A Complete Axiomatization of Branching Bisimilarity for a Simple Process Language with Probabilistic Choice

R.J. van Glabbeek [1,2], J.F. Groote [3], and E.P. de Vink [3]

[1] Data61, CSIRO, Sydney, Australia
[2] Computer Science and Engineering, University of New South Wales, Australia
[3] Department of Mathematics and Computer Science,
Eindhoven University of Technology, Eindhoven, The Netherlands
rvg@cs.stanford.edu, J.F.Groote@tue.nl, evink@win.tue.nl

Abstract. This paper proposes a notion of branching bisimilarity for non-deterministic probabilistic processes. In order to characterize the corresponding notion of rooted branching probabilistic bisimilarity, an equational theory is proposed for a basic, recursion-free process language with non-deterministic as well as probabilistic choice. The proof of completeness of the axiomatization builds on the completeness of strong probabilistic bisimilarity on the one hand and on the notion of a concrete process, i.e. a process that does not display (partially) inert τ-moves, on the other hand. The approach is first presented for the non-deterministic fragment of the calculus and next generalized to incorporate probabilistic choice, too.

This paper is dedicated to Catuscia Palamidessi, on the occasion of her 60th birthday. An extended abstract appears in [16].

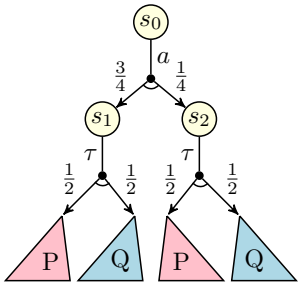
1 Introduction

In [11], in a setting of a process language featuring both non-deterministic and probabilistic choice, Yuxin Deng and Catuscia Palamidessi propose an equational theory for a notion of weak bisimilarity and prove its soundness and completeness. Not surprisingly, the axioms dealing with a silent step are reminiscent to the well-known τ-laws of Milner [26,27]. The process language treated in [11] includes recursion, thereby extending the calculus and axiomatization of [6]. While the weak transitions of [11] can be characterized as finitary, infinitary semantics is treated in [15], providing a sound and complete axiomatization also building on the seminal work of Milner [27].

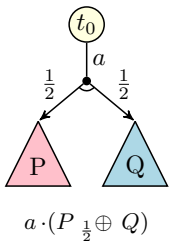
In this paper we focus on branching bisimilarity in the sense of [17], rather than on weak bisimilarity as in [6,11,15]. In the non-probabilistic setting branching bisimilarity has the advantage over weak bisimilarity that it has far more efficient algorithms [18,19]. Furthermore, it has a strong logical underpinning [9]. It would be very attractive to have these advantages available also in the probabilistic case, where model checking is more demanding. See also the initial work reported in [21].

For a similarly basic process language as in [11], without recursion though, we propose a notion of branching probabilistic bisimilarity as well as a sound and complete equational axiomatization. Hence, instead of lifting all τ-laws to the probabilistic setting, we only need to do this for the B-axiom of [17], the single axiom capturing inert silent steps. For what is referred to as the alternating model [22], branching probabilistic bisimilarity has been studied in [2,3]. Also [28] discusses branching probabilistic bisimilarity. However, the proposed notions of branching bisimilarity are either no congruence for the parallel operator, or they invalidate the identities below which we desire. The paper [1] proposes a complete theory for a variant of branching bisimilarity that is not consistent with the first τ-law unfortunately.

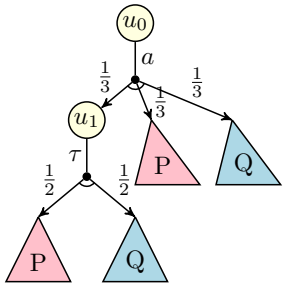
Our investigation is led by the wish to identify the three processes below, involving as a subprocess a probabilistic choice between P and Q. Essentially, ignoring the occurrence of the action a involved, the three processes represent (i) a probabilistic choice of weight $\frac{3}{4}$ between to instances of the subprocess mentioned, (ii) the subprocess on its own, and (iii) a probabilistic choice of weight $\frac{1}{3}$ for the subprocess and a rescaling of the subprocess, in part overlapping.



$a \cdot \Big(\partial\big(\tau \cdot (P \mathrel{_{\frac{1}{2}}\!\oplus} Q)\big) \mathrel{_{\frac{3}{4}}\!\oplus} \partial\big(\tau \cdot (P \mathrel{_{\frac{1}{2}}\!\oplus} Q)\big)\Big)$



$a \cdot (P \mathrel{_{\frac{1}{2}}\!\oplus} Q)$



$a \cdot \Big(\partial\big(\tau \cdot (P \mathrel{_{\frac{1}{2}}\!\oplus} Q)\big) \mathrel{_{\frac{1}{3}}\!\oplus} (P \mathrel{_{\frac{1}{2}}\!\oplus} Q)\Big)$

In our view, all three processes starting from s_0, t_0, and u_0 are equivalent. The behavior that can be observed from them when ignoring τ-steps and coin tosses to resolve probabilistic choices is the same. This leads to a definition of probabilistic branching bisimilarity that hitherto was not proposed in the literature and appears to be the pendant of weak distribution bisimilarity defined by [13].

As for [11] we seek to stay close to the treatment of the non-deterministic fragment of the process calculus at hand. However, as an alternate route in proving completeness, we rely on the definition of a concrete process. We first apply the approach for strictly non-deterministic processes and *mutatis mutandis* for the whole language allowing processes that involve both non-deterministic and probabilistic choice. For now, let's call a process concrete if it doesn't exhibit inert transitions, i.e. τ-transitions that don't change the potential behavior of the process essentially. The approach we follow first establishes soundness for branching (probabilistic) bisimilarity and soundness and completeness for strong (probabilistic) bisimilarity. Because of the non-inertness of the silent steps involved, strong and branching bisimilarity coincide for concrete processes. The

trick then is to relate a pair of branching (probabilistically) bisimilar processes to a corresponding pair of concrete processes. Since these are also branching (probabilistically) bisimilar as argued, they are consequently strongly (probabilistically) bisimilar, and, voilà, provably equal by the completeness result for strong (probabilistic) bisimilarity.

The remainder of the paper is organized as follows. In Section 2 we gather some notation regarding probability distributions. For illustration purposes Section 3 treats the simpler setting of non-deterministic processes reiterating the completeness proof for the equational theory of [17] for rooted branching bisimilarity. Next, after introducing branching probabilistic bisimilarity and some of its fundamental properties in Sections 4 and 5, respectively, in Section 6 we prove the main result, viz. the completeness of an equational theory for rooted branching probabilistic bisimilarity, following the same lines set out in Section 3. In Section 7 we wrap up and make concluding remarks.

2 Preliminaries

Let $\mathit{Distr}(X)$ be the set of distributions over the set X of finite support. The support of a distribution μ is denoted as $\mathit{spt}(\mu)$. Each distribution $\mu \in \mathit{Distr}(X)$ can be represented as $\mu = \bigoplus_{i\in I} p_i * x_i$ when $\mu(x_i) = p_i$ for $i \in I$ and $\sum_{i\in I} p_i = 1$. We assume I to be a finite index set. In concrete cases, when no confusion arises, the separator $*$ is omitted from the notation. For convenience later, we do not require $x_i \neq x_{i'}$ for $i \neq i'$ nor $p_i > 0$ for $i, i' \in I$.

We use $\delta(x)$ to denote the Dirac distribution for $x \in X$. For $\mu, \nu \in \mathit{Distr}(X)$ and $r \in [0, 1]$ we define $\mu \,{}_r\!\oplus\, \nu \in \mathit{Distr}(X)$ by $(\mu \,{}_r\!\oplus\, \nu)(x) = r \cdot \mu(x) + (1-r) \cdot \nu(x)$. By definition $\mu \,{}_0\!\oplus\, \nu = \nu$ and $\mu \,{}_1\!\oplus\, \nu = \mu$. For an index set I, $p_i \in [0, 1]$ and $\mu_i \in \mathit{Distr}(X)$, we define $\bigoplus_{i\in I} p_i * \mu_i \in \mathit{Distr}(X)$ by $(\bigoplus_{i\in I} p_i * \mu_i)(x) = \sum_{i\in I} p_i \cdot \mu_i(x)$ for $x \in X$. For $\mu = \bigoplus_{i\in I} p_i * \mu_i$, $\nu = \bigoplus_{i\in I} p_i * \nu_i$, and $r \in [0, 1]$ it holds that $\mu \,{}_r\!\oplus\, \nu = \bigoplus_{i\in I} (\mu_i \,{}_r\!\oplus\, \nu_i)$.

For a binary relation $\mathcal{R} \subseteq \mathit{Distr}(X) \times \mathit{Distr}(X)$ we use $\mathcal{R}^\dagger$ to denote its symmetric closure.

3 Completeness: the non-deterministic case

In this section we present an approach to prove completeness of an axiomatic theory for branching bisimilarity exploiting the notion of a concrete process in the setting of a basic process language. In the remainder of the paper we extend the approach to a process language involving probabilistic choice.

We assume to be given a set of actions $\mathcal{A}$ including the so-called silent action τ. The process language we consider is called a Minimal Process Language in [4]. It provides inaction $\mathbf{0}$, a prefix construct for each action $a \in \mathcal{A}$, and non-deterministic choice.

Definition 3.1 (Syntax). The class $\mathcal{E}$ of non-deterministic processes over $\mathcal{A}$, with typical element E, is given by

$$E ::= \mathbf{0} \mid \alpha \cdot E \mid E + E$$

with actions α from $\mathcal{A}$.

The process $\mathbf{0}$ cannot perform any action, $\alpha \cdot E$ can perform action α and subsequently behave as E, and $E_1 + E_2$ represents the choice in behavior between E_1 and E_2.

For $E \in \mathcal{E}$ we define its complexity $c(E)$ by $c(\mathbf{0}) = 0$, $c(\alpha \cdot E) = c(E) + 1$, and $c(E + F) = c(E) + c(F)$.

The behavior of processes in $\mathcal{E}$ is given by a structured operational semantics going back to [24].

Definition 3.2 (Operational semantics). The transition relation $\rightarrow \subseteq \mathcal{E} \times \mathcal{A} \times \mathcal{E}$ is given by

$$\frac{}{\alpha \cdot E \xrightarrow{\alpha} E}\ (\textsc{pref})$$

$$\frac{E_1 \xrightarrow{\alpha} E_1}{E_1 + E_2 \xrightarrow{\alpha} E_1}\ (\textsc{nd-choice}\,1) \qquad \frac{E_2 \xrightarrow{\alpha} E_2}{E_1 + E_2 \xrightarrow{\alpha} E_2}\ (\textsc{nd-choice}\,2)$$

We have auxiliary definitions and relations derived from the transition relation of Definition 3.2. A process $E' \in \mathcal{E}$ is called a derivative of a process $E \in \mathcal{E}$ iff $E_0, \ldots, E_n \in \mathcal{E}$ and $\alpha_1, \ldots, \alpha_n$ exist such that $E \equiv E_0$, $E_{i-1} \xrightarrow{\alpha_i} E_i$, and $E_n \equiv E'$. We define $der(E) = \{\, E' \in \mathcal{E} \mid E' \text{ derivative of } E \,\}$. Furthermore, for $E, E' \in \mathcal{E}$ and $\alpha \in \mathcal{A}$ we write $E \xrightarrow{(\alpha)} E'$ iff $E \xrightarrow{\alpha} E'$, or $\alpha = \tau$ and $E = E'$. We use $\Rightarrow$ to denote the reflexive transitive closure of $\xrightarrow{(\tau)}$.

The definitions of strong and branching bisimilarity for $\mathcal{E}$ are standard and adapted from [17,26].

Definition 3.3 (Strong and branching bisimilarity).

(a) A symmetric relation $\mathcal{R} \subseteq \mathcal{E} \times \mathcal{E}$ is called a *strong bisimulation relation* iff for all $E, E', F \in \mathcal{E}$ if $E \,\mathcal{R}\, F$ and $E \xrightarrow{\alpha} E'$ then there is an $F' \in \mathcal{E}$ such that

$$F \xrightarrow{\alpha} F' \text{ and } E' \,\mathcal{R}\, F'.$$

(b) A symmetric relation $\mathcal{R} \subseteq \mathcal{E} \times \mathcal{E}$ is called a *branching bisimulation relation* iff for all $E, E', F \in \mathcal{E}$ if $E \,\mathcal{R}\, F$ and $E \xrightarrow{\alpha} E'$, then there are $\bar{F}, F' \in \mathcal{E}$ such that

$$F \Rightarrow \bar{F},\ \bar{F} \xrightarrow{(\alpha)} F',\ E \,\mathcal{R}\, \bar{F}, \text{ and } E' \,\mathcal{R}\, F'.$$

(c) Strong bisimilarity, denoted by $\leftrightarroweq \subseteq \mathcal{E} \times \mathcal{E}$, and branching bisimilarity, written as $\leftrightarroweq_b \subseteq \mathcal{E} \times \mathcal{E}$, are defined as the largest strong bisimulation relation on $\mathcal{E}$ and the largest branching bisimulation relation on $\mathcal{E}$, respectively.

Clearly, in view of the definitions, strong bisimilarity between two processes implies branching bisimilarity between the two processes.

If for a transition $E \xrightarrow{\tau} E'$ we have that $E \leftrightarroweq_b E'$, the transition is called *inert*. A process $\bar{E}$ is called *concrete* iff it has no inert transitions, i.e., if $E' \in der(\bar{E})$ and $E' \xrightarrow{\tau} E''$, then $E' \not\leftrightarroweq_b E''$. We write $\mathcal{E}_{cc} = \{\, \bar{E} \in \mathcal{E} \mid \bar{E} \text{ concrete} \,\}$.

Next we introduce a restricted form of branching bisimilarity, called rooted branching bisimilarity, instigated by the fact that branching bisimilarity itself is not a congruence for the choice operator. This makes branching bisimilarity unsuitable for equational reasoning where it is natural to replace subterms by equivalent terms. Note that weak bisimilarity has the same problem [26].

For example, we have for any process E that E and $\tau \cdot E$ are branching bisimilar, but in the context of a non-deterministic alternative they may not, i.e., it is not necessarily the case $E + F \leftrightarroweq_b \tau \cdot E + F$. More concretely, although $\mathbf{0} \leftrightarroweq_b \tau \cdot \mathbf{0}$, it does not hold that $\mathbf{0} + b \cdot \mathbf{0} \leftrightarroweq_b \tau \cdot \mathbf{0} + b \cdot \mathbf{0}$. The τ-move of $\tau \cdot \mathbf{0} + b \cdot \mathbf{0}$ to $\mathbf{0}$ has no counterpart in $\mathbf{0} + b \cdot \mathbf{0}$ because $\mathbf{0} + b \cdot \mathbf{0} \not\leftrightarroweq_b \mathbf{0}$.

Definition 3.4. A symmetric $\mathcal{R} \subseteq \mathcal{E} \times \mathcal{E}$ is called a rooted branching bisimulation relation iff for all $E, F \in \mathcal{E}$ such that $E \,\mathcal{R}\, F$ it holds that if $E \xrightarrow{\alpha} E'$ for $\alpha \in \mathcal{A}$, $E' \in \mathcal{E}$ then $F \xrightarrow{\alpha} F'$ and $E' \leftrightarroweq_b F'$ for some $F' \in \mathcal{E}$. Rooted branching bisimilarity, denoted by $\leftrightarroweq_{rb} \subseteq \mathcal{E} \times \mathcal{E}$, is defined as the largest rooted branching bisimulation relation.

The definition of rooted branching bisimilarity boils down to calling processes $E, F \in \mathcal{E}$ rooted branching bisimilar, notation $E \leftrightarroweq_{rb} F$, iff (i) $E \xrightarrow{\alpha} E'$ implies $F \xrightarrow{\alpha} F'$ and $E' \leftrightarroweq_b F'$ for some $F' \in \mathcal{E}$ and, vice versa, (ii) $F \xrightarrow{\alpha} F'$ implies $E \xrightarrow{\alpha} E'$ and $E' \leftrightarroweq_b F'$ for some $E' \in \mathcal{E}$. The formulation of Definition 3.4 for the nondeterministic processes of this section corresponds directly to the definition of rooted branching *probabilistic* bisimulation that we will introduce in Section 4, see Definition 4.5.

Direct from the definitions we see $\leftrightarroweq \subseteq \leftrightarroweq_{rb} \subseteq \leftrightarroweq_b$. As implicitly announced we have a congruence result for rooted branching bisimilarity.

Lemma 3.5 ([17]). $\leftrightarroweq_{rb}$ is a congruence on $\mathcal{E}$ for the operators $\cdot$ and $+$.

It is well-known that strong and branching bisimilarity for $\mathcal{E}$ can be equationally characterized [4,17,26].

Definition 3.6 (Axiomatization of $\leftrightarroweq$ and $\leftrightarroweq_{rb}$). The theory AX is given by the axioms A1 to A4 listed in Table 1. The theory AX^b contains in addition the axiom B.

If two processes are provably equal, they are rooted branching bisimilar.

Lemma 3.7 (Soundness). For all $E, F \in \mathcal{E}$, if $AX^b \vdash E = F$ then $E \leftrightarroweq_{rb} F$.

A1	$E + F = F + E$
A2	$(E + F) + G = E + (F + G)$
A3	$E + E = E$
A4	$E + \mathbf{0} = E$
B	$\alpha \cdot (\, F + \tau \cdot (E + F)\,) = \alpha \cdot (E + F)$

Table 1. Axioms for strong and branching bisimilarity

Proof (Sketch). First one shows that the left-hand side and the right-hand side of the axioms of AX^b are rooted branching bisimilar. Next, one observes that rooted branching bisimilarity is a congruence. □

It is well-known that strong bisimilarity is equationally characterized by the axioms A1 to A4 of Table 1.

Theorem 3.8 (AX sound and complete for $\leftrightarrows$). For all processes $E, F \in \mathcal{E}$ it holds that $AX \vdash E = F$ iff $E \leftrightarrows F$.

Proof. See for example [26, Section 7.4]. □

For concrete processes that have no inert transitions, branching bisimilarity and strong bisimilarity coincide. Hence, in view of Theorem 3.8, branching bisimilarity implies equality for AX.

Lemma 3.9. For all concrete $\bar{E}, \bar{F} \in \mathcal{E}_{cc}$, if $\bar{E} \leftrightarrows_b \bar{F}$ then both $\bar{E} \leftrightarrows \bar{F}$ and $AX \vdash \bar{E} = \bar{F}$.

Proof (Sketch). Consider $\bar{E}, \bar{F} \in \mathcal{E}_{cc}$ such that $\bar{E} \leftrightarrows_b \bar{F}$. Let $\mathcal{R}$ be a branching bisimulation relation relating $\bar{E}$ and $\bar{F}$. Define $\mathcal{R}'$ as the restriction of $\mathcal{R}$ to the derivatives of $\bar{E}$ and $\bar{F}$, i.e., $\mathcal{R}' = \mathcal{R} \cap ((der(\bar{E}) \times der(\bar{F})) \cup (der(\bar{F}) \times der(\bar{E})))$. Then $\mathcal{R}'$ is a strong bisimulation relation, since none of the processes involved admits an inert τ-transition. By the completeness of AX, see Theorem 3.8, it follows that $AX \vdash \bar{E} = \bar{F}$. □

We are now in a position to prove the main technical result of this section, viz. that branching bisimilarity implies equality under a prefix. In the proof the notion of a concrete process plays a central role.

Lemma 3.10.

(a) For all processes $E \in \mathcal{E}$, a concrete process $\bar{E} \in \mathcal{E}_{cc}$ exists such that $E \leftrightarrows_b \bar{E}$ and $AX^b \vdash \alpha \cdot E = \alpha \cdot \bar{E}$ for all $\alpha \in \mathcal{A}$.
(b) For all processes $F, G \in \mathcal{E}$, if $F \leftrightarrows_b G$ then $AX^b \vdash \alpha \cdot F = \alpha \cdot G$ for all $\alpha \in \mathcal{A}$.

Proof. We prove statements (a) and (b) by simultaneously induction on $c(E)$ and $\max\{c(F), c(G)\}$, respectively.

Basis, $c(E) = 0$. We have that $E = \mathbf{0} + \cdots + \mathbf{0}$. Hence, take $\bar{E} = \mathbf{0}$. Clearly, part (a) of the lemma holds as $\mathbf{0}$ is concrete, $E \leftrightarrows_b \mathbf{0}$ and $AX^b \vdash \alpha \cdot E = \alpha \cdot \mathbf{0}$ for all $\alpha \in \mathcal{A}$.

Induction step for (a): $c(E) > 0$. The process E can be written as $\sum_{i\in I}\ \alpha_i \cdot E_i$ for some finite I and suitable $\alpha_i \in \mathcal{A}$ and $E_i \in \mathcal{E}$.

First suppose that for some $i_0 \in I$ we have $\alpha_{i_0} = \tau$ and $E_{i_0} \leftrightarrows_b E$. Then $AX \vdash E = H + \tau.E_{i_0}$, where $H := \sum_{i\in I\setminus\{i_o\}} \alpha_i \cdot E_i$. By the induction hypothesis (a), there is a term $\bar{E}_{i_0} \in \mathcal{E}_{cc}$ such that $E_{i_0} \leftrightarrows_b \bar{E}_{i_0}$. We claim that $\bar{E}_{i_0} \leftrightarrows_b E_{i_0} + H$.

For suppose $\bar{E}_{i_0} \xrightarrow{\alpha} F$. Then $E_{i_0} \Rightarrow E'_{i_0} \xrightarrow{(\alpha)} G$ where $\bar{E}_{i_0} \leftrightarrows_b E'_{i_0}$ and $F \leftrightarrows_b G$. In case $E_{i_0} = E'_{i_0}$ it follows that $E_{i_0} \xrightarrow{(\alpha)} G$. Since $\bar{E}_{i_o}$ is concrete, either $\alpha \neq \tau$ or $F \not\leftrightarrows_b \bar{E}_{i_0}$. Hence, $\alpha \neq \tau$ or $G \not\leftrightarrows_b E_{i_0}$. So $E_{i_0} \xrightarrow{\alpha} G$. Consequently, $E_{i_0} + H \xrightarrow{\alpha} G$. In case $E_{i_0} \neq E'_{i_0}$ we have $E_{i_0} + H \Rightarrow E'_{i_0} \xrightarrow{(\alpha)} G$.

Now suppose $E_{i_0} + H \xrightarrow{\alpha} F$. Then either $E_{i_0} \xrightarrow{\alpha} F$ or $H \xrightarrow{\alpha} F$. In the first case we have $\bar{E}_{i_0} \Rightarrow \bar{E}'_{i_0} \xrightarrow{(\alpha)} G$ where $E_{i_0} \leftrightarrows_b \bar{E}'_{i_0}$ and $F \leftrightarrows_b G$, while in the latter case $E \xrightarrow{\alpha} F$, and since $E \leftrightarrows_b E_{i_0} \leftrightarrows_b \bar{E}_{i_0}$ we have $\bar{E}_{i_0} \Rightarrow \bar{E}'_{i_0} \xrightarrow{(\alpha)} G$ where $E \leftrightarrows_b \bar{E}'_{i_0}$ and $F \leftrightarrows_b G$. Because $\bar{E}_{i_0}$ is concrete, $\bar{E}'_{i_o} = \bar{E}_{i_0}$. Thus $\bar{E}_{i_0} \xrightarrow{(\alpha)} G$ with $F \leftrightarrows_b G$, which was to be shown.

Hence $E_{i_0} \leftrightarrows_b \bar{E}_{i_0} \leftrightarrows_b E_{i_0} + H$. Clearly $c(E_{i_0}), c(E_{i_0} + H) < c(E)$. Therefore, by the induction hypothesis (b), $AX^b \vdash \tau \cdot E_{i_0} = \tau \cdot (E_{i_0} + H)$. By the induction hypothesis (a), there is a term $\bar{E} \in \mathcal{E}_{cc}$ such that $\bar{E} \leftrightarrows_b E_{i_0} + H$ and $AX^b \vdash \alpha \cdot \bar{E} = \alpha \cdot (E_{i_0} + H)$. Now we have $E \leftrightarrows_b E_{i_0} \leftrightarrows_b E_{i_0} + H \leftrightarrows_b \bar{E}$. Therefore,

$$\begin{aligned} AX^b \vdash \alpha \cdot E &= \alpha \cdot (H + \tau \cdot E_{i_0}) \\ &= \alpha \cdot (H + \tau \cdot (E_{i_0} + H)) && \text{(since } AX^b \vdash \tau \cdot E_{i_0} = \tau \cdot (E_{i_0} + H)\text{)} \\ &= \alpha \cdot (E_{i_0} + H) && \text{(use axiom B)} \\ &= \alpha \cdot \bar{E} && \text{(by the choice of } \bar{E}\text{)}. \end{aligned}$$

Hence, we have shown the existence of a desired process $\bar{E}$ with the required properties.

Now suppose, for all $i \in I$ we have $\alpha_i \neq \tau$ or $E_i \not\leftrightarrows_b E$. Clearly $c(E_i) < c(E)$ for all $i \in I$. By the induction hypothesis we can find, for all $i \in I$, concrete $\bar{E}_i$ such that $\bar{E}_i \leftrightarrows_b E_i$ and $AX^b \vdash \alpha \cdot \bar{E}_i = \alpha \cdot E_i$ for all $\alpha \in \mathcal{A}$. Define $\bar{E} = \sum_{i\in I}\ \alpha_i \cdot \bar{E}_i$. Then $\bar{E} \leftrightarrows_b E$ and $\bar{E}$ is concrete too, since $\bar{E}_i \leftrightarrows_b E_i \not\leftrightarrows_b E \leftrightarrows_b \bar{E}$ for $i \in I$ in case $\alpha_i = \tau$. Moreover, $AX^b \vdash E = \bar{E}$, since $E = \sum_{i\in I}\ \alpha_i \cdot E_i = \sum_{i\in I}\ \alpha_i \cdot \bar{E}_i = \bar{E}$. Hence, for $\alpha \in \mathcal{A}$, $AX^b \vdash \alpha \cdot E = \alpha \cdot \bar{E}$.

Both the base and the induction step for (b): $\max\{c(F), c(G)\} \geqslant 0$. Suppose $F \leftrightarrows_b G$. Pick $\bar{F}, \bar{G} \in \mathcal{E}_{cc}$ such that $F \leftrightarrows_b \bar{F}$ and $AX^b \vdash \alpha \cdot F = \alpha \cdot \bar{F}$ for all $\alpha \in \mathcal{A}$, and similarly for G and $\bar{G}$. Then we have $\bar{F} \leftrightarrows_b \bar{G}$. Since $\bar{F}$ and $\bar{G}$ are concrete it follows that $AX \vdash \bar{F} = \bar{G}$, see Lemma 3.9. Now pick any $\alpha \in \mathcal{A}$. Then we have $AX^b \vdash \alpha \cdot F = \alpha \cdot \bar{F} = \alpha \cdot \bar{G} = \alpha \cdot G$. □

By now we have gathered sufficient building blocks to prove the main result of this section.

Theorem 3.11 (AX^b sound and complete for $\leftrightarrows_{rb}$). For all processes $E, F \in \mathcal{E}$ it holds that $E \leftrightarrows_{rb} F$ iff $AX^b \vdash E = F$.

Proof. In view of Lemma 3.7 we only need to prove completeness of AX^b for rooted branching bisimilarity. Suppose $E, F \in \mathcal{E}$ and $E \leftrightarrows_{rb} F$. Let $E =$

$\sum_{i\in I}\ \alpha_i \cdot E_i$ and $F = \sum_{j\in J}\ \beta_j \cdot F_j$ for suitable index sets I and J, $\alpha_i, \beta_j \in \mathcal{A}$, $E_i, F_j \in \mathcal{E}$. Since $E \leftrightarrows_{rb} F$ we have (i) for all $i \in I$ there is a $j \in J$ such that $\alpha_i = \beta_j$ and $E_i \leftrightarrows_b F_j$, and, symmetrically, (ii) for all $j \in J$ there is an $i \in I$ such that $\alpha_i = \beta_j$ and $E_i \leftrightarrows_b F_j$. Put $K = \{\, (i,j) \in I \times J \mid (\alpha_i = \beta_j) \wedge (E_i \leftrightarrows_b F_j) \,\}$. Define the processes $G, H \in \mathcal{E}$ by

$$G = \textstyle\sum_{k\in K}\ \gamma_k \cdot G_k \quad \text{and} \quad H = \sum_{k\in K}\ \zeta_k \cdot H_k$$

where, for $i \in I$, $\gamma_k = \alpha_i$ and $G_k \equiv E_i$ if $k = (i,j)$ for some $j \in J$, and, similarly for $j \in J$, $\zeta_k = \beta_j$ and $H_k \equiv F_j$ if $k = (i,j)$ for some $i \in I$. Then G and H are well-defined. Moreover, $AX \vdash E = G$ and $AX \vdash F = H$.

For $k \in K$, say $k = (i,j)$, it holds that $\gamma_k = \alpha_i = \beta_j = \zeta_k$ and $G_k \equiv E_i \leftrightarrows_b F_j \equiv H_k$, by definition of K. By Lemma 3.10b we obtain, for all $k \in K$, $AX^b \vdash \gamma_k \cdot G_k = \zeta_k \cdot H_k$. From this we get

$$AX^b \vdash E = \textstyle\sum_{i\in I}\ \alpha_i \cdot E_i = \sum_{k\in K}\ \gamma_k \cdot G_k = \sum_{k\in K}\ \zeta_k \cdot H_k = \sum_{j\in J}\ \beta_j \cdot F_j = F$$

which concludes the proof of the theorem. □

4 Branching bisimilarity for probabilistic processes

In this section we define branching bisimilarity for probabilistic processes.

Following [6], we start with adapting the syntax of processes, now distinguishing non-deterministic processes $E \in \mathcal{E}$ and probabilistic processes $P \in \mathcal{P}$.

Definition 4.1 (Syntax). The classes $\mathcal{E}$ and $\mathcal{P}$ of non-deterministic and probabilistic processes over $\mathcal{A}$, respectively, ranged over by E and P, are given by

$$E ::= \mathbf{0} \mid \alpha \cdot P \mid E + E$$
$$P ::= \partial(E) \mid P\ {}_r\!\oplus\ P$$

with actions α from $\mathcal{A}$ where $r \in (0,1)$.

The probabilistic process $P_1\ {}_r\!\oplus\ P_2$ executes the behavior of P_1 with probability r and the behavior P_2 with probability $1-r$. By convention, $P\ {}_1\!\oplus\ Q$ denotes P and $P\ {}_0\!\oplus\ Q$ denotes Q.

We again introduce the complexity measure c, now for non-deterministic and probabilistic processes, based on the depth of a process. The complexity measure $c : \mathcal{E} \cup \mathcal{P} \to \mathbb{N}$ is given by $c(\mathbf{0}) = 0$, $c(\alpha \cdot P) = c(P) + 1$, $c(E + F) = c(E) + c(F)$, and $c(\partial(E)) = c(E) + 1$, $c(P\ {}_r\!\oplus\ Q) = c(P) + c(Q)$.

As usual SOS semantics for $\mathcal{E}$ and $\mathcal{P}$ makes use of two types of transition relations [22,6].

Definition 4.2 (Operational semantics).

(a) The transition relations $\rightarrow \subseteq \mathcal{E} \times \mathcal{A} \times \mathit{Distr}(\mathcal{E})$ and $\mapsto \subseteq \mathcal{P} \times \mathit{Distr}(\mathcal{E})$ are given by

$$\frac{P \mapsto \mu}{\alpha \cdot P \xrightarrow{\alpha} \mu}\,(\textsc{pref})$$

$$\frac{E_1 \xrightarrow{\alpha} \mu_1}{E_1 + E_2 \xrightarrow{\alpha} \mu_1}\,(\textsc{nd-choice}\,1) \qquad \frac{E_2 \xrightarrow{\alpha} \mu_2}{E_1 + E_2 \xrightarrow{\alpha} \mu_2}\,(\textsc{nd-choice}\,2)$$

$$\frac{}{\partial(E) \mapsto \delta(E)}\,(\textsc{Dirac}) \qquad \frac{P_1 \mapsto \mu_1 \quad P_2 \mapsto \mu_2}{P_1 \,{}_r\!\oplus\, P_2 \mapsto \mu_1 \,{}_r\!\oplus\, \mu_2}\,(\textsc{p-choice})$$

(b) The transition relation $\rightarrow \subseteq \mathit{Distr}(\mathcal{E}) \times \mathcal{A} \times \mathit{Distr}(\mathcal{E})$ is such that $\mu \xrightarrow{\alpha} \mu'$ whenever $\mu = \bigoplus_{i \in I} p_i * E_i$, $\mu' = \bigoplus_{i \in I} p_i * \mu'_i$, and $E_i \xrightarrow{\alpha} \mu'_i$ for all $i \in I$.

With $[\![P]\!]$, for $P \in \mathcal{P}$, we denote the unique distribution μ such that $P \mapsto \mu$.

The transition relation $\rightarrow$ on distributions allows for a probabilistic combination of non-deterministic alternatives resulting in a so-called combined transition, cf. [29,28]. For example, for $E \equiv a \cdot (P \,{}_{1/2}\!\oplus\, Q) + a \cdot (P \,{}_{1/3}\!\oplus\, Q)$, the Dirac process $\delta(E) \equiv \delta(a \cdot (P \,{}_{1/2}\!\oplus\, Q) + a \cdot (P \,{}_{1/3}\!\oplus\, Q))$ provides an a-transition to $[\![P \,{}_{1/2}\!\oplus\, Q]\!]$ as well as an a-transition to $[\![P \,{}_{1/3}\!\oplus\, Q]\!]$. However, since for distribution $\delta(E)$ it holds that $\delta(E) = \frac{1}{2}\delta(E) \oplus \frac{1}{2}\delta(E)$ there is also a transition

$$\delta(E) = \tfrac{1}{2}\delta(E) \oplus \tfrac{1}{2}\delta(E) \xrightarrow{a} \tfrac{1}{2}[\![P \,{}_{1/2}\!\oplus\, Q]\!] \oplus \tfrac{1}{2}[\![P \,{}_{1/3}\!\oplus\, Q]\!] = [\![P \,{}_{5/12}\!\oplus\, Q]\!].$$

As noted in [30], the ability to combine transitions is crucial for obtaining transitivity of probabilistic process equivalences that take internal actions into account.

Referring to the example in the introduction, the processes of t_0 and u_0 will be identified. However, without the splitting of the source distribution μ as provided by Definition 4.2, we are not able to relate t_0 and u_0 directly, or rather their direct derivatives, while meeting the natural transfer conditions (see Definition 4.4). The difficulty arises when both P and Q can do a τ-transition to non-bisimilar processes.

In preparation to the definition of the notion of branching probabilistic bisimilarity below we introduce some notation.

Definition 4.3. For $\mu, \mu' \in \mathit{Distr}(\mathcal{E})$ and $\alpha \in \mathcal{A}$ we write $\mu \xrightarrow{(\alpha)} \mu'$ iff (i) $\mu \xrightarrow{\alpha} \mu'$, or (ii) $\alpha = \tau$ and $\mu = \mu_1 \,{}_r\!\oplus\, \mu_2$, $\mu' = \mu'_1 \,{}_r\!\oplus\, \mu'_2$ such that $\mu_1 \xrightarrow{\tau} \mu'_1$ and $\mu_2 = \mu'_2$ for some $r \in [0,1]$. We use $\Rightarrow$ to denote the reflexive transitive closure of $\xrightarrow{(\tau)}$.

Thus, for example,

$$\tfrac{1}{3}\delta(\tau \cdot (P \,{}_{1/2}\!\oplus\, Q)) \oplus \tfrac{2}{3}[\![P \,{}_{1/2}\!\oplus\, Q]\!] \xrightarrow{(\tau)} [\![P \,{}_{1/2}\!\oplus\, Q]\!] \quad \text{and}$$
$$\tfrac{1}{2}\delta(\tau \cdot \partial(\tau \cdot P)) \oplus \tfrac{1}{3}\delta(\tau \cdot P) \oplus \tfrac{1}{6}[\![P]\!] \Rightarrow [\![P]\!].$$

We are now in a position to define strong probabilistic bisimilarity and branching probabilistic bisimilarity. Note that the notion of strong probabilistic bisimilarity is the variant with combined transitions as defined in [29,6].

Definition 4.4 (Strong and branching probabilistic bisimilarity).

(a) A symmetric relation $\mathcal{R} \subseteq \mathit{Distr}(\mathcal{E}) \times \mathit{Distr}(\mathcal{E})$ is called *decomposable* iff for all $\mu, \nu \in \mathit{Distr}(\mathcal{E})$ such that $\mu \mathcal{R} \nu$ and $\mu = \bigoplus_{i \in I} p_i * \mu_i$ there are $\nu_i \in \mathit{Distr}(\mathcal{E})$, for $i \in I$, such that

$$\nu = \bigoplus_{i \in I} p_i * \nu_i \text{ and } \mu_i \mathcal{R} \nu_i \text{ for all } i \in I.$$

(b) A decomposable relation $\mathcal{R} \subseteq \mathit{Distr}(\mathcal{E}) \times \mathit{Distr}(\mathcal{E})$ is called a *strong probabilistic bisimulation relation* iff for all $\mu, \nu \in \mathit{Distr}(\mathcal{E})$ such that $\mu \mathcal{R} \nu$ and $\mu \xrightarrow{\alpha} \mu'$ there is a $\nu' \in \mathit{Distr}(\mathcal{E})$ such that

$$\nu \xrightarrow{\alpha} \nu' \text{ and } \mu' \mathcal{R} \nu'.$$

(c) A symmetric relation $\mathcal{R} \subseteq \mathit{Distr}(\mathcal{E}) \times \mathit{Distr}(\mathcal{E})$ is called *weakly decomposable* iff for all $\mu, \nu \in \mathit{Distr}(\mathcal{E})$ such that $\mu \mathcal{R} \nu$ and $\mu = \bigoplus_{i \in I} p_i * \mu_i$ there are $\bar{\nu}, \nu_i \in \mathit{Distr}(\mathcal{E})$, for $i \in I$, such that

$$\nu \Rightarrow \bar{\nu},\ \mu \mathcal{R} \bar{\nu},\ \bar{\nu} = \bigoplus_{i \in I} p_i * \nu_i,\ \text{and } \mu_i \mathcal{R} \nu_i \text{ for all } i \in I.$$

(d) A weakly decomposable relation $\mathcal{R} \subseteq \mathit{Distr}(\mathcal{E}) \times \mathit{Distr}(\mathcal{E})$ is called a *branching* probabilistic bisimulation relation iff for all $\mu, \nu \in \mathit{Distr}(\mathcal{E})$ such that $\mu \mathcal{R} \nu$ and $\mu \xrightarrow{\alpha} \mu'$, there are $\bar{\nu}, \nu' \in \mathit{Distr}(\mathcal{E})$ such that

$$\nu \Rightarrow \bar{\nu},\ \bar{\nu} \xrightarrow{(\alpha)} \nu',\ \mu \mathcal{R} \bar{\nu},\ \text{and } \mu' \mathcal{R} \nu'.$$

(e) Strong probabilistic bisimilarity, denoted by $\leftrightarrows \subseteq \mathit{Distr}(\mathcal{E}) \times \mathit{Distr}(\mathcal{E})$, and branching probabilistic bisimilarity, written as $\leftrightarrows_b \subseteq \mathit{Distr}(\mathcal{E}) \times \mathit{Distr}(\mathcal{E})$, are respectively defined as the largest strong probabilistic bisimulation relation on $\mathit{Distr}(\mathcal{E})$ and as the largest branching probabilistic bisimulation relation on $\mathit{Distr}(\mathcal{E})$.

By comparison, on finite processes, as used in this paper, the branching probabilistic bisimilarity of Segala & Lynch [29] can be defined in our framework exactly as in (d) and (e) above, but taking a decomposable instead of a weakly decomposable relation. This yields a strictly finer equivalence, distinguishing the processes s_0, t_0 and u_0 from the introduction.

The notion of decomposability has been adopted from [23] and weak decomposability from [25]. The underlying idea stems from [10]. These notions provide a convenient dexterity to deal with behavior of sub-distributions, e.g., to distinguish $\frac{1}{2}\partial(a \cdot \partial(\mathbf{0})) \oplus \frac{1}{2}\partial(b \cdot \partial(\mathbf{0}))$ from $\partial(\mathbf{0})$, as well as combined behavior.

Our definition of branching probabilistic bisimilarity is based on distributions rather than on states and has similarity with the notion of weak distribution bisimilarity proposed by Eisentraut et al. in [13]. Consider the running example of [13], reproduced in Figure 1 and reformulated in terms of the process language at hand. The states ① and ⑥ are identified with respect to weak distribution bisimilarity as detailed in [13]. Correspondingly, putting

$$\begin{aligned} E_1 &= \tau \cdot \big(\partial(\tau \cdot \partial(\tau \cdot P + c \cdot Q + \tau \cdot R) + c \cdot Q + \tau \cdot R) \;{}_{1/2}\!\oplus \\ &\qquad \partial(\tau \cdot (\partial(\tau \cdot P + c \cdot Q + \tau \cdot R) \;{}_{1/2}\!\oplus\; \partial(\mathbf{0})))\big) \\ E_6 &= \tau \cdot (\partial(\tau \cdot P + c \cdot Q + \tau \cdot R) \;{}_{3/4}\!\oplus\; \partial(\mathbf{0})) \end{aligned}$$

the non-deterministic processes E_1 and E_6 are identified with respect to branching probabilistic bisimilarity.

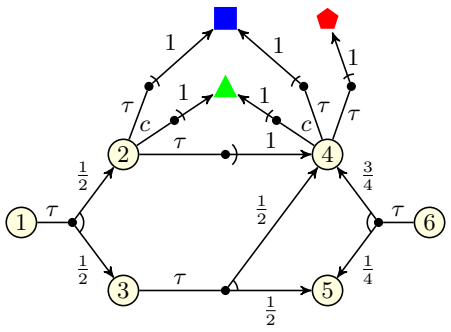


Fig. 1. Probabilistic automaton of [13]

Note that strong and branching probabilistic bisimilarity are well-defined since any union of strong or branching probabilistic bisimulation relations is again a strong or branching probabilistic bisimulation relation. In particular, (weak) decomposability is preserved under arbitrary unions.

As we did for the non-deterministic setting, we introduce a notion of rooted branching probabilistic bisimilarity for distributions over processes.

Definition 4.5. A symmetric and decomposable relation $\mathcal{R} \subseteq \mathit{Distr}(\mathcal{E}) \times \mathit{Distr}(\mathcal{E})$ is called a rooted branching probabilistic bisimulation relation iff for all $\mu, \nu \in \mathit{Distr}(\mathcal{E})$ such that $\mu \,\mathcal{R}\, \nu$ it holds that if $\mu \xrightarrow{\alpha} \mu'$ for $\alpha \in \mathcal{A}$, $\mu' \in \mathit{Distr}(\mathcal{E})$ then $\nu \xrightarrow{\alpha} \nu'$ and $\mu' \leftrightarrows_b \nu'$ for some $\nu' \in \mathit{Distr}(\mathcal{E})$. Rooted branching probabilistic bisimilarity, denoted by $\leftrightarrows_{rb} \subseteq \mathit{Distr}(\mathcal{E}) \times \mathit{Distr}(\mathcal{E})$, is defined as the largest rooted branching probabilistic bisimulation relation.

Since any union of rooted branching probabilistic bisimulation relations is again a rooted branching probabilistic bisimulation relation, rooted branching probabilistic bisimilarity $\leftrightarrows_{rb}$ is well-defined.

Note, the two probabilistic processes

$$P = \partial(\tau \cdot \partial(a \cdot \partial(\mathbf{0}))) \,{}_{1/2}\!\oplus\, \partial(b \cdot \partial(\mathbf{0})) \quad \text{and} \quad Q = \partial(a \cdot \partial(\mathbf{0})) \,{}_{1/2}\!\oplus\, \partial(b \cdot \partial(\mathbf{0}))$$

are *not* rooted branching probabilistically bisimilar. Any rooted branching probabilistic bisimulation relation is by decomposability required to relate the respective probabilistic components $\partial(\tau \cdot \partial(a \cdot \partial(\mathbf{0})))$ and $\partial(a \cdot \partial(\mathbf{0}))$, which clearly do not meet the transfer condition. Thus, since $\partial(\tau \cdot \partial(a \cdot \partial(\mathbf{0}))) \not\leftrightarrows_{rb} \partial(a \cdot \partial(\mathbf{0}))$ also $P \not\leftrightarrows_{rb} Q$.

Two non-deterministic processes are considered to be strongly, rooted branching, or branching probabilistically bisimilar iff their Dirac distributions are,

i.e., $E \leftrightarrows F$ iff $\delta(E) \leftrightarrows \delta(F)$, $E \leftrightarrows_{rb} F$ iff $\delta(E) \leftrightarrows_{rb} \delta(F)$, and $E \leftrightarrows_b F$ iff $\delta(E) \leftrightarrows_b \delta(F)$. Two probabilistic processes are considered to be strongly, rooted branching, or branching probabilistically bisimilar iff their associated distributions over $\mathcal{E}$ are.

We show that branching probabilistic bisimilarity, although not a congruence for non-deterministic choice, is a congruence for probabilistic choice. We first need a technical result.

Lemma 4.6. Let I and J be finite index sets, $p_i, q_j \in [0,1]$ and $\xi, \mu_i, \nu_j \in \mathit{Distr}(\mathcal{E})$, for $i \in I$ and $j \in J$, with $\xi = \bigoplus_{i\in I} p_i * \mu_i$ and $\xi = \bigoplus_{j\in J} q_j * \nu_j$. Then there are $r_{ij} \in [0,1]$ and $\varrho_{ij} \in \mathit{Distr}(\mathcal{E})$ such that $\sum_{i\in I} r_{ij} = q_j$, $\sum_{j\in J} r_{ij} = p_i$, $p_i * \mu_i = \bigoplus_{j\in J} r_{ij} * \varrho_{ij}$ for all $i \in I$, and $q_j * \nu_j = \bigoplus_{i\in I} r_{ij} * \varrho_{ij}$ for all $j \in J$.

Proof. Let $r_{ij} = \displaystyle\sum_{E\in spt(\xi)} \frac{p_i\mu_i(E)\, q_j\nu_j(E)}{\xi(E)}$ for all $i \in I$ and $j \in J$. In case $r_{ij} = 0$ choose $\varrho_{ij} \in \mathit{Distr}(\mathcal{E})$ arbitrarily. Otherwise, define for all $E \in \mathcal{E}$, $i \in I$, $j \in J$:

$$\varrho_{ij}(E) = \begin{cases} \dfrac{p_i\mu_i(E)\, q_j\nu_j(E)}{r_{ij}\, \xi(E)} & \text{if } \xi(E) > 0, \\ 0 & \text{otherwise.} \end{cases}$$

With these definitions it is straightforward to check the required properties. □

Lemma 4.7. Let $\mu_1, \mu_2, \nu_1, \nu_2 \in \mathit{Distr}(\mathcal{E})$ and $r \in (0,1)$. If $\mu_1 \leftrightarrows_b \nu_1$ and $\mu_2 \leftrightarrows_b \nu_2$ then $\mu_1 \,{}_r\!\oplus\, \mu_2 \leftrightarrows_b \nu_1 \,{}_r\!\oplus\, \nu_2$.

Proof. Suppose $\mu_1 \leftrightarrows_b \nu_1$ and $\mu_2 \leftrightarrows_b \nu_2$ through branching probabilistic bisimulation relations $\mathcal{R}_1$ and $\mathcal{R}_2$. We show that the relation $\mathcal{R} = \{\, \langle \xi' \,{}_s\!\oplus\, \xi'', \eta' \,{}_s\!\oplus\, \eta'' \rangle \mid \xi' \,\mathcal{R}_1\, \eta',\ \xi'' \,\mathcal{R}_2\, \eta'',\ s \in (0,1) \,\}$ is a branching probabilistic bisimulation relation relating $\mu_1 \,{}_r\!\oplus\, \mu_2$ with $\nu_1 \,{}_r\!\oplus\, \nu_2$.

Symmetry is straightforward. We show that $\mathcal{R}$ is weakly decomposable. So, assume $\xi \,\mathcal{R}\, \eta$ and $\xi = \bigoplus_{i\in I} p_i * \xi_i$. Thus, $\xi = \xi' \,{}_s\!\oplus\, \xi''$ and $\eta = \eta' \,{}_s\!\oplus\, \eta''$ with $\xi' \,\mathcal{R}_1\, \eta'$ and $\xi'' \,\mathcal{R}_2\, \eta''$ for suitable $\xi', \xi'', \eta', \eta'' \in \mathit{Distr}(\mathcal{E})$. By Lemma 4.6 there must be $s'_i, s''_i \geqslant 0$ and $\xi'_i, \xi''_i \in \mathit{Distr}(\mathcal{E})$, for $i \in I$, such that

$$\begin{aligned} \xi' &= \textstyle\bigoplus_{i\in I} s'_i/s * \xi'_i\,, \\ \xi'' &= \textstyle\bigoplus_{i\in I} s''_i/(1{-}s) * \xi''_i\,, \\ \xi_i &= (s'_i/p_i * \xi'_i) \oplus (s''_i/p_i * \xi''_i) \quad \text{for all } i \in I\,, \end{aligned}$$

$\sum_{i\in I} s'_i = s$, $\sum_{i\in I} s''_i = 1{-}s$, and $s'_i + s''_i = p_i$ for all $i \in I$. Since $\mathcal{R}_1$ and $\mathcal{R}_2$ are weakly decomposable, there are $\bar\eta', \bar\eta'', \eta'_i, \eta''_i \in \mathit{Distr}(\mathcal{E})$ for $i \in I$ such that

$$\begin{array}{llll} \eta' \Rightarrow \bar\eta' & \xi' \,\mathcal{R}_1\, \bar\eta', & \bar\eta' = \textstyle\bigoplus_{i\in I} s'_i/s * \eta'_i, & \xi'_i \,\mathcal{R}_1\, \eta'_i, \\ \eta'' \Rightarrow \bar\eta'' & \xi'' \,\mathcal{R}_2\, \bar\eta'' & \bar\eta'' = \textstyle\bigoplus_{i\in I} s''_i/(1{-}s) * \eta''_i & \xi''_i \,\mathcal{R}_1\, \eta''_i \end{array}$$

for all $i \in I$. Therefore, we can conclude that

$$\eta' \,{}_s\!\oplus\, \eta'' \Rightarrow \bar\eta' \,{}_s\!\oplus\, \bar\eta'' \quad \text{and} \quad (\xi' \,{}_s\!\oplus\, \xi'')\, \mathcal{R}\, (\bar\eta' \,{}_s\!\oplus\, \bar\eta'')\,.$$

Moreover,

$$\begin{aligned}\bar{\eta}' \,{}_s\!\oplus\, \bar{\eta}'' &= \left(\bigoplus_{i\in I} s_i'/s * \eta_i'\right) {}_s\!\oplus\, \left(\bigoplus_{i\in I} s_i''/(1-s) * \eta_i''\right)\\ &= \left(\bigoplus_{i\in I} s_i' * \eta_i'\right) \oplus \left(\bigoplus_{i\in I} s_i'' * \eta_i''\right)\\ &= \bigoplus_{i\in I} p_i * (\eta_i' \,{}_{s_i'/p_i}\!\oplus\, \eta_i'')\end{aligned}$$

and $\xi_i = (\xi_i' \,{}_{s_i'/p_i}\!\oplus\, \xi_i'')\,\mathcal{R}\,(\eta_i' \,{}_{s_i'/p_i}\!\oplus\, \eta_i'')$ for all $i \in I$. This finishes the argument that $\mathcal{R}$ is decomposable.

Next, we show that $\mathcal{R}$ satisfies the transfer property for bisimulations. Suppose we have $(\xi_1 \,{}_r\!\oplus\, \xi_2)\mathcal{R}(\eta_1 \,{}_r\!\oplus\, \eta_2)$, thus $\xi_1\mathcal{R}_1\xi_2$ and $\eta_1\mathcal{R}_2\eta_2$. If $\xi_1 \,{}_r\!\oplus\, \xi_2 \xrightarrow{\alpha} \xi'$ then $\xi_1 \xrightarrow{\alpha} \xi_1'$, $\xi_2 \xrightarrow{\alpha} \xi_2'$ and $\xi' = \xi_1' \,{}_r\!\oplus\, \xi_2'$ for suitable $\xi_1', \xi_2' \in \mathit{Distr}(\mathcal{E})$. By assumption, $\bar{\eta}_1, \eta_1'$ and $\bar{\eta}_2, \eta_2'$ exist such that $\eta_1 \Rightarrow \bar{\eta}_1 \xrightarrow{(\alpha)} \eta_1'$, $\eta_2 \Rightarrow \bar{\eta}_2 \xrightarrow{(\alpha)} \eta_2'$, $\xi_1\,\mathcal{R}_1\,\bar{\eta}_1$, $\xi_2\,\mathcal{R}_2\,\bar{\eta}_2$, $\xi_1'\,\mathcal{R}_1\,\eta_1'$, and $\xi_2'\,\mathcal{R}_2\,\eta_2'$. From this we obtain $\eta_1 \,{}_r\!\oplus\, \eta_2 \Rightarrow \bar{\eta}_1 \,{}_r\!\oplus\, \bar{\eta}_2 \xrightarrow{(\alpha)} \eta'$, $\xi_1 \,{}_r\!\oplus\, \xi_2\,\mathcal{R}\,\bar{\eta}_1 \,{}_r\!\oplus\, \bar{\eta}_2$ and $\xi'\,\mathcal{R}\,\eta'$ for $\eta' = \eta_1' \,{}_r\!\oplus\, \eta_2'$. □

A direct consequence of the previous lemma is that if $P_1 \leftrightarrows_b Q_1$ and $P_2 \leftrightarrows_b Q_2$ then $P_1 \,{}_r\!\oplus\, P_2 \leftrightarrows_b Q_1 \,{}_r\!\oplus\, Q_2$.

Lemma 4.8 (Congruence). The relations $\leftrightarrows$, $\leftrightarrows_{rb}$, and $\leftrightarrows_b$ on $\mathcal{E}$ and $\mathcal{P}$ are equivalence relations, and the relations $\leftrightarrows$ and $\leftrightarrows_{rb}$ are congruences on $\mathcal{E}$ and $\mathcal{P}$.

Proof. The proof of $\leftrightarrows$, $\leftrightarrows_{rb}$, and $\leftrightarrows_b$ being equivalence relations involves a number of straightforward auxiliary results, in particular for the case of transitivity, and are omitted here.

Regarding congruence the interesting cases are for non-deterministic and probabilistic choice with respect to rooted branching probabilistic bisimilarity. Suppose $E_1 \leftrightarrows_{rb} F_1$ and $E_2 \leftrightarrows_{rb} F_2$. Then $\mathcal{R} = \{\langle \delta(E_1 + E_2), \delta(F_1 + F_2)\rangle\}^\dagger$ is a rooted branching probabilistic bisimulation relation. Clearly, $\mathcal{R}$ is symmetric and decomposable. Moreover, if $\delta(E_1 + E_2) \xrightarrow{\alpha} \mu'$, then either $\delta(E_1) \xrightarrow{\alpha} \mu'$, $\delta(E_2) \xrightarrow{\alpha} \mu'$, or $\delta(E_1) \xrightarrow{\alpha} \mu_1'$, $\delta(E_2) \xrightarrow{\alpha} \mu_2'$ and $\mu' = \mu_1' \,{}_r\!\oplus\, \mu_2'$ for suitable $\mu_1', \mu_2' \in \mathit{Distr}(\mathcal{E})$ and $r \in (0,1)$. We only consider the last case, as the first two are simpler. Hence, we can find $\nu_1', \nu_2' \in \mathit{Distr}(\mathcal{E})$ such that $\delta(F_1) \xrightarrow{\alpha} \nu_1'$, $\delta(F_2) \xrightarrow{\alpha} \nu_2'$, $\mu_1' \leftrightarrows_b \nu_1'$, and $\mu_2' \leftrightarrows_b \nu_2'$. From this it follows that $\delta(F_1 + F_2) \xrightarrow{\alpha} \nu'$ and $\mu' \leftrightarrows_b \nu'$ for $\nu' = \nu_1' \,{}_r\!\oplus\, \nu_2'$ using Lemma 4.7.

Suppose $P_1 \leftrightarrows_{rb} Q_1$ and $P_2 \leftrightarrows_{rb} Q_2$ with $\mathcal{R}_1$ and $\mathcal{R}_2$ rooted branching probabilistic bisimulation relations relating $[\![P_1]\!]$ with $[\![Q_1]\!]$, and $[\![P_2]\!]$ with $[\![Q_2]\!]$, respectively, and fix some $r \in (0,1)$. Then $\mathcal{R} = \{\langle \mu_1 \,{}_r\!\oplus\, \mu_2, \nu_1 \,{}_r\!\oplus\, \nu_2\rangle \mid \mu_1\mathcal{R}_1\nu_1,\ \mu_2\mathcal{R}_2\nu_2\}$ is a rooted branching probabilistic bisimulation relation relating $[\![P_1 \,{}_r\!\oplus\, P_2]\!]$ with $[\![Q_1 \,{}_r\!\oplus\, Q_2]\!]$. Symmetry is straightforward and decomposability can be shown along the lines of the proof of weak decomposability for Lemma 4.7.

So we are left to prove the transfer property. Suppose $(\mu_1 \,{}_r\!\oplus\, \mu_2)\mathcal{R}(\nu_1 \,{}_r\!\oplus\, \nu_2)$, thus $\mu_1\mathcal{R}_1\mu_2$ and $\nu_1\mathcal{R}_2\nu_2$. If $\mu_1 \,{}_r\!\oplus\, \mu_2 \xrightarrow{\alpha} \mu'$ then $\mu_1 \xrightarrow{\alpha} \mu_1'$, $\mu_2 \xrightarrow{\alpha} \mu_2'$ and $\mu' = \mu_1' \,{}_r\!\oplus\, \mu_2'$ for suitable $\mu_1', \mu_2' \in \mathit{Distr}(\mathcal{E})$. By assumption, ν_1' and ν_2' exist such that $\nu_1 \xrightarrow{\alpha} \nu_1'$, $\nu_2 \xrightarrow{\alpha} \nu_2'$, $\mu_1' \leftrightarrows_b \nu_1'$, and $\mu_2' \leftrightarrows_b \nu_2'$. From this we obtain $\nu_1 \,{}_r\!\oplus\, \nu_2 \xrightarrow{\alpha} \nu'$ and by Lemma 4.7 $\mu' \leftrightarrows_b \nu'$ for $\nu' = \nu_1' \,{}_r\!\oplus\, \nu_2'$. □

5 A few fundamental properties of branching bisimilarity

In this section we show two fundamental properties of branching probabilistic bisimilarity that we need further on: the stuttering property, known from [17] for non-deterministic processes, and cancellativity of probabilistic choice with respect to $\leftrightarrows_b$.

Lemma 5.1 (Stuttering Property). If $\mu \Rightarrow \bar{\mu} \Rightarrow \nu$ and $\mu \leftrightarrows_b \nu$ then $\mu \leftrightarrows_b \bar{\mu}$.

Proof. We show that the relation $\leftrightarrows_b \cup \{(\mu, \bar{\mu}), (\bar{\mu}, \mu)\}$ is a branching probabilistic bisimulation.

First suppose $\mu \xrightarrow{\alpha} \mu'$. Then there are $\bar{\nu}, \nu' \in \mathit{Distr}(\mathcal{E})$ such that

$$\nu \Rightarrow \bar{\nu},\ \bar{\nu} \xrightarrow{(\alpha)} \nu',\ \mu \leftrightarrows_b \bar{\nu},\ \text{and}\ \mu' \leftrightarrows_b \nu'.$$

Since $\bar{\mu} \Rightarrow \nu$, we have $\bar{\mu} \Rightarrow \bar{\nu}$, which had to be shown. Now suppose $\bar{\mu} \xrightarrow{\alpha} \mu'$. Then certainly $\mu \Rightarrow \bar{\mu} \xrightarrow{\alpha} \mu'$.

To show weak decomposability, suppose $\mu = \bigoplus_{i\in I} p_i * \mu_i$. Then there are $\bar{\nu}, \nu_i \in \mathit{Distr}(\mathcal{E})$, for $i \in I$, such that

$$\nu \Rightarrow \bar{\nu},\ \mu \mathcal{R} \bar{\nu},\ \bar{\nu} = \bigoplus_{i\in I} p_i * \nu_i,\ \text{and}\ \mu_i \mathcal{R} \nu_i \text{ for all } i \in I.$$

Again it suffices to point out that $\bar{\mu} \Rightarrow \bar{\nu}$. Conversely, suppose $\bar{\mu} = \bigoplus_{i\in I} p_i * \bar{\mu}_i$. Then $\mu \Rightarrow \bar{\mu} = \bigoplus_{i\in I} p_i * \bar{\mu}_i$. □

For $S \subseteq \mathcal{E}$ and $\mu \in \mathit{Distr}(\mathcal{E})$, define $\mu(S) = \sum_{E\in\mathcal{E}} \mu(E)$. Now two distributions μ and ν are strong probabilistic bisimilar iff for each bisimulation equivalence class $S \subseteq \mathcal{E}$ one has $\mu(S) = \nu(S)$. The proof is essentially the same as that of Lemma 5.2 below. However, such a property does not hold for branching probabilistic bisimilarity, due to the use of weak decomposability instead of decomposability. But it does hold when restricting attention to a class of processes on which weak decomposability reduces to decomposability.

Call a distribution $\mu \in \mathit{Distr}(\mathcal{E})$ $\leftrightarrows_b$-*stable* iff, for all $\bar{\mu} \in \mathit{Distr}(\mathcal{E})$,

$$\mu \Rightarrow \bar{\mu} \text{ and } \mu \leftrightarrows_b \bar{\mu} \text{ implies } \bar{\mu} = \mu\ , \tag{1}$$

i.e., if it cannot perform internal activity without leaving its branching bisimulation equivalence class. Note that if a distribution $\mu \,{}_r\!\oplus\, \nu$ with $r \in (0,1)$ is $\leftrightarrows_b$-stable, then so are μ and ν.

Lemma 5.2. If μ and ν are $\leftrightarrows_b$-stable then $\mu \leftrightarrows_b \nu$ iff $\mu(S) = \nu(S)$ for each $\leftrightarrows_b$-equivalence class S.

Proof. Suppose $\mu \leftrightarrows_b \nu$. Let $\mu = \bigoplus_{i\in I_1} p_i * E_i$. By weak decomposability, $\nu \Rightarrow \bar{\nu} = \bigoplus_{i\in I} p_i * \nu_i$ with $\nu \leftrightarrows_b \bar{\nu}$ and $\delta(E_i) \leftrightarrows_b \nu_i$ for all $i \in I$. By (1), as $\nu \leftrightarrows_b \bar{\nu}$, we have $\bar{\nu} = \nu$.

Let, for each $i \in I$, $\nu_i = \bigoplus_{j\in J_i} p_{ij} * F_{ij}$. Note, $\sum_{j\in J_i} p_{ij} = 1$. By weak decomposability, there are $\mu_{ij} \in \mathit{Distr}(\mathcal{E})$, for $j \in J_i$, such that $\delta(E_i) \Rightarrow$

$\bar{\mu}_i := \bigoplus_{i \in J_i} p_{ij} * \mu_{ij}$, $\nu_i \leftrightarrows_b \bar{\mu}_i$ and $\mu_{ij} \leftrightarrows_b \delta(F_{ij})$ for all $j \in J_i$. By (1) and $\leftrightarrows_b$-stability of $\delta(E_i)$, it follows that $\delta(E_i) = \bar{\mu}_i$ and hence $\mu_{ij} = \delta(E_i)$. Writing $E_{ij} := E_i$, $q_{ij} := p_i \cdot p_{ij}$ and $K = \{\, ij \mid i \in I \wedge j \in J_i \,\}$ we obtain

$$\mu = \bigoplus_{k \in K} q_k * E_k\,,\ \ \nu = \bigoplus_{k \in K} q_k * F_k\,,\ \text{ and } \delta(E_k)\,\mathcal{R}\,\delta(F_k) \text{ for all } k \in K.$$

Now, for any $\leftrightarrows_b$-equivalence class $S \subseteq \mathcal{E}$ it holds that $E_k \in S \Leftrightarrow F_k \in S$ for all $k \in K$. So,

$$\mu(S) = \textstyle\sum_{k \in K,\, E_k \in S} q_k = \sum_{k \in K,\, F_k \in S} q_k = \nu(S)\,.$$

The reverse direction of Lemma 5.2 is straightforward with Lemma 4.7. □

The next lemma holds because in this paper we consider finite processes only.

Lemma 5.3. For each $\mu \in \mathit{Distr}(\mathcal{E})$ there is a $\leftrightarrows_b$-stable $\mu' \leftrightarrows_b \mu$ with $\mu \Rightarrow \mu'$.

Proof Sketch: Define the *weight* of a distribution by $w(\mu) = \sum_{E \in \mathcal{E}} \mu(E) \cdot c(E)$, i.e., the weighted average of the complexities of the states in its support. Now $E \xrightarrow{\alpha} \mu$ implies $w(\mu) < w(\delta(E))$, and thus $\mu \xrightarrow{\alpha} \mu'$ implies $w(\mu') < w(\mu)$, and $\mu \Rightarrow \mu'$ implies $w(\mu') \leqslant w(\mu)$. For $\mu \in \mathit{Distr}(\mathcal{E})$ let $T_\mu := \{\, \mu' \mid \mu' \leftrightarrows_b \mu \wedge \mu \Rightarrow \mu' \,\}$ and define

$$sw(\mu) := \inf_{\mu' \in T_\mu} w(\mu')\,.$$

In [10] it is shown that for any $\mu \in \mathit{Distr}(\mathcal{E})$, the set $\{\, \mu' \mid \mu \Rightarrow \mu' \,\}$ is compact. This concept is defined by regarding a probability distribution over a finite set of n states as a point in the n-dimensional Euclidean space $\mathbb{R}^n$. Similarly it can be shown that the set T_μ is compact. This is a consequence of the finitary nature of the space under consideration. The infimum over the compact set will be reached, and therefore there exists a derivation $\mu \Rightarrow \mu'$ with $\mu' \leftrightarrows_b \mu$ and $w(\mu') = sw(\mu)$. By construction μ' must be $\leftrightarrows_b$-stable. □

Lemma 5.4 (Cancellativity). Let $\mu, \mu', \nu, \nu' \in \mathit{Distr}(\mathcal{E})$. If $\mu \,{}_r\!\oplus\, \nu \leftrightarrows_b \mu' \,{}_r\!\oplus\, \nu'$ with $r \in (0, 1]$ and $\nu \leftrightarrows_b \nu'$, then $\mu \leftrightarrows_b \mu'$.

Proof. Let $\mu \,{}_r\!\oplus\, \nu \leftrightarrows_b \mu' \,{}_r\!\oplus\, \nu'$ with $r \in (0, 1]$ and $\nu \leftrightarrows_b \nu'$. By Lemma 5.3 there is a $\leftrightarrows_b$-stable distribution $\xi \leftrightarrows_b \mu \,{}_r\!\oplus\, \nu$ with $\mu \,{}_r\!\oplus\, \nu \Rightarrow \xi$. By weak decomposability, there are $\bar{\xi} \leftrightarrows_b \xi$, $\bar{\mu} \leftrightarrows_b \mu$ and $\bar{\nu} \leftrightarrows_b \nu$ with $\xi \Rightarrow \bar{\xi} = \bar{\mu} \,{}_r\!\oplus\, \bar{\nu}$. By the $\leftrightarrows_b$-stability of ξ we have $\bar{\xi} = \xi$. Likewise there are distributions $\bar{\mu}' \leftrightarrows_b \mu'$ and $\bar{\nu}' \leftrightarrows_b \nu'$ such that $\bar{\mu}' \,{}_r\!\oplus\, \bar{\nu}'$ is $\leftrightarrows_b$-stable, $\mu' \,{}_r\!\oplus\, \nu' \leftrightarrows_b \bar{\mu}' \,{}_r\!\oplus\, \bar{\nu}'$ and $\mu' \,{}_r\!\oplus\, \nu' \Rightarrow \bar{\mu}' \,{}_r\!\oplus\, \bar{\nu}'$.

Since $\bar{\mu} \,{}_r\!\oplus\, \bar{\nu} \leftrightarrows_b \bar{\mu}' \,{}_r\!\oplus\, \bar{\nu}'$, and using the $\leftrightarrows_b$-stability of $\bar{\mu} \,{}_r\!\oplus\, \bar{\nu}$ and $\bar{\mu}' \,{}_r\!\oplus\, \bar{\nu}'$, it follows by Lemma 5.2 that $(\bar{\mu} \,{}_r\!\oplus\, \bar{\nu})(S) = (\bar{\mu}' \,{}_r\!\oplus\, \bar{\nu}')(S)$ for every $\leftrightarrows_b$-equivalence class of states S. Since $\bar{\nu} \leftrightarrows_b \bar{\nu}'$, we likewise have $\bar{\nu}(S) = \bar{\nu}'(S)$. Using that $(\bar{\mu} \,{}_r\!\oplus\, \bar{\nu})(S) = r \cdot \bar{\mu}(S) + (1{-}r) \cdot \bar{\nu}(S)$,

$$\bar{\mu}(S) = \frac{(\bar{\mu} \,{}_r\!\oplus\, \bar{\nu})(S) - (1{-}r) \cdot \bar{\nu}(S)}{r} = \frac{(\bar{\mu}' \,{}_r\!\oplus\, \bar{\nu}')(S) - \bar{\nu}'(S)}{r} = \bar{\mu}'(S).$$

Thus, by Lemma 5.2, $\bar{\mu} \leftrightarrows_b \bar{\mu}'$, and consequently $\mu \leftrightarrows_b \mu'$. □

6 Completeness: the probabilistic case

In this section we provide a sound and complete equational characterization of rooted branching probabilistic bisimilarity. The completeness result is obtained along the same lines as the corresponding result for branching bisimilarity for the non-deterministic processes in Section 3. We extend and adapt the non-deterministic theories AX and AX^b of Section 3.

Definition 6.1 (Axiomatization of $\leftrightarrows$ and $\leftrightarrows_{rb}$). The theory AX_p is given by the axioms A1 to A4, the axioms P1 to P3 and C listed in Table 2. The theory AX_p^b contains in addition the axioms BP and G.

The axioms A1–A4 for non-deterministic processes are as before. Regarding probabilistic processes, for the axioms P1 and P2 dealing with commutativity and associativity, we need to take care of the probabilities involved. For P2, it follows from the given restrictions that also $(1-r)s = (1-r')s'$, i.e., the probability for Q to execute is equal for the left-hand and right-hand side of the equation. Axiom P3 expresses that a probabilistic choice between equal processes can be eliminated. Axiom C expresses that any two nondeterministic transitions can be executed in a combined fashion: one with probability r and one with the complementary probability $1-r$.

The axioms P1 and P2 allow us to write each probabilistic process P as

$$\partial(E_1) \,{}_{r_1}\!\oplus\, (\partial(E_2) \,{}_{r_2}\!\oplus\, (\partial(E_3) \,{}_{r_3}\!\oplus\, \cdots))$$

for non-deterministic processes E_i. In the sequel we denote such a process by $\bigoplus_{i\in I} p_i * E_i$ with $p_i = r_i \prod_{j=1}^{i-1}(1 - r_j)$. More specifically, if a probabilistic process P corresponds to a distribution $\bigoplus_{i\in I} p_i * E_i$, then we have $AX_p \vdash P = \bigoplus_{i\in I} p_i * E_i$, as can be shown by induction on the structure of P.

For axioms BP and G of Table 2 we introduce the notation $E \sqsubseteq P$ for $E \in \mathcal{E}$, $P \in \mathcal{P}$. We define

$$E \sqsubseteq P \quad \text{iff} \quad \forall \alpha \in \mathcal{A},\, \mu \in \mathit{Distr}(\mathcal{E})\colon E \xrightarrow{\alpha} \mu \implies \exists \nu \in \mathit{Distr}(\mathcal{E})\colon [\![P]\!] \xrightarrow{(\alpha)} \nu \wedge \mu \leftrightarrows_b \nu\,.$$

Thus, we require that every transition of the non-deterministic process E can be directly matched by the probabilistic process P. Note, if $E \sqsubseteq P$ and $\delta(E) \xrightarrow{\alpha} \mu$, then $[\![P]\!] \xrightarrow{(\alpha)} \nu$ for some $\nu \in \mathit{Distr}(\mathcal{E})$ such that $\mu \leftrightarrows_b \nu$: If $\delta(E) \xrightarrow{\alpha} \mu$, then $\mu = \bigoplus_{i\in I} p_i * \mu_i$ and $E \xrightarrow{\alpha} \mu_i$ for suitable $p_i \geqslant 0$, $\mu_i \in \mathit{Distr}(\mathcal{E})$. Since $E \sqsubseteq P$, we have for each $i \in I$ that $[\![P]\!] \xrightarrow{(\alpha)} \nu_i$ for some $\nu_i \in \mathit{Distr}(\mathcal{E})$ satisfying $\mu_i \leftrightarrows_b \nu_i$. Hence $[\![P]\!] \xrightarrow{(\alpha)} \nu := \bigoplus_{i\in I} p_i * \nu_i$ and $\mu \leftrightarrows_b \nu$ by Lemma 4.7.

Axiom BP is an adaptation of axiom B of the theory AX^b to the probabilistic setting of AX_p^b. In the setting of non-deterministic processes the implication $F \xrightarrow{\alpha} F' \implies E \xrightarrow{\alpha} E' \wedge F' \leftrightarrows_b E'$ for some E' is captured by $E + F \leftrightarrows_{rb} E$. If we reformulate axiom B as $E + F = E \implies \alpha \cdot (F + \tau \cdot E) = \alpha \cdot E$, then it becomes more similar to axiom BP in Table 2.

As to BP, in the context of a preceding action α and a probabilistic process Q, a non-deterministic alternative E that is also offered by a probabilistic process after a τ-prefix can be dispensed with, together with the prefix τ. In a formulation without the prefix α and the probabilistic alternative Q, but with the specific condition $E \sqsubseteq P$, and retaining the τ-prefix on the right-hand side, the axiom BP shows similarity with axioms T2 and T3 in [15] which, in turn, are reminiscent of axioms T1 and T2 of [11]; these axioms stem from Milner's second τ-law [26].

A1	$E + F = F + E$
A2	$(E + F) + G = E + (F + G)$
A3	$E + E = E$
A4	$E + \mathbf{0} = E$
P1	$P \,{}_r\!\oplus\, Q = Q \,{}_{1-r}\!\oplus\, P$
P2	$P \,{}_r\!\oplus\, (Q \,{}_s\!\oplus\, R) = (P \,{}_{\bar{r}}\!\oplus\, Q) \,{}_{\bar{s}}\!\oplus\, R$ where $r = \bar{r}\,\bar{s}$ and $(1-r)(1-s) = 1-\bar{s}$
P3	$P \,{}_r\!\oplus\, P = P$
C	$\alpha \cdot P + \alpha \cdot Q = \alpha \cdot P + \alpha \cdot (P \,{}_r\!\oplus\, Q) + \alpha \cdot Q$
BP	if $E \sqsubseteq P$ then $\alpha \cdot \big(\partial(\, E + \tau \cdot P\,) \,{}_r\!\oplus\, Q\big) = \alpha \cdot \big(P \,{}_r\!\oplus\, Q\big)$
G	if $E \sqsubseteq \partial(F)$ then $\alpha \cdot (\partial(E + F) \,{}_r\!\oplus\, Q) = \alpha \cdot (\partial(F) \,{}_r\!\oplus\, Q)$

Table 2. Axioms for strong and rooted branching probabilistic bisimilarity

Let us illustrate the working of axiom BP. Consider the non-deterministic process $E = b \cdot \partial(\mathbf{0})$ and the probabilistic process $P = \partial(a \cdot \partial(\mathbf{0}) + b \cdot \partial(\mathbf{0})) \,{}_{1/2}\!\oplus\, \partial(b \cdot \partial(\mathbf{0}))$. Then we have $E \sqsubseteq P$, i.e.

$$b \cdot \partial(\mathbf{0}) \sqsubseteq \partial(a \cdot \partial(\mathbf{0}) + b \cdot \partial(\mathbf{0})) \,{}_{1/2}\!\oplus\, \partial(b \cdot \partial(\mathbf{0})).$$

Therefore, we have by application of axiom BP the provable equality

$$\begin{aligned} AX_p^b \vdash \alpha \cdot \big(\partial(b \cdot \partial(\mathbf{0}) + \tau \cdot (\partial(a \cdot \partial(\mathbf{0}) + b \cdot \partial(\mathbf{0})) \,{}_{1/2}\!\oplus\, \partial(b \cdot \partial(\mathbf{0})))) \,{}_r\!\oplus\, Q\big) = \\ \alpha \cdot \big((\partial(a \cdot \partial(\mathbf{0}) + b \cdot \partial(\mathbf{0})) \,{}_{1/2}\!\oplus\, \partial(b \cdot \partial(\mathbf{0}))) \,{}_r\!\oplus\, Q\big)\ . \end{aligned}$$

Another example is $a \cdot (P_1 \,{}_r\!\oplus\, P_2) \sqsubseteq \partial(b \cdot R + a \cdot P_1) \,{}_r\!\oplus\, \partial(c \cdot S + a \cdot P_2)$, so

$$\begin{aligned} AX_p^b \vdash \alpha \cdot \big(\partial(a \cdot (P_1 \,{}_r\!\oplus\, P_2) + \tau \cdot (\partial(b \cdot R + a \cdot P_1) \,{}_r\!\oplus\, \partial(c \cdot S + a \cdot P_2))) \,{}_r\!\oplus\, Q\big) = \\ \alpha \cdot \big((\partial(b \cdot R + a \cdot P_1) \,{}_r\!\oplus\, \partial(c \cdot S + a \cdot P_2)) \,{}_r\!\oplus\, Q\big)\ . \end{aligned}$$

An example illustrating the use of (α), rather than α, as label of the matching transition of $[\![P]\!]$ in the definition of $\sqsubseteq$ is

$$\tau \cdot (\partial(b \cdot P + \tau \cdot Q) \,{}_r\!\oplus\, Q) \sqsubseteq \partial(b \cdot P + \tau \cdot Q)$$

from which we obtain

$$AX_p^b \vdash \alpha \cdot \Big(\partial\big(\tau \cdot (\partial(b \cdot P + \tau \cdot Q) \mathbin{{}_r\!\oplus} Q) + \tau \cdot (\partial(b \cdot P + \tau \cdot Q))\big) \mathbin{{}_r\!\oplus} R\Big) = \alpha \cdot \big((\partial(b \cdot P + \tau \cdot Q)) \mathbin{{}_r\!\oplus} R\big) .$$

The axiom G roughly is a variant of BP without the τ prefixing the process P. A typical example, matching the one above, is

$$AX_p^b \vdash \alpha \cdot \Big(\partial\big(\tau \cdot (\partial(b \cdot P + \tau \cdot Q) \mathbin{{}_r\!\oplus} Q) + (b \cdot P + \tau \cdot Q)\big) \mathbin{{}_r\!\oplus} R\Big) = \alpha \cdot \big((\partial(b \cdot P + \tau \cdot Q)) \mathbin{{}_r\!\oplus} R\big) .$$

The occurrences of the prefix $\alpha \cdot \_$ in BP and G are related to the root condition for non-deterministic processes, cf. axiom B in Section 3.

Lemma 6.2. The following simplifications of the axiom BP are derivable:

$$\begin{array}{rl} (i) & AX_p^b \vdash \alpha \cdot \partial(\, E + \tau \cdot P\,) = \alpha \cdot P \quad \text{if } E \sqsubseteq P, \\ (ii) & AX_p^b \vdash \alpha \cdot (\partial(\, \tau \cdot P) \mathbin{{}_r\!\oplus} R\,) = \alpha \cdot (P \mathbin{{}_r\!\oplus} R) \text{ and} \\ (iii) & AX_p^b \vdash \alpha \cdot \partial(\, \tau \cdot P) = \alpha \cdot P\,. \end{array}$$

Proof. The proof of the first equality requires an application of P3:

$$\begin{array}{ll} AX_p^b \vdash & \alpha \cdot \partial(E + \tau \cdot P) \overset{\text{P3}}{=} \\ & \alpha \cdot \big(\partial(E + \tau \cdot P) \mathbin{{}_{\frac{1}{2}}\!\oplus} \partial(E + \tau \cdot P)\big) \overset{\text{BP}}{=} \\ & \alpha \cdot \big(P \mathbin{{}_{\frac{1}{2}}\!\oplus} \partial(E + \tau \cdot P)\big) \overset{\text{P1}}{=} \\ & \alpha \cdot \big(\partial(E + \tau \cdot P) \mathbin{{}_{\frac{1}{2}}\!\oplus} P\big) \overset{\text{BP}}{=} \\ & \alpha \cdot \big(P \mathbin{{}_{\frac{1}{2}}\!\oplus} P\big) \overset{\text{P3}}{=} \alpha \cdot P\,. \end{array}$$

The proof of the second equality uses A4:

$$\begin{array}{ll} AX_p^b \vdash & \alpha \cdot \big(\partial(\tau \cdot P) \mathbin{{}_r\!\oplus} R\big) \overset{\text{A4}}{=} \\ & \alpha \cdot \big(\partial(\mathbf{0} + \tau \cdot P) \mathbin{{}_r\!\oplus} R\big) \overset{\text{BP}}{=} \\ & \alpha \cdot \big(P \mathbin{{}_r\!\oplus} R\big) \end{array}$$

The last equation can be proven in a similar way as the first property, using the second one. □

Similar simplifications of axiom G can be found.

Using the properties in the lemma above the process identities mentioned in the introduction can easily be proven. Returning to the processes E_1 and E_6

related to Figure 1, we have

$$\begin{aligned}
AX_p^b \vdash E_1 \quad &= \quad \tau\cdot\big(\partial(\tau\cdot\partial(\tau\cdot P + c\cdot Q + \tau\cdot R) + c\cdot Q + \tau\cdot R) \\
&\qquad {}_{1/2}\oplus\ \partial(\tau\cdot(\partial(\tau\cdot P + c\cdot Q + \tau\cdot R)\ {}_{1/2}\oplus\ \partial(\mathbf{0})))\big) \\
&\overset{\text{BP}}{=} \quad \tau\cdot\big(\partial(\tau\cdot P + c\cdot Q + \tau\cdot R) \\
&\qquad {}_{1/2}\oplus\ \partial(\tau\cdot(\partial(\tau\cdot P + c\cdot Q + \tau\cdot R)\ {}_{1/2}\oplus\ \partial(\mathbf{0})))\big) \\
&\overset{6.2\ (ii),\ \text{P1}}{=} \quad \tau\cdot\big(\partial(\tau\cdot P + c\cdot Q + \tau\cdot R) \\
&\qquad {}_{1/2}\oplus\ (\partial(\tau\cdot P + c\cdot Q + \tau\cdot R)\ {}_{1/2}\oplus\ \partial(\mathbf{0}))\big) \\
&\overset{\text{P2}}{=} \quad \tau\cdot\big((\partial(\tau\cdot P + c\cdot Q + \tau\cdot R)_{2/3}\oplus \\
&\qquad \partial(\tau\cdot P + c\cdot Q + \tau\cdot R))\ {}_{3/4}\oplus\ \partial(\mathbf{0})\big) \\
&\overset{\text{P3}}{=} \quad \tau\cdot(\partial(\tau\cdot P + c\cdot Q + \tau\cdot R)\ {}_{3/4}\oplus\ \partial(\mathbf{0})) = E_6\,.
\end{aligned}$$

Soundness of the theory AX_p for strong probabilistic bisimilarity and of the theory AX_p^b for rooted branching probabilistic bisimilarity is straightforward.

Lemma 6.3 (Soundness). For all $P, Q \in \mathcal{P}$, if $AX_p \vdash P = Q$ then $P \leftrightarrows Q$, and if $AX_p^b \vdash P = Q$ then $P \leftrightarrows_{rb} Q$.

Proof. As usual, in view of $\leftrightarrows$ and $\leftrightarrows_{rb}$ being congruences, one only needs to prove the left-hand and right-hand sides of the axioms to be strongly or rooted branching probabilistically bisimilar. We only treat the cases of the axioms BP and G with respect to rooted branching probabilistic bisimilarity.

For BP, by Definition 4.5 and Lemma 4.7, it suffices to show that $P \leftrightarrows_b \partial(E + \tau\cdot P)$ if $E \sqsubseteq P$. Suppose $\delta(E + \tau\cdot P) \xrightarrow{\alpha} \mu$. We distinguish two cases: (i) $\delta(E) \xrightarrow{\alpha} \mu$; (ii) $\alpha = \tau$, $\delta(E) \xrightarrow{\tau} \mu'$ and $\mu = [\![P]\!]\ {}_r\oplus\ \mu'$ for some $r \in (0,1]$. For (i), by definition of $E \sqsubseteq P$, we have $[\![P]\!] \xrightarrow{(\alpha)} \nu$ and $\mu \leftrightarrows_b \nu$ for suitable $\nu \in \mathit{Distr}(\mathcal{E})$. For (ii), again by $E \sqsubseteq P$, we have $[\![P]\!] \xrightarrow{(\tau)} \nu'$ and $\mu' \leftrightarrows_b \nu'$. Thus $[\![P]\!] = [\![P]\!]\ {}_r\oplus\ [\![P]\!] \xrightarrow{(\tau)} \nu$ and $\mu \leftrightarrows_b \nu$ for $\nu = [\![P]\!]\ {}_r\oplus\ \nu'$, as was to be shown. Conversely, $[\![P]\!] \xrightarrow{\alpha} \mu$ trivially implies that $\delta(E + \tau\cdot P) \Rightarrow [\![P]\!] \xrightarrow{(\alpha)} \mu$. The requirement on weak decomposability also holds trivially.

For G, by Definition 4.5 and Lemma 4.7, it suffices to show that $E + F \leftrightarrows_b F$ if $E \sqsubseteq \partial(F)$. Put $\mathcal{R} = \{\langle E + F, F\rangle\}^\dagger \cup \leftrightarrows_b$. We verify that $\mathcal{R}$ is a branching probabilistic bisimulation. Naturally, $\delta(E) \xrightarrow{\alpha} \mu$ implies $\delta(E+F) \xrightarrow{\alpha} \mu$, and also weak decomposability is easy. Finally, suppose $\delta(E + F) \xrightarrow{\alpha} \mu$. Since $E \sqsubseteq \partial(F)$ now we have $\delta(E) \xrightarrow{(\alpha)} \nu$ for some ν with $\mu \leftrightarrows_b \nu$. □

As for the process language with non-deterministic processes only, we aim at a completeness proof that is built on completeness of strong bisimilarity and the notion of a concrete process. Equational characterization of strong probabilistic bisimilarity has been addressed by various authors. The theory AX_p provides a sound and complete theory. For a proof, see e.g. [23].

Lemma 6.4. The theory AX_p is sound and complete for strong bisimilarity.

The next lemma provides a more state-based characterization of strong probabilistic bisimilarity.

Lemma 6.5. Let $\mathcal{R} \subseteq \mathit{Distr}(\mathcal{E}) \times \mathit{Distr}(\mathcal{E})$ be a decomposable relation such that

$$\mu_1 \,\mathcal{R}\, \nu_1 \text{ and } \mu_2 \,\mathcal{R}\, \nu_2 \quad \text{implies} \quad (\mu_1 \,{}_r\!\oplus\, \mu_2) \,\mathcal{R}\, (\nu_1 \,{}_r\!\oplus\, \nu_2) \tag{2}$$

and for each pair $E, F \in \mathcal{E}$

$$\delta(E) \,\mathcal{R}\, \delta(F) \text{ and } E \xrightarrow{\alpha} \mu' \quad \text{implies} \quad \delta(F) \xrightarrow{\alpha} \nu' \text{ and } \mu' \,\mathcal{R}\, \nu' \tag{3}$$

for a suitable $\nu' \in \mathit{Distr}(\mathcal{E})$. Then $\mu \,\mathcal{R}\, \nu$ implies $\mu \leftrightarrows \nu$.

Proof. We show that $\mathcal{R}$ is a strong probabilistic bisimulation relation. So, let $\mu, \nu \in \mathit{Distr}(\mathcal{E})$ such that $\mu \,\mathcal{R}\, \nu$ and $\mu \xrightarrow{\alpha} \mu'$. By Definition 4.2(b) we have $\mu = \bigoplus_{i \in I} p_i * E_i$, $\mu' = \bigoplus_{i \in I} p_i * \mu'_i$, and $E_i \xrightarrow{\alpha} \mu'_i$ for all $i \in I$. Since $\mathcal{R}$ is decomposable, there are $\nu_i \in \mathit{Distr}(\mathcal{E})$, for $i \in I$, such that

$$\nu = \textstyle\bigoplus_{i \in I} p_i * \nu_i \quad \text{and} \quad \delta(E_i) \,\mathcal{R}\, \nu_i \text{ for all } i \in I.$$

Let, for each $i \in I$, $\nu_i = \bigoplus_{j \in J_i} p_{ij} * F_{ij}$. Since $\mathcal{R}$ is decomposable, there are $\mu_{ij} \in \mathit{Distr}(\mathcal{E})$, for $j \in J_i$, such that

$$\delta(E_i) = \textstyle\bigoplus_{i \in J_i} p_{ij} * \mu_{ij} \quad \text{and} \quad \mu_{ij} \,\mathcal{R}\, \delta(F_{ij}) \text{ for all } j \in J_i.$$

Here $\mu_{ij} = \delta(E_i)$. Writing $E_{ij} := E_i$, $q_{ij} := p_i \cdot p_{ij}$ and $K = \{(i,j) \mid i \in I \wedge j \in J_i\}$ we obtain

$$\mu = \textstyle\bigoplus_{k \in K} q_k * E_k \;,\; \nu = \bigoplus_{k \in K} q_k * F_k \quad \text{and} \quad \delta(E_k) \,\mathcal{R}\, \delta(F_k) \text{ for all } k \in K.$$

Let $\mu'_{ij} := \mu'_i$ for all $i \in I$ and $j \in J_i$. Then $\mu' = \bigoplus_{k \in K} q_k * \mu'_k$. Using that $E_k \xrightarrow{\alpha} \mu'_k$ for all $k \in K$, there must be distributions ν'_k for $k \in K$ such that

$$\delta(F_k) \xrightarrow{\alpha} \nu'_k \quad \text{and} \quad \mu'_k \,\mathcal{R}\, \nu'_k.$$

By Definition 4.2(b) this implies $\nu \xrightarrow{\alpha} \nu'$, for $\nu' := \bigoplus_{k \in K} q_k * \nu'_k$. Moreover, (2) yields $\mu' \,\mathcal{R}\, \nu'$. □

The following technical lemma expresses that two rooted branching probabilistically bisimilar processes can be represented in a similar way.

Lemma 6.6. For all $Q, R \in \mathcal{P}$, if $Q \leftrightarrows_{rb} R$ then there are an index set I as well as for all $i \in I$ suitable $p_i > 0$ and $F_i, G_i \in \mathcal{E}$ such that $F_i \leftrightarrows_{rb} G_i$, $AX_p \vdash Q = \bigoplus_{i \in I} p_i * F_i$ and $AX_p \vdash R = \bigoplus_{i \in I} p_i * G_i$.

Proof. Suppose $AX_p \vdash Q = \bigoplus_{j \in J} q_j * F'_j$. Since $Q \leftrightarrows_{rb} R$ and $\leftrightarrows_{rb}$ is decomposable, the process R can be written as $\bigoplus_{j \in J} q_j * R_j$ with $R_j \in \mathcal{P}$ for $j \in J$, such that $\partial(F_j) \leftrightarrows_{rb} R_j$. Therefore, each distribution R_j can be written as $\bigoplus_{k \in K_j} r_{jk} * G_{jk}$ where $\partial(F'_j) \leftrightarrows_{rb} \partial(G_{jk})$ for all $j \in J$ and $k \in K_j$. We now define $F_{jk} = F'_j$ for $j \in J$ and $k \in K_j$. Then, using the axioms P1, P2 and P3 we can derive

$$AX_p \vdash Q = \textstyle\bigoplus_{j \in J} \bigoplus_{k \in K_j} q_j r_{jk} * F_{jk}$$
$$AX_p \vdash R = \textstyle\bigoplus_{j \in J} \bigoplus_{k \in K_j} q_j r_{jk} * G_{jk}$$

with $F_{jk} \leftrightarrows_b G_{jk}$ for $j \in J$ and $k \in K_j$. This proves the lemma. □

Similar to the non-deterministic case, a transition $E \xrightarrow{\tau} \mu$ is called *inert* iff $\delta(E) \leftrightarrows_b \mu$. Typical cases of inert transitions include

$$\tau \cdot P \xrightarrow{\tau} [\![P]\!] ,$$
$$E + \tau \cdot \partial(E) \xrightarrow{\tau} \delta(E) .$$

Furthermore, a transition $E \xrightarrow{\tau} \mu_1 \,{}_r\!\oplus\, \mu_2$ with $r \in (0,1]$ and $\delta(E) \leftrightarrows_b \mu_1$ is called *partially inert*. A typical case is

$$\tau \cdot (\partial(b \cdot P + \tau \cdot Q) \,{}_r\!\oplus\, Q) + b \cdot P + \tau \cdot Q \xrightarrow{\tau} \delta(b \cdot P + \tau \cdot Q) \,{}_r\!\oplus\, [\![Q]\!] .$$

Here $\delta\big(\tau \cdot (\partial(b \cdot P + \tau \cdot Q) \,{}_r\!\oplus\, Q) + b \cdot P + \tau \cdot Q\big) \leftrightarrows_b \delta(b \cdot P + \tau \cdot Q)$ because $\delta(b \cdot P + \tau \cdot Q) \xrightarrow{(\tau)} \delta(b \cdot P + \tau \cdot Q) \,{}_r\!\oplus\, [\![Q]\!]$.

In Section 3 a process is called concrete if it does not exhibit an inert transition. In the setting with probabilistic choice we need to be more careful. For example, we also want to exclude processes of the form

$$\partial(\tau \cdot P) \,{}_{1/2}\!\oplus\, \partial(a \cdot Q)) \quad \text{and} \quad \partial(a \cdot P) \,{}_{1/2}\!\oplus\, \partial(b \cdot \big(\partial(\tau \cdot Q) \,{}_{1/3}\!\oplus\, Q\big))$$

from being concrete, although they cannot perform a transition by themselves at all. Therefore, we define the *derivatives* $der(P) \subseteq \mathcal{E}$ of a probabilistic process $P \in \mathcal{P}$ by

$$der(P \,{}_r\!\oplus\, Q) := der(P) \cup der(Q)$$
$$der(\partial(\textstyle\sum_{i \in I} \alpha_i \cdot P_i)) := \{ \textstyle\sum_{i \in I} \alpha_i \cdot P_i \} \cup \bigcup_{i \in I} der(P_i)$$

and define a process $\bar{P} \in \mathcal{P}$ to be *concrete* iff none of its derivatives can perform a partially inert transition, i.e., if there is no transition $E \xrightarrow{\tau} \mu_1 \,{}_r\!\oplus\, \mu_2$ with $E \in der(\bar{P})$, $r \in (0,1]$ and $\delta(E) \leftrightarrows_b \mu_1$. A non-deterministic process $\bar{E}$ is called concrete if the probabilistic process $\partial(\bar{E})$ is. Moreover, we define two sets of concrete processes:

$$\mathcal{E}_{cc} = \{ \bar{E} \in \mathcal{E} \mid \bar{E} \text{ is concrete} \} \quad \text{and} \quad \mathcal{P}_{cc} = \{ \bar{P} \in \mathcal{P} \mid \bar{P} \text{ is concrete} \}.$$

Furthermore, we call a process $E \in \mathit{Distr}(\mathcal{E})$ *rigid* iff there is no inert transition $E \xrightarrow{\tau} \mu$, and write $\mathcal{E}_r = \{ \bar{E} \in \mathcal{E} \mid \bar{E} \text{ is rigid} \}$. Naturally, $\mathcal{E}_{cc} \subseteq \mathcal{E}_r$.

We use concrete and rigid processes to build the proof of the completeness result for rooted branching probabilistic bisimilarity on top of the completeness proof of strong probabilistic bisimilarity. The following lemma lists all properties of concrete and rigid processes we need in our completeness proof.

Lemma 6.7.

(a) If $E = \sum_{i \in I} \alpha_i \cdot P_i$ with $P_i \in \mathcal{P}_{cc}$ and, for all $i \in I$, $\alpha_i \neq \tau$ or $[\![P_i]\!]$ cannot be written as $\mu_1 \,{}_r\!\oplus\, \mu_2$ with $r \in (0,1]$ and $\delta(E) \leftrightarrows_b \mu_1$, then $E \in \mathcal{E}_{cc}$.
(b) If $P_1, P_2 \in \mathcal{P}_{cc}$ then $P_1 \,{}_r\!\oplus\, P_2 \in \mathcal{P}_{cc}$.
(c) If $\mu = \bigoplus_{i \in I} p_i * \mu_i \in \mathit{Distr}(\mathcal{E}_{cc})$ with each $p_i > 0$, then each $\mu_i \in \mathit{Distr}(\mathcal{E}_{cc})$.
(d) If $\mu \in \mathit{Distr}(\mathcal{E}_{cc})$ and $\mu \xrightarrow{(\alpha)} \mu'$ then $\mu' \in \mathit{Distr}(\mathcal{E}_{cc})$.

(e) If $\mu \in \mathit{Distr}(\mathcal{E}_r)$ and $\mu \Rightarrow \mu'$ with $\mu \leftrightarrows_b \mu'$ then $\mu = \mu'$.
(f) If $E \in \mathcal{E}_{cc}$, $F \in \mathcal{E}$, and $\mu, \nu \in \mathit{Distr}(\mathcal{E})$ are such that $E \leftrightarrows_b F$, $E \xrightarrow{\alpha} \mu$, $\delta(F) \xrightarrow{(\alpha)} \nu$ and $\mu \leftrightarrows_b \nu$, then $\delta(F) \xrightarrow{\alpha} \nu$.
(g) If $\mu \leftrightarrows_b \bigoplus_{i\in I} p_i * \nu_i$ for $\mu \in \mathit{Distr}(\mathcal{E}_r)$ then $\mu = \bigoplus_{i\in I} p_i * \mu_i$ for certain $\mu_i \leftrightarrows_b \nu_i$.

Proof. Properties (a), (b), (c) and (d) follow immediately from the definitions, in the case of (d) also using Definition 4.2(b).

For (e), let $\mu \in \mathit{Distr}(\mathcal{E}_r)$ and $\mu \Rightarrow \mu'$ with $\mu \leftrightarrows_b \mu'$. Towards a contradiction, suppose $\mu \neq \mu'$. Then there must be a distribution $\bar{\mu} \neq \mu$ such that $\mu \xrightarrow{(\tau)} \bar{\mu}$ and $\bar{\mu} \Rightarrow \mu'$. We may even choose $\bar{\mu}$ such that the transition $\mu \xrightarrow{(\tau)} \bar{\mu}$ acts on only one (rigid) state in the support of μ, i.e. there are $E \in \mathcal{E}$, $r \in (0,1]$ and $\rho, \nu \in \mathit{Distr}(\mathcal{E})$ such that $\mu = \delta(E) \,{}_r\!\oplus \rho$, $E \xrightarrow{\tau} \nu$ and $\bar{\mu} = \nu \,{}_r\!\oplus \rho$. By Lemma 5.1 $\delta(E) \,{}_r\!\oplus \rho = \mu \leftrightarrows_b \bar{\mu} = \nu \,{}_r\!\oplus \rho$. Hence by Lemma 5.4 $\delta(E) \leftrightarrows_b \nu$. So the transition $E \xrightarrow{\tau} \nu$ is inert, contradicting $E \in \mathcal{E}_r$.

To establish (f), suppose $E \in \mathcal{E}_{cc}$, $F \in \mathcal{E}$, and $\mu, \nu \in \mathit{Distr}(\mathcal{E})$ are such that $E \leftrightarrows_b F$, $E \xrightarrow{\alpha} \mu$, $\delta(F) \xrightarrow{(\alpha)} \nu$ and $\mu \leftrightarrows_b \nu$. Assume $\alpha = \tau$, for otherwise the statement is trivial. Then $\delta(F) \xrightarrow{\tau} \nu_1$ and $\nu = \nu_1 \,{}_r\!\oplus \delta(F)$ for some $\nu_1 \in \mathit{Distr}(\mathcal{E})$ and $r \in [0,1]$. Since $\leftrightarrows_b$ is weakly decomposable, there are $\bar{\mu}, \mu_1, \mu_2 \in \mathit{Distr}(\mathcal{E})$ such that $\mu \Rightarrow \bar{\mu}$, $\mu \leftrightarrows_b \bar{\mu}$, $\bar{\mu} = \mu_1 \,{}_r\!\oplus \mu_2$, $\mu_1 \leftrightarrows_b \nu_1$ and $\mu_2 \leftrightarrows_b \delta(F)$. Since μ is concrete, using case (d) of the lemma, $\bar{\mu} = \mu$ by case (e). Thus $E \xrightarrow{\tau} \mu_1 \,{}_r\!\oplus \mu_2$ with $\delta(E) \leftrightarrows_b \delta(F) \leftrightarrows_b \mu_2$. Since E is concrete, this transition cannot be partially inert. Thus, we must have $r = 1$. It follows that $\delta(F) \xrightarrow{\alpha} \nu$.

Regarding (g), if $\mu \leftrightarrows_b \bigoplus_{i\in I} p_i * \nu_i$ for $\mu \in \mathit{Distr}(\mathcal{E}_r)$, then $\mu \Rightarrow \bar{\mu} := \bigoplus_{i\in I} p_i * \mu_i$ with $\mu_i \leftrightarrows_b \nu_i$ by weak decomposability of $\leftrightarrows_b$. By (e) we have $\bar{\mu} = \mu$. □

Lemma 6.8. For all $\bar{P}, \bar{Q} \in \mathcal{P}_{cc}$, if $\bar{P} \leftrightarrows_b \bar{Q}$ then $\bar{P} \leftrightarrows \bar{Q}$ and $AX_p \vdash \bar{P} = \bar{Q}$.

Proof. Let $\mathcal{R} := \leftrightarrows_b \cap (\mathit{Distr}(\mathcal{E}_{cc}) \times \mathit{Distr}(\mathcal{E}_{cc}))$. Then, by Lemma 6.7(c)–(d), $\mathcal{R}$ is a branching probabilistic bisimulation relation relating $\bar{P}$ and $\bar{Q}$. We show that $\mathcal{R}$ moreover satisfies the conditions of Lemma 6.5. Condition (2) is a direct consequence of Lemmas 4.7 and 6.7(b). That $\mathcal{R}$ is decomposable follows since it is weakly decomposable, in combination with Lemma 6.7(e). Now, in order to verify condition (3), suppose $\delta(E) \,\mathcal{R}\, \delta(F)$ and $E \xrightarrow{\alpha} \mu$. Then $\delta(F) \Rightarrow \bar{\nu} \xrightarrow{(\alpha)} \nu$ for some $\bar{\nu}, \nu \in \mathcal{P}$ with $\delta(E) \,\mathcal{R}\, \bar{\nu}$ and $\mu \,\mathcal{R}\, \nu$. By Lemma 6.7(e) we have $\bar{\nu} = \delta(F)$. Thus $\delta(F) \xrightarrow{(\alpha)} \nu$. Hence, using Lemma 6.7(f) it follows that $\delta(F) \xrightarrow{\alpha} \nu$. With $\mathcal{R}$ satisfying conditions (2) and (3), Lemma 6.5 yields $\bar{P} \leftrightarrows \bar{Q}$. By Lemma 6.4 we obtain $AX_p \vdash \bar{P} = \bar{Q}$. □

Before we are in a position to prove our main result we need one more technical lemma. Here we write $AX_p^b \vdash P_1 \approx P_2$ as a shorthand for

$$\forall \alpha \in \mathcal{A}\, \forall Q \in \mathcal{P}\, \forall r \in (0,1) \colon AX_p^b \vdash \alpha \cdot (P_1 \,{}_r\!\oplus\, Q) = \alpha \cdot (P_2 \,{}_r\!\oplus\, Q)\,.$$

For example, using axiom BP, if $E \sqsubseteq P$ then $AX_p^b \vdash \partial(E + \tau \cdot P) \approx P$. Likewise, using G, if $E \sqsubseteq \partial(F)$ then $\partial(E + F) \approx \partial(F)$. As in the proof of Lemma 6.2(i), from $AX_p^b \vdash P_1 \approx P_2$ it also follows that $AX_p^b \vdash \alpha \cdot P_1 \approx \alpha \cdot P_2$ for all $\alpha \in \mathcal{A}$. In the proof of the lemma we rely on the axioms BP and G.

Lemma 6.9.

(a) For each non-deterministic process $E \in \mathcal{E}$ there is a concrete probabilistic process $\bar{P} \in \mathcal{P}_{cc}$ such that $AX_p^b \vdash \partial(E) \approx \bar{P}$.
(b) For each probabilistic process $P \in \mathcal{P}$ there is a concrete probabilistic process $\bar{P} \in \mathcal{P}_{cc}$ such that $AX_p^b \vdash \alpha \cdot P = \alpha \cdot \bar{P}$ for all $\alpha \in \mathcal{A}$.
(c) For all probabilistic processes $Q, R \in \mathcal{P}$, if $Q \leftrightarrows_b R$ then $AX_p^b \vdash \alpha \cdot Q = \alpha \cdot R$ for all $\alpha \in \mathcal{A}$.

Proof. By simultaneous induction on $c(E)$, $c(P)$, and $\max\{c(Q), c(R)\}$. The base case, which applies to case (a) only, is clear, since the process $\mathbf{0} + \cdots + \mathbf{0}$ is concrete.

Case (a) for $c(E) > 0$. The process E can be written as $\sum_{i \in I} \alpha_i \cdot P_i$ for some index set I and suitable $\alpha_i \in \mathcal{A}$ and $P_i \in \mathcal{P}$. Pick by the induction hypothesis (b), for each $i \in I$, a concrete probabilistic process $\bar{P}_i \in \mathcal{P}_{cc}$ with $AX_p^b \vdash \alpha_i \cdot \bar{P}_i = \alpha_i \cdot P_i$. Now $AX_p \vdash E = \bar{E}$ for $\bar{E} := \sum_{i \in I} \alpha_i \cdot \bar{P}_i$. We distinguish two cases.

(i) First suppose that for some $i_0 \in I$ we have $\alpha_{i_0} = \tau$ and $\bar{P}_{i_0} \leftrightarrows_b \partial(\bar{E})$. Then $AX_p^b \vdash E = H + \tau.\bar{P}_{i_0}$, where $H := \sum_{i \in I \setminus \{i_0\}} \alpha_i \cdot \bar{P}_i$. It now suffices to show that $H \sqsubseteq \bar{P}_{i_0}$, because then axiom BP yields $AX_p^b \vdash \partial(E) \approx \bar{P}_{i_0}$. So, suppose $H \xrightarrow{\alpha} \mu$. Then $\bar{E} \xrightarrow{\alpha} \mu$. Since $\partial(\bar{E}) \leftrightarrows_b \bar{P}_{i_0}$, we have $[\![\bar{P}_{i_0}]\!] \Rightarrow \bar{\nu} \xrightarrow{(\alpha)} \nu$ where $\delta(\bar{E}) \leftrightarrows_b \bar{\nu}$ and $\mu \leftrightarrows_b \nu$. Because $\bar{P}_{i_0}$ is concrete, $[\![\bar{P}_{i_0}]\!] = \bar{\nu}$ by Lemma 6.7(e). Thus $[\![\bar{P}_{i_0}]\!] \xrightarrow{(\alpha)} \nu$, which was to be shown.

(ii) Next suppose that $\alpha_i \neq \tau$ or $P_i \not\leftrightarrows_b \partial(\bar{E})$, for all $i \in I$, i.e., $\bar{E}$ is rigid. We will show that there is a concrete process $\bar{C} \in \mathcal{E}_{cc}$ such that $AX_p^b \vdash \partial(\bar{E}) \approx \partial(\bar{C})$. We proceed with induction on the number of indices $k \in I$ such that $\alpha_k = \tau$ and $[\![P_k]\!]$ can be written as $\mu_1 \,{}_r\!\oplus\, \mu_2$ with $r \in (0,1)$ and $\delta(\bar{E}) \leftrightarrows_b \mu_1$. As $\bar{E}$ is rigid, there are no such indices with $r = 1$.

Base case: If there are no such k, then $\bar{C} := \bar{E} \in \mathcal{E}_{cc}$ by Lemma 6.7(a).

Induction step: Let $i_0 \in I$ be an index such that $\alpha_{i_0} = \tau$ and $[\![P_{i_0}]\!]$ can be written as $\mu_1 \,{}_r\!\oplus\, \mu_2$ with $r \in (0,1)$ and $\delta(\bar{E}) \leftrightarrows_b \mu_1$. First we show that it is possible to write $[\![P_{i_0}]\!]$ in such way while ensuring that μ_2 itself cannot be written as $\nu_1 \,{}_s\!\oplus\, \nu_2$ with $s \in (0,1)$ and $\delta(\bar{E}) \leftrightarrows_b \nu_1$. Namely, when $\mu_1 = \bigoplus_{j \in J} p_j * F_j$, then by Lemma 6.7(g), using that $\bar{E} \in \mathcal{E}_r$, $\delta(\bar{E}) = \bigoplus_{j \in J} p_j * \xi_j$ with $\delta(F_j) \leftrightarrows_b \xi_j$. So $\xi_j = \delta(\bar{E})$ for all $j \in J$. Now we split $[\![P_{i_0}]\!]$ in such a way between μ_1 and μ_2, that for all $F \in \mathit{spt}(\mu_1)$ we have $F \leftrightarrows_b \bar{E}$ and for all $G \in \mathit{spt}(\mu_2)$ we have $G \not\leftrightarrows_b \bar{E}$. This ensures that $\mu_1 \leftrightarrows_b \delta(\bar{E})$, while μ_2 cannot be written as $\nu_1 \,{}_s\!\oplus\, \nu_2$ with $s \in (0,1)$ and $\delta(\bar{E}) \leftrightarrows_b \nu_1$, since on the one hand $\mathit{spt}(\nu_1) \subseteq \mathit{spt}(\mu_2)$ and on the other hand $G \leftrightarrows_b \bar{E}$ for all $G \in \mathit{spt}(\nu_1)$.

Let $H := \sum_{i \in I \setminus \{i_0\}} \alpha_i \cdot \bar{P}_i$. Then $\bar{E} = \tau \cdot P_{i_0} + H$. By induction, there is a $\bar{C} \in \mathcal{E}_{cc}$ with $AX_p^b \vdash \partial(H) \approx \partial(\bar{C})$. So it suffices to show that $AX_p^b \vdash \partial(\bar{E}) \approx \partial(H)$. This time, this follows by axiom G, as soon as we obtain $\tau \cdot P_{i_0} \sqsubseteq \partial(H)$. By axioms P1–3, there are $P, P' \in \mathcal{P}_{cc}$, such that (a) $AX_p \vdash P_{i_0} = P' \,{}_r\!\oplus\, P$, (b) for all $F \in \mathit{spt}([\![P']\!])$ we have $F \leftrightarrows_b \bar{E}$ and (c) $[\![P]\!]$ cannot be written as $\nu_1 \,{}_s\!\oplus\, \nu_2$

with $s \in (0,1)$ and $\delta(\bar{E}) \leftrightarrows_b \nu_1$. Furthermore, by Lemma 6.8, all $F \in spt([\![P']\!])$ can be proven equal using AX_p. Thus $AX_p \vdash P_{i_0} = \partial(F) \,{}_r\!\oplus\, P$.

We claim that $\delta(F) \xrightarrow{\tau} \mu'$ for some μ' with $\mu' \leftrightarrows_b [\![P]\!]$. This can be shown as follows: Since $\bar{E} \xrightarrow{\tau} \delta(F) \,{}_r\!\oplus\, [\![P]\!]$ and $\bar{E} \leftrightarrows_b F$, we have $\delta(F) \xrightarrow{(\tau)} \mu$ for some $\mu \leftrightarrows_b \delta(F) \,{}_r\!\oplus\, [\![P]\!]$. Applying the definition of $\xrightarrow{(\tau)}$, we obtain $\delta(F) \xrightarrow{\tau} \mu'$ for some μ' with $\mu = \partial(F) \,{}_s\!\oplus\, \mu'$ and $s \in [0,1]$. Moreover, by Lemma 6.7(g), using that μ is concrete and thus rigid, $\mu = \eta_1 \,{}_r\!\oplus\, \eta_2$ with $\eta_1 \leftrightarrows_b \delta(F)$ and $\eta_2 \leftrightarrows_b [\![P]\!]$. Since $F \in \mathcal{E}_{cc}$, no fraction of the distribution μ' can be branching bisimilar to $\delta(F)$. Likewise, no fraction of η_2 can be bisimilar to $\delta(F)$, for then by Lemma 6.7(g) a fraction of $[\![P]\!]$ would be bisimilar to $\delta(E)$, contradicting (c) above. Thus $s = r$ and $\mu' = \eta_2 \leftrightarrows_b [\![P]\!]$. This proves $\delta(F) \xrightarrow{\tau} \mu'$ for some μ' with $\mu' \leftrightarrows_b [\![P]\!]$ as claimed.

Next, we show that $\bar{E} \leftrightarrows_b H \leftrightarrows_b F$. Let $\mathcal{R}$ be the smallest symmetric relation that contains $\leftrightarrows_b$ as well as $\{(\delta(H), \delta(\bar{E})), (\delta(H), \delta(F))\}$, and moreover satisfies $\mu_1 \,\mathcal{R}\, \nu_1 \wedge \mu_2 \,\mathcal{R}\, \nu_2 \implies (\mu_1 \,{}_r\!\oplus\, \mu_2) \,\mathcal{R}\, (\nu_1 \,{}_r\!\oplus\, \nu_2)$. We show that $\mathcal{R}$ is a branching bisimulation. Weak decomposability is fairly straightforward—compare the proof of Lemma 4.7. Also trivially, it suffices to check the transfer condition for the pairs $(\delta(H), \delta(\bar{E}))$, $(\delta(H), \delta(F))$, $(\delta(F), \delta(\bar{H}))$ and $(\delta(\bar{E}), \delta(H))$.

For $\delta(H) \,\mathcal{R}\, \delta(\bar{E})$, assume $\delta(H) \xrightarrow{\alpha} \varrho$. Then also $\delta(\bar{E}) \xrightarrow{\alpha} \varrho$. For $\delta(H) \,\mathcal{R}\, \delta(F)$, assume $\delta(H) \xrightarrow{\alpha} \varrho$. Then also $\delta(\bar{E}) \xrightarrow{\alpha} \varrho$, and since $E \leftrightarrows_b F$ this move can be matched by $\delta(F)$.

For $\delta(F) \,\mathcal{R}\, \delta(H)$, assume $\delta(F) \xrightarrow{\alpha} \varrho$. Since $\bar{E} \leftrightarrows_b F$, we have $\delta(\bar{E}) \xrightarrow{(\alpha)} \eta$ for some $\eta \leftrightarrows_b \varrho$. Here we immediately applied Lemma 6.7(e), using that $\bar{E}$ is rigid. Since F is concrete, no fraction of the distribution ϱ can be branching bisimilar to $\delta(F)$, or to $\delta(E)$. Using that ϱ is concrete, applying Lemma 6.7(g), this implies that no fraction of η can be branching bisimilar to $\delta(E)$. Consequently, we in fact have $\delta(\bar{E}) \xrightarrow{\alpha} \eta$. Moreover, no fraction of the transition $\delta(\bar{E}) \xrightarrow{\alpha} \eta$ can stem from the transition $\bar{E} \xrightarrow{\tau} [\![P_{i_0}]\!] = \delta(F) \,{}_r\!\oplus\, [\![P]\!]$. It follows that $\delta(H) \xrightarrow{\alpha} \eta$ with $\eta \leftrightarrows_b \varrho$.

For $\delta(\bar{E}) \,\mathcal{R}\, \delta(H)$, let $\delta(\bar{E}) \xrightarrow{\alpha} \varrho$. In case $\alpha \neq \tau$, trivially $\delta(H) \xrightarrow{\alpha} \varrho$ and we are done. So assume $\alpha = \tau$, First consider the case that $\varrho = \delta(F) \,{}_r\!\oplus\, [\![P]\!]$. For this case, we have shown above that $\delta(F) \xrightarrow{\tau} \mu'$ for some μ' with $\mu' \leftrightarrows_b [\![P]\!]$. Hence, by the previous case, $\delta(H) \xrightarrow{\tau} \eta$ for some η with $\eta \leftrightarrows_b \mu' \leftrightarrows_b [\![P]\!]$. Consequently, $\delta(H) \xrightarrow{(\tau)} \delta(H) \,{}_r\!\oplus\, \eta$. Furthermore, $\varrho = (\delta(F) \,{}_r\!\oplus\, [\![P]\!]) \,\mathcal{R}\, (\delta(H) \,{}_r\!\oplus\, \eta)$. The more general case is that $\varrho = (\delta(F) \,{}_r\!\oplus\, [\![P]\!]) \,{}_s\!\oplus\, \varrho'$ and $H \xrightarrow{\tau} \varrho'$ for some $s \in [0,1]$. Now $\delta(H) \xrightarrow{(\tau)} (\delta(H) \,{}_r\!\oplus\, \eta) \,{}_s\!\oplus\, \varrho'$ and $\varrho \,\mathcal{R}\, (\delta(H) \,{}_r\!\oplus\, \eta) \,{}_s\!\oplus\, \varrho'$.

Finally, we can show that $\tau \cdot P_{i_0} \sqsubseteq \partial(H)$, where $[\![P_{i_0}]\!] = \delta(F) \,{}_r\!\oplus\, [\![P]\!]$. This follows because $\delta(H) \xrightarrow{(\tau)} \delta(H) \,{}_r\!\oplus\, \eta$ for some $\eta \leftrightarrows_b [\![P]\!]$, as argued above. Using that $\delta(F) \leftrightarrows_b \delta(H)$, one has $[\![P_{i_0}]\!] \leftrightarrows_b \delta(H) \,{}_r\!\oplus\, \eta$.

Case (b). Suppose $P = \bigoplus_{i \in I} p_i * E_i$. By case (a) we can choose concrete $\bar{P}_i$ for each index $i \in I$, such that $AX_p^b \vdash \partial(E_i) \approx \bar{P}_i$. Put $\bar{P} = \bigoplus_{i \in I} p_i * \bar{P}_i$. Then $\bar{P} \in \mathcal{P}_{cc}$ by Lemma 6.7(b). By the definition of $\approx$ it follows that $AX_p^b \vdash \alpha \cdot P = \alpha \cdot \bar{P}$ for arbitrary $\alpha \in \mathcal{A}$.

Case (c). By the proof of part (b) we can find concrete $\bar{Q}, \bar{R} \in \mathcal{P}_{cc}$ such that $AX_p^b \vdash \alpha \cdot Q = \alpha \cdot \bar{Q}$ and $AX_p^b \vdash \alpha \cdot R = \alpha \cdot \bar{R}$ for all $\alpha \in \mathcal{A}$. Using soundness

(Lemma 6.3) this implies $\alpha \cdot Q \leftrightarrows_{rb} \alpha \cdot \bar{Q}$ and $\alpha \cdot R \leftrightarrows_{rb} \alpha \cdot \bar{R}$, and hence $Q \leftrightarrows_b \bar{Q}$ and $R \leftrightarrows_b \bar{R}$. By Lemma 6.8 we obtain from $\bar{Q} \leftrightarrows_b \bar{R}$ that $AX_p \vdash \bar{Q} = \bar{R}$ and hence $AX_p^b \vdash \alpha \cdot \bar{Q} = \alpha \cdot \bar{R}$ for $\alpha \in \mathcal{A}$. This implies $AX_p^b \vdash \alpha \cdot Q = \alpha \cdot R$ for $\alpha \in \mathcal{A}$ and finishes the proof. □

By now we have gathered all ingredients for showing that the theory AX_p^b is an equational characterization of rooted branching probabilistic bisimilarity. It is noted that in the proof of the theorem we exploit axiom C.

Theorem 6.10 (AX_p^b sound and complete for $\leftrightarrows_{rb}$). For all non-deterministic processes $E, F \in \mathcal{E}$ and all probabilistic processes $P, Q \in \mathcal{P}$ it holds that $E \leftrightarrows_{rb} F$ iff $AX_p^b \vdash E = F$ and $P \leftrightarrows_{rb} Q$ iff $AX_p^b \vdash P = Q$.

Proof. As we have settled the soundness of AX_p^b in Lemma 6.3, it remains to show that AX_p^b is complete. So, let $E, F \in \mathcal{E}$ such that $E \leftrightarrows_{rb} F$. Suppose $E = \sum_{i \in I} \alpha_i \cdot P_i$ and $F = \sum_{j \in J} \beta_j \cdot Q_j$ for suitable index sets I, J, actions α_i, β_j, and probabilistic processes P_i, Q_j.

Since, for each $i \in I$, $E \xrightarrow{\alpha_i} [\![P_i]\!]$ we have $\delta(F) \xrightarrow{\alpha_i} \bigoplus_{j \in J_i} q_{ij} * Q_j$ and $P_i \leftrightarrows_b \bigoplus_{j \in J_i} q_{ij} * Q_j$ for some subset $J_i \subseteq J$ and suitable $q_{ij} \geqslant 0$. Similarly, there exist for $j \in J$ a subset $I_j \subseteq I$ and $p_{ij} \geqslant 0$ such that $\delta(E) \xrightarrow{\beta_j} \bigoplus_{i \in I_j} p_{ij} * P_i$ and $Q_j \leftrightarrows_b \bigoplus_{i \in I_j} p_{ij} * P_i$. By $|J| + |I|$ series of applications of axiom C we obtain

$$AX_p \vdash E = \textstyle\sum_{i \in I} \alpha_i \cdot P_i + \sum_{j \in J} \beta_j \cdot (\bigoplus_{i \in I_j} p_{ij} * P_i), \text{ and} \tag{4}$$

$$AX_p \vdash F = \textstyle\sum_{j \in J} \beta_j \cdot Q_j + \sum_{i \in I} \alpha_i \cdot (\bigoplus_{j \in J_i} q_{ij} * Q_j)\,. \tag{5}$$

Since $P_i \leftrightarrows_b \bigoplus_{j \in J_i} q_{ij} * Q_j$ and $Q_j \leftrightarrows_b \bigoplus_{i \in I_j} p_{ij} * P_i$ we obtain by Lemma 6.9

$$AX_p^b \vdash \alpha_i \cdot P_i = \alpha_i \cdot \textstyle\bigoplus_{j \in J_i} q_{ij} * Q_j \text{ and } AX_p^b \vdash \beta_j \cdot Q_j = \beta_j \cdot \bigoplus_{i \in I_j} p_{ij} * P_i$$

for $i \in I$, $j \in J$. Combining this with Equations (4) and (5) yields $AX_p^b \vdash E = F$.

Now, let $P, Q \in \mathcal{P}$ such that $P \leftrightarrows_{rb} Q$. By Lemma 6.6 we have

$$AX_p \vdash P = \textstyle\bigoplus_{i \in I} p_i * E_i \qquad AX_p \vdash Q = \bigoplus_{i \in I} p_i * F_i \qquad \forall i \in I \colon E_i \leftrightarrows_{rb} F_i$$

for a suitable index set I, $p_i > 0$, $E_i, F_i \in \mathcal{E}$, for $i \in I$. By the conclusion of the first paragraph of this proof we have $AX_p^b \vdash E_i = F_i$ for $i \in I$. Hence $AX_p^b \vdash P = Q$. □

7 Concluding remarks

We presented an axiomatization of rooted branching probabilistic bisimilarity and proved its soundness and completeness. In doing so, we aimed to stay close to a straightforward completeness proof for the axiomatization of rooted branching bisimilarity for non-deterministic processes that employed concrete processes,

which is also presented in this paper. In particular, the route via concrete processes guided us to find the right formulation of the axioms BP and G for branching bisimilarity in the probabilistic case.

Future work will include the study of the extension of the setting of the present paper with a parallel operator [12]. In particular a congruence result for the parallel operator should be obtained, which for the mixed non-deterministic and probabilistic setting can be challenging. Also the inclusion of recursion [11,15] is a clear direction for further research.

The present conditional form of axioms BP and G is only semantically motivated. However, the axiom G has a purely syntactic counterpart of the form[4]

$$\alpha \cdot \big(\partial(\textstyle\sum_{i\in I} \tau \cdot (P_i \,{}_{r_i}\!\oplus\, \partial(E + \sum_{i\in I} \tau \cdot P_i)) + E + \sum_{i\in I} \tau \cdot P_i) \,{}_{r}\!\oplus\, Q \big) \\ = \alpha \cdot (\partial(E + \textstyle\sum_{i\in I} \tau \cdot P_i) \,{}_{r}\!\oplus\, Q) \,.$$

Admittedly, this form is a bit complicated to work with. An alternative approach could be to axiomatize the relation $\sqsubseteq$, or perhaps to introduce and axiomatize an auxiliary process operator $+'$ such that $E \sqsubseteq P$ can be translated into the condition $E +' P = P$ or similar.

Also, we want to develop a minimization algorithm for probabilistic processes modulo branching probabilistic bisimilarity. Eisentraut et al. propose in [13] an algorithm for deciding equivalence with respect to weak distribution bisimilarity relying on a state-based characterization, a result presently not available in our setting. Other work and proposals for weak bisimilarity include [8,14,31], but these do not fit well with the installed base of our toolset [7]. For the case of strong probabilistic bisimilarity without combined transitions we recently developed in [20] an algorithm improving upon the early results of [5]. In [31] a polynomial algorithm for Segala's probabilistic branching bisimilarity, which differs from our notion of probabilistic branching bisimilarity, is defined. We hope to arrive at an efficient algorithm by combining ideas from [32,33,31] and of [19,18].

References

1. S. Andova and S. Georgievska. On compositionality, efficiency, and applicability of abstraction in probabilistic systems. In M. Nielsen et al., editor, *Proc. SOFSEM 2009*, pages 67–78. LNCS 5404, 2009.
2. S. Andova, S. Georgievska, and N. Trcka. Branching bisimulation congruence for probabilistic systems. *Theoretical Computer Science*, 413:58–72, 2012.
3. S. Andova and T.A.C. Willemse. Branching bisimulation for probabilistic systems: Characteristics and decidability. *Theoretical Computer Science*, 356:325–355, 2006.
4. J.C.M. Baeten, T. Basten, and M.A. Reniers. *Process Algebra: Equational Theories of Communicating Processes*. Cambridge Tracts in Theoretical Computer Science 50. CUP, 2010.

[4] The extended abstract of this paper [16] also proposed a purely syntactic counterpart of axiom B; this turned out to be incorrect, however.

5. C. Baier, B. Engelen, and M.E. Majster-Cederbaum. Deciding bisimilarity and similarity for probabilistic processes. *Journal of Computer and System Sciences*, 60:187–231, 2000.
6. E. Bandini and R. Segala. Axiomatizations for probabilistic bisimulation. In F. Orejas et al., editor, *Proc. ICALP 2001*, pages 370–381. LNCS 2076, 2001.
7. O. Bunte, J.F. Groote, J.J.A. Keiren, M. Laveaux, T. Neele, E.P. de Vink, A. Wijs, J.W. Wesselink, and T.A.C. Willemse. The mCRL2 toolset for analysing concurrent systems. In T. Vojnar and L. Zhang, editors, *Proc. TACAS 2019*, pages 21–39. LNCS 11428, 2019.
8. S. Cattani and R. Segala. Decision algorithms for probabilistic bisimulation. In L. Brim et al., editor, *Proc. CONCUR 2002*, pages 371–386. LNCS 2421, 2002.
9. R. De Nicola and F.W. Vaandrager. Three logics for branching bisimulation. *Journal of the ACM*, 42(2):458–487, 1995.
10. Y. Deng, R.J. van Glabbeek, M. Hennessy, and C.C. Morgan. Testing finitary probabilistic processes (extended abstract). In M. Bravetti and G. Zavattaro, editors, *Proc. CONCUR'09*, LNCS 5710, pages 274–288, 2009.
11. Y. Deng and C. Palamidessi. Axiomatizations for probabilistic finite-state behaviors. *Theoretical Computer Science*, 373:92–114, 2007.
12. Y. Deng, C. Palamidessi, and J. Pang. Compositional reasoning for probabilistic finite-state behaviors. In A. Middeldorp et al., editor, *Processes, Terms and Cycles: Steps on the Road to Infinity*, pages 309–337. LNCS 3838, 2005.
13. C. Eisentraut, H. Hermanns, J. Krämer, A. Turrini, and L. Zhang. Deciding bisimilarities on distributions. In K. Joshi et al., editor, *Proc. QEST 2013*, pages 72–88. LNCS 8054, 2013.
14. L.M. Ferrer Fioriti, V. Hashemi, H. Hermanns, and A. Turrini. Deciding probabilistic automata weak bisimulation: theory and practice. *Formal Aspects of Computing*, 28:09–143, 2016.
15. N. Fisher and R.J. van Glabbeek. Axiomatising infinitary probabilistic weak bisimilarity of finite-state behaviours. *Journal of Logical and Algebraic Methods in Programming*, 102:64–102, 2019.
16. R.J. van Glabbeek, J.F. Groote, and E.P. de Vink. A complete axiomatization of branching bisimilarity for a simple process language with probabilistic choice (extended abstract). In M.S. Alvim, K. Chatzikokolakis, C. Olarte, and F. Valencia, editors, *The Art of Modelling Computational Systems: A Journey from Logic and Concurrency to Security and Privacy - Essays Dedicated to Catuscia Palamidessi on the Occasion of Her 60th Birthday*, LNCS 11760, pages 139–162, 2019.
17. R.J. van Glabbeek and W.P. Weijland. Branching time and abstraction in bisimulation semantics. *Journal of the ACM*, 43:555–600, 1996.
18. J.F. Groote, D.N. Jansen, J.J.A. Keiren, and A. Wijs. An $O(m\log n)$ algorithm for computing stuttering equivalence and branching bisimulation. *ACM Transactions on Computational Logic*, 18(2):13:1–13:34, 2017.
19. J.F. Groote and F.W. Vaandrager. An efficient algorithm for branching bisimulation and stuttering equivalence. In M. Paterson, editor, *Proc. ICALP'90*, pages 626–638. LNCS 443, 1990.
20. J.F. Groote, H.J. Rivera Verduzco, and E.P. de Vink. An efficient algorithm to determine probabilistic bisimulation. *Algorithms*, 11(9):131,1–22, 2018.
21. J.F. Groote and E.P. de Vink. Problem solving using process algebra considered insightful. In J.-P. Katoen, R. Langerak, and A. Rensink, editors, *ModelEd, TestEd, TrustEd – Essays Dedicated to Ed Brinksma on the Occasion of His 60th Birthday*, pages 48–63. LNCS 10500, 2017.

22. H. Hansson and B. Jonsson. A calculus for communicating systems with time and probabilities. In *Proc. RTSS 1990*, pages 278–287. IEEE, 1990.
23. M. Hennessy. Exploring probabilistic bisimulations, part I. *Formal Aspects of Computing*, 24:749–768, 2012.
24. M. Hennessy and R. Milner. On observing nondeterminism and concurrency. In J.W. de Bakker & J. van Leeuwen, editor, *Proc. ICALP 1980*, pages 299–309. LNCS 85, 1980.
25. M.D. Lee and E.P. de Vink. Logical characterization of bisimulation for transition relations over probability distributions with internal actions. In P. Faliszewski, A. Muscholl, and R. Niedermeier, editors, *Proc. MFCS 2016*, LIPIcs 58, pages 29:1–29:14. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2016.
26. R. Milner. *Communication and Concurrency*. Prentice Hall, 1989.
27. R. Milner. A complete axiomatization for observational congruence of finite-state behaviours. *Information and Computation*, 81(2):227–247, 1989.
28. R. Segala. *Modeling and Verification of Randomized Distributed Real-Time Systems*. PhD thesis, MIT, 1995. Technical Report MIT/LCS/TR–676.
29. R. Segala and N.A. Lynch. Probabilistic simulations for probabilistic processes. In B. Jonsson & J. Parrow, editor, *Proc. CONCUR 94*, pages 481–496. LNCS 836, 1994.
30. M. Stoelinga. Alea Jacta est*: Verification of probabilistic, real-time and parametric systems*. PhD thesis, Radboud Universiteit, 2002.
31. A. Turrini and H. Hermanns. Polynomial time decision algorithms for probabilistic automata. *Information and Computation*, 244:134–171, 2015.
32. A. Valmari. Simple bisimilarity minimization in $O(m\log n)$ time. *Fundamenta Informaticae*, 105(3):319–339, 2010.
33. A. Valmari and G. Franceschinis. Simple $O(m\log n)$ time Markov chain lumping. In J. Esparza and R. Majumdar, editors, *Proc. TACAS 2010*, pages 38–52. LNCS 6015, 2010.