ELSEVIER

Theoretical Computer Science 282 (2002) 33–51

Theoretical Computer Science

www.elsevier.com/locate/tcs

Testing preorders for probabilistic processes can be characterized by simulations ☆, ☆☆

Bengt Jonsson, Wang Yi *

Department of Computer Systems, Uppsala University Box 325, S-751 05 Uppsala, Sweden

Abstract

Transition systems are well established as a semantic model for distributed systems. There are several preorders that serve as criteria for refinement of an abstract transition system to a more concrete one. To reason about probabilistic phenomena such as failures and randomization, we need to extend models and methods that have proven successful for nonprobabilistic systems to a probabilistic setting. In this paper, we develop a refinement preorder for a probabilistic extension of the transition systems model. The preorder is based on a notion of testing, where refinement corresponds to an improvement in the "worst-case" behavior of a process. The main result of the paper is that this preorder can be described by a notion of probabilistic simulation, which generalizes the standard simulation preorder for ordinary transition system. To our knowledge, this simulation preorder has not been previously described in the literature, and is strictly weaker than previously proposed simulations for probabilistic transition systems. © 2002 Elsevier Science B.V. All rights reserved.

Keywords: Probabilistic transition system; Semantics; Probabilistic testing; Refinement and simulation

1. Introduction

To study probabilistic phenomena such as randomization and failure rates in distributed computing, many researchers have focused on extending models and methods that have proven successful for nonprobabilistic systems to the probabilistic setting. In the nonprobabilistic setting, transition systems are well established as a basic semantic model for concurrent and distributed systems (e.g. [19, 20, 22]).

☆ Supported in part by the Swedish Board for Industrial and Technical Development (NUTEK) and by the Swedish Research Council for Engineering Sciences (TFR).

☆☆ To the fond memory of Linda Christoff.

* Corresponding author.

E-mail addresses: bengt@docs.uu.se (B. Jonsson), yi@docs.uu.se (W. Yi).

PII: S0304-3975(01)00044-5

In the literature, the model of transition systems has been extended to the probabilistic case by adding a mechanism for representing probabilistic choice (e.g. [29,6,7,17, 21,23–25]). In the nonprobabilistic case there are two principal methods for reasoning about systems: to specify and prove properties in some logic and to establish a preorder or equivalence relation between two transition systems. Both are very useful e.g. in a stepwise development process. An abstract transition system model can be analyzed by proving properties in some logic. The abstract model can then be refined in a sequence of steps, where correctness is preserved in each step by establishing a preorder relation between the refined transition system and the refining one. To keep it manageable, it is often necessary to decompose the transition system model, implying that compositionality is an important property of a preorder.

In this paper, we use probabilistic transition systems to describe processes, which may contain probabilistic and nondeterministic choices independently. This model is essentially that by Wang and Larsen [34], the so-called alternating model by Hansson and Jonsson [7], the concurrent Markov chain model [31], has also been studied by Segala and Lynch [28, 27]; it can also be seen as a nondeterministic extension of the purely probabilistic automata of Rabin [25] or the reactive model by Larsen and Skou [17] that do not include any nondeterministic choice construct. To develop a notion of refinement for probabilistic and nondeterministic systems, we study the testing framework of [34], that extend the work by de Nicola and Hennessy [5] to the probabilistic setting. The idea is to define the preorders in terms of the ability of systems to pass tests. Tests are simply processes with the additional ability to report success or failure, and so this set-up has the advantage of basing the preorder on a notion of "observation" (in this case through synchronization), which yields automatically compositional preorders.

The contribution of this paper is to show that the refinement relation adapted from the work of [34] can be fully characterized by a notion of simulation between probabilistic processes. When restricted to nonprobabilistic processes, this relation coincides with ordinary simulation [10].

It may seem a little surprising that a preorder defined in terms of testing, which is a "linear-time" concept, is characterized by a simulation relation, which is a "branching-time" relation. The explanation is that the probabilistic choices of tests have the effect of "copying" the intermediate states of a process under test into a number of copies, and that the testing of each copy is performed independently. The "copying ability" has been adopted by [1] in characterizing observational equivalence by testing.

This paper is a continuation of our earlier work [11, 14, 15]. In that work, testing preorders were characterized in terms of rather complex tree-structures called "chains" or "probabilistic computation trees". This paper presents a substantially improved result, since simulation is a much simpler concept and more adequate for algorithmic analysis.

Over the past years, a number of models for describing probabilistic aspects of transition systems in the form of e.g. Markov chains, Process Algebras, Timed Petri Nets, etc. have been proposed [6, 8, 9, 17, 18, 21, 23, 24, 30]. Logics and associated methods for probabilistic systems can be found in e.g. [4, 8, 9, 16, 17]. Several (bi)simulation-based preorders between probabilistic systems have been investigated, e.g. [6]. Jonsson and Larsen [12], Segala and Lynch [28], and Wang [33] present simulation-based preorders for probabilistic processes. These are not based on some independent notion of "testing". Testing-based preorders of probabilistic processes have also been studied by Christoff [2] and by Cleaveland et al. [3] and by Yuen et al. [35, 32]. These works consider a pure probabilistic model [29], and therefore their preorders do not capture the notion of refinement in the sense of being "less nondeterministic". The work which is closest to the current one is by Segala [27], who define essentially the same testing preorders as in this work. Segala does not develop an alternative characterization of the testing preorder in terms of e.g., simulations, but proves that when defining the compositional testing preorder, then it suffices to consider a unique "canonical" context: the compositional precongruence is obtained by comparing systems composed with this canonical context.

For instance, the combined preorder $\sqsubseteq$ in [3] does not correspond to a decrease in the possible outcomes under test. Yuen et al. [35] consider only one testing preorder for a given class of tests, and e.g., Christoff considers a very restricted class of tests. These works do not consider the issue of compositionality either. Wu et al. [32] also studied fully abstract and compositional characterization of testing in a purely probabilistic setting (not including nondeterminism). Larsen and Skou [17] obtain an analogy to our result that the probabilistic must-testing preorder is equivalent to refusal simulation. They show that the corresponding equivalence called 2/3-bisimulation can be obtained by a probabilistic testing procedure, which however is quite different from ours and involves explicit copying of the process under test.

The rest of the paper is organized as follows. In the next section, we present the necessary definitions for probabilistic transition systems and testing semantics for such systems. Section 4 defines the notion of simulation between probabilistic processes, and contains the main characterization theorem for the may-testing preorder. Section 6 gives some concluding remarks.

2. Probabilistic processes and tests

We consider a model of probabilistic transition systems, containing probabilistic and nondeterministic choices as independent concepts. We define tests as probabilistic transition systems, where certain states are "accepting". We define testing preorders on the basis of the probabilities with which tests reach an accepting state when interacting with a process.

2.1. Preliminaries

A *weighting* on a set S is a function $\sigma : S \to \mathscr{R}_{\geqslant 0}$ from S to nonnegative real numbers. For a set S, we use $\sigma(S)$ to denote $\sum_{s \in S} \sigma(s)$. A *probability distribution* on a finite set S is a weighting σ on S such that $\sigma(S) = 1$. A *subdistribution* on a finite set S is a weighting σ on S such that $\sigma(S) \leqslant 1$. We use $s \in \sigma$ to denote that $\sigma(s) > 0$. The *support* of a weighting *dist* is the set of elements s with $s \in \sigma$. Let $Weight(S)$ and $Dist(S)$ denote the sets of weightings and probability distributions on S, respectively. If $\sigma_1, \ldots, \sigma_n$ are weightings on S and $w_1, \ldots, w_n$ are nonnegative real numbers, then $\sum_{i=1}^{n} w_i \sigma_i$ is also a weighting on S, with obvious meaning. We will sometimes identify a single state s with the distribution that assigns probability 1 to the state s.

If σ is a weighting on S and ρ is a weighting on R, then $\sigma \times \rho$ is a weighting on $S \times R$, defined by $(\sigma \times \rho)(\langle s, r \rangle) = \sigma(s) * \rho(r)$. If σ is a weighting on S and $h : S \mapsto R$ is a function from S to R, then $h(\sigma)$ is a weighting on R, defined by $h(\sigma)(r) = \sum_{h(s)=r} \sigma(s)$. If σ and ρ are weightings on S, then $\sigma \leqslant \rho$ denotes that $\sigma(s) \leqslant \rho(s)$ for all $s \in S$.

2.2. Probabilistic processes

We assume a finite set $\mathscr{A}ct$ of atomic actions, ranged over by a and b.

Definition 1. A (*probabilistic*) *transition system* is a pair $\langle S, \rightarrow \rangle$, where
- S is a nonempty finite set of *states*, and
- $\rightarrow \subseteq S \times \mathscr{A}ct \times Dist(S)$ is a finite *transition relation*.

We use $s \xrightarrow{a} \sigma$ to denote that $\langle s, a, \sigma \rangle \in \rightarrow$. A (*probabilistic*) *process* is a tuple $\langle \langle S, \rightarrow \rangle, \sigma_0 \rangle$, where $\langle S, \rightarrow \rangle$ is a probabilistic transition system, and $\sigma_0 \in Dist(S)$ is an *initial probability distribution* on S.

We use $s \xrightarrow{a}$ to denote that there is a σ such that $s \xrightarrow{a} \sigma$, We say that a state s is *terminal* (written $s \not\rightarrow$) if there is no a and σ such that $s \xrightarrow{a} \sigma$. A *finite tree* is a process $\langle \langle S, \rightarrow \rangle, \sigma_0 \rangle$ such that states and distributions in S form a tree under the union of the relations $\in$ and $\rightarrow$, with σ_0 as the root.

Each state of a probabilistic transition system has a potential for future dynamic behavior. When an action is performed, the system makes a probabilistic "choice" of next state. Thus, at each point in time, a snapshot of the system state will be a distribution over possible states.

2.3. Composition and testing

To study compositionality, we define a synchronous parallel composition operator for probabilistic transition systems, in which two processes $\mathscr{P}$ and $\mathscr{Q}$ execute in parallel while synchronizing on all actions in $\mathscr{A}ct$.

Definition 2. Let $\langle S, \rightarrow \rangle$ and $\langle R, \rightarrow \rangle$ be two transition systems. Their composition, denoted $\langle S, \rightarrow \rangle \| \langle R, \rightarrow \rangle$, is the transition system $\langle U, \rightarrow \rangle$, where
- $U = S \times R$. A pair $(s, r) \in U$ is denoted as $s \| r$.
- $\rightarrow \subseteq U \times \mathscr{A}ct \times Dist(U)$ is defined by

$$s \| r \xrightarrow{a} \sigma \times \rho \quad \text{iff } s \xrightarrow{a} \sigma \quad \text{and} \quad r \xrightarrow{a} \rho.$$

The composition of two processes $\mathscr{P} = \langle\langle S, \rightarrow\rangle, \sigma_0\rangle$ and $\mathscr{Q} = \langle\langle R, \rightarrow\rangle, \rho_0\rangle$, denoted $\mathscr{P} \| \mathscr{Q}$, is the process $\langle\langle S, \rightarrow\rangle \| \langle R, \rightarrow\rangle, \sigma_0 \times \rho_0\rangle$.

It can be shown that the parallel composition operator enjoys all the desired properties such as commutativity and associativity that a parallel composition operator in a process algebra should possess.

Following Wang and Larsen [34], we define tests as finite trees with a certain subset of the terminal states being "accepting states".

Definition 3. A (*probabilistic*) *test* is a tuple $\langle\langle\langle T, \rightarrow\rangle, \tau_0\rangle, F\rangle$, where $\langle\langle T, \rightarrow\rangle, \tau_0\rangle$ is a finite tree, and $F \subseteq T$ is a set of *success-states*, each of which is terminal.

A test $\mathscr{T}$ is applied to a process $\mathscr{P}$ by putting the process $\mathscr{P}$ in parallel with the test $\mathscr{T}$ and observing whether the test reaches a success state.

We define a testing system as the parallel composition of a process and a test.

Definition 4. Let $\mathscr{P} = \langle\langle S, \rightarrow\rangle, \sigma_0\rangle$ be a process and $\mathscr{T} = \langle\langle\langle T, \rightarrow\rangle, \tau_0\rangle, F\rangle$ be a test. The composition of $\mathscr{P}$ and $\mathscr{T}$, denoted as $\mathscr{P} \| \mathscr{T}$ is a so-called *testing system*, defined as the process $\langle\langle S, \rightarrow\rangle, \sigma_0\rangle \| \langle\langle T, \rightarrow\rangle, \tau_0\rangle$ with success states $S \times F$.

Our intention is that a testing system defines a probability of reaching a success-state. However, since from each state there may be several outgoing transitions, such a probability is not uniquely defined. We will be interested in the maximal probabilities of success. These can be defined inductively on the structure of the testing system.

Definition 5. Let $\mathscr{P} \| \mathscr{T}$ be a testing system, composed of the process $\mathscr{P} = \langle\langle S, \rightarrow\rangle, \sigma_0\rangle$ and the test $\mathscr{T} = \langle\langle\langle T, \rightarrow\rangle, \tau_0\rangle, F\rangle$. For each state $s \| t$ of $\mathscr{P} \| \mathscr{T}$ we define its *maximal probability of sucess*, denoted as $t\lceil s\rceil$ inductively by

- If $s \| t$ is terminal, then $t\lceil s\rceil = 1$ if t is a success-state, else $t\lceil s\rceil = 0$.
- If $s \| t$ is not terminal, then

$$t\lceil s\rceil = \max_{s\|t \xrightarrow{a} \sigma\times\tau} \left(\sum_{s'\|t'} (\sigma \times \tau)(s' \| t') * t'\lceil s\rceil \right).$$

For a distribution σ on S and a distribution τ on T, we define

$$\tau\lceil\sigma\rceil = \sum_{s\|t} (\sigma \times \tau)(s\|t) * t\lceil s\rceil.$$

We define $\mathscr{T}\lceil\mathscr{P}\rceil = \sigma_0\lceil\tau_0\rceil$.

We note that, using the definition of $\tau\lceil\sigma\rceil$, we can make a simpler definition of $t\lceil s\rceil$ as

$$t\lceil s\rceil = \max_{s\|t \xrightarrow{a} \sigma\times\tau} \tau\lceil\sigma\rceil.$$

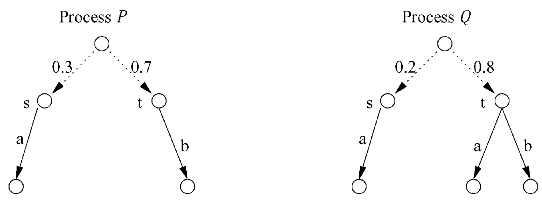

Fig. 1. $\mathscr{P} \sqsubseteq_{\text{may}} \mathscr{Q}$.

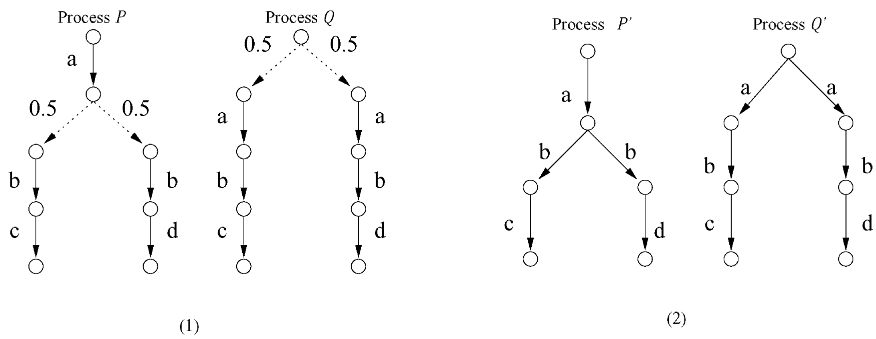

Fig. 2. (1) $\mathscr{P} \sqsubseteq \mathscr{Q}$ and $\mathscr{Q} \not\sqsubseteq \mathscr{P}$. (2) $\mathscr{Q}' \sqsubseteq \mathscr{P}'$ and $\mathscr{P}' \not\sqsubseteq \mathscr{Q}'$.

We now define a may-preorder of testing, which abstract from the set of possible expected outcomes when testing a process $\mathscr{P}$ by a test $\mathscr{T}$: *may* testing considers the highest possible expected outcome of $\mathscr{P}\|\mathscr{T}$.

Definition 6. Given two processes $\mathscr{P}$ and $\mathscr{Q}$, define

$$\mathscr{P} \sqsubseteq_{\text{may}} \mathscr{Q} \quad \text{iff } \forall \mathscr{T}: \ \mathscr{T}\lceil \mathscr{P} \rceil \leqslant \mathscr{T}\lceil \mathscr{Q} \rceil.$$

The intention behind the definition of $\sqsubseteq_{\text{may}}$ is that intuitively, $\mathscr{P} \sqsubseteq_{\text{may}} \mathscr{Q}$ should means that $\mathscr{P}$ refines $\mathscr{Q}$ with respect to "safety properties". The motivation is the following. We can regard the success-states of a test as states defining when the tester has observed some "bad" or "unacceptable" behavior. A process then refines another one if it has a smaller potential for "bad behavior" with respect to any test. In the definition of $\mathscr{P} \sqsubseteq_{\text{may}} \mathscr{Q}$, this means that the maximal probability of observing bad behavior of $\mathscr{P}$ should not exceed the maximal probability of observing bad behavior of $\mathscr{Q}$.

For example, consider process $\mathscr{P}$ and $\mathscr{Q}$ in Fig. 1. The probability that $\mathscr{P}$ may pass a test is always less or equal to the probability $\mathscr{Q}$ may pass the same test; therefore $\mathscr{P} \sqsubseteq_{\text{may}} \mathscr{Q}$.

Fig. 2 show two examples of $\sqsubseteq$-related processes. In Fig. 2(1), we have $\mathscr{P} \sqsubseteq \mathscr{Q}$ but not $\mathscr{Q} \sqsubseteq \mathscr{P}$: this is due to the fact that $\mathscr{Q}$ performs a probabilistic choice earlier than $\mathscr{P}$, and that then a test can let its nondeterministic choice depend on the outcome of the probabilistic choice in $\mathcal{Q}$. In Fig. 2(2), we have $\mathcal{Q}' \sqsubseteq \mathcal{P}'$ but not $\mathcal{P}' \sqsubseteq \mathcal{Q}'$: this is due to the fact that the probabilistic choice in a test can take copies of the intermediate states after performing a in $\mathcal{P}'$ and in $\mathcal{Q}'$. Since $\mathcal{P}'$ has not yet performed the nondeterministic choice when copying occurs, the outcome of the nondeterministic choice can be made different in the two copies, leading to a larger set of expected outcomes in the testing system for $\mathcal{P}'$ than $\mathcal{Q}'$.

2.4. Congruence properties

A useful property of preorders is that they are compositional in the sense that they are precongruences with respect to parallel composition operators, parallel composition operator $||$. Our testing preorder $\sqsubseteq_{\mathrm{may}}$ is indeed a precongruence with respect to $||$, which is not surprising because our testing framework is defined in terms of the synchronous operator. A more interesting case is the asynchronous parallel composition operator which is also known as the interleaving operator in CSP.

Definition 7. Let $\langle S, \rightarrow \rangle$ and $\langle R, \rightarrow \rangle$ be two transition systems. For a state s, we use $\mathbf{1}_s$ to denote the unit distribution with $\mathbf{1}_s(s) = 1$ and $\mathbf{1}_s(s') = 0$ for $s' \neq s$. Their asynchronous composition, denoted $\langle S, \rightarrow \rangle ||| \langle R, \rightarrow \rangle$, is the transition system $\langle U, \rightarrow \rangle$, where

- $U = S \times R$. A pair $(s, r) \in U$ is denoted as $s|||r$.
- $\rightarrow \subseteq U \times \mathcal{A}ct \times Dist(U)$ is defined by
  1. $s|||r \xrightarrow{a} \sigma \times \mathbf{1}_r$ if $s \xrightarrow{a} \sigma$, and
  2. $s|||r \xrightarrow{a} \mathbf{1}_s \times \rho$ if $r \xrightarrow{a} \rho$.

The composition of two processes $\mathcal{P} = \langle \langle S, \rightarrow \rangle, \sigma_0 \rangle$ and $\mathcal{Q} = \langle \langle R, \rightarrow \rangle, \rho_0 \rangle$, denoted as $\mathcal{P}|||\mathcal{Q}$, is the process $\langle \langle S, \rightarrow \rangle ||| \langle R, \rightarrow \rangle, \sigma_0 \times \rho_0 \rangle$.

It can be shown that the synchronous parallel composition operator enjoys all the desired properties such as commutativity and associativity. More importantly it preserves our testing preorder as the synchronous operator.

Proposition 1. *For arbitrary processes* $\mathcal{P}, \mathcal{Q}, \mathcal{R}$, $\mathcal{P} \sqsubseteq_{\mathrm{may}} \mathcal{Q}$ *implies*

1. $\mathcal{P}||\mathcal{R} \sqsubseteq_{\mathrm{may}} \mathcal{Q}||\mathcal{R}$,
2. $\mathcal{P}|||\mathcal{R} \sqsubseteq_{\mathrm{may}} \mathcal{Q}|||\mathcal{R}$.

3. Probabilistic simulation

In this section, we define a simulation relation between probabilistic processes. In the next section, we will prove that this relation characterizes the may-testing preorder.

We must first generalize the notion of "computation step" from the nonprobabilistic setting to our framework. In Definition 1, the initial "snapshot" of a probabilistic process is given by its initial distribution. From each state in this distribution, there are in general several possible first transitions. Since the initial "snapshot" is a distribution

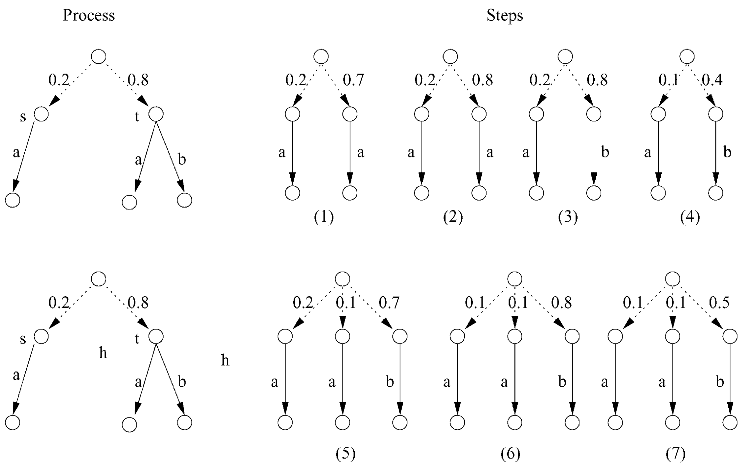

Fig. 3. Seven example steps of a process.

rather than a state, the first computation step of the process is naturally defined to be a distribution over possible first actions, which results in a new distribution over states, representing a next "snapshot" of the process.

We formalize this notion of "computation step" from a distribution (or more generally, from a weighting) by defining the notion of a *step*, which is a natural generalization of transition from the nonprobabilistic setting to the one in this paper.

Definition 8. Let $\langle S, \rightarrow \rangle$ be a probabilistic transition system. A *step* is a weighting on $\mathscr{A}ct \times Dist(S)$.

- A *step from a state* s (recall that a state is identified with the unit distribution over s) is a subdistribution over the set $\{\langle a, \sigma' \rangle : s \xrightarrow{a} \sigma'\}$.
- A *step from a weighting* of form $\sigma = \sum_{i=1}^{n} w_i s_i$ is of form $\sum_{i=1}^{n} w_i \phi_i$, where ϕ_i is a step from s_i for $i = 1, \ldots, n$.

We shall use $\mathsf{step}(s)$ to denote the set of steps from state s. A step of a distribution is a subdistribution ϕ over combinations of actions and next distributions, which is of form $\sum_1^n \sigma(s_i) * \phi_i$ where $\phi_i \in \mathsf{step}(s_i)$. We shall use $\mathsf{step}(\sigma)$ to denote the set of steps from σ.

As an example, in Fig. 3 we show seven example steps from the initial distribution of a process. Note that from a given distribution, there may be infinitely many different steps. We say that a step ϕ is an *a-step* if $a' = a$ for all $\langle a', \sigma' \rangle$ in the support of ϕ. For example, in Fig. 3, (1) and (2) are a-steps.

Definition 9.

- A *normal step* from a state s is a unit distribution over a pair $\langle a, \sigma' \rangle$ such that $s \xrightarrow{a} \sigma'$.

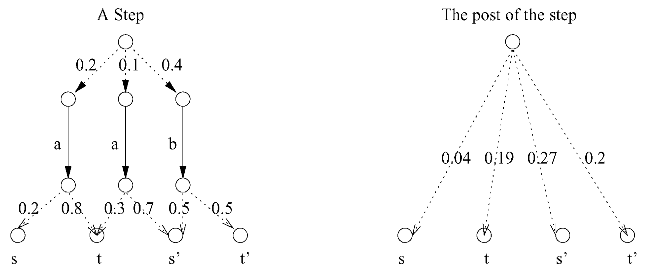

Fig. 4. A step and its post weighting.

- A *normal step* from a weighting of form $\sigma = \sum_{i=1}^{n} w_i s_i$, where all s_i are different, is of form $\sum_{i=1}^{n} w_i \phi_i$ where ϕ_i is a normal step from s_i for $i = 1, \ldots, n$.

That is, a normal step is obtained by choosing a unique transition from each state in the weighting. Since each state in a weighting in general has several outgoing transitions, there are many (but finitely many) normal steps from each distribution. For example, in Fig. 3, (2) and (3) are the two normal steps of the shown process. We note that the normal steps determine all other steps in the sense that any step can be obtained as a subdistribution on the set of normal steps.

We define post on steps by

$$\mathsf{post}(\phi) = \sum_{\langle a,\sigma'\rangle} \phi(\langle a,\sigma'\rangle) * \sigma',$$

i.e., $\mathsf{post}(\phi)$ is the weighting obtained by projecting a step onto the "next" distribution in its transitions. The notion of post weighting is analogous to the notions of next state in the nonprobabilistic setting. In Fig. 4, we show a step, and the post weightings for action a, b and the step itself.

We can now define the notion of simulation between weightings.

Definition 10 (*Probabilistic simulation*). Let $\langle S, \rightarrow\rangle$ and $\langle R, \rightarrow\rangle$ be two probabilistic transition systems. A relation $\lhd \subseteq (\mathit{Weight}(S) \times \mathit{Weight}(R))$ between weightings on S and weightings on R is a *probabilistic simulation* if $\sigma \lhd \rho$ implies that

- $\sigma(S) \leqslant \rho(R)$, and
- for each normal step ϕ from σ there is a step ψ from ρ and a function $h : \mathrm{supp}(\phi) \mapsto \mathsf{step}(\rho)$ (i.e., from pairs $\langle a, \sigma'\rangle$ in the support of ϕ to steps from ρ) such that
  - $h(\langle a,\sigma'\rangle)$ is an a-step from ψ for each $\langle a,\sigma'\rangle$ in the support of ϕ,
  - $h(\phi) \leqslant \psi$, i.e., the image of ϕ under h is "covered" by ψ, and
  - for each pair $\langle a,\sigma'\rangle$ in the support of ϕ we have

$$\sigma' \lhd \mathsf{post}(h(\langle a,\sigma'\rangle)).$$

For two probabilistic processes $\mathscr{P} = \langle\langle S, \rightarrow\rangle, \sigma_0\rangle$ and $\mathscr{Q} = \langle\langle R, \rightarrow\rangle, \rho_0\rangle$, we say that $\mathscr{P}$ *is simulated by* $\mathscr{Q}$ if there is a probabilistic simulation $\lhd \subseteq (\mathit{Weight}(S) \times \mathit{Weight}(R))$ such that $\sigma_0 \lhd \rho_0$.

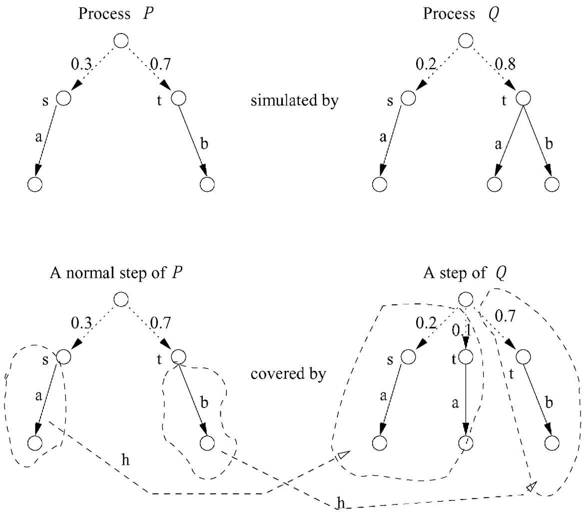

Fig. 5. A proof for $P \lhd Q$.

Intuitively, a weighting σ is simulated by a weighting ρ if the total "mass" of σ is at most that of ρ (first condition), and if each step ϕ from σ can be simulated by a step ψ from ρ in the sense that each "next transition" $\langle a, \sigma' \rangle$ in the support of ϕ can be covered by an a-step from ρ, such that the weighted sum (weighted wrp. to ϕ) of all the weightings $h(\langle a, \sigma' \rangle)$ is covered by ψ, and such that σ' is simulated by the next-state distribution obtained from $h(\langle a, \sigma' \rangle)$. In Fig. 5, we illustrate why process P is simulated by process Q. Note that $P \sqsubseteq_{\mathrm{may}} Q$ as shown in Fig. 1.

4. Correspondence between testing and simulation

In this section, we will present the main results of the paper, namely that the may testing preorder, defined in Definition 6, can be characterized by the simulation relation defined in Definition 10.

It may seem a little surprising that a preorder defined in terms of testing, which is a "linear-time" activity, is characterized by a simulation relation, which is a "branching-time" relation. The explanation is that the probabilistic choices of tests have the effect of "copying" the process under test into a number of copies, and that the testing of each copy is performed independently [1].

We first extend the definition of testing to steps in a natural way. For a test state t and a step ϕ, define

$$t[\phi] = \sum_{\langle a, \sigma' \rangle \in \phi} \left(\max_{t \xrightarrow{a} \tau'} \phi(\langle a, \sigma' \rangle) * \tau' \lceil \sigma' \rceil \right).$$

For a distribution τ on T and a step ϕ, define

$$\tau[\phi] = \sum_{t \in T} \tau(t) * t\lceil\phi\rceil.$$

Proposition 2. *The following linearity properties hold for test outcomes.*
1. $\tau\lceil\sigma\rceil$ *is linear in both arguments, where* τ *is a distribution over states of a test, and* σ *is a distribution over states.*
2. $\tau\lceil\phi\rceil$ *is linear in both arguments, where* τ *is a distribution over states of a test, and* ϕ *is a step.*

A central component in the main theorem is the following proposition, which relates the outcome $t\lceil\sigma\rceil$ of testing a distribution to the outcomes of testing the steps from σ.

Proposition 3.
- *If* ϕ *is a step from* σ, *then* $\tau\lceil\phi\rceil \leqslant \tau\lceil\sigma\rceil$ *for any* τ.
- *If* σ *is a distribution and* t *is a state of a test with outgoing transitions* $t \xrightarrow{a_1} \tau_1, \ldots, t \xrightarrow{a_n} \tau_n$, *then there is a normal step* ϕ *from* σ *with support* $\langle a_1, \sigma_1' \rangle, \ldots, \langle a_n, \sigma_n' \rangle$ *such that*

$$t\lceil\sigma\rceil = \sum_{i=1}^{n} (\phi(\langle a_i, \sigma_i \rangle) * \tau_i\lceil\sigma_i'\rceil).$$

Proof. To prove the first claim, assume first that τ is a unit distribution over a state t of a test, and that σ is a unit distribution over a state s. Then ϕ is a subdistribution over the set $\{\langle a, \sigma' \rangle : s \xrightarrow{a} \sigma'\}$. We first rewrite the definition of $t\lceil\phi\rceil$, i.e.,

$$t\lceil\phi\rceil = \sum_{s \xrightarrow{a} \sigma'} \phi(\langle a, \sigma' \rangle) \left(\max_{t \xrightarrow{a} \tau'} \tau'\lceil\sigma'\rceil \right).$$

The fact that ϕ is a subdistribution over the set $\{\langle a, \sigma' \rangle : s \xrightarrow{a} \sigma'\}$ implies that

$$\sum_{s \xrightarrow{a} \sigma'} \phi(\langle a, \sigma' \rangle) \left(\max_{t \xrightarrow{a} \tau'} \tau'\lceil\sigma'\rceil \right) \leqslant \max_{s \xrightarrow{a} \sigma'} \max_{t \xrightarrow{a} \tau'} \tau'\lceil\sigma'\rceil.$$

The second term is by definition equal to $t\lceil\sigma\rceil$, which implies

$$t[\phi] \leqslant t\lceil\sigma\rceil.$$

The proof is extended to distributions τ over test states, and distributions σ by linearity of $\tau\lceil\phi\rceil$ and $\tau\lceil\sigma\rceil$.

To prove the second claim, assume again that σ is a unit distribution over a state s. Then

$$t\lceil s\rceil = \max_{s \xrightarrow{a} \sigma'} \max_{t \xrightarrow{a} \tau'} \tau'\lceil\sigma'\rceil.$$

Let $\tau'_{\max}$ and $\sigma'_{\max}$ be such that

$$\tau'_{\max}\lceil\sigma'_{\max}\rceil = \max_{s \xrightarrow{a} \sigma'} \max_{t \xrightarrow{a} \tau'} \tau'\lceil\sigma'\rceil.$$

Let $\phi_{\max}$ be the unit distribution over $s \xrightarrow{a} \sigma'_{\max}$. By definition, $\phi_{\max}$ is a normal step from s, which satisfies

$$t\lceil\phi_{\max}\rceil = \tau'_{\max}\lceil\sigma'_{\max}\rceil$$

from which the claim follows. As in the previous case, the claim is extended to arbitrary weightings σ by the linearity properties of Proposition 2.

We are now ready to prove the main characterization theorem of the paper.

Theorem 1. *$\sigma \sqsubseteq_{\text{may}} \rho$ if and only if there is a probabilistic simulation $\lhd$ such that $\sigma \lhd \rho$.*

A special case is the characterization between processes:

Corollary 1. *$\mathscr{P} \sqsubseteq_{\text{may}} \mathscr{Q}$ if and only if $\mathscr{P}$ is simulated by $\mathscr{Q}$.*

Proof. *If-direction*: Assume that $\sigma \lhd \rho$. We must prove that for each distribution τ over states of a test, we have $\tau\lceil\sigma\rceil \leqslant \tau\lceil\rho\rceil$. We prove this by induction over the structure of τ.

- If τ is a unit distribution over a terminal state t, then $\tau\lceil\sigma\rceil = \sigma(S)$ if t is successful and 0 otherwise. Thus $\tau\lceil\sigma\rceil \leqslant \tau\lceil\rho\rceil$ follows from the condition $\sigma(S) \leqslant \rho(R)$ in Definition 10.
- If τ is a unit distribution over a nonterminal state t, then by Proposition 3 there is a normal step ϕ from σ with support $\langle a_1, \sigma'_1\rangle, \ldots, \langle a_n, \sigma'_n\rangle$, and outgoing transitions $t \xrightarrow{a_1} \tau'_1, \ldots, t \xrightarrow{a_n} \tau'_n$ from t such that

  $$t\lceil\sigma\rceil = \sum_{i=1}^{n} (\phi(\langle a_i, \sigma'_i\rangle) * \tau'_i\lceil\sigma'_i\rceil).$$

  Since $\sigma \lhd \rho$, by the second condition in Definition 10, there is a step ψ from ρ and a mapping h from the support of ϕ to steps from ρ such that for each $i = 1, \ldots, n$ we have

  $$\sigma'_i \lhd \mathsf{post}(h(\langle a_i, \sigma'_i\rangle)),$$

  where $\mathsf{post}(h(\langle a_i, \sigma'_i\rangle))$ by definition is equal to $\sum_{\rho'} h(\langle a_i, \sigma'_i\rangle)(\langle a_i, \rho'\rangle)$. By the inductive hypothesis applied to each τ'_i, we infer that

  $$\tau'_i\lceil\sigma'_i\rceil \leqslant \tau'_i\left\lceil \sum_{\rho'} h(\langle a_i, \sigma'_i\rangle)(\langle a_i, \rho'\rangle) * \rho' \right\rceil.$$

By the lineary properties of Proposition 2, the second term is equal to

$$\sum_{\rho'} h(\langle a_i, \sigma_i' \rangle)(\langle a_i, \rho' \rangle) * \tau_i' \lceil \rho' \rceil.$$

By combining the above inequalities, and rearranging the summation order, we obtain

$$t\lceil \sigma \rceil \leqslant \sum_{\rho'} \sum_{i=1}^{n} \phi(\langle a_i, \sigma_i' \rangle) * h(\langle a_i, \sigma_i' \rangle)(\langle a_i, \rho' \rangle) * \tau_i' \lceil \rho' \rceil.$$

The second condition of Definition 10 requires that $h(\phi) \leqslant \psi$, i.e., that

$$\sum_{i=1}^{n} (\phi(\langle a_i, \sigma_i' \rangle) * h(\langle a_i, \sigma_i' \rangle)(\langle a_i, \rho' \rangle)) \leqslant \psi(\langle a_i, \rho' \rangle)$$

for each ρ', which implies that

$$t\lceil \sigma \rceil \leqslant \sum_{\rho'} \psi(\langle a_i, \rho' \rangle) * \tau_i' \lceil \rho' \rceil.$$

By the definition of $t\lceil \psi \rceil$, this implies $t\lceil \sigma \rceil \leqslant t\lceil \psi \rceil$, which by Proposition 3 implies $t\lceil \sigma \rceil \leqslant t\lceil \rho \rceil$, since ψ is a step from ρ.

– If τ is a distribution over the states $t_1, \ldots, t_n$ the result follows by linearity of testing outcome, stated in Proposition 2.

This concludes the proof for this direction.

Only If-direction: We shall prove that the relation $\sqsubseteq_{\mathrm{may}}$ is a probabilistic simulation, by checking that it satisfies the conditions in Definition 10. So, consider σ and ρ such that $\sigma \sqsubseteq_{\mathrm{may}} \rho$. By considering the effect of a test which succeeds immediately with probability 1, we infer the first condition $\sigma(S) \leqslant \rho(R)$.

To infer the second condition, let ϕ be an arbitrary normal step from σ. We must now show that there is a step ψ from ρ which satisfies the conditions in Definition 10.

Let $\langle a_1, \sigma_1' \rangle, \ldots, \langle a_n, \sigma_n' \rangle$ be the support of ϕ. Define $\phi_i = \phi(\langle a_i, \sigma_i' \rangle) * \langle a_i, \sigma_i' \rangle$ so that ϕ_i is an a_i-step with $\mathsf{post}(\phi_i) = \phi(\langle a_i, \sigma_i' \rangle) * \sigma_i'$ and $\phi = \sum_{i=1}^{n} \phi_i$. In other words, ϕ_i is the "ith element" of ϕ. Let Ψ be the set of tuples $\langle \psi_1, \ldots, \psi_n \rangle$ of steps from ρ such that ψ_i is an a_i-step and such that $\sum_{i=1}^{n} \psi_i$ is a step from ρ. For a vector $\tau_1, \ldots, \tau_n$ of n tests, define the test $\sum_{i=1}^{n} a_i.\tau_i$, using a CCS-like notation, as a unit distribution over a test state t with outgoing transitions $t \xrightarrow{a_1} \tau_1, \ldots, t \xrightarrow{a_n} \tau_n$. For any tuple $\langle vect\tau n \rangle$ tests, and any tuple $\langle \psi_1, \ldots, \psi_n \rangle$ of steps such that ψ_i is an a_i-step, define

$$\langle \psi_1, \ldots, \psi_n \rangle (\langle \tau_1, \ldots, \tau_n \rangle) = \sum_{i=1}^{n} \tau_i \lceil \mathsf{post}(\psi_i) \rceil.$$

By Proposition 3, we have

$$\langle \psi_1, \ldots, \psi_n \rangle (\langle \tau_1, \ldots, \tau_n \rangle) \leqslant \sum_{i=1}^{n} a_i.\tau_i \lceil \psi \rceil \leqslant \sum_{i=1}^{n} a_i.\tau_i \lceil \rho \rceil,$$

and similarly

$$\langle \phi_1,\ldots,\phi_n\rangle(\langle \tau_1,\ldots,\tau_n\rangle) \leqslant \sum_{i=1}^{n} a_i.\tau_i\lceil \phi\rceil \leqslant \sum_{i=1}^{n} a_i.\tau_i\lceil \sigma\rceil.$$

On the other hand, Proposition 3 also states that there is a tuple $\langle \psi_1,\ldots,\psi_n\rangle \in \Psi$ such that

$$\langle \psi_1,\ldots,\psi_n\rangle(\langle \tau_1,\ldots,\tau_n\rangle) = \sum_{i=1}^{n} a_i.\tau_i\lceil \psi\rceil = \sum_{i=1}^{n} a_i.\tau_i\lceil \rho\rceil.$$

Since $\sigma \sqsubseteq_{\text{may}} \rho$, this implies that for each tuple $\langle \tau_1,\ldots,\tau_n\rangle$ of test distributions, there is a tuple $\langle \psi_1,\ldots,\psi_n\rangle \in \Psi$ such that

$$\langle \phi_1,\ldots,\phi_n\rangle(\langle \tau_1,\ldots,\tau_n\rangle) \leqslant \langle \psi_1,\ldots,\psi_n\rangle(\langle \tau_1,\ldots,\tau_n\rangle).$$

The central part of the proof is to infer from the fact that Ψ is convex, that the quantifiers in the preceding property can be reversed, i.e., that the following claim holds

Claim. There is a tuple $\langle \psi_1,\ldots,\psi_n\rangle \in \Psi$ such that

$$\langle \phi_1,\ldots,\phi_n\rangle(\langle \tau_1,\ldots,\tau_n\rangle) \leqslant \langle \psi_1,\ldots,\psi_n\rangle(\langle \tau_1,\ldots,\tau_n\rangle)$$

for each tuple $\langle \tau_1,\ldots,\tau_n\rangle$ of test distributions.

Using this claim, which will be proven later, define $h : \text{supp}(\phi) \mapsto Weight(\mathscr{A}ct \times Dist(S))$ by

$$h(\langle a_i, \sigma_i'\rangle) = \frac{1}{\phi(\langle a_i, \sigma_i'\rangle)} * \psi_i.$$

We can now check that h satisfies the three conditions in Definition 10.

- Since ψ_i is an a_i-step, it follows that $h(\langle a_i, \sigma_i'\rangle)$ is an a_i-step.
- Since

  $$h(\phi_i) = h(\phi(\langle a_i, \sigma_i'\rangle) * \langle a_i, \sigma_i'\rangle) = \phi(\langle a_i, \sigma_i'\rangle) * h(\langle a_i, \sigma_i'\rangle) = \psi_i$$

  and $\sum_i \psi_i = \psi$, we obtain $h(\phi) \leqslant \psi$.
- By letting τ_i be arbitrary and $\tau_j = 0$ for $j \neq i$, we conclude that $\tau_i\lceil \mathsf{post}(\phi_i)\rceil \leqslant \tau_i\lceil \mathsf{post}(\psi_i)\rceil$ for any test τ_i, implying that $\mathsf{post}(\phi_i) \sqsubseteq_{\text{may}} \mathsf{post}(\psi_i)$. Observing that $\mathsf{post}(\phi_i) = \phi(\langle a_i, \sigma_i'\rangle) * \sigma_i'$ and that $\mathsf{post}(\psi_i) = \phi(\langle a_i, \sigma_i'\rangle) * h(\langle a_i, \sigma_i'\rangle)$ we have proven this case, which concludes the proof.

Proof of Claim. It remains to prove the claim. The proof relies crucially on the fact that Ψ is a convex set. To exploit this convexity, we will employ Hahn–Banach's theorem from functional analysis, which assumes that tests and steps are elements in a topological vector space. We must therefore develop some machinery which relates tests and steps with a topological vector space. Here, we define how this can be done.

Let T be a universal set containing all test states in any test. Identify test states which are isomorphic in the sense that the finite trees which they can reach are isomorphic. Let a *test combination* be a finite linear combination $\sum_{i=i}^{k} \alpha_i * t_i$ of different test states $t_1, \ldots, t_k$ where $\alpha_1, \ldots, \alpha_k$ are arbitrary (nonnegative or negative) real numbers. Let 0 denote the empty test combination. Let $\bar{\mathscr{T}}$ be the set of n-tuples $\bar{\tau} = \langle \tau_1, \ldots, \tau_n \rangle$ of test combinations. The set $\bar{\mathscr{T}}$ is a linear vector space if we define $\alpha\bar{\tau} + \beta\bar{\tau}'$ for arbitrary real numbers α and β as the tuple $\langle \tau_1'', \ldots, \tau_n'' \rangle$ where τ_i'' is $\alpha * \tau_i + \beta * \tau_i'$. We note that $\bar{\mathscr{T}}$ can be spanned from basis vectors of form $\langle 0, \ldots, t, \ldots, 0 \rangle$ where all components except one are 0, and t is an arbitrary test state in an arbitrary position. We note that a test combination $\sum_{i=i}^{k} \alpha_i * t_i$ in which all α_i are nonnegative and $\sum_{i=i}^{k} \alpha_i \leqslant 1$ can be viewed as a test, and vice versa that any test can be viewed as such a test combination.

Let $\mathscr{F}$ be the set of linear functionals on $\bar{\mathscr{T}}$. Each linear functional is uniquely determined by its value on the basis vectors in $\bar{\mathscr{T}}$, as defined in the previous paragraph. The set $\mathscr{F}$ is also a linear vector space, which we equip with the topology of pointwise convergence. This means that an infinite sequence $f_1, f_2, f_3, \ldots$ of functionals converges to a limit f iff for each $\bar{\tau} \in \bar{\mathscr{T}}$, the sequence $f_1(\bar{\tau}), f_2(\bar{\tau}), f_3(\bar{\tau}), \ldots$ converges to $f(\bar{\tau})$. It is a result of functional analysis (e.g., [26, Chapter 3]), that the space of *continuous* functionals on $\mathscr{F}$ is the same as $\bar{\mathscr{T}}$, using the identification $\bar{\tau}(f) = f(\bar{\tau})$ for $\bar{\tau} \in \bar{\mathscr{T}}$ and $f \in \mathscr{F}$.

Each $\langle \psi_1, \ldots, \psi_n \rangle \in \Psi$ can be viewed as a linear functional on $\bar{\mathscr{T}}$, defined by $\langle \psi_1, \ldots, \psi_n \rangle(\langle 0, \ldots, t, \ldots, 0 \rangle) = t\lceil \mathsf{post}(\psi_i) \rceil$, where t is the ith component of $\langle 0, \ldots, t, \ldots, 0 \rangle$. In particular, for a tuple $\langle \tau_1, \ldots, \tau_n \rangle$ of test distributions $\langle \psi_1, \ldots, \psi_n \rangle(\langle \tau_1, \ldots, \tau_n \rangle = \sum_{i=1}^{n} a_i.\tau_i \lceil \mathsf{post}(\psi_i) \rceil$. Similarly, we can view $\langle \phi_1, \ldots, \phi_n \rangle$ as a linear functional on $\bar{\mathscr{T}}$, defined by $\langle \phi_1, \ldots, \phi_n \rangle(\langle 0, \ldots, t, \ldots, 0 \rangle) = t\lceil \mathsf{post}(\phi_i) \rceil$.

Now define $\Psi\downarrow$ as the set of linear functionals f on $\bar{\mathscr{T}}$ for which there is a $\langle \psi_1, \ldots, \psi_n \rangle$ in Ψ such that

$$f(\langle 0, \ldots, t, \ldots, 0 \rangle) \leqslant \langle \psi_1, \ldots, \psi_n \rangle(\langle 0, \ldots, t, \ldots, 0 \rangle)$$

for each basis vector $\langle 0, \ldots, t, \ldots, 0 \rangle$. We note that $\Psi \subseteq \Psi\downarrow$, and that a functional which maps each basis vector to a nonpositive value is in $\Psi\downarrow$. The important property of $\Psi\downarrow$ is that it is a convex and closed set of functionals. This follows from the fact that Ψ is convex and compact.

We now claim that $\langle \phi_1, \ldots, \phi_n \rangle \in \Psi\downarrow$. Namely, if $\langle \phi_1, \ldots, \phi_n \rangle \notin \Psi\downarrow$, then by the Hahn–Banach theorem [26, Chapter 3] there is a continuous functional f on $\mathscr{F}$ such that $f(\langle \phi_1, \ldots, \phi_n \rangle) > f(\langle \psi_1, \ldots, \psi_n \rangle)$ for any $\langle \psi_1, \ldots, \psi_n \rangle \in \Psi\downarrow$. Since the continuous functionals on $\mathscr{F}$ are given by $\bar{\mathscr{T}}$, this means that there is a tuple $\langle \tau_1, \ldots, \tau_n \rangle$ in $\bar{\mathscr{T}}$ such that

$$\langle \phi_1, \ldots, \phi_n \rangle(\langle \tau_1, \ldots, \tau_n \rangle) > \langle \psi_1, \ldots, \psi_n \rangle(\langle \tau_1, \ldots \tau_n \rangle)$$

for any $\langle \psi_1, \ldots, \psi_n \rangle \in \Psi\downarrow$. The tuple $\langle \tau_1, \ldots, \tau_n \rangle$ must furthermore be a linear combination of basis vectors, in which the coefficient for each basis vector is nonnegative; otherwise if the coefficient in $\langle \tau_1, \ldots, \tau_n \rangle$ which corresponds to some basis vector $\langle 0, \ldots, t, \ldots, 0 \rangle$ is negative, then the functional f which maps $\langle 0, \ldots, t, \ldots, 0 \rangle$ to $-K$ and all other basis vectors to 0 is in $\Psi\!\downarrow$ for arbitrary $K > 0$. If K is sufficiently large, we get

$$\langle \phi_1, \ldots, \phi_n \rangle (\langle \tau_1, \ldots, \tau_n \rangle) \leqslant f(\langle \tau_1, \ldots, \tau_n \rangle),$$

thus violating the conclusion of the Hahn–Banach theorem. Since $\langle \tau_1, \ldots, \tau_n \rangle$ has only nonnegative coefficients, we can rescale it by a constant factor so that $\sum_{i=1}^{n} a_i.\tau_i \langle \tau_1, \ldots, \tau_n \rangle$ becomes a test. However, then the conclusion of the Hahn–Banach theorem contradicts the fact that there is a $\langle \psi_1, \ldots, \psi_n \rangle \in \Psi$ such that

$$\langle \phi_1, \ldots, \phi_n \rangle (\langle \tau_1, \ldots, \tau_n \rangle) \leqslant \langle \psi_1, \ldots, \psi_n \rangle (\langle \tau_1, \ldots, \tau_n \rangle) = \sum_{i=1}^{n} a_i.\tau_i \langle \tau_1, \ldots, \tau_n \rangle \lceil \rho \rceil .$$

Having proved that $\langle \phi_1, \ldots, \phi_n \rangle \in \Psi\!\downarrow$, we conclude that there is a $\langle \psi_1, \ldots, \psi_n \rangle \in \Psi$ such that

$$\langle \phi_1, \ldots, \phi_n \rangle (\langle \tau_1, \ldots, \tau_n \rangle) \leqslant \langle \psi_1, \ldots, \psi_n \rangle (\langle \tau_1, \ldots, \tau_n \rangle)$$

for each tuple $\langle \tau_1, \ldots, \tau_n \rangle$ of tests. This concludes the proof of the claim. □

5. Comparison with other preorders

For a survey on preorders for probabilistic processes, we refer to [13]. In this section, we relate the existing preorders in the literature to the testing preorder studied in this paper.

As an example, in Fig. 6 we show the initial normal steps of a process $\mathscr{P}$ and the initial normal steps of a process $\mathscr{Q}$. Note that each initial step of $\mathscr{P}$ is also an initial

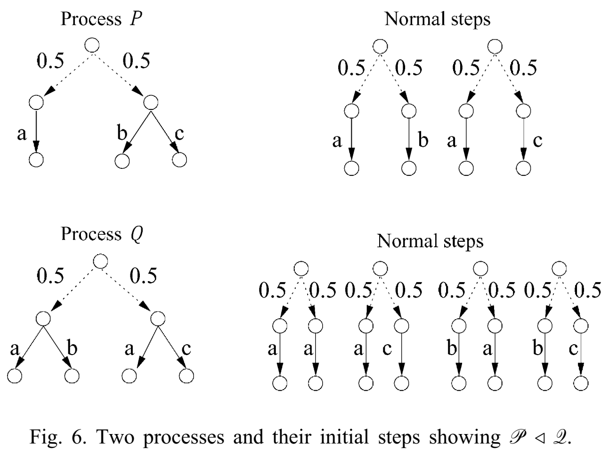

Fig. 6. Two processes and their initial steps showing $\mathscr{P} \lhd \mathscr{Q}$.

step of $\mathscr{Q}$, which implies that $\mathscr{P} \triangleleft \mathscr{Q}$. However, there is no obvious mapping from states of $\mathscr{P}$ to "simulating" states of $\mathscr{Q}$ (the right state of $\mathscr{P}$ cannot be simulated by any state of $\mathscr{Q}$): this is the reason for defining $\triangleleft$ in terms of the initial normal steps of a process.

In [28, 27], a simulation is defined, which can be seen as a specialization of our simulation to the case where the simulated weighting is a state. Using this simulation, processes $\mathscr{P}$ and $\mathscr{Q}$ in Fig. 6 are not comparable. In fact, all the exiting preorders such as probabilistic bisimulation and simulation described in [13] distinguish the two processes.

6. Conclusion

In this paper, we have considered a model of probabilistic transition systems, in which the concept of probabilistic choice is independent from that of nondeterministic choice. We have defined a refinement preorder, based on a notion of testing, where refinement corresponds to an improvement of all possible "worst-case" behaviors of a process. The main result is that this preorder can be described by a notion of probabilistic simulation. For nonprobabilistic systems, this simulation coincides with the standard simulation.

The notion of simulation that we have described is, to our knowledge, not previously described in the literature. In particular, it is coarser than any of the simulation preorders defined by Segala and Lynch [28]. Our results show that it appears to be a natural generalization of standard simulation to the probabilistic setting.

Acknowledgements

Prof. Svante Janson at the Department of Mathematics, Uppsala University, contributed significantly in the application the Hahn–Banach theorem in the proof of the main theorem.

References

[1] S. Abramsky, Observation equivalence as a testing equivalence, Theoret. Comput. Sci. 53 (2,3) (1987) 225–241.

[2] I. Christoff, Testing equivalences and fully abstract models for probabilistic processes, in: Baeten (Ed.), Proc. CONCUR, Amsterdam, Vol. 458, Lecture Notes in Computer Science, Springer, Berlin, 1990, pp. 126–140.

[3] R. Cleaveland, S. Smolka, A. Zwarico, Testing preorders for probabilistic processes, in Proc. ICALP '92, 1992.

[4] C. Courcoubetis, M. Yannakakis, The complexity of probabilistic verification, in Proc. 29th Ann. Symp. Foundations of Computer Science 1988 pp. 338–345.

[5] R. de Nicola, M. Hennessy, Testing equivalences for processes, Theoret. Comput. Sci. 34 (1984) 83–133.

[6] A. Giacalone, C. Jou, S.A. Smolka, Algebraic reasoning for probabilistic concurrent systems, in Proc. IFIP TC2 Working Conf. on Programming Concepts and Methods, Sea of Galilee, April 1990.
[7] H. Hansson, B. Jonsson, A calculus for communicating systems with time and probabilities, in Proc. 11th IEEE Real-Time Systems Symp. Orlando FL 1990.
[8] H. Hansson, B. Jonsson, A logic for reasoning about time and reliability., Formal Aspects Comput. 6 (1994) 512–535.
[9] S. Hart, M. Sharir, Probabilistic temporal logics for finite and bounded models, in Proc. 16th ACM Symp. on Theory of Computing, 1984, pp. 1–13.
[10] B. Jonsson, Simulations between specifications of distributed systems, in Proc. CONCUR '91, Theories of Concurrency: Unification and Extension, Vol. 527, Lecture Notes in Computer Science, Springer, Amsterdam, Holland, 1991.
[11] B. Jonsson C. Ho-Stuart, W. Yi, Testing and refinement for nondeterministic and probabilistic processes, in: Langmaack, de Roever, Vytopil (Eds.), Formal Techniques in Real-Time and Fault-Tolerant Systems, Vol. 863, Lecture Notes in Computer Science, Springer, Berlin, 1994, pp. 418–430.
[12] B. Jonsson, K. Larsen, Specification and refinement of probabilistic processes, in Proc. 6th IEEE Int. Symp. on Logic in Computer Science, Amsterdam, Holland, July 1991.
[13] B. Jonsson, K. Larsen, W. Yi, Probabilistic extensions in: process algebra, in Handbook of Process Algebra, Elsevier, Amsterdam, 2000, to appear.
[14] B. Jonsson, W. Yi, Compositional testing preorders for probabilistic processes, in Proc. 10th IEEE Internat. Symp. on Logic in Computer Science, 1995, pp. 431–441.
[15] B. Jonsson, W. Yi, Fully abstract characterization of probabilistic may testing, in: Katoen (Ed.), ARTS'99, Formal Methods for Real-Time and Probabilistic Systems, 5th Internat. AMAST Workshop, Vol. 1601, Lecture Notes in Computer Science, Springer, Berlin, 1999, pp. 1–18.
[16] D. Kozen, A probabilistic pdl, in Proc. 15th ACM Symp. on Theory of Computing, 1983, pp. 291–297.
[17] K.G. Larsen, A. Skou, Bisimulation through probabilistic testing, Inform. Control 94 (1) (1991) 1–28.
[18] Gavin Lowe, Probabilities and Priorities in Timed CSP, D.Phil Thesis, Oxford, 1993.
[19] Z. Manna, A. Pnueli, The anchored version of the temporal framework, in: de Bakker, de Roever, Rozenberg (Eds.), Linear Time, Branching Time and Partial Order in Logics and Models for Concurrency, Vol. 354, Lecture Notes in Computer Science, Springer, Berlin, 1989, pp. 201–284.
[20] R. Milner, Communication and Concurrency, Prentice-Hall, Englewood Cliffs, NJ, 1989.
[21] M.K. Molloy, Performance analysis using stochastic Petri nets, IEEE Trans. Comput. C-31 (9) (1982) 913–917.
[22] G. Plotkin, A structural approach to operational semantics, Technical Report DAIMI FN-19, Computer Science Department, Aarhus University, Denmark, 1981.
[23] A. Pnueli, L. Zuck, Verification of multiprocess probabilistic protocols, Distr. Comput. 1 (1) (1986) 53–72.
[24] S. Purushothaman, P.A. Subrahmanyam, Reasoning about probabilistic behavior in concurrent systems, IEEE Trans. Software Eng. SE-13 (6) (1989) 740–745.
[25] M.O. Rabin, Probabilistic automata, Inform. Control 6 (1963) 230–245.
[26] W. Rudin, Functional Analysis, McGraw-Hill, New York, 1991.
[27] R. Segala, A compositional trace-based semantics for probabilistic automata, in Proc. CONCUR '95, 6th Int. Conf. on Concurrency Theory, Vol. 962, Lecture Notes in Computer Science, Springer, Berlin, 1995, pp. 234–248.
[28] R. Segala, N.A. Lynch, Probabilistic simulations for probabilistic processes, Nordic J. Comput. 2 (2) (1995) 250–273.
[29] R. van Glabbeek, S.A. Smolka, B. Steffen, C. Tofts, Reactive, generative, and stratified models of probabilistic processes, in Proc. 5th IEEE Int. Symp. on Logic in Computer Science, 1990, pp. 130–141.
[30] M.Y. Vardi, P. Wolper, An automata-theoretic approach to automatic program verification, in Proc. 1st IEEE Int. Symp. on Logic in Computer Science, 1986, pp. 332–344.
[31] M.Y. Vardi, Automatic verification of probabilistic concurrent finite-state programs, in Proc. 26th Ann. Symp. Foundations of Computer Science, 1985, pp. 327–338.
[32] S.-H. Wu, S.A. Smolka, E.W. Stark, Composition and behaviors of probabilistic I/O-Automata, Theoret. Comput. Sci. 176 (1–2) (1997) 1–37.

[33] W. Yi, Algebraic reasoning for real-time probabilistic processes with uncertain information, in: Langmaack, de Roever, Vytopil (Eds.), Formal Techniques in Real-Time and Fault-Tolerant Systems, Vol. 863, Lecture Notes in Computer Science, Springer, Berlin, 1994, pp. 680–693.

[34] Wang Yi, K. Larsen, Testing probabilistic and nondeterministic processes, in Protocol Specification, Testing, and Verification, Vol. XII, 1992.

[35] S. Yuen, R. Cleaveland, Z. Dayar, S.A. Smolka, Fully abstract characterizations of testing preorders for probabilistic processes, in: Jonsson, Parrow (Eds.), Proc. CONCUR '94, 5th Int. Conf. on Concurrency Theory, Vol. 836, Lecture Notes in Computer Science, Springer, Berlin, 1994, pp. 497–512.