Realization of Probabilistic Automata: Categorical Approach

Paulo Mateus, Amílcar Sernadas, Cristina Sernadas

CMA - Departamento de Matemática
Instituto Superior Técnico, Lisbon, Portugal

Abstract. We present a categorical framework to study probabilistic automata starting by obtaining aggregation and interconnection as universal constructions. We also introduce the notion of probabilistic behavior in order to get adjunctions between probabilistic behavior and probabilistic automata. Thus we are able to extend to the probabilistic setting free and minimal realizations as universal constructions.

1 Introduction

Probabilistic automata [Rab63,Paz66] are central in the theory of unreliable systems, namely for providing the appropriate semantic domain (see for instance [BDEP97,LS91,vGSST95]). In particular we adopt the Moore model, that is, the outputs are assigned to the states.

In [MSS99,SM99] we provided a (pre)categorical characterization for several combinations of probabilistic automata. However, we had to work with structures weaker than categories [Ehr65,Cop80] because composition of morphisms was not always defined. Herein we adopt a different approach by considering that the random source (probability space) is fixed, avoiding the notion of morphism between probability spaces. Of course this option is more restrictive but it allow us to stay in the categorical setting. Incidentally it is also the perspective usually adopted in probability theory.

We start by characterizing aggregation and interconnection (by input calling) as universal constructions, that is, free aggregation corresponds to product and interconnection to Cartesian lifting in the same style as presented in [WN95].

We also introduce the notion of probabilistic behavior allowing us to establish adjunctions between automata and behavior. In this way, we are able to extend to the probabilistic setting the classical result about the universality of minimal and free realizations [Gog73,AT89].

In section 2 of the paper we present the category of (Moore) probabilistic automata. We go on in section 3 showing that finite products and Cartesian liftings exist. We also analyze the probabilistic meaning of aggregating independent automata. Section 4 is dedicated to showing that free realization is universal. For this purpose we introduce the concepts of accessible state and probabilistic behavior. Then we show that there is an adjunction between the categories of probabilistic behavior and probabilistic automata. In section 5 we prove that minimal realization is also universal.

We assume that the reader is familiar with basic aspects of category theory namely Cartesian liftings (see [BW90]) and fibred adjunctions (see [Bén85]).

2 Probabilistic automata

We start by recalling a few notions of basic measure and probability theory (for further details see for instance [Hal69]). A *probability space* is a triple $\langle \Omega, \mathcal{F}, P \rangle$ where Ω is a non-empty set (of outcomes); $\mathcal{F}$ is a σ-algebra (each element is an event) over Ω and P is a measure (a probability) over $\langle \Omega, \mathcal{F} \rangle$ such that $P(\Omega) = 1$.

In the sequel we need to use the n-th product probability space of a probability space $\mathcal{P} = \langle \Omega, \mathcal{F}, P \rangle$ for each $n \in \mathbb{N}$ defined as follows: $\mathcal{P}^n = \langle \Omega^n, \mathcal{F}^n, P^n \rangle$ where $\mathcal{F}^n$ is the smallest σ-algebra containing $\prod_{i=1}^n \mathcal{F}$ and P^n is the extension of $P^* : \prod_{i=1}^n \mathcal{F} \to [0,1]$ such that $P^*(\mathcal{F}_1 \ldots \mathcal{F}_n) = \prod_{i=1}^n P(\mathcal{F}_i)$ (see [Hal69] for details). Observe that $\mathcal{P}^0 = \langle \{*\}, 2^{\{*\}}, P^0 \rangle$ where P^0 is uniquely defined.

Whenever Ω is a countable set we usually take $\mathcal{F}$ to be 2^Ω. Then, it is enough to work with the notion of *probability presentation* as a pair $\langle \Omega, p \rangle$ where Ω is non-empty countable set of outcomes and $p : \Omega \to [0,1]$ is a map such that $\sum_{\omega \in \Omega} p(\omega) = 1$. This map can be extended to a probability $P : 2^\Omega \to [0,1]$ where $P(B) = \sum_{\omega \in B} p(\omega)$. Once again we need the n-product of a probability presentation $\mathcal{P} = \langle \Omega, p \rangle$ for each $n \in \mathbb{N}$ defined as follows: $\mathcal{P}^n = \langle \Omega^n, p^n \rangle$ where $p^n(\omega_1 \ldots \omega_n) = \prod_{i=1}^n p(\omega_i)$. The n-product can be extended to a probability space $\mathcal{P}^n = \langle \Omega^n, 2^{\Omega^n}, P^n \rangle$ where P^n is the extension of p^n.

A *random quantity* over a probability presentation $\langle \Omega, p \rangle$ and a set Q is a map $f : \Omega \to Q$. In the particular case of Q being $\mathbb{R}$, the random quantity is a random variable. Two random quantities f_1, f_2 over $\mathcal{P}$ and Q are *independent* iff $P(f_1^{-1}(q_1) \cap f_2^{-1}(q_2)) = P(f_1^{-1}(q_1)) \times P(f_2^{-1}(q_2))$ for all $q_1, q_2 \in Q$.

A (Moore) probabilistic automaton is, roughly speaking, a device with an internal state that receiving an input (from a specified set I, the input alphabet) changes probabilistically its state to another and emits an output signal (from a specified set O, the output alphabet).

Definition 2.1. A *(Moore) probabilistic automaton* over a probabilistic presentation $\mathcal{P} = \langle \Omega, p \rangle$ is a tuple $m = \langle I, O, S, \delta, \Lambda \rangle$ where:

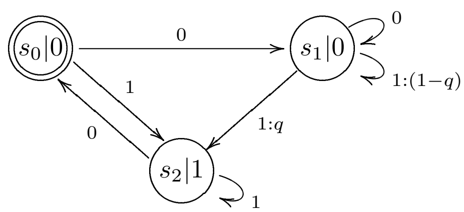
- I is a finite pointed set with a distinguished element $\perp$;
- O is a finite set;
- S is a countable pointed set with a distinguished element s_0;
- $\delta = \{\delta_s^i\}_{i \in I, s \in S}$ where each δ_s^i is a random quantity over $\mathcal{P}$ and S;
- $\Lambda : S \to O$ is a map;

such that $\delta_s^\perp = \lambda \omega \in \Omega.\ s$ for all $s \in S$. ∎

The set I is the *input alphabet* and $\perp$ is the *idle input* that we will need later on when dealing with interconnection. An input different from $\perp$ is called a *proper input*. The set O is the *output alphabet*. The elements of S are called *states* and s_0 is the *initial state*. The random quantity δ_s^i is the *random transition map* from state s on input i. The map Λ is the *output map*.

For instance, the probability $p_{s_1}^i(s_2)$ of reaching a state s_2 from s_1 on input i is $P(\{\omega \in \Omega : \delta_{s_1}^i(\omega) = s_2\})$. Observe that $\sum_{s_2 \in S} p_{s_1}^i(s_2) = 1$ for all $s_1 \in S$ and $i \in I$.

Example 2.2. Consider an unreliable binary discrete channel (with memory) that sends bits without any error except if it has just sent 00. In this case if a 0 is received it will be successfully transmitted. However if a 1 is received, it will be transmitted successfully with probability q. The probability space that we have to fix has two outcomes, one representing success ω_1 (1 is received after 00 and transmitted successfully) and ω_2 represents the other case. Therefore $\mathcal{P} = \langle\{\omega_1, \omega_2\}, p\rangle$ with $p(\omega_1) = q$. The set of states is $S = \{s_0, s_1, s_2\}$.



The random transition maps are as follows:

- $\delta_{s_0}^0 = \lambda\omega.s_1$;
- $\delta_{s_0}^1 = \lambda\omega.s_2$;
- $\delta_{s_1}^0 = \lambda\omega.s_1$;
- $\delta_{s_1}^1(\omega_1) = s_2$ and $\delta_{s_1}^1(\omega_2) = s_1$;
- $\delta_{s_2}^0 = \lambda\omega.s_0$;
- $\delta_{s_2}^1 = \lambda\omega.s_2$.

That is, all quantities are deterministic with the exception of $\delta_{s_1}^1$, which is a Bernoulli random quantity with success probability q.

In the sequel it is useful to consider the full subcategories of $\mathbf{Set}_*$, $\mathbf{cSet}_*$ and $\mathbf{fSet}_*$ spanned, respectively, by all countable and by all finite sets.

Definition 2.3. Let m and m' be probabilistic automata over the same $\mathcal{P} = \langle\Omega, p\rangle$. A *probabilistic automaton morphism* $f : m \to m'$ is a tuple

$$f = \langle \overline{f}, \overline{\overline{f}}, \underline{f} \rangle$$

where:

- $\overline{f} : I \to I'$ is a morphism in $\mathbf{fSet}_*$;
- $\overline{\overline{f}} : O \to O'$ is a map;
- $\underline{f} : S \to S'$ is a morphism in $\mathbf{cSet}_*$

such that for all $i \in I$, $s \in S$ and $\omega \in \Omega$:

- ${\delta'}^{\overline{f}(i)}_{\underline{f}(s)}(\omega) = \underline{f}(\delta^i_s(\omega))$;
- $\Lambda'(\underline{f}(s)) = \overline{\overline{f}}(\Lambda(s))$. ∎

The notion of probabilistic automaton morphism implies the following relationship between probabilities

$$P(\{\omega \in \Omega \ : \ {\delta'}^{\overline{f}(i)}_{\underline{f}(s)}(\omega) = s'\}) = \sum_{r \in \underline{f}^{-1}(s')} P(\{\omega \in \Omega \ : \ \delta^i_s(\omega) = r\}).$$

Prop/Definition 2.4. Probabilistic automata over $\mathcal{P}$ and their morphisms constitute the category $\mathbf{PAut}_{\mathcal{P}}$. ∎

3 Aggregation and interconnection

We now turn our attention to the basic mechanisms for combining probabilistic automata, that is, free aggregation and interconnection of inputs.

Proposition 3.1. The category $\mathbf{PAut}_{\mathcal{P}}$ is finitely Cartesian.

Proof.
(i) Terminal object:
Consider the automaton with a singleton input alphabet, a singleton output alphabet and a singleton state space. Note that δ and Λ are uniquely defined.

(ii) Binary products:
A product of m_1 and m_2 is $m_1 \times m_2 = \langle I_1 \times I_2, O_1 \times O_2, S_1 \times S_2, \delta, \Lambda_1 \times \Lambda_2\rangle$ endowed with the obvious projections $\pi_k : m \to m_k$ with $k \in \{1, 2\}$ and where

$$\delta^{i_1 i_2}_{s_1 s_2} = \langle {\delta_1}^{i_1}_{s_1}, {\delta_2}^{i_2}_{s_2}\rangle : \Omega \to S_1 \times S_2.$$

It is straightforward to check that each π_k is a morphism.

Universal property:
Let $f_k : m' \to m_k$ be a morphism for $k \in \{1, 2\}$, then the morphism $f : m' \to m_1 \times m_2$ where:

- $\overline{f} = \langle \overline{f_1}, \overline{f_2}\rangle : I' \to I_1 \times I_2$;
- $\overline{\overline{f}} = \langle \overline{\overline{f_1}}, \overline{\overline{f_2}}\rangle : O' \to O_1 \times O_2$;
- $\underline{f} = \langle \underline{f_1}, \underline{f_2}\rangle : S' \to S_1 \times S_2$;

Clearly f is the only morphism such that $\pi_k \circ f = f_k$ with $k \in \{1, 2\}$; therefore we only show that f is a morphism, indeed :

- $\delta^{\overline{f}(i')}_{\underline{f}(s')}(\omega) = \delta^{\langle \overline{f}_1(i'), \overline{f}_2(i')\rangle}_{\langle \underline{f}_1(i'), \underline{f}_2(i')\rangle}(\omega) = \langle {\delta_1}^{\overline{f}_1(i')}_{\underline{f}_1(s')}(\omega), {\delta_2}^{\overline{f}_2(i')}_{\underline{f}_2(s')}(\omega)\rangle =$
  $\langle \underline{f}_1({\delta'}^{i'}_{s'}(\omega)), \underline{f}_2({\delta'}^{i'}_{s'}(\omega))\rangle = \underline{f}({\delta'}^{i'}_{s'}(\omega))$;

– $\Lambda(\underline{f}(s')) = \Lambda(\langle \underline{f}_1(s'), \underline{f}_2(s')\rangle) = \langle \Lambda_1(\underline{f}_1(s')), \Lambda_2(\underline{f}_2(s'))\rangle = \langle \overline{\overline{f}}_1(\Lambda'(s')), \overline{\overline{f}}_2(\Lambda'(s'))\rangle = \overline{\overline{f}}(\Lambda'(s')))$. □

Observe that:

$$P(\{\omega \in \Omega \ : \ \delta_k{}^{i_k}_{s_k}(\omega) = s'_k\}) = \sum_{s \in \underline{\pi}_k^{-1}(s'_k)} P(\{\omega \in \Omega \ : \ \delta^i_s(\omega) = r\})$$

for all $\overline{\pi}(i) = i_k$, $\underline{\pi}(s) = s_k$ and $k \in \{1, 2\}$.

Definition 3.2. Let m_1 and m_2 be probabilistic automata. The *free aggregation* of m_1 with m_2 is the automaton $m_1||m_2 = m_1 \times m_2$, i. e., the vertex of the product of m_1 and m_2. ■

Note that, since our automata share the same probability presentation it maybe the case that two different automata have dependent random transition maps, meaning that they are not totally independent from a probabilistic point of view. The result bellow provides a necessary and sufficient condition for achieving probabilistic independence.

Proposition 3.3. Let m_1 and m_2 be probabilistic automata over $\mathcal{P}$. Then $p^{i_1 i_2}_{s_1 s_2}(s'_1 s'_2) = p_1{}^{i_1}_{s_1}(s'_1) \times p_2{}^{i_2}_{s_2}(s'_2)$ iff $\delta_1{}^{i_1}_{s_1}$ is independent from $\delta_2{}^{a_2}_{s_2}$ for all $s_1 \in S_1$, $s_2 \in S_2$, $i_1 \in I_1$ and $i_2 \in I_2$.

Proof. Straightforward by definition of independence. □

Example 3.4. Consider the following two independent probabilistic automata. Assume that $\langle\{\omega_1, \omega_2, \omega_2, \omega_4\}, p\rangle$ with $p(\omega_1) = q^2$ and $p(\omega_2) = p(\omega_3) = q(1 - q)$. For the sake of simplicity we only present the random transition map of the initial states:

	ω_1	ω_2	ω_3	ω_4
${\delta'}^{\perp'}_{s'_0}$	s'_0	s'_0	s'_0	s'_0
${\delta'}^{0'}_{s'_0}$	s'_0	s'_0	s'_1	s'_1
${\delta'}^{1'}_{s'_0}$	s'_1	s'_1	s'_0	s'_0

	ω_1	ω_2	ω_3	ω_4
${\delta''}^{\perp''}_{s''_0}$	s''_0	s''_0	s''_0	s''_0
${\delta''}^{0''}_{s''_0}$	s''_0	s''_1	s''_0	s''_1
${\delta''}^{1''}_{s''_0}$	s''_1	s''_0	s''_1	s''_0

if we aggregate these two automata we obtain an automaton with nine inputs. The random transition map for the state $s'_0 s''_0$ of the combined automaton is:

	ω_1	ω_2	ω_3	ω_4
$\delta^{\bot'\bot''}_{s'_0 s''_0}$	$s'_0 s''_0$	$s'_0 s''_0$	$s'_0 s''_0$	$s'_0 s''_0$
$\delta^{\bot'0''}_{s'_0 s''_0}$	$s'_0 s''_0$	$s'_0 s''_1$	$s'_0 s''_0$	$s'_0 s''_1$
$\delta^{\bot'1''}_{s'_0 s''_0}$	$s'_0 s''_1$	$s'_0 s''_0$	$s'_0 s''_1$	$s'_0 s''_0$
$\delta^{0'\bot''}_{s'_0 s''_0}$	$s'_0 s''_0$	$s'_0 s''_0$	$s'_1 s''_0$	$s'_1 s''_0$
$\delta^{0'0''}_{s'_0 s''_0}$	$s'_0 s''_0$	$s'_0 s''_1$	$s'_1 s''_0$	$s'_1 s''_1$
$\delta^{0'1''}_{s'_0 s''_0}$	$s'_0 s''_1$	$s'_0 s''_0$	$s'_1 s''_1$	$s'_1 s''_0$
$\delta^{1'\bot''}_{s'_0 s''_0}$	$s'_1 s''_0$	$s'_1 s''_0$	$s'_0 s''_0$	$s'_0 s''_0$
$\delta^{1'0''}_{s'_0 s''_0}$	$s'_1 s''_0$	$s'_1 s''_1$	$s'_0 s''_0$	$s'_0 s''_1$
$\delta^{1'1''}_{s'_0 s''_0}$	$s'_1 s''_1$	$s'_1 s''_0$	$s'_0 s''_1$	$s'_0 s''_0$

Interaction can be achieved by restricting the pairing of actions from each component. To this end we use the following universal construction over the obvious forgetful functor $\mathit{Inp} : \mathbf{PAut}_{\mathcal{P}} \to \mathbf{fSet}_*$ that maps each probabilistic automaton to its input space.

Proposition 3.5. The functor *Inp* is a fibration with splitting cleavage

$$k = \{k(\overline{f}, m')\}_{m' \in \mathbf{PAut}_{\mathcal{P}}, \overline{f} \in \hom(I, \mathit{Inp}(m'))}$$

where:

- $k(\overline{f}, m') = \langle \overline{f}, \mathrm{id}_{O'}, \mathrm{id}_{S'} \rangle : m \to m'$;
- $m = \langle I, O', S', \delta, \Lambda' \rangle$;
- $\delta^i_{s'} = \delta'^{\overline{f}(i)}_{s'}$.

Proof. It is easy to see that m is indeed an automaton and that $k(\overline{f}, m)$ is a morphism in $\mathbf{PAut}_{\mathcal{P}}$.

Universal property:

Let $h : m'' \to m' \in \mathbf{PAut}_{\mathcal{P}}$ and $\overline{g} : I'' \to I \in \mathbf{fSet}_*$ such that $\overline{f} \circ \overline{g} = \overline{h}$. Consider now $\overline{\overline{g}} = \overline{\overline{h}}$ and $\underline{g} = \underline{h}$ where $g : m'' \to m'$; clearly g is the only triple such that $f \circ g = h$ and therefore we only show that g is a morphism in $\mathbf{PAut}_{\mathcal{P}}$:

- $\delta^{\overline{g}(i'')}_{\underline{g}(s'')}(\omega) = \delta'^{\overline{f}(\overline{g}(i''))}_{\underline{g}(s'')}(\omega) = \delta'^{\overline{h}(i'')}_{\underline{h}(s'')}(\omega) = \underline{h}(\delta''^{i''}_{s''}(\omega)) = \underline{g}(\delta''^{i''}_{s''}(\omega))$;

- $\Lambda(\underline{g}(s'')) = \Lambda'(\underline{h}(s'')) = \overline{\overline{h}}(\Lambda''(s'')) = \overline{\overline{g}}(\Lambda''(s''))$.

Finally k is a splitting cleavage:

- $k(\mathrm{id}_I, m) = \mathrm{id}_m$;
- $k(\overline{f}, m'') \circ k(\overline{g}, m') = \langle \overline{f} \circ \overline{g}, \mathrm{id}_{O''}, \mathrm{id}_{S''} \rangle : m \to m''$ where $\delta^i_{s''} = \delta'^{\overline{g}(i)}_{s''} = \delta''^{\overline{f}(\overline{g}(i))}_{s''}$ and so $k(\overline{f}, m') \circ k(\overline{g}, m) = k(\overline{f} \circ \overline{g}, m'')$. ◻

Definition 3.6. Let m' and m'' be probabilistic automata, i' an input in I' and i'' an input in I''. Then, the *interconnection of* m' *and* m'' *by* i' *calling* i'' is

$$m'||_{i'>>i''}m'' = \mathrm{dom}(k(\overline{f}, m'||m''))$$

where $\overline{f} : ((I' \setminus \{i'\}) \times I'') \cup \{\langle i', i''\rangle\} \hookrightarrow I' \times I''$; ■

Example 3.7. Recall the automaton obtained in Example 3.4 and suppose that now we impose that $0'$ calls $0''$. To define $\delta||_{0'>>0''}$ for the initial state we just drop the random quantities $\delta^{0'\perp''}_{s'_0 s''_0}$ $\delta^{0'1''}_{s'_0 s''_0}$ of δ, that is:

	ω_1	ω_2	ω_3	ω_4
$\delta\|\|_{0'>>0''}{}^{\perp'\perp''}_{s'_0 s''_0}$	$s'_0 s''_0$	$s'_0 s''_0$	$s'_0 s''_0$	$s'_0 s''_0$
$\delta\|\|_{0'>>0''}{}^{\perp'0''}_{s'_0 s''_0}$	$s'_0 s''_0$	$s'_0 s''_1$	$s'_0 s''_0$	$s'_0 s''_1$
$\delta\|\|_{0'>>0''}{}^{\perp'1''}_{s'_0 s''_0}$	$s'_0 s''_1$	$s'_0 s''_0$	$s'_0 s''_1$	$s'_0 s''_0$
$\delta\|\|_{0'>>0''}{}^{0'0''}_{s'_0 s''_0}$	$s'_0 s''_0$	$s'_0 s''_1$	$s'_1 s''_0$	$s'_1 s''_1$
$\delta\|\|_{0'>>0''}{}^{1'\perp''}_{s'_0 s''_0}$	$s'_1 s''_0$	$s'_1 s''_0$	$s'_0 s''_0$	$s'_0 s''_0$
$\delta\|\|_{0'>>0''}{}^{1'0''}_{s'_0 s''_0}$	$s'_1 s''_0$	$s'_1 s''_1$	$s'_0 s''_0$	$s'_0 s''_1$
$\delta\|\|_{0'>>0''}{}^{1'1''}_{s'_0 s''_0}$	$s'_1 s''_1$	$s'_1 s''_0$	$s'_0 s''_1$	$s'_0 s''_0$

4 Unfolding

In this section we examine the notion of probabilistic behavior of an automaton. Furthermore, we study what is the relationship between the behavior of a combined automaton with the behavior of its components, capitalizing in the universal characterizations provided in the last section. As in classical sequential automaton, only accessible states are relevant for determining the behavior of an automaton.

Definition 4.1. The set of *accessible states* of an automaton m, A_m, is inductively defined in the following way: $s_0 \in A_m$; $s_2 \in A_m$ provided that $s_2 \in \mathrm{cod}(\delta^i_{s_1})$ for some $i \in I$ and $s_1 \in A_m$. An automaton m is *accessible* iff $A_m = S$. Finally, we call $\mathbf{aPAut}_{\mathcal{P}}$ the full subcategory of $\mathbf{PAut}_{\mathcal{P}}$ spanned by all accessible automata. ■

From the probabilistic point of views it seems more natural to say that the set of probabilistically accessible states is defined as follows: $s_0 \in pA_m$; $s_2 \in pA_m$ provided that $p^i_{s_1}(s_2) > 0$ for some $i \in I$ and $s_1 \in pA_m$. Of course $pA_m \subseteq A_m$. Whenever $p(\omega) > 0$ for all $\omega \in \Omega$ then the two notions coincide. Nothing is lost if we consider that the probability presentation we work with has this property.

Proposition 4.2. Morphisms in $\mathbf{PAut}_{\mathcal{P}}$ preserve accessibility, that is, if $f : m \to m'$ is a morphism and $s \in A_m$ then $\underline{f}(s) \in A_{m'}$.

Proof. By induction on the structure of A_m:
base: $\underline{f}(s_0) = s'_0 \in A_{m'}$;
induction step: $s_2 = \delta^i_{s_1}(\omega)$ with $s_1 \in A_m$ then, by definition of morphism,

$$\underline{f}(s_2) = \delta'^{\overline{f}(i)}_{\underline{f}(s_1)}(\omega).$$

By induction hypothesis, $\underline{f}(s_1) \in A_{m'}$ and therefore $\underline{f}(s_2) \in A_{m'}$. □

It is easy to see taking into account the probabilistic transfer properties of morphisms that morphisms also preserve probabilistic accessibility.

Corollary 4.3. $\mathbf{aPAut}_{\mathcal{P}}$ is a coreflexive subcategory of $\mathbf{PAut}_{\mathcal{P}}$.

Proof. Let m be a probabilistic automaton, consider the accessible automaton $m_A = \langle I, O, A_m, \delta|_{I \times A_m}, \Lambda|_{A_m} \rangle$ endowed with the morphism

$$\iota = \langle \mathrm{id}_I, \mathrm{id}_O, \underline{\iota} \rangle : m_A \to m,$$

where $\underline{\iota} : A_m \hookrightarrow S$. It is easy to see that m_A is a probabilistic automaton and that ι is a morphism.

Universal property:

Let m' be a accessible automaton and $h : m' \to m \in \mathbf{PAut}_{\mathcal{P}}$. Then by Proposition 4.2, $\mathrm{cod}(\underline{f}) \subseteq A_{m'}$, and therefore $f : m \to m'_A$ is a morphism. Furthermore $h : m' \to m_A$ is the only morphism such that $\iota \circ h = h$ by definition of ι. □

The above result asserts the existence a functor $Acc : \mathbf{PAut}_{\mathcal{P}} \to \mathbf{aPAut}_{\mathcal{P}}$ that is right adjoint to the inclusion functor from $\mathbf{aPAut}_{\mathcal{P}}$ to $\mathbf{PAut}_{\mathcal{P}}$. Roughly speaking, this functor maps each automaton to its "subautomaton" containing just the accessible states. Since Acc is right adjoint, its preserves limits and in particular products; hence $Acc(m'||m'') = Acc(m')||Acc(m'')$. With respect to the other construction a further result is relevant:

Proposition 4.4. The coreflection presented in Corollary 4.3 is fibred with respect to *Inp*.

Proof. Let m be an automaton, its coreflection $\iota : m \to m_A$ as defined in Corollary 4.3 is such that $Inp(\iota) = \mathrm{id}_I$ and furthermore, $Inp \circ Acc = Inp$. □

Hence *Acc* preserves Cartesian morphisms by *Inp*. Moreover $Inp : \mathbf{aPAut}_{\mathcal{P}} \to \mathbf{fSet}_*$ is a fibration. In what concerns runs, a Moore probabilistic automata over $\mathcal{P}$ with input alphabet I can be seen as a sequential automata, or even a F-automata [AT89], if we set the sequential input alphabet to be $I\Omega$ and forget the probabilities. This observation motivates the following definition of probabilistic behavior:

Definition 4.5. A *probabilistic behavior* over a probability presentation $\mathcal{P}$ is a tuple $B = \langle I, O, \beta \rangle$ where:

- I is a finite pointed set with a distinguished element $\perp$;
- O is a finite set;
- $\beta = \{\beta_x\}_{x \in I^*}$ where each β_x is a random quantity over $\mathcal{P}^{|x|}$ and O;

such that $\beta_{x_1 \perp x_2}(\boldsymbol{\omega_1} \omega \boldsymbol{\omega_2})) = \beta_{x_1 x_2}(\boldsymbol{\omega_1}\boldsymbol{\omega_2})$ for all $x_1, x_2 \in I^*$, $\omega \in \Omega$, $\boldsymbol{\omega_1} \in \Omega^{|x_1|}$ and $\boldsymbol{\omega_2} \in \Omega^{|x_2|}$. ∎

The sets I and O have the same meaning as before. The random quantity β_x, called *random behavior*, gives the output on sequence of inputs x. The probability of obtaining output o on sequence of inputs x is $P^{|x|}(\{\boldsymbol{\omega} \in \Omega^{|x|} \ : \ \beta_x(\boldsymbol{\omega}) = o\})$.

We introduce some useful notation. The elements of $(I\Omega)^*$ are called *runs*. The elements of $((I \setminus \{\perp\})\Omega)^*$ are called *proper runs* over $\mathcal{P}$ and I and we denote this set by $\mathrm{pRun}_{\mathcal{P},I}$. Given $i_1\omega_1 \dots i_n\omega_n \in (I\Omega)^*$ and $\overline{f} : I \to I'$, we denote $\overline{f}(i_1)\omega_1 \dots \overline{f}(i_n)\omega_n$ by $\overline{f}(i_1\omega_1 \dots i_n\omega_n)$.

Definition 4.6. A *probabilistic behavior morphism* is a pair

$$f = \langle \overline{f}, \overline{\overline{f}} \rangle : \langle I, O, \beta \rangle \to \langle I', O', \beta' \rangle$$

where:

- $\overline{f} : I \to I'$ is a morphism in $\mathbf{fSet}_*$;
- $\overline{\overline{f}} : O \to O'$ is a map;

such that $\overline{\overline{f}}(\beta_x) = \beta'_{\overline{f}(x)}$ for all $x \in I^*$ and $\boldsymbol{\omega} \in \Omega^{|x|}$. ∎

Prop/Definition 4.7. Probabilistic behaviors over $\mathcal{P}$ and their morphisms constitute the category $\mathbf{PBeh}_{\mathcal{P}}$. ∎

We call the obvious forgetful functor that maps each probabilistic behavior to its input alphabet by $bInp : \mathbf{PBeh}_{\mathcal{P}} \to \mathbf{fSet}_*$. We want to establish and adjunction between the category of probabilistic behaviors and the category of probabilistic automata. For this purpose is is important to note that the random transition map of an automaton m can be generalized to sequence of inputs. That is, let m be an automaton then $\delta^* = \{{\delta^*}^x_s\}_{x \in I^*, s \in S}$ where ${\delta^*}^x_s : \Omega^{|x|} \to S$ is inductively defined in the following way:

- ${\delta^*}^\epsilon_s = s$;
- ${\delta^*}^{xi}_s(\boldsymbol{\omega}\omega) = \delta^i_{{\delta^*}^x_s(\boldsymbol{\omega})}(\omega)$.

It is easy to see that a state s of an automaton m is accessible iff there exists a $x \in I^*$ and $\boldsymbol{\omega} \in \Omega^{|x|}$ such that ${\delta^*}^x_{s_0}(\boldsymbol{\omega}) = s$. Therefore, the preservation of accessibility by probabilistic automaton morphisms, Proposition 4.2, is a simple corollary of the following lemma:

Lemma 4.8. Let $f : m \to m'$ be a morphism in $\mathbf{PAut}_{\mathcal{P}}$, then for all $i \in I^*$ and $\boldsymbol{\omega} \in \Omega^{|x|}$:

$$\underline{f}({\delta^*}^x_s(\boldsymbol{\omega})) = {\delta'^*}^{\overline{f}(x)}_{\underline{f}(s)}(\boldsymbol{\omega}).$$

Proof. By induction on the size of σ:
base: $\underline{f}(\delta^{*\epsilon}_{s}) = \underline{f}(s) = \delta'^{*\epsilon}_{\underline{f}(s)}$;
induction step:
$\underline{f}(\delta^{*xi}_{s}(\boldsymbol{\omega}\omega)) = \underline{f}(\delta^{i}_{\delta^{*x}_{s}(\boldsymbol{\omega})}(\omega)) = \delta'^{\overline{f}(i)}_{\underline{f}(\delta^{*x}_{s}(\boldsymbol{\omega}))}(\omega) = \delta'^{\overline{f}(i)}_{\delta'^{*\overline{f}(x)}_{\underline{f}(s)}(\boldsymbol{\omega})}(\omega) = \delta'^{*\overline{f}(xi)}_{\underline{f}(s)}(\boldsymbol{\omega}\omega)$.

□

We now can establish the unfolding functor from probabilistic automata to probabilistic behaviors.

Prop/Definition 4.9. The functor *Unf* : $\mathbf{aPAut}_{\mathcal{P}} \to \mathbf{PBeh}_{\mathcal{P}}$ is defined as follows:

- $\mathit{Unf}(m) = \langle I, O, \{\Lambda \circ \delta^{*x}_{s_0}\}_{x \in I^*}\rangle$;
- $\mathit{Unf}(\langle \overline{f}, \overline{\overline{f}}, \underline{f}\rangle) = \langle \overline{f}, \overline{\overline{f}}\rangle$.

Proof.

- *Unf*(m) is a probabilistic behavior:
  It is easy to see by induction on the length of x_2 that:
$$\delta^{*x_1 \perp x_2}_{s}(\boldsymbol{\omega}_1 \omega \boldsymbol{\omega}_2) = \delta^{*x_1 x_2}_{s}(\boldsymbol{\omega}_1 \boldsymbol{\omega}_2)$$
  and therefore $\Lambda(\delta^{*x_1 \perp x_2}_{s}(\boldsymbol{\omega}_1 \omega \boldsymbol{\omega}_2)) = \Lambda(\delta^{*x_1 x_2}_{s}(\boldsymbol{\omega}_1 \boldsymbol{\omega}_2))$;
- *Unf*(f) is a probabilistic behavior morphism:
  $\overline{\overline{f}}(\Lambda(\delta^{*x}_{s_0}(\boldsymbol{\omega}))) = \Lambda'(\underline{f}(\delta^{*x}_{s_0}(\boldsymbol{\omega})))$ (by Lemma 4.8)
  $= \Lambda'(\delta'^{*\overline{f}(x)}_{\underline{f}(s_0)}(\boldsymbol{\omega})$.

□

Theorem 4.10. The functor *Unf* has a left adjoint. Furthermore the adjunction is fibred with respect to *Inp* and *bInp*.

Proof.
Left adjoint:
Let *Free* : $\mathbf{PBeh}_{\mathcal{P}} \to \mathbf{aPAut}_{\mathcal{P}}$ be such that:

- *Free*$(\langle I, O, \beta\rangle) = \langle I, O, \mathrm{pRun}_{\mathcal{P},I}, \delta, \Lambda\rangle$ where:
  - $\delta^{i}_{\sigma}(\omega) = \sigma i \omega$ for all $i \in I \setminus \{\perp\}$, $\omega \in \Omega$ and $\sigma \in \mathrm{pRun}_{\mathcal{P},I}$;
  - $\Lambda(i_1\omega_1 \ldots i_n\omega_n) = \beta_{i_1 \ldots i_n}(\omega_1 \ldots \omega_n)$.

  It is clear that *Free*$(\langle I, O, \beta\rangle)$ is an accessible automaton.
- *Free*$(\langle \overline{f}, \overline{\overline{f}}\rangle) = \langle \overline{f}, \overline{\overline{f}}, \overline{f}\rangle$. We proceed by checking that *Free*(f) is a probabilistic automata morphism:
  - $\overline{f}(\delta^{i}_{\sigma}(\omega)) = \overline{f}(\sigma i \omega) = \overline{f}(\sigma)\overline{f}(i)\omega = \delta'^{\overline{f}(i)}_{\overline{f}(\sigma)}(\omega)$ for all $i \in I \setminus \{\perp\}$;
  - $\underline{f}(\delta^{\perp}_{\sigma}(\omega)) = \underline{f}(\sigma) = \delta'^{\perp'}_{\underline{f}(\sigma)}(\omega) = \delta'^{\overline{f}(\perp)}_{\underline{f}(\sigma)}(\omega)$;
  - $\overline{\overline{f}}(\Lambda(i_1\omega_1 \ldots i_n\omega_n)) = \overline{\overline{f}}(\beta_{i_1 \ldots i_n}(\omega_1 \ldots \omega_n)) =$
    $\beta'_{\overline{f}(i_1 \ldots i_n)}(\omega_1 \ldots \omega_n) = \Lambda'(\overline{f}(i_1\omega_1 \ldots i_n\omega_n))$.

Counit:

Let δ' and Λ' be the random transition map and the output map of *Free*(*Unf*(m)) respectively. The counit of the adjunction is the family

$$\varepsilon_m = \langle \mathrm{id}_I, \mathrm{id}_O, \underline{\varepsilon}_m \rangle : \mathit{Free}(\mathit{Unf}(m)) \to m$$

where $\underline{\varepsilon}_m(i_1\omega_1 \ldots i_n\omega_n) = {\delta^*}^{i_1 \ldots i_n}_{s_0}(\omega_1 \ldots \omega_n)$ for every $m \in \mathbf{aPAut}_\mathcal{P}$. We verify that ε_m is a morphism in $\mathbf{aPAut}_\mathcal{P}$:

– $\delta^i_{\underline{\varepsilon}_m(i_1\omega_1 \ldots i_n\omega_n)}(\omega) = \delta^i_{{\delta^*}^{i_1 \ldots i_n}_{s_0}(\omega_1 \ldots \omega_n)}(\omega) = {\delta^*}^{i_1 \ldots i_n i}_{s_0}(\omega_1 \ldots \omega_n \omega) =$ $\underline{\varepsilon}_m(i_1\omega_1 \ldots i_n\omega_n i\omega) = \underline{\varepsilon}_m({\delta'}^i_{i_1\omega_1 \ldots i_n\omega_n}(\omega))$;
– $\Lambda(\underline{\varepsilon}_m(i_1\omega_1 \ldots i_n\omega_n i\omega)) = \Lambda({\delta^*}^{i_1 \ldots i_n}_{s_0}(\omega_1 \ldots \omega_n)) = \Lambda'(i_1\omega_1 \ldots i_n\omega_n)$.

Finally we check that ε is a natural transformation:

$$\underline{f}(\underline{\varepsilon}_{m_1}(i_1\omega_1 \ldots i_n\omega_n)) = \underline{f}({\delta_1^*}^{i_1 \ldots i_n}_{s_0}(\omega_1 \ldots \omega_n)) = {\delta_2^*}^{\overline{f}(i_1) \ldots \overline{f}(i_n)}_{\underline{f}(s_0)}(\omega_1 \ldots \omega_n) = \underline{\varepsilon}_{m_2}(\overline{f}(i_1\omega_1 \ldots i_n\omega_n)).$$

Universal Property:

Let $\langle \overline{f}, \overline{\overline{f}}, \underline{f} \rangle : \mathit{Free}(B) \to m_1$ be a morphism in $\mathbf{PAut}_\mathcal{P}$. The pair

$$\langle \overline{f}, \overline{\overline{f}} \rangle : B \to \mathit{Unf}(m_1)$$

is a morphism in $\mathbf{PBeh}_\mathcal{P}$:

$$\overline{\overline{f}}(\beta_{i_1 \ldots i_n}(\omega_1 \ldots \omega_n)) = \overline{\overline{f}}(\Lambda(i_1\omega_1 \ldots i_n\omega_n)) = \Lambda_1(\underline{f}(i_1\omega_1 \ldots i_n\omega_n)) = \Lambda_1(\underline{f}({\delta^*}^{i_1 \ldots i_n}_{s_0}(\omega_1 \ldots \omega_n))) = \Lambda_1({\delta_1^*}^{\overline{f}(i_1 \ldots i_n)}_{\underline{f}(s_0)}(\omega_1 \ldots \omega_n))).$$

Clearly $\varepsilon_{m'} \circ \mathit{Free}(\langle \overline{f}, \overline{\overline{f}} \rangle) = \langle \overline{f}, \overline{\overline{f}}, \underline{f} \rangle$:

$$\underline{\varepsilon}_{m_1}(\overline{f}(i_1\omega_1 \ldots i_n\omega_n)) = {\delta_1^*}^{\overline{f}(i_1 \ldots i_n)}_{s_{1\,0}}(\omega_1 \ldots \omega_n) = \underline{f}({\delta^*}^{i_1 \ldots i_n}_{\epsilon}(\omega_1 \ldots \omega_n)) = \underline{f}(i_1\omega_1 \ldots i_n\omega_n).$$

The uniqueness requirement is straightforward.

Fibred adjunction:

Clearly we have that *Inp*∘*Free* = *bInp* and *bInp*∘*Unf* = *Inp*; furthermore $\mathit{Inp}(\varepsilon_m) = \mathrm{id}_I$. □

A simple corollary of this theorem is that all constructs presented in Section 3 are preserved by *Unf*. Furthermore it is easy to show that *bInp* is a fibration.

5 Minimal realization

Now we show that there is a universal minimal realization for each probabilistic behavior. For this purpose, we fix an input alphabet, that is, we work with the fibers induced by *Inp* and *bInp*. Thus, let I be some finite pointed set we call $\mathbf{PAut}_{\mathcal{P},I}$ the fiber of $\mathbf{PAut}_\mathcal{P}$ induced by *Inp* and I. We also call $\mathbf{aPAut}_{\mathcal{P},I}$ the co-reflexive subcategory of $\mathbf{PAut}_{\mathcal{P},I}$ spanned by all accessible automata. In a similar way we call $\mathbf{PBeh}_{\mathcal{P},I}$ the fiber of $\mathbf{PBeh}_{\mathcal{P}}$ induced by *bInp* and I. The first step of minimization is to merge states that are indistinguishable.

Definition 5.1. Let m be an accessible automaton over a probability presentation $\mathcal{P}$. We say that $\rho \subseteq S^2$ is a congruence relation over m iff ρ is an equivalence relation; $\delta^i_{s_1}(\omega)\rho\delta^i_{s_2}(\omega)$ for all $i \in I$ and $\omega \in \Omega$ whenever $s_1\rho s_2$; $\Lambda(s_1) = \Lambda(s_2)$ whenever $s_1\rho s_2$. ∎

Prop/Definition 5.2. Let m be a probabilistic automaton and ρ a congruence relation over m. The quotient automaton $m/\rho = \langle I, O, S/\rho, \delta_\rho, \Lambda_\rho\rangle$ is such that: $S/\rho = \{[s]_\rho \mid s \in S\}$ where $[s]_\rho = \{s' \mid s'\rho s\}$; ${\delta_\rho}^i_{[s]_\rho}(\omega) = [\delta^i_s(\omega)]_\rho$; $\Lambda_\rho([s]_\rho) = \Lambda(s)$. ∎

The next step is to find the greatest congruence relation over an automaton.

Proposition 5.3. Let m be a probabilistic automaton and consider $\approx \subseteq S^2$ defined as follows: $s_1 \approx s_2$ iff $\Lambda({\delta^*}^{i_1\ldots i_n}_{s_1}(\omega_1\ldots\omega_n)) = \Lambda({\delta^*}^{i_1\ldots i_n}_{s_2}(\omega_1\ldots\omega_n))$. Then $\approx$ is a congruence relation over m and for any congruence relation ρ over m, $\rho \subseteq \approx$.

Proof. We verify that $\approx$ is a congruence (clearly it is an equivalence relation):

- If $s_1 \approx s_2$ then $\Lambda({\delta^*}^{i_1\ldots i_n}_{\delta^i_{s_1}(\omega)}(\omega_1\ldots\omega_n)) = \Lambda({\delta^*}^{i_1\ldots i_n i}_{s_1}(\omega_1\ldots\omega_n\omega)) =$
  $\Lambda({\delta^*}^{i_1\ldots i_n i}_{s_2}(\omega_1\ldots\omega_n\omega)) = \Lambda({\delta^*}^{i_1\ldots i_n}_{\delta^i_{s_2}(\omega)}(\omega_1\ldots\omega_n))$.
- If $s_1 \approx s_2$ then $\Lambda(s_1) = \Lambda({\delta^*}^{\epsilon}_{s_1}) = \Lambda({\delta^*}^{\epsilon}_{s_2}) = \Lambda(s_2)$.

Moreover consider now another congruence over m, ρ, we show that $\rho \subseteq \approx$, that is, if $s_1\rho s_2$ then $s_1 \approx s_2$: (By induction on n)

- $\Lambda({\delta^*}^{\epsilon}_{s_1}) = \Lambda(s_1) = \Lambda(s_2) = \Lambda({\delta^*}^{\epsilon}_{s_2})$;
- $\Lambda({\delta^*}^{ii_1\ldots i_n}_{s_1}(\omega\omega_1\ldots\omega_n)) = \Lambda({\delta^*}^{i_1\ldots i_n}_{\delta^i_{s_1}(\omega)}(\omega_1\ldots\omega_n)) =$
  $\Lambda({\delta^*}^{i_1\ldots i_n}_{\delta^i_{s_2}(\omega)}(\omega_1\ldots\omega_n)) = \Lambda({\delta^*}^{ii_1\ldots i_n}_{s_2}(\omega\omega_1\ldots\omega_n))$. □

Clearly an automaton m is minimal iff $\approx_m = \Delta_S$, that is $s_1 \approx_m s_2$ iff $s_1 = s_2$. We can present the main theorem of this section but before we need an auxiliary result:

Lemma 5.4. Let $f : m \to m'$ be a morphism in $\mathbf{aPAut}_{\mathcal{P},I}$, then $\underline{f}([s]_\approx) \subseteq [\underline{f}(s)]_{\approx'}$ for all $s \in S$.

Proof.
Suppose that $s_1 \approx s_2$ then:
$\Lambda'({\delta'^*}^{i_1\ldots i_n}_{\underline{f}(s_1)}(\omega_1\ldots\omega_n)) = \Lambda'(\underline{f}({\delta^*}^{i_1\ldots i_n}_{s_1}(\omega_1\ldots\omega_n))) = \overline{\overline{f}}(\Lambda({\delta^*}^{i_1\ldots i_n}_{s_1}(\omega_1\ldots\omega_n))) = \overline{\overline{f}}(\Lambda({\delta^*}^{i_1\ldots i_n}_{s_2}(\omega_1\ldots\omega_n))) = \Lambda'(\underline{f}({\delta^*}^{i_1\ldots i_n}_{s_2}(\omega_1\ldots\omega_n))) = \Lambda'({\delta'^*}^{i_1\ldots i_n}_{\underline{f}(s_2)}(\omega_1\ldots\omega_n))$.
Hence $\underline{f}(s_1) \approx' \underline{f}(s_2)$. □

Theorem 5.5. The functor $\mathit{Unf}\colon \mathbf{aPAut}_{\mathcal{P},I} \to \mathbf{PBeh}_{\mathcal{P},I}$ has a right adjoint.

Proof.
Right adjoint:
Let $\mathit{Min}: \mathbf{PBeh}_{\mathcal{P},I} \to \mathbf{aPAut}_{\mathcal{P},I}$ be such that:

- $\mathit{Min}(B) = \mathit{Free}(B)/\approx$. Clearly, $\mathit{Min}(B)$ is an accessible automaton.
- $\mathit{Min}(\overline{\overline{f}}) = \langle \overline{\overline{f}}, \underline{f}_{\approx} \rangle$ where $\underline{f}_{\approx} = \mathrm{id}_{\mathrm{pRun}_{\mathcal{P},I}\approx}$ that is, $\underline{f}_{\approx}([\sigma]_{\approx}) = [\sigma]_{\approx'}$. Note that $\mathit{Free}(\overline{\overline{f}}) = \langle \overline{\overline{f}}, \mathrm{id}_{\mathrm{pRun}_{\mathcal{P},I}} \rangle$ and therefore, by Lemma 5.4, $[\sigma]_{\approx} \subseteq [\sigma]_{\approx'}$. Hence, $\underline{f}_{\approx}$ is well defined. Moreover $\mathit{Min}(\overline{\overline{f}})$ is a morphism :
  - $\underline{f}_{\approx}(\delta_{\approx}{}^{i}_{[\sigma]_{\approx}}(\omega)) = \underline{f}_{\approx}([\sigma i\omega]_{\approx}) = [\sigma i\omega]_{\approx'} = \delta'_{\approx'}{}^{i}_{[\sigma]_{\approx'}}(\omega) =$ $\delta'_{\approx'}{}^{i}_{\underline{f}_{\approx}([\sigma]_{\approx})}(\omega)$ for all $i \in I \setminus \{\bot\}$ and $\omega \in \Omega$;
  - $\underline{f}_{\approx}(\delta_{\approx}{}^{\bot}_{[\sigma]_{\approx}}(\omega)) = \underline{f}_{\approx}([\sigma]_{\approx}) = [\sigma]_{\approx'} = \delta'_{\approx'}{}^{\bot}_{[\sigma]_{\approx'}}(\omega) = \delta'_{\approx'}{}^{\bot}_{\underline{f}_{\approx}([\sigma]_{\approx})}(\omega)$ for all $\omega \in \Omega$;
  - $\overline{\overline{f}}(\Lambda_{\approx}([\sigma]_{\approx})) = \overline{\overline{f}}(\Lambda(\sigma)) = \Lambda'(\sigma) = \Lambda'([\sigma]_{\approx'})$.

Unit:
Let δ' and Λ' be the random transition map and the output map of $\mathit{Free}(\mathit{Unf}(m))$ respectively. The unit of the adjunction is the family

$$\eta_m = \langle \mathrm{id}_O, \underline{\eta}_m \rangle : m \to \mathit{Min}(\mathit{Unf}(m))$$

where $\underline{\eta}_m : S \to \mathrm{pRun}_{\mathcal{P},I}/\approx$ is such that $\underline{\eta}_m(s) = [\sigma]_{\approx}$ for any $\sigma = i_1\omega_1 \dots i_n\omega_n$ such that $\delta^*{}^{i_1 \dots i_n}_{s_0}(\omega_1 \dots \omega_n) = s$. The automaton m is accessible and hence for all $s \in S$ there exists at least one $\sigma \in \mathrm{pRun}_{\mathcal{P},I}$ fulfilling the previous condition. We now check the good definition of $\underline{\eta}_m$. Consider $\rho \subseteq (\mathrm{pRun}_{\mathcal{P},I})^2$ where

$$\rho = \{\langle i_1\omega_1 \dots i_n\omega_n, i'_1\omega'_1 \dots i'_k\omega'_k \rangle \;:\; \delta^*{}^{i_1 \dots i_n}_{s_0}(\omega_1 \dots \omega_n) = \delta^*{}^{i'_1 \dots i'_k}_{s_0}(\omega'_1 \dots \omega'_k)\}.$$

We verify that ρ is a congruence over $Free(\mathit{Unf}(m))$. Clearly it is an equivalence relation, moreover if $i_1\omega_1 \dots i_n\omega_n \;\rho\; i'_1\omega'_1 \dots i'_k\omega'_k$ then:

- $i_1\omega_1 \dots i_n\omega_n i\omega \;\rho\; i'_1\omega'_1 \dots i'_k\omega'_k i\omega$, hence $\delta'^{i}_{i_1\omega_1 \dots i_n\omega_n}(\omega) \;\rho\; \delta'^{i}_{i'_1\omega'_1 \dots i'_k\omega'_k}(\omega)$;
- $\Lambda'(i_1\omega_1 \dots i_n\omega_n) = \Lambda(\delta^*{}^{i_1 \dots i_n}_{s_0}(\omega_1 \dots \omega_n)) =$
  $\Lambda(\delta^*{}^{i'_1 \dots i'_k}_{s_0}(\omega'_1 \dots \omega'_k)) = \Lambda'(i'_1\omega'_1 \dots i'_k\omega'_k)$.

Assume that $\sigma_1, \sigma_2 \in \mathrm{pRun}_{\mathcal{P},I}$ are such that $\underline{\eta}_m(s) = [\sigma_1]_{\approx}$ and $\sigma_1\rho\sigma_2$ (i.e. $\underline{\eta}_m(s)$ is also equal to $[\sigma_2]_{\approx}$); then since $\rho \subseteq\approx$ we have $[\sigma_1]_{\approx} = [\sigma_2]_{\approx}$ and hence $\underline{\eta}_m$ is well defined. In the sequel we denote by σ_s a proper run such that $\sigma_s = i_1\omega_1 \dots i_n\omega_n$ and $\delta^*{}^{i_1 \dots i_n}_{s_0}(\omega_1 \dots \omega_n) = s$. We now check that η_m is a morphism:

- $\underline{\eta}_m(\delta^i_s(\omega)) = \underline{\eta}_m(\delta^i_{\delta^*{}^{i_1 \dots i_n}_{s_0}(\omega_1 \dots \omega_n)}(\omega)) = \underline{\eta}_m(\delta^*{}^{i_1 \dots i_n i}_{s_0}(\omega_1 \dots \omega_n\omega)) =$
  $[\sigma_s i\omega]_{\approx} = \delta'_{\approx}{}^{i}_{[\sigma_s]_{\approx}}(\omega) = \delta_{\approx}{}^{i}_{\underline{\eta}_m(s)}(\omega)$;

– $\Lambda(s) = \Lambda(\delta^{*}{}^{i_1 \ldots i_n}_{s_0}(\omega_1 \ldots \omega_n)) = \Lambda'(\sigma_s) = \Lambda'_{\approx}([\sigma_s]_{\approx}) = \Lambda'_{\approx}(\underline{\eta}_m(s))$.

Furthermore we show that η is a natural transformation:
$(\mathrm{id}_{\mathrm{pRun}_{\mathcal{P},I}\approx} \circ \underline{\eta}_{m_1})(s_1) = (\mathrm{id}_{\mathrm{pRun}_{\mathcal{P},I}\approx} \circ \underline{\eta}_{m_1})(\delta^{*}_1{}^{i_1 \ldots i_n}_{s_0^1}(\omega_1 \ldots \omega_n)) =$
$\mathrm{id}_{\mathrm{pRun}_{\mathcal{P},I}\approx}([\sigma_{s_1}]_{\approx_1}) = [\sigma_{s_1}]_{\approx_2} = \underline{\eta}_{m_2}(\delta^{*}_2{}^{i_1 \ldots i_n}_{s_0^2}(\omega_1 \ldots \omega_n)) = (\underline{\eta}_{m_2} \circ \underline{f})(s_1)$.
Universal Property:
Let $\langle \overline{\overline{f}}, \underline{f} \rangle : m_1 \to Min(B)$ be a morphism in $\mathbf{aPAut}_{\mathcal{P},I}$. Then, $\overline{\overline{f}} : Unf(m_1) \to B$ is a morphism in $\mathbf{PBeh}_{\mathcal{P},I}$:

– $\overline{\overline{f}}(\Lambda_1(\delta^{*}_1{}^{i_1 \ldots i_n}_{s_0}(\omega_1 \ldots \omega_n))) = \Lambda_{\approx}(\underline{f}(\delta^{*}_1{}^{i_1 \ldots i_n}_{s_0}(\omega_1 \ldots \omega_n))) =$
$\Lambda_{\approx}(\delta_{\approx}{}^{*}{}^{i_1 \ldots i_n}_{[\varepsilon]_{\approx}}(\omega_1 \ldots \omega_n)) = \beta(i_1\omega_1 \ldots i_n\omega_n)$.

Clearly $Min(\overline{\overline{f}}) \circ \eta_m = \langle \overline{\overline{f}}, \underline{f} \rangle$:
$\mathrm{id}_{\mathrm{pRun}_{\mathcal{P},I}\approx}(\underline{\eta}_m(s)) = \mathrm{id}_{\mathrm{pRun}_{\mathcal{P},I}\approx}(\underline{\eta}_m(\delta^{*}_1{}^{i_1 \ldots i_n}_{s_0}(\omega_1 \ldots \omega_n))) = \mathrm{id}_{\mathrm{pRun}_{\mathcal{P},I}\approx}([\sigma_s]_{\approx_1}) =$
$[\sigma_s]_{\approx} = \delta_{\approx}{}^{*}{}^{i_1 \ldots i_n}_{[\epsilon]_{\approx}}(\omega_1 \ldots \omega_n) = \underline{f}(\delta^{*}{}^{i_1 \ldots i_n}_{s_0}(\omega_1 \ldots \omega_n)) = \underline{f}(s)$.
The uniqueness requirement is straightforward. □

As usual, the minimal realization is obtained by applying the minimization procedure to the free realization. The congruence $\approx$ over $Free(B)$ is called the (probabilistic) Nerode equivalence for the behavior B. Since we have fixed the input alphabet, the preservation of aggregation and interconnection via *Min* is meaningless, since these constructs are only defined when we change the input alphabets of the automata.

6 Conclusions

We have characterized both aggregation and interconnection of probabilistic automata by means of universal constructs. Furthermore we have shown that minimal and free realization for probabilistic behavior are both universal. Finally we also have shown that *Unf*, the functor that maps each probability automaton to its behavior, preserves the constructions in mind.

We manage to achieve the results above by assuming that the random source (probability presentation) is fixed. Otherwise we have to define the notion of morphism between probability spaces and work with weaker structures than categories [MSS99]. However certain constructions can not be explained with a single random source, such as state constraints. We intend to extend the work to a generic random source (probability space where the σ-algebra is not the 2^{Ω} and Ω is not countable). Another interesting research direction that we intend to pursue is the study of probabilistic properties like first passage times (of an output, of a state) and how they propagate over aggregation and interconnection as well as free and minimal realizations.

Acknowledgements

This work was partially supported by Fundação para a Ciência e a Tecnologia, the PRAXIS XXI Projects PRAXIS/P/MAT/10002/1998 ProbLog, PCEX/P /MAT/46/96 ACL and 2/2.1/TIT/1658/95 LogComp, as well as by the ESPRIT IV Working Groups 22704 ASPIRE and 23531 FIREworks.

References

[AT89] J. Adámek and V. Trnková. *Automata and Algebras in Categories*. Kluwer Academic Publishers, Dordrecht/Boston/London, 1989.

[BDEP97] R. Blute, J. Desharnais, A. Edalat, and P. Panangaden. Bisimulation for labelled Markov processes. In *Proceedings, Twelth Annual IEEE Symposium on Logic inComputer Science*, pages 149–158, Warsaw, Poland, 29 June–2 July 1997. IEEE Computer Society Press.

[Bén85] J. Bénabou. Fibred categories and the foundations of naive category theory. *Journal of Symbolic Logic*, 50:10–37, 1985.

[BW90] M. Barr and C. Wells. *Category Theory for Computing Science*. Prentice-Hall International Series in Computer Science. Prentice-Hall, 1990.

[Cop80] L. Coppey. Quelques problèmes typiques concernant les graphes. *Diagrammes*, 3:C1–C46, 1980.

[Ehr65] C. Ehresmann. *Catégories et structures*. Dunod, 1965.

[Gog73] J. Goguen. Realization is universal. *Mathematical Systems Theory*, 6:359–374, 1973.

[Hal69] P. Halmos. *Measure Theory*. Van Nostrand, New York, NY, 1969. (July 1969 reprinting).

[LS91] K. Larsen and A. Skou. Bisimulation through probabilistic testing. *Information and Computation*, 94(1):1–28, September 1991.

[MSS99] P. Mateus, A. Sernadas, and C. Sernadas. Precategories for combining probabilistic automata. *Electronic Notes in Theoretical Computer Science*, 1999. Early version presented at FIREworks Meeting, Magdeburg, May 15-16, 1998. Presented at CTCS'99, Edinburgh, September 10-12, 1999. In print.

[Paz66] A. Paz. Some aspects of probabalistic automata. *Information and Control*, 9(1):26–60, February 1966.

[Rab63] M. Rabin. Probabilistic automata. *Information and Control*, 6(3):230–245, September 1963.

[SM99] L. Schröder and P. Mateus. Universal aspects of probabilistic automata. Research report, Section of Computer Science, Department of Mathematics, Instituto Superior Técnico, 1049-001 Lisboa, Portugal, 1999. Submitted for publication.

[vGSST95] R. van Glabbeek, S. Smolka, B. Steffen, and C. Tofts. Reactive, generativem and stratified models for probabilistic processes. *Information and Computation*, 121(1):59–80, 1995.

[WN95] G. Winskel and M. Nielsen. Models of concurrency. In D. Gabbay S. Abramsky and T. Maibaum, editors, *Handbook of Logic in Computer Science 4*, pages 1–148. Oxford Science Publications, 1995.