \ & \pi * (\textstyle\bigoplus_{i=1}^m \rho_i * (p_i; p'')) \oplus \pi^c * (\bigoplus_{j=1}^n \sigma_j * (p'_j; p''))
\end{aligned}
$$

$$= (\pi * (p; p'')) \oplus (\pi^c * (p'; p''))$$
$$= (p; p'') \oplus_\pi (p'; p'').$$

□

We have now gathered sufficient auxiliary results in order to be able to provide a fixed point characterization for $\mathcal{D}$.

Lemma 4.8 *Let* $Sem = \mathcal{L}_{pr} \to SemRef \to_1 \mathbb{P}$. *Define the higher-order transformation* $\Psi\colon Sem \to Sem$ *by*

$$\begin{aligned}
\Psi(S)(a)(\eta) &= \eta(a) \\
\Psi(S)(s; s')(\eta) &= \Psi(S)(s)(\eta); S(s')(\eta) \\
\Psi(S)(s \oplus_\pi s')(\eta) &= \Psi(S)(s)(\eta) \oplus_\pi \Psi(S)(s')(\eta) \\
\Psi(S)(s\langle a \rightsquigarrow s'\rangle)(\eta) &= \Psi(S)(s)(\eta[\Psi(S)(s')(\eta)/a]) \\
\Psi(S)(x)(\eta) &= \Psi(S)(D(x))(\eta)
\end{aligned}$$

for $S \in Sem$. *Then it holds that:*

(a) Ψ *is well-defined.*

(b) Ψ *is* $\frac{1}{2}$*-contractive.*

Proof.

(a) We check by induction on $wgt(s)$ *that* $\Psi(S)(s)$ *is nonexpansive in* η, *for any* $S \in Sem$. *We only cover three cases. (The cases for* a *and* x *are straightforward.) Choose* $\eta_1, \eta_2 \in SemRef$.

$[s; s']$ $\quad d(\Psi(S)(s; s')(\eta_1), \Psi(S)(s; s')(\eta_2))$

$$\begin{aligned}
&= d(\Psi(S)(s)(\eta_1); S(s')(\eta_1), \Psi(S)(s)(\eta_2); S(s')(\eta_2)) \\
&\leq \text{[`;' nonexpansive/contractive]} \\
&\qquad \max\{\, d(\Psi(S)(s)(\eta_1), \Psi(S)(s)(\eta_2)), \\
&\qquad\qquad \tfrac{1}{2} d(S(s')(\eta_1), S(s')(\eta_2)) \,\} \\
&\leq \text{[induction hypothesis for } s\text{; property } S \in Sem] \;\; d(\eta_1, \eta_2)
\end{aligned}$$

$[s \oplus_\pi s']$ $\quad d(\Psi(S)(s \oplus_\pi s')(\eta_1), \Psi(S)(s \oplus_\pi s')(\eta_2))$

$$\begin{aligned}
&= d(\Psi(S)(s)(\eta_1) \oplus_\pi \Psi(S)(s')(\eta_1), \\
&\qquad \Psi(S)(s)(\eta_2) \oplus_\pi \Psi(S)(s')(\eta_2)) \\
&\leq \text{[`}\oplus\text{' nonexpansive]} \\
&\qquad \max\{\, d(\Psi(S)(s)(\eta_1), \Psi(S)(s)(\eta_2)), \\
&\qquad\qquad d(\Psi(S)(s')(\eta_1), \Psi(S)(s')(\eta_2)) \,\}
\end{aligned}$$

$\leq$ *[induction hypothesis for s, s']* $d(\eta_1, \eta_2)$

$[s\langle a \rightsquigarrow s' \rangle]$ $\quad d(\Psi(S)(s\langle a \rightsquigarrow s' \rangle)(\eta_1), \Psi(S)(s\langle a \rightsquigarrow s' \rangle)(\eta_2))$

$= d(\Psi(S)(s)(\eta_1[\Psi(S)(s')(\eta_1)/a]),$

$\Psi(S)(s)(\eta_2[\Psi(S)(s')(\eta_2)/a]))$

$=$ *[induction hypothesis for s]*

$d(\eta_1[\Psi(S)(s')(\eta_1)/a], \eta_2[\Psi(S)(s')(\eta_2)/a])$

$\leq$ *[definition d on SemRef]*

$\max\{\, d(\eta_1, \eta_2), d(\Psi(S)(s')(\eta_1), \Psi(S)(s')(\eta_2)) \,\}$

$\leq$ *[induction hypothesis for s']* $d(\eta_1, \eta_2)$

(b) We prove by induction on $\mathrm{wgt}(s)$ *that*

$$d(\Psi(S_1)(s)(\eta), \Psi(S_2)(s)(\eta)) \leq \tfrac{1}{2} d(S_1, S_2)$$

for any $S_1, S_2 \in$ Sem, $s \in \mathcal{L}_{pr}$, $\eta \in$ SemRef. We treat three cases (leaving the cases of a and x to the reader).

$[s; s']$ $\quad d(\Psi(S_1)(s; s')(\eta), \Psi(S_2)(s; s')(\eta))$

$= d(\Psi(S_1)(s)(\eta); S_1(s')(\eta), \Psi(S_2)(s)(\eta); S_2(s')(\eta))$

$\leq$ *['$;$' nonexpansive/contractive]*

$\max\{\, d(\Psi(S_1)(s)(\eta), \Psi(S_2)(s)(\eta)),$

$\tfrac{1}{2} d(S_1(s')(\eta), S_2(s')(\eta)) \,\}$

$\leq$ *[induction hypothesis for s; definition d on Sem]*

$\tfrac{1}{2} d(S_1, S_2)$

$[s \oplus_\pi s']$ $\quad d(\Psi(S_1)(s \oplus_\pi s')(\eta), \Psi(S_2)(s \oplus_\pi s')(\eta))$

$= d(\Psi(S_1)(s)(\eta) \oplus_\pi \Psi(S_1)(s')(\eta),$

$\Psi(S_2)(s)(\eta) \oplus_\pi \Psi(S_2)(s')(\eta))$

$\leq$ *['$\oplus_\pi$' nonexpansive]*

$\max\{\, d(\Psi(S_1)(s)(\eta), \Psi(S_2)(s)(\eta)),$

$d(\Psi(S_1)(s')(\eta), \Psi(S_2)(s')(\eta)) \,\}$

$\leq$ *[induction hypothesis for s, s']* $\tfrac{1}{2} d(S_1, S_2)$

$[s\langle a \rightsquigarrow s' \rangle]$ $\quad d(\Psi(S_1)(s\langle a \rightsquigarrow s' \rangle)(\eta), \Psi(S_2)(s\langle a \rightsquigarrow s' \rangle)(\eta))$

$$\begin{aligned}
&= d(\Psi(S_1)(s)(\eta[\Psi(S_1)(s')(\eta)/a]),\\
&\qquad \Psi(S_2)(s)(\eta[\Psi(S_2)(s')(\eta)/a]))\\
&\leq \textit{[ultrametricity]}\\
&\quad \max\{\; d(\Psi(S_1)(s)(\eta[\Psi(S_1)(s')(\eta)/a]),\\
&\qquad\qquad \Psi(S_1)(s)(\eta[\Psi(S_2)(s')(\eta)/a])),\\
&\qquad\quad d(\Psi(S_1)(s)(\eta[\Psi(S_2)(s')(\eta)/a]),\\
&\qquad\qquad \Psi(S_2)(s)(\eta[\Psi(S_2)(s')(\eta)/a]))\;\}\\
&\leq \textit{[}\Psi(S_1)(s)\textit{ nonexpansive in }\eta\textit{; induction hypothesis for }s\textit{]}\\
&\quad \max\{\; d(\Psi(S_1)(s')(\eta), \Psi(S_2)(s')(\eta)), \tfrac{1}{2}d(S_1,S_2)\;\}\\
&= \textit{[induction hypothesis for }s'\textit{]}\;\; \tfrac{1}{2}d(S_1,S_2). \qquad \Box
\end{aligned}$$

Note the usage above of the ultrametricity, i.e. the strong triangle inequality, which holds for the space $\mathcal{M}(Act^\infty \setminus \{\epsilon\})$.

5 Correctness

In this section we will establish the correctness of the denotational semantics $\mathcal{D}$ for $\mathcal{L}_{pr}$ with respect to its operational model $\mathcal{O}[\![\cdot]\!]$. As the functionality of $\mathcal{D}$ differs form that of $\mathcal{O}$, viz. $\mathcal{D}\colon \mathcal{L}_{pr} \to \mathit{SemRef} \to \mathcal{M}(Act^\infty \setminus \{\epsilon\})$ versus $\mathcal{O}\colon \mathit{Res} \to \mathcal{M}(Act^\infty)$ we will use an intermediate function $\mathcal{E}$ that is based on $\mathcal{D}$ for its definition, but agrees with $\mathcal{O}$ for its functionality. The main lemma of this section, Lemma 5.2, exploits Banach's Fixed Point Theorem to show that $\mathcal{O}$ and $\mathcal{E}$ in fact coincide.

First we need a mechanism, as proposed in [HVB99], to combine syntactical refinement sequences $R \in \mathit{Ref}$ and semantical refinements $\eta \in \mathit{SemRef}$.

Lemma 5.1 *Let the function $\cdot \rhd \cdot\colon \mathit{Ref} \times \mathit{SemRef} \to \mathit{SemRef}$ be inductively given by*

$$\epsilon \rhd \eta = \eta$$

$$(R \cdot \langle a \rightsquigarrow s\rangle) \rhd \eta = R \rhd \eta[\mathcal{D}(s)(\eta)/a].$$

Then it holds that

(a) $\mathcal{D}(s\langle a_1 \rightsquigarrow s_1\rangle\langle a_2 \rightsquigarrow s_2\rangle \cdots \langle a_n \rightsquigarrow s_n\rangle)(\eta) = \mathcal{D}(s)(\langle a_1 \rightsquigarrow s_1\rangle\langle a_2 \rightsquigarrow s_2\rangle \cdots \langle a_n \rightsquigarrow s_n\rangle \rhd \eta)$;

(b) $\mathcal{D}(s_1\langle a \rightsquigarrow s_2\rangle)(R \rhd \eta) = \mathcal{D}(s_1)((\langle a \rightsquigarrow s_2\rangle \cdot R) \rhd \eta)$.

Proof. *Induction on n for part (a). Application of part (a) for part (b).* $\Box$

Next we present the intermediate semantical mapping $\mathcal{E}$ and prove that $\mathcal{E}$ is a fixed point of the higher order transformation Φ of Lemma 3.7. Since, by Banach's Fixed Point Theorem, Φ has exactly one fixed point —which is $\mathcal{O}$— it follows that $\mathcal{O} = \mathcal{E}$. The definition of $\mathcal{E}$ makes both use of the denotational semantics $\mathcal{D}$, for resumptions of the format $s : R$, and of the semantical operators defined on the domain $\mathbb{P}$, for resumptions of the format $r_1 * r_2$ where '$*$' is either a sequential or a probabilistic operator.

Lemma 5.2 *Let the mapping $\mathcal{E}\colon Res \to \mathcal{M}(Act^\infty)$ be given as follows:*

$$\begin{aligned} \mathcal{E}(E) &= Dir(\epsilon) \\ \mathcal{E}(s : R) &= \mathcal{D}(s)(R \triangleright \eta_{id}) \\ \mathcal{E}(r_1 * r_2) &= \mathcal{E}(r_1) * \mathcal{E}(r_2) \quad \textit{for } * \in \{;, \oplus_\pi\}. \end{aligned}$$

Then it holds that $\Phi(\mathcal{E}) = \mathcal{E}$.

Proof. *It is straightforwardly checked that $\mathcal{E}(r) \in \mathbb{P}$ for $r \neq E$, hence $\mathcal{E}$ is well-defined. We prove that $\Phi(\mathcal{E}) = \mathcal{E}$ by weight-induction for resumptions. We only exhibit a few typical cases:*

$[(s_1 * s_2) : R \textit{ for } * \in \{;, \oplus_\pi\}]$ $\quad \Phi(\mathcal{E})((s_1 * s_2) : R)$

$$\begin{aligned} &= \textit{[transition rule (Op)]}\ \ \Phi(\mathcal{E})((s_1 : R) * (s_2 : R)) \\ &= \textit{[induction hypothesis]}\ \ \mathcal{E}((s_1 : R) * (s_2 : R)) \\ &= \textit{[definition of } \mathcal{E}\textit{]}\ \ \mathcal{E}(s_1 : R) * \mathcal{E}(s_2 : R) \\ &= \textit{[definition of } \mathcal{E}\textit{]}\ \ \mathcal{D}(s_1)(R \triangleright \eta_{id}) * \mathcal{D}(s_2)(R \triangleright \eta_{id}) \\ &= \textit{[definition of } \mathcal{D}\textit{]}\ \ \mathcal{D}(s_1 * s_2)(R \triangleright \eta_{id}) \\ &= \textit{[definition of } \mathcal{E}\textit{]}\ \ \mathcal{E}((s_1 * s_2) : R) \end{aligned}$$

$[s_1\langle a \rightsquigarrow s_2\rangle : R]$ $\quad \Phi(\mathcal{E})(s_1\langle a \rightsquigarrow s_2\rangle : R)$

$$\begin{aligned} &= \textit{[transition rule (Ref)]}\ \ \Phi(\mathcal{E})(s_1 : \langle a \rightsquigarrow s_2\rangle \cdot R) \\ &= \textit{[induction hypothesis]}\ \ \mathcal{E}(s_1 : \langle a \rightsquigarrow s_2\rangle \cdot R) \\ &= \textit{[definition of } \mathcal{E}\textit{]}\ \ \mathcal{D}(s_1)((\langle a \rightsquigarrow s_2\rangle \cdot R) \triangleright \eta_{id}) \\ &= \textit{[Lemma 5.1]}\ \ \mathcal{D}(s_1\langle a \rightsquigarrow s_2\rangle)(R \triangleright \eta_{id}) \\ &= \mathcal{E}(s_1\langle a \rightsquigarrow s_2\rangle : R) \end{aligned}$$

$[r_1; r_2]$ *Suppose* $r_1 \xrightarrow{a}_D r_1'$. *Then* $r_1; r_2 \xrightarrow{a}_D r_1'; r_2$.
$\Phi(\mathcal{E})(r_1; r_2)$

$$\begin{aligned} &= \textit{[transition rule (Seq)]}\ \ a \cdot \mathcal{E}(r_1'; r_2) \\ &= \textit{[definition of } \mathcal{E}\textit{]}\ \ a \cdot (\mathcal{E}(r_1'); \mathcal{E}(r_2)) \\ &= \textit{[definition ';']}\ \ (a \cdot \mathcal{E}(r_1')); \mathcal{E}(r_2) \\ &= \textit{[definition } \Phi\textit{]}\ \ \Phi(\mathcal{E})(r_1); \mathcal{E}(r_2) \end{aligned}$$

$= $ *[induction hypothesis for r_1]* $\mathcal{E}(r_1); \mathcal{E}(r_2)$

$= $ *[definition $\mathcal{E}$]* $\mathcal{E}(r_1; r_2)$

Suppose $r_1 \Rightarrow_D \pi * r_1' \oplus \pi^c * r_1''$. *Then* $r_1; r_2 \Rightarrow_D \pi * (r_1'; r_2) \oplus \pi^c * (r_1''; r_2)$.
$\Phi(\mathcal{E})(r_1; r_2)$

$= $ *[definition Φ]* $\pi * \Phi(\mathcal{E})(r_1'; r_2) \oplus \pi^c * \Phi(\mathcal{E})(r_1''; r_2)$

$= $ *[induction hypothesis]* $\pi * \mathcal{E}(r_1'; r_2) \oplus \pi^c * \mathcal{E}(r_1''; r_2)$

$= $ *[definition of $\mathcal{E}$]* $\pi * (\mathcal{E}((r_1'); \mathcal{E}(r_2)) \oplus \pi^c * (\mathcal{E}(r_1''); \mathcal{E}(r_2))$

$= $ *[Lemma 4.7]* $(\pi * \mathcal{E}(r_1') \oplus \pi^c * \mathcal{E}(r_1'')); \mathcal{E}(r_2)$

$= $ *[definition Φ]* $\Phi(\mathcal{E})(r_1); \mathcal{E}(r_2)$

$= $ *[induction hypothesis for r_1]* $\mathcal{E}(r_1); \mathcal{E}(r_2)$

$= $ *[definition $\mathcal{E}$]* $\mathcal{E}(r_1; r_2)$

$[r_1 \oplus_\pi r_2]$ $\quad \Phi(\mathcal{E})(r_1 \oplus_\pi r_2)$

$= $ *[transition rules (*PChoice*)]* $\pi * \mathcal{E}(r_1) \oplus \pi^c * \mathcal{E}(r_2)$

$= $ *[definition $\oplus_\pi$]* $\mathcal{E}(r_1) \oplus_\pi \mathcal{E}(r_2)$

$= $ *[definition $\mathcal{E}$]* $\mathcal{E}(r_1 \oplus_\pi r_2)$. □

From the lemma we immediately obtain the correctness result for the denotational semantics $\mathcal{D}$ for $\mathcal{L}_{pr}$.

Theorem 5.3 *For all $s \in \mathcal{L}_{pr}$, $\mathcal{O}[\![\cdot]\!] = \mathcal{D}(s)(\eta_{id})$ on $\mathcal{L}_{pr}$.*

Proof. *We have $\mathcal{O}[\![s]\!] = \mathcal{O}(s : \epsilon) = \mathcal{E}(s : \epsilon) = \mathcal{D}(s)(\eta_{id})$ for any $s \in \mathcal{L}_{pr}$.* □

6 Full abstraction

In this section we establish for the semantical mapping $\mathcal{D}: \mathcal{L}_{pr} \to \mathit{SemRef} \to \mathbb{P}$ full abstraction with respect to $\mathcal{O}[\![\cdot]\!]$, i.e. we will show, for any $s_1, s_2 \in \mathcal{L}_{pr}$, that

$$\mathcal{D}(s_1) = \mathcal{D}(s_2) \iff \mathcal{O}[\![C[s_1]]\!] = \mathcal{O}[\![C[s_2]]\!] \text{ for all contexts } C[\cdot].$$

The route to the main technical lemma of this section, namely Lemma 6.7, passes the following ideas:

- If a statement s has denotations with respect to the semantical refinements η_1, η_2 of distance $2^{-(n+1)}$ then the semantical refinements η_1, η_2 have a distance of at least $2^{-(n+1)}$ on the collection of the first n actions occuring in any run of s.
- A finitary semantical refinement, i.e. a semantical refinement which delivers another denotation than $\mathit{Dir}(a)$ for finitely many actions a only, and

which moreover delivers a convex combination of point measures over finite sequences, can be represented by a syntactical refinement sequence.

The discussion here is restricted to the general outline of the technique and to the particularities for the probabilistic setting of $\mathcal{L}_{pr}$. In [HVB99] more details can be found for a nonprobabilistic process language with action refinement.

We start with a definition for $act_n(s)$ which indicates the first n actions that may occur in a run of a statement s.

Definition 6.1 For $n \in \mathbb{N}$ and $s \in Stat$, the subset $act_n(s)$ of Act is inductively given by

$$\begin{aligned} act_0(s) &= \emptyset \\ act_{n+1}(a) &= \{a\} \\ act_{n+1}(x) &= act_{n+1}(s) \text{ where } D(x) = s \\ act_{n+1}(s_1; s_2) &= act_{n+1}(s_1) \cup act_n(s_2) \\ act_{n+1}(s_1 \oplus_\pi s_2) &= act_{n+1}(s_1) \cup act_{n+1}(s_2) \\ act_{n+1}(s_1\langle a \rightsquigarrow s_2\rangle) &= (act_{n+1}(s_1) \setminus \{a\}) \cup act_{n+1}(s_2). \end{aligned}$$

For $s \in Stat$ the set $act(s) \subseteq Act$ is given by $act(s) = \bigcup_n act_n(s)$.

The next lemma handles the first idea for the full abstractness theorem below.

Lemma 6.2 *Let $n \in \mathbb{N}$ and $s \in Stat$. If $d(\eta_1, \eta_2) \leq 2^{-n}$ on $act_n(s)$ then it holds that $d(\mathcal{D}(s)(\eta_1), \mathcal{D}(s)(\eta_2)) \leq 2^{-n}$, for all $\eta_1, \eta_2 \in SemRef$.*

Proof. *Induction on n and subinduction on $wgt(s)$. In order to illustrate a typical argument, we exhibit the subcase for $s_1 \oplus_\pi s_2$ in the case for $n + 1$: If $d(\eta_1, \eta_2) \leq 2^{-(n+1)}$ on $act_{n+1}(s_1 \oplus_\pi s_2)$, then, since $act_{n+1}(s_1 \oplus_\pi s_2) = act_{n+1}(s_1) \cup act_{n+1}(s_2)$, we have that $d(\eta_1, \eta_2) \leq 2^{-(n+1)}$ on $act_{n+1}(s_1, s_2)$. Thus, it follows that $d(\mathcal{D}(s_i)(\eta_1), \mathcal{D}(s_i)(\eta_2)) \leq 2^{-(n+1)}$ for $i = 1, 2$, by the induction hypothesis for s_1 and s_2. By compositionality of $\mathcal{D}$ and nonexpansiveness of $\oplus_\pi$, we obtain*

$$\begin{aligned} & d(\mathcal{D}(s_1 \oplus_\pi s_2)(\eta_1), \mathcal{D}(s_1 \oplus_\pi s_2)(\eta_2)) \\ \leq\ & \max\{\, d(\mathcal{D}(s_1)(\eta_1), \mathcal{D}(s_1)(\eta_2)), d(\mathcal{D}(s_2)(\eta_1), \mathcal{D}(s_2)(\eta_2)) \,\} \\ \leq\ & 2^{-(n+1)}. \end{aligned}$$

□

The following lemma is preparatory to the second idea for Theorem 6.8 as reflected by Lemma 6.6. In the proof of Lemma 6.3 we exploit the so-called '$\varepsilon \leq \frac{1}{2}\varepsilon$'-principle. In a metric space two elements coincide iff their distance equals 0. So for a collection of pairs of elements we have equality of their components iff the supremum of their distances is 0. Calling that supremum ε it therefore suffices to show that $\varepsilon \leq \frac{1}{2}\varepsilon$ for which 0 is the only nonnegative real that makes the inequality hold.

Lemma 6.3 *It holds that* $\mathcal{D}(s)(\eta_1) = \mathcal{D}(s)(\eta_2)$, *for* $s \in Stat$ *and* $\eta_1, \eta_2 \in SemRef$ *such that* $\eta_1 = \eta_2$ *on* $\mathsf{act}(s)$.

Proof. *Define* $\varepsilon = \sup\{ d(\mathcal{D}(s)(\eta_1), \mathcal{D}(s)(\eta_2)) \mid \eta_1 = \eta_2 \text{ on } \mathsf{act}(s) \}$. *One shows by induction on* $\mathsf{wgt}(s)$ *that* $d(\mathcal{D}(s)(\eta_1), \mathcal{D}(s)(\eta_2)) \leq \frac{1}{2}\varepsilon$. *From this it follows that* $\varepsilon = 0$. *Hence* $d(\mathcal{D}(s)(\eta_1), \mathcal{D}(s)(\eta_2)) = 0$ *and* $\mathcal{D}(s)(\eta_1) = \mathcal{D}(s)(\eta_2)$ *for* s, η_1, η_2 *such that* $\eta_1 = \eta_2$ *on* $\mathsf{act}(s)$. *By way of example we provide the case for* $s_1; s_2$*:*

$$
\begin{aligned}
& d(\mathcal{D}(s_1; s_2)(\eta_1), \mathcal{D}(s_1; s_2)(\eta_2)) \\
\leq\ & [\text{‘;’ nonexpansive/contractive}] \\
& \quad \max\{ d(\mathcal{D}(s_1)(\eta_1), \mathcal{D}(s_1)(\eta_2)), \tfrac{1}{2} d(\mathcal{D}(s_2)(\eta_1), \mathcal{D}(s_2)(\eta_2)) \} \\
=\ & [\text{induction hypothesis for } s_1,\ \mathsf{act}(s_2) \subseteq \mathsf{act}(s_1; s_2),\ \text{definition } \varepsilon]\ \tfrac{1}{2}\varepsilon. \qquad \square
\end{aligned}
$$

The next lemma involves a technicality having to do with iterated refinement versus simultaneous substitution.

Lemma 6.4

(a) *Suppose* $a_1, \ldots, a_n \in Act$ *are pairwise distinct, and* $s_1, \ldots, s_n \in Stat$ *are such that* $\mathsf{act}(s_i) \cap \{ a_1, \ldots, a_n \} = \emptyset$ *for* $1 \leq i \leq n$. *Then it holds that*

$$\mathcal{D}(s\langle a_i \rightsquigarrow s_i \rangle_{i=1}^n)(\eta) = \mathcal{D}(s)(\eta[p_i/a_i]_{i=1}^n)$$

where $p_i = \mathcal{D}(s_i)(\eta)$ *for* $1 \leq i \leq n$.

(b) *Suppose* $\bar{a}_i, a'_j$ $(1 \leq i, j \leq n)$ *are pairwise distinct. Then it holds that*

$$\mathcal{D}(s\langle \bar{a}_i \rightsquigarrow a'_i \rangle_{i=1}^n)(\eta) = \mathcal{D}(s)(\eta[\eta(a'_i)/\bar{a}_i]_{i=1}^n).$$

Proof. *Part (a) goes by induction on* n *using Lemma 6.3. Part (b) follows from part (a).* $\square$

We have now arrived at the second idea on our way to the full abstractness of $\mathcal{D}$. First we need a definition.

Definition 6.5 A semantical refinement $\eta \in SemRef$ is called *finitary* if the following conditions are fulfilled:

- for all $a \in Act$ it holds that $\eta(a)$ is a finitary probability distribution over Act^+,
- $\eta(a) \neq \{a\}$ for finitely many $a \in Act$.

The crux underlying he proof of Lemma 6.6 is that any convex combination of Dirac-measures of finite words can be syntactically represented. For example, the distribution $\frac{1}{2} * Dir(a) \oplus \frac{1}{3} * Dir(bc) \oplus \frac{1}{6} * Dir(ade)$ can be represented by the statement $a \oplus_{1/2} ((b; c) \oplus_{2/3} (a; d; e))$, in the sense that $\mathcal{D}(a \oplus_{1/2} ((b; c) \oplus_{2/3} (a; d; e)))(\eta_{id}) = \frac{1}{2} * Dir(a) \oplus \frac{1}{3} * Dir(bc) \oplus \frac{1}{6} * Dir(ade)$.

Lemma 6.6 *Let* $\eta \in SemRef$ *be a finitary semantical refinement and* $A \subseteq Act$ *a finite set of actions. Then there exists, for all* $n \in \mathbb{N}$, *a refinement sequence*

$\langle a_i \rightsquigarrow s_i \rangle_{i=1}^k$ *such that*

$$d(\mathcal{D}(s)(\eta), \mathcal{D}(s\langle a_i \rightsquigarrow s_i \rangle_{i=1}^k)(\eta_{id})) \leq 2^{-n},$$

for all $s \in \mathit{Stat}$ *with* $\mathrm{act}_n(s) \subseteq A$.

Proof. *If* p *is a finitary probability distribution over* Act^+, *say* $p = \bigoplus_{i=1}^m \rho_i * q_i$ *for* $m \geq 1$, $\rho_1, \ldots, \rho_m > 0$ *such that* $\rho_1 + \cdots + \rho_m = 1$, $q_1, \ldots, q_m \in \mathrm{Act}^+$, *the statement* $\mathit{stat}(p)$ *is given by* $\mathit{stat}(p) = \bigoplus_{i=1}^m \rho_i * \mathit{stat}'(q_i)$ *where* $\mathit{stat}'(a) = a$, $\mathit{stat}'(a \cdot q) = a; \mathit{stat}'(q)$. *(Note that* $\mathcal{L}_{pr}$ *provides binary probabilistic composition only. Further details on transforming arbitrary finite probabilistic composition into repeated binary probabilistic is omitted here.) It is straightforwardly checked that* $\mathcal{D}(\mathit{stat}(p))(\eta_{id}) = p$ *by simultaneous induction on* m *and the lengths of the* q_i*'s.*

Suppose $\bar{a}_1, \ldots, \bar{a}_\ell$ *are all actions* a *such that* $\eta(s) \neq a$. *We are done if we show*

$$d(\mathcal{D}(s)(\eta), \mathcal{D}(s\langle \bar{a}_i \rightsquigarrow \mathit{stat}(\eta(\bar{a}_i)) \rangle_{i=1}^\ell)(\eta_{id})) \leq 2^{-n}.$$

(Some caution has to be taken though, in order to prevent clashes of actions. See [HVB99].) As η *is finitary, only finitely many actions are involved. The lemma then follows using Lemma 6.2 and Lemma 6.4.* $\square$

We have now arrived at the main technical result of this section.

Lemma 6.7 *If* $s', s'' \in \mathit{Stat}$ *satisfy* $\mathcal{D}(s') \neq \mathcal{D}(s'')$ *then* $\mathcal{O}[\![C[s']]\!] \neq \mathcal{O}[\![C[s'']]\!]$ *for some context* $C[\cdot]$.

Proof. *Suppose* $\mathcal{D}(s') \neq \mathcal{D}(s'')$. *We can choose* $\eta \in \mathit{SemRef}$ *and* $n \in \mathbb{N}$ *such that* $d(\mathcal{D}(s')(\eta), \mathcal{D}(s'')(\eta)) = 2^{-n}$. *Let* η' *be finitary such that* $d(\eta, \eta') \leq 2^{-(n+1)}$ *on* $\mathrm{act}_n(s') \cup \mathrm{act}_n(s'')$. *By Lemma 6.2 and ultrametricity we then obtain*

$$d(\mathcal{D}(s')(\eta'), \mathcal{D}(s'')(\eta') = 2^{-n}.$$

Pick, applying Lemma 6.6 and again ultrametricity, a refinement sequence $\langle a_i \rightsquigarrow s_i \rangle_{i=1}^k$ *such that*

$$d(\mathcal{D}(s'\langle a_i \rightsquigarrow s_i \rangle_{i=1}^k)(\eta_{id}), \mathcal{D}(s''\langle a_i \rightsquigarrow s_i \rangle_{i=1}^k)(\eta_{id})) = 2^{-n},$$

hence $\mathcal{D}[\![s'\langle a_i \rightsquigarrow s_i \rangle_{i=1}^k]\!] \neq \mathcal{D}[\![s''\langle a_i \rightsquigarrow s_i \rangle_{i=1}^k]\!]$. *Define the context* $C[\cdot] = (\cdot)\langle a_i \rightsquigarrow s_i \rangle_{i=1}^k$. *Then, by Theorem 5.3, it follows that* $\mathcal{O}[\![C[s']]\!] \neq \mathcal{O}[\![C[s'']]\!]$. $\square$

The correctness result of Section 5 and Lemma 6.7 have paved the way for a proof of the full abstractness of the semantical mapping $\mathcal{D}$ with respect to the operational semantics $\mathcal{O}[\![\cdot]\!]$ of $\mathcal{L}_{pr}$.

Theorem 6.8 $\mathcal{D}\colon \mathcal{L}_{\mathit{ref}} \to \mathit{SemRef} \to \mathbb{P}$ *is fully abstract with respect to* $\mathcal{O}[\![\cdot]\!]$.

Proof. *Suppose* $\mathcal{D}(s_1) \neq \mathcal{D}(s_2)$ *for two statements* $s_1, s_2 \in \mathit{Stat}$. *Then by Lemma 6.7 there exists a context* $C[\cdot]$ *such that* $\mathcal{O}[\![C[s_1]]\!] \neq \mathcal{O}[\![C[s_2]]\!]$*: Suppose* $\mathcal{D}(s_1) = \mathcal{D}(s_2)$ *for two statements* $s_1, s_2 \in \mathit{Stat}$. *By definition of* $\mathcal{D}$ *we have, for any context* $C[\cdot]$ *and semantical refinement* η, *that* $\mathcal{D}(C[s_1])(\eta) =$

$\mathcal{D}(C[s_2])(\eta)$. In particular $\mathcal{D}[\![C[s_1]]\!] = \mathcal{D}[\![C[s_2]]\!]$, hence $\mathcal{O}[\![C[s_1]]\!] = \mathcal{O}[\![C[s_2]]\!]$ by Theorem 5.3. We conclude that, for any $s_1, s_2 \in Stat$,

$$\mathcal{D}(s_1) = \mathcal{D}(s_2) \iff \mathcal{O}[\![C[s_1]]\!] = \mathcal{O}[\![C[s_2]]\!] \text{ for any context } C[\cdot],$$

i.e., $\mathcal{D}\colon Stat \to SemRef \to \mathbb{P}$ is fully abstract with respect to $\mathcal{O}[\![\cdot]\!]$. □

7 Concluding remarks

For the abstract process language $\mathcal{L}_{pr}$ with probabilistic choice and action refinement we have developed an operational semantics $\mathcal{O}$ using syntactic refinement sequences and a denotational semantics $\mathcal{D}$ using semantical refinements. The denotational semantics is shown to be fully i abstract with respect to the operational model; the denotational semantics identifies exactly those statements that have the same operational meaning in all contexts.

The case-study for $\mathcal{L}_{pr}$ shows that the general techniques for metric operational and denotational semantics remain in place in the setting of probabilistic programming. In fact, the domain of probability measures of compact support is a suitable complete ultrametric space for the modeling of discrete probabilistic choice, also in the presence of a specific construct such as action refinement. In particular, the method for proving completeness of the denotational semantics of [HVB99] —based on the distance of two statements that have different meanings in the denotational model— carries over to the setting of the probabilistic domain.

References

[Ace90] L. Aceto. *Action Refinement in Process Algebras.* PhD thesis, University of Sussex, 1990.

[AH93] L. Aceto and M. Hennessy. Towards action-refinement in process algebras. *Information and Computation*, 103:204–269, 1993.

[BK97] C. Baier and M.Z. Kwiatkowska. Domain equations for probabilistic processes (extended abstract). In C. Palamidessi and J. Parrow, editors, *Proc. Express'97.* ENTCS 7, 1997.

[BV94] J.W. de Bakker and E.P. de Vink. Bisimulation semantics for concurrency with atomicity and action refinement. *Fundamenta Informaticae*, 20:3–34, 1994.

[BV96] J.W. de Bakker and E.P. de Vink. *Control Flow Semantics.* The MIT Press, 1996.

[BW01] Franck van Breugel and James Worrell. Towards quantitative verification of probabilistic transition systems. In Fernando Orejas, Paul G. Spirkis, and Jan van Leeuwen, editors, *Proc. ICALP'01*, pages 421–432. LNCS 2076, 2001.

[Chr90] I. Christoff. Testing equivalences and fully abstract models for probabilistic processes. In J.C.M Baeten and J.W. Klop, editors, *Proc. CONCUR'90*, pages 126–140. LNCS 458, 1990.

[CS95] J.P. Courtiat and D.E. Saidouni. Relating maximality-based semantics to action refinement in process algebras. In D. Hogrefe and S. Leue, editors, *Formal Description Techniques VII*, pages 292–308. Chapman & Hall, 1995.

[DD89] Ph. Darondeau and P. Degano. Causal trees. In G. Ausiello, M. Dezani-Ciancaglini, and S. Ronchi Della Rocca, editors, *Proc. ICALP'89*, pages 234–248. LNCS 372, 1989.

[DD93] P. Darondeau and P. Degano. Refinement of actions in event structures and causal trees. *Theoretical Computer Science*, 118:21–48, 1993.

[DG95] P. Degano and R. Gorrieri. A causal operational semantics of action refinement. *Information and Computation*, 122:97–119, 1995.

[DGJP99] J. Derarnais, V. Gupta, R. Jagadiasan, and P. Panagaden. Metrics for labelled transition systems. In J.C.M Baeten and S. Mauw, editors, *Proc. CONCUR'99*, pages 258–273. LNCS 1664, 1999.

[Dug76] J. Dugundji. *Topology.* Allyn and Bacon, 1976.

[Eng89] R. Engelking. *General Topology.* Sigma Series in Pure Mathematics 6, Heldermann Verlag, revised and completed edition, 1989.

[GGR96] U. Goltz, R. Gorrieri, and A. Rensink. Comparing syntactic and semantic action refinement. *Information and Computation*, 125:118–143, 1996.

[Gor91] R. Gorrieri. *Refinement, Atomicity and Transactions for Process Description Languages.* PhD thesis, University of Pisa, 1991. Also available as Technical Report TD–2/91, Dipartimento di Informatica, Università degli Studi di Pisa.

[GRN98] C. Gregorio-Rodríguez and M. Nuñez. Denotational semantics for probabilistic refusal testing. In M. Huth and M.Z. Kwiatkowska, editors, *Proc. ProbMIV'98*. ENTCS 22, 1998.

[GSS95] R.J. van Glabbeek, S.A Smolka, and B. Steffen. Reactive, generative and stratified models of probabilistic processes. *Information and Computation*, 121:59–80, 1995. Preliminary version (co-authored by C.M.N. Tofts) appeared in Proc. LICS'90, Philadelphia.

[Hal74] P.R. Halmos. *Measure Theory*, volume 18 of *Graduate Texts in Mathematics.* Springer, reprint edition, 1974.

[Har98] J.I. den Hartog. Comparative semantics for a process language with probabilistic choice and non-determinism. Technical Report IR–445, Vrije Universiteit, Amsterdam, February 1998.

[HV99a] J.I. den Hartog and E.P. de Vink. Mixing up nondeterminism and probability: A preliminary report. *ENTCS*, 22, 1999.

[HV99b] J.I. den Hartog and E.P. de Vink. Taking chances on $\|$ and *fail*: Extending strong and probabilistic bisimulation. Technical Report IR–454, Vrije Universiteit, Amsterdam, 1999.

[HVB99] J.I. den Hartog, E.P. de Vink, and J.W. de Bakker. Full abstractness of a metric semantics for action refinement. *Fundamenta Informaticae*, 40:335–382, 1999.

[KN96] M.Z. Kwiatkowska and G.J. Norman. Probabilistic metric semantics for a simple language with recursion. In *Proc. MFCS'96*, pages 419–430. LNCS 1113, 1996.

[KN98] M.Z. Kwiatkowska and G.J. Norman. A fully abstract metric-space denotational semantics for reactive probabilistic processes. In *Proc. Express'98*. ENTCS 13, 1998.

[LS91] K.G. Larsen and A. Skou. Bismulation through probabilistic testing. *Information and Computation*, 94:1–28, 1991.

[Mis00] M. Mislove. Nondeterminism and probabilistic choice: Obeying the laws. In *Proc. CONCUR'00*, pages 350–364. LNCS 1877, 2000.

[NEL88] M Nielsen, U. Engberg, and K.S. Larsen. Fully abstract models for a process language with refinement. In J.W. de Bakker, W.P. de Roever, and G. Rozenberg, editors, *Proc. REX School/Workshop on Linear Time, Branching Time and Partial Order in Logics and Models for Concurrency*, pages 523–548. LNCS 354, 1988.

[NFL95] M. Nunez, D. de Frutos, and L. Llana. Acceptance trees for probabilistic processes. In I. Lee and S.A. Smolka, editors, *Proc. CONCUR'95*, pages 249–263. LNCS 962, 1995.

[Ren93] A. Rensink. *Models and Methods for Action Refinement.* PhD thesis, University of Twente, 1993.

[RT94] J.J.M.M. Rutten and D. Turi. Initial algebra and final coalgebra semantics for concurrency. In J.W. de Bakker, W.-P. de Roever, and G. Rozenberg, editors, *Proc. REX School/Symposium "A Decade of Concurrency"*, pages 530–582. LNCS 803, 1994.

[Rud66] W. Rudin. *Real and Complex Analysis.* McGraw-Hill, 1966.

[Sei95] K. Seidel. Probabilistic communicating processes. *Theoretical Computer Science*, 152:219–249, 1995.

[Sto77] J.E. Stoy. *Denotational Semantics—the Scott-Strachey approach to programming language theory.* MIT Press, 1977.

[Vog91] W. Vogler. Failures semantics based on interval semiwords is a congruence for refinement. *Distributed Computing*, 4:139–162, 1991.

[Vog92] W. Vogler. *Modular Construction and Partial Order Semantics of Petri Nets.* LNCS 625, 1992.

[VR99] E.P. de Vink and J.J.M.M. Rutten. Bisimulation for probabilistic transition systems: a coalgebraic approach. *Theoretical Computer Science*, 221:271–293, 1999.