A Complete Axiomatisation of Distribution-Based Branching Bisimilarity for Non-Deterministic and Probabilistic Choice

R.J. van Glabbeek*

School of Informatics, University of Edinburgh, UK

School of Computer Science and Engineering, University of New South Wales, Australia

J.F. Groote

Department of Mathematics and Computer Science, Eindhoven University of Technology, The Netherlands

E.P. de Vink**

Department of Mathematics and Computer Science, Eindhoven University of Technology, The Netherlands

---

Abstract

This paper proposes a notion of branching bisimilarity for non-deterministic probabilistic processes. In order to characterise 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 axiomatisation 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 generalised to incorporate probabilistic choice, too.

---

1. Introduction

In [13], 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 [34, 35]. The process language treated in [13] includes recursion, thereby extending the calculus and axiomatisation of [7]. While the weak transitions of [13] can be characterised as finitary, infinitary semantics is treated in [17], providing a sound and complete axiomatisation also building on the seminal work of Milner [35].

In this paper we focus on branching bisimilarity in the sense of [22], rather than on weak bisimilarity as in [7, 13, 17]. In the non-probabilistic setting branching bisimilarity has the advantage

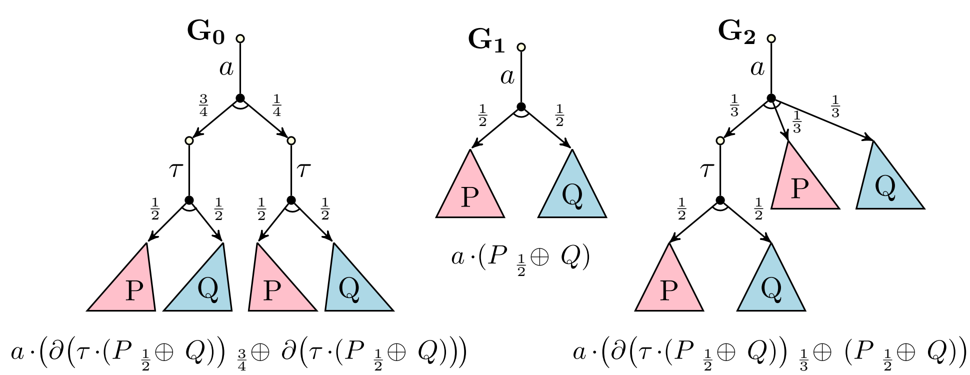
*Supported by Royal Society Wolfson Fellowship RSWF\R1\221008.

**Corresponding author.

over weak bisimilarity that it has substantially more efficient algorithms [23, 26]. Furthermore, branching bisimilarity has a strong logical underpinning [11]. It would be attractive to have these advantages available also in the probabilistic case, in particular for the support of model checking which is more demanding in the probabilistic setting than in the non-deterministic one. See also the initial work reported in [28].

For a similarly basic process language as in [13], without recursion though, we propose a notion of branching probabilistic bisimilarity as well as a sound and complete equational axiomatisation of its rooted version. Hence, instead of lifting all τ-laws to the probabilistic setting, we need to do this here for the well-known B-axiom of [22], the single axiom capturing inert silent steps. For what is referred to as the alternating model [29], branching probabilistic bisimilarity has been studied in [2, 3]. Also [36, 37] discuss 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.

In view of the above, our investigation is led by the wish to identify the three processes below, involving as a subprocess a probabilistic choice between probabilistic processes P and Q with equal probability for each. Essentially, ignoring the occurrence of the initial action a, the three processes represent (i) a probabilistic choice between two instances of the subprocess mentioned, the one with probability $\frac{3}{4}$, the other with probability $\frac{1}{4}$, (ii) the subprocess on its own, and (iii) a probabilistic choice between the subprocess guarded by a τ-prefix with probability $\frac{1}{3}$ and a rescaling of the subprocess, selected with probability $\frac{2}{3}$ for P and Q together, thus with probability $\frac{1}{3}$ for P and Q individually.



In our view, the three processes starting from $\mathbf{G_0}$, $\mathbf{G_1}$ and $\mathbf{G_2}$ are to be identified. The behaviour that can be observed from them when ignoring τ-steps and exploiting 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 [15].

As for [13] 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 a novel definition, viz. that 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 behaviour 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.

Related work. Our branching probabilistic bisimulation semantics is essentially *distribution-based*, in the sense that it employs bisimulation relations between probability distributions of states that cannot be reduced to relations between states. This feature makes it coarser, or less discriminating, than the state-based branching probabilistic bisimulation semantics of Segala & Lynch [37], which distinguishes the processes $\mathbf{G_0}$, $\mathbf{G_1}$ and $\mathbf{G_2}$. Distribution-based notions of weak probabilistic simulation and bisimulation semantics were explored in [12] and [15]. The standard pair of processes $a \cdot (\tau \cdot b + c)$ vs. $a \cdot (\tau \cdot b + c) + a \cdot b$ that are equivalent for weak bisimilarity but inequivalent for branching bisimulation (see e.g. [25]) yields the same observation when translated to the probabilistic setting: identified by weak distribution equivalence as introduced in [15] but different with respect to branching probabilistic bisimulation proposed here. However, the paper [15] additionally presents a decision procedure for their probabilistic equivalence based on the notion of maximal end components and on earlier results reported in [32].

A state-based approach to branching probabilistic bisimilarity by Andova and Willemse is presented in [3]. The focus in the paper is on the handling of τ-loops in probabilistic processes represented by finite bipartite graphs. The ensuing behavioural notion can be characterised in terms of concrete coloured traces involving so-called blends of colours. The technique of [3] generalises the paradigm of coloured traces for the non-deterministic setting originating from [22] to the setting of mixed non-deterministic and probabilistic processes. However, equivalence based on concrete coloured traces is finer grained than the branching bisimilarity as proposed here. For example, referring forward to Figure 2, the processes $\mathbf{T}_1$ to $\mathbf{T}_2$ are not identified in the setting of [3], contrary to the present paper, because in [3] there is no means to identify the equal blend of the two colours $b \cdot (\frac{1}{3}P \oplus \frac{2}{3}Q)$ and $b \cdot (\frac{2}{3}P \oplus \frac{1}{3}Q)$ with the single colour blend of $b \cdot (\frac{1}{2}P \oplus \frac{1}{2}Q)$.

The comprehensive account [5] of the 'probabilistic bisimulation spectrum with silent moves' focuses on the analysis of branching, delay, η, vs. weak bisimilarity (in various stuttering and divergence flavours) for which corresponding Hennessy/Milner style modal logics are shown to be sound and complete. The paper predominantly considers state-based behavioural equivalences. As argued in [15], state-based equivalences with equivalences on distributions induced by so-called lifting do not deal with silent moves in the way aimed for in [15]—and here. The processes $\mathbf{G_0}$, $\mathbf{G_1}$, and $\mathbf{G_2}$ above are all distinguished in these state-based equivalences because the distributions involved assign different probabilities to (the non-deterministic processes in the support of) P and Q, and $\tau \cdot (\frac{1}{2}P \oplus \frac{1}{2}Q)$.

Our syntax for processes is two-sorted, and comprises nondeterministic processes, ranged over by E, F, and probabilistic processes, ranged over by P, Q. Following [7, 12], nondeterministic processes denote states in a probabilistic labelled transition system, whereas probabilistic processes denote probability distributions of states. They are connected through the operator ∂, which turns a nondeterministic process E into a probabilistic processes $\partial(E)$, denoting the Dirac distribution $\delta(E)$, which assigns all its probabilistic weight to the state E. In [12] the operator ∂ was elided, thereby identifying the processes E and $\partial(E)$. This practice naturally leads to semantic equivalences $\sim$ satisfying

$$E \sim F \Leftrightarrow \partial(E) \sim \partial(F) \; . \tag{1}$$

In fact, this property holds for any semantic equivalence $\sim$ from the literature that we know of, and for which both sides are defined.

In [20], which is an extended abstract of an earlier version of the present paper, we present a complete axiomatisation of a form of branching probabilistic bisimulation semantics that on nondeterministic processes coincides with the version in the present paper, but on probabilistic processes it is strictly finer. Whereas that semantics satisfies (1), our present semantics merely has the congruence property $E \sim F \Rightarrow \partial(E) \sim \partial(F)$. This is because for nondeterministic processes we impose a root condition, making branching probabilistic bisimilarity into a congruence for the CCS choice operator $+$, whereas we refrain from doing so for probabilistic processes.

The remainder of the paper is organised as follows. In Section 2 we gather some notation regarding probability distributions. For illustration purposes Section 3 treats the simpler setting of nondeterministic processes, reiterating the completeness proof for the equational theory of [22] for rooted branching bisimilarity. Next, after introducing probabilistic processes in Section 4 and branching probabilistic bisimilarity and some of its fundamental properties in Section 5, we prove in Section 6 the main result, viz. the completeness of an equational theory for rooted branching probabilistic bisimilarity, exploiting the notion of a concrete process and 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 probability distributions of finite support over the set X. The support of a distribution μ is denoted as $\mathit{spt}(\mu)$, thus $\mathit{spt}(\mu) = \{\, x \in X \mid \mu(x) > 0 \,\}$. Each distribution $\mu \in \mathit{Distr}(X)$ can be represented in the form $\mu = \bigoplus_{i \in I} p_i \cdot x_i$ where $\mu(x_i) = p_i$ for $i \in I$ and $\sum_{i \in I} p_i = 1$ for some finite index set I. For convenience later, we do not require $x_i \neq x_{i'}$ for $i \neq i'$ nor $p_i > 0$ for $i, i' \in I$. So, the representation of μ is not unique.

We use $\delta(x)$ to denote the Dirac distribution for $x \in X$ with $\delta(x)(x) = 1$ and $\delta(x)(y) = 0$ for $y \in X$, $y \neq x$. 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 $\bigoplus_{i \in I} p_i \cdot \mu_i \in \mathit{Distr}(X)$ by $(\bigoplus_{i \in I} p_i \cdot \mu_i)(x) = \sum_{i \in I} p_i \cdot \mu_i(x)$ for $x \in X$. For $\mu = \bigoplus_{i \in I} p_i \cdot \mu_i$, $\nu = \bigoplus_{i \in I} p_i \cdot \nu_i$, and $r \in [0,1]$ it holds that $\mu \,{}_r\!\oplus\, \nu = \bigoplus_{i \in I} (\mu_i \,{}_r\!\oplus\, \nu_i)$. For a subset $X' \subseteq X$ and distribution $\mu \in \mathit{Distr}(X)$, we occasionally write $\mu[X']$ for $\sum_{x \in X'} \mu(x)$.

Given a binary relation $\mathcal{R} \subseteq \mathit{Distr}(X) \times \mathit{Distr}(X)$ between distributions, its *convex closure* $cc(\mathcal{R})$ is defined by $cc(\mathcal{R}) := \{ (\bigoplus_{i \in I} p_i \cdot \mu_i, \bigoplus_{i \in I} p_i \cdot \nu_i) \mid \forall i \in I.\ (\mu_i, \nu_i) \in \mathcal{R} \wedge \sum_{i \in I} p_i = 1 \}$.

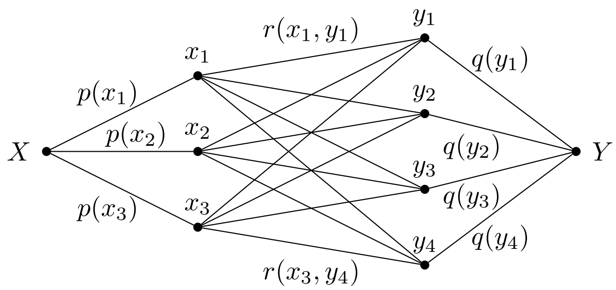


Figure 1: Distributions p on X, q on Y, and r on $X \times Y$.

In the sequel we make frequent use of the following property. If $p : X \to \mathbb{R}$ and $q : Y \to \mathbb{R}$ are (weight) functions of finite support such that $p[X] = q[Y]$, then there is an $r : X \times Y \to \mathbb{R}$ satisfying $p(x) = \sum_{y \in Y} r(x, y)$ for all $x \in X$ and $q(y) = \sum_{x \in X} r(x, y)$ for all $y \in Y$. See Figure 2. For p and q distributions one can define $r(x, y) = p(x)q(y)$. A direct proof is by application of the max-flow min-cut theorem assigning capacity 1 to the edges (x_i, y_j), cf. [19].

3. Concrete processes

In this section we present an approach to prove completeness of an axiomatic theory for branching bisimilarity exploiting the notion of a concrete process. To explicate the concept, we consider a basic process language with inaction, prefix, and non-deterministic choice only. The result is not new, but the approach is non-standard. In the remainder of the paper we extend the approach to establish the completeness of an axiomatisation of branching probabilistic bisimulation.

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 a constant for inaction $\mathbf{0}$, a prefix construct for each action $\alpha \in \mathcal{A}$, and non-deterministic choice between to processes.

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 $\mathcal{A}$.

As technical aid below, we define for $E \in \mathcal{E}$ 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 behaviour of processes in $\mathcal{E}$ is as usual and given by a structural operational semantics going back to [31].

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

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

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

Thus, 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 behaviour between that of E_1 and of E_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 $n \geqslant 0$, $E_0, \ldots, E_n \in \mathcal{E}$, and $\alpha_1, \ldots, \alpha_n$ exist such that $E = E_0$, $E_{i-1} \xrightarrow{\alpha_i} E_i$ for $1 \leqslant i \leqslant n$, and $E_n = E'$. We define $der(E) = \{ E' \in \mathcal{E} \mid E' \text{ is a derivative of } E \}$. 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 $\Longrightarrow$ to denote the reflexive transitive closure of $\xrightarrow{(\tau)}$.

The definitions of strong and branching bisimilarity for $\mathcal{E}$ are standard and adapted from [22, 34].

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 $E, E', F \in \mathcal{E}$ such that $E \mathrel{\mathcal{R}} F$ and $E \xrightarrow{\alpha} E'$ there is an $F' \in \mathcal{E}$ such that

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

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

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

(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. Thus $\leftrightarroweq \subseteq \leftrightarroweq_b$.

The notion of an *inert* transition is well-known, see [22]: if for a transition $E \xrightarrow{\tau} E'$ we have that $E \leftrightarroweq_b E'$, the transition is called *inert*. Much less well-known is the derived notion of a *concrete* process, going back to [24]: a process $\bar{E}$ is called concrete iff it has no inert transitions, i.e., if $\bar{E}' \in der(\bar{E})$ and $\bar{E}' \xrightarrow{\tau} \bar{E}''$, then $\bar{E}' \not\leftrightarroweq_b \bar{E}''$. Note, for $\bar{E}' \in der(\bar{E})$ we have $der(\bar{E}') \subseteq der(\bar{E})$, thus $\bar{E}'$ is concrete if $\bar{E}$ is. A straightforward example of a concrete process is $a \cdot \mathbf{0} + b \cdot \mathbf{0}$ in which no τ-actions occur at all, but also $a \cdot \mathbf{0} + \tau \cdot b \cdot \mathbf{0}$ is a concrete process since $a \cdot \mathbf{0} + \tau \cdot b \cdot \mathbf{0} \not\leftrightarroweq_b b \cdot \mathbf{0}$ (assuming $a \neq b$). 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, cf. [18]. 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, cf. [34].

For example, we have for any process $E \in \mathcal{E}$ 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 that

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

Table 1: Axioms for strong and branching bisimilarity

$E{+}F \leftrightarroweq_b \tau \cdot E{+}F$. More concretely, although $\mathbf{0} \leftrightarroweq_b \tau \cdot \mathbf{0}$, it doesn't 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 $\mathbf{0} + b \cdot \mathbf{0} \not\leftrightarroweq_b \mathbf{0}$. Intuitively, the summand $\tau \cdot \mathbf{0}$ can preempt non-deterministic alternatives whereas the summand $\mathbf{0}$ cannot.

Definition 3.4. Two nondeterministic processes $E, F \in \mathcal{E}$ are *rooted branching bisimilar*, notation $E \leftrightarroweq_{rb} F$, if for each transition $E \xrightarrow{\alpha} E'$ with $\alpha \in \mathcal{A}$ there is a transition $F \xrightarrow{\alpha} F'$ with $E' \leftrightarroweq_b F'$, and, vice versa, for each transition $F \xrightarrow{\alpha} F'$ there is a transition $E \xrightarrow{\alpha} E$ with $E' \leftrightarroweq_b F'$.

When comparing processes $E, F \in \mathcal{E}$, rooted branching bisimilarity requires 'strong' bisimilarity at the root, i.e. for E and F themselves, and allows branching bisimilarity for the derivatives of E and F.

Direct from the definitions we obtain $\leftrightarroweq \subseteq \leftrightarroweq_{rb} \subseteq \leftrightarroweq_b$. As eluded upon, we have a congruence result for rooted branching bisimilarity. A proof is given in [22].

Lemma 3.5. $\leftrightarroweq_{rb}$ is a congruence on $\mathcal{E}$ for the operators $\cdot$ and $+$. □

In [22] it is also shown that $\leftrightarroweq_{rb}$ is the coarsest, or largest, congruence included in $\leftrightarroweq_b$. It is well-known that both strong bisimilarity and branching bisimilarity for $\mathcal{E}$ can be equationally characterised [4, 22, 34]. In line with the so-called root condition of Definition 3.4, a prefix context $\alpha \cdot \_$ is added in the B-axiom.

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 with respect to the theory AX^b, then they are rooted branching bisimilar as well.

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

Proof. (Sketch) It is easy to see that the left-hand side and the right-hand side of the axioms of AX^b are rooted branching bisimilar. For example, for $\alpha \in \mathcal{A}$ and $E, F \in \mathcal{E}$, the processes $\alpha \cdot (F + \tau \cdot (E + F))$ and $\alpha \cdot (E + F)$ in axiom B both have an α-transition as their only transition, which yield the branching bisimilar processes $F + \tau \cdot (E + F)$ and $E + F$, respectively. To finish the proof of this lemma, one observes that rooted branching bisimilarity is a congruence, see Lemma 3.5. □

In order to obtain a completeness result for AX^b modulo $\leftrightarrow_{rb}$ we deviate from the usual approach to prepare the stage for the proof of completeness with respect to branching probabilistic bisimilarity as presented in Section 6. Here, we will proceed along the following route.

1. First we observe that the theory AX, without the B-axiom, is (sound and) complete with respect to strong bisimilarity; this is Theorem 3.8.

2. Next, we obtain a result stating that for concrete processes, which have by definition no inert τ-transitions, branching bisimilarity implies strong bisimilarity, and hence, the axiom set AX is complete for branching bisimilarity if processes are concrete, see Lemma 3.9.

3. Then we have a technical result, relating to each process $E \in \mathcal{E}$ a concrete and branching bisimilar process $\bar{E} \in \mathcal{E}_{cc}$ such that E and $\bar{E}$ are equal for AX^b. This is Lemma 3.10.

4. Finally we combine the above results to obtain completeness of AX^b for $\leftrightarrow_{rb}$ as stated by Theorem 3.11.

So, we start off by noting that strong bisimilarity is equationally characterised by the axioms A1 to A4 of Table 1. See for example [34, Section 7.4] for a proof.

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

Next we consider concrete processes and branching bisimilarity. Since by their definition, concrete processes have no inert transitions, it holds that branching bisimilarity and strong bisimilarity coincide. Hence, by the above theorem, Theorem 3.8, branching bisimilarity implies equality for AX.

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

Sketch. Consider $\bar{E}, \bar{F} \in \mathcal{E}_{cc}$ such that $\bar{E} \leftrightarrow_b \bar{F}$. Define the relation $\mathcal{R} \subseteq \mathcal{E} \times \mathcal{E}$ to be the restriction of branching bisimilarity $\leftrightarrow_b$ to the derivatives of $\bar{E}$ and $\bar{F}$, i.e., $\mathcal{R} = \leftrightarrow_b \cap ((der(\bar{E}) \times der(\bar{F})) \cup (der(\bar{F}) \times der(\bar{E})))$. Then $\mathcal{R}$ is a strong bisimulation relation, since none of the processes involved admits an inert τ-transition. In more detail, if $\hat{E} \,\mathcal{R}\, \hat{F}$ and $\hat{E} \xrightarrow{\alpha} \hat{E}'$, then $\hat{F} \Longrightarrow \tilde{F}$ and $\tilde{F} \xrightarrow{(\alpha)} \hat{F}'$ for suitable processes $\tilde{F}$ and $\hat{F}'$ with $\tilde{F} \,\mathcal{R}\, \hat{F}$ and $\hat{F} \leftrightarrow_b \hat{E}'$. Since $\hat{F} \in der(\bar{E}) \cup der(\bar{F})$ is a concrete process as well, we must have $\hat{F} = \tilde{F}$. Thus $\hat{F} \xrightarrow{(\alpha)} \hat{F}'$. If $\alpha = \tau$ and $\hat{F}$ and $\hat{F}'$ would coincide, it follows that $\hat{E} \xrightarrow{\tau} \hat{E}'$ while $\hat{E} \leftrightarrow_b \hat{F} \leftrightarrow_b \hat{F}' \leftrightarrow_b \hat{E}'$, which cannot be since $\hat{E}$ is concrete. Thus $\hat{F} \xrightarrow{\alpha} \hat{F}'$ for $\hat{F}' \leftrightarrow_b \hat{E}'$ and showing that $\mathcal{R}$ is a strong bisimulation relation and $\bar{E} \leftrightarrow \bar{F}$.

To finish the proof of the lemma, by the completeness of AX with respect to strong bisimulation, see Theorem 3.8, it follows that $AX \vdash \bar{E} = \bar{F}$. □

We have now arrived at the main technical lemma of this section, viz. the result that branching bisimilarity implies equality for AX^b under a prefix. In the proof the notion of a concrete process plays a central role. On the one hand, the lemma aims to reduce the question of equality for general processes to the question of equality for concrete processes by appointing a concrete and branching bisimilar counterpart for each non-deterministic process. On the other hand, the lemma guarantees equality in the context of a prefix for branching bisimilar processes.

Lemma 3.10.

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

Proof. We prove statements (a) and (b) by simultaneous induction on $c(E)$ and $\max\{c(F), c(G)\}$, respectively. The complexity measure c is given right after Definition 3.1.

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

Induction step, $c(E) > 0$: The process E can be written as $\sum_{i \in I} \alpha_i \cdot E_i$ for some finite index set I and suitable actions $\alpha_i \in \mathcal{A}$ and subprocesses $E_i \in \mathcal{E}$. We distinguish two cases.

Case I. We first assume that for some $i_o \in I$ we have $\alpha_{i_o} = \tau$ and $E_{i_o} \leftrightarroweq_b E$. Then it holds that $AX \vdash E = \tau.E_{i_o} + H$, where $H = \sum_{i \in I \setminus \{i_o\}} \alpha_i \cdot E_i$. By the induction hypothesis for part (a), there is a concrete process $\bar{E}_{i_o} \in \mathcal{E}_{cc}$ such that $E_{i_o} \leftrightarroweq_b \bar{E}_{i_o}$. We claim that $\bar{E}_{i_o} \leftrightarroweq_b E_{i_o} + H$.

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

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

We conclude that $E_{i_o} \leftrightarroweq_b \bar{E}_{i_o} \leftrightarroweq_b E_{i_o} + H$ as claimed. By definition of c it holds that $c(E_{i_o}), c(E_{i_o} + H) < c(\tau \cdot E_{i_o} + H) = c(E)$. Therefore, by the induction hypothesis for part (b) for the two processes E_{i_o} and $E_{i_o} + H$, it holds that $AX^b \vdash \tau \cdot E_{i_o} = \tau \cdot (E_{i_o} + H)$, which we will use below. By the induction hypothesis for part (a), there is a process $\bar{E} \in \mathcal{E}_{cc}$ such that $\bar{E} \leftrightarroweq_b E_{i_o} + H$ and $AX^b \vdash \alpha \cdot \bar{E} = \alpha \cdot (E_{i_o} + H)$ for every $\alpha \in \mathcal{A}$. Observe that $E \leftrightarroweq_b E_{i_o} \leftrightarroweq_b E_{i_o} + H \leftrightarroweq_b \bar{E}$. Therefore, we can calculate

$$
\begin{aligned}
AX^b \vdash \alpha \cdot E &= \alpha \cdot (\tau \cdot E_{i_o} + H) \\
&= \alpha \cdot (\tau \cdot (E_{i_o} + H) + H) && \text{Since } AX^b \vdash \tau \cdot E_{i_o} = \tau \cdot (E_{i_o} + H) \\
&= \alpha \cdot (E_{i_o} + H) && \text{Axiom B} \\
&= \alpha \cdot \bar{E} && \text{Choice of } \bar{E}.
\end{aligned}
$$

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

Case II. Now suppose, for all $i \in I$ we have $\alpha_i \neq \tau$ or $E_i \not\leftrightarroweq_b E$. Clearly $c(E_i) < c(E)$ for all $i \in I$. By the induction hypothesis for part (a) we can find, for all $i \in I$, a concrete process $\bar{E}_i$ such that $\bar{E}_i \leftrightarroweq_b E_i$ and $AX^b \vdash \alpha \cdot \bar{E}_i = \alpha \cdot E_i$ for every action $\alpha \in \mathcal{A}$. Define $\bar{E} = \sum_{i \in I} \alpha_i \cdot \bar{E}_i$. Then $\bar{E} \leftrightarroweq_b E$ and $\bar{E}$ is concrete too, since $\bar{E}_i \leftrightarroweq_b E_i \not\leftrightarroweq_b E \leftrightarroweq_b \bar{E}$ 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 all actions $\alpha \in \mathcal{A}$, it holds that $AX^b \vdash \alpha \cdot E = \alpha \cdot \bar{E}$.

Basis, $\max\{c(F), c(G)\} = 0$: As for the base case for E, we have $F, G \leftrightarroweq_b \mathbf{0}$ and $AX^b \vdash \alpha \cdot F = \alpha \cdot \mathbf{0} = \alpha \cdot G$.

Induction step, $\max\{c(F), c(G)\} > 0$: Suppose $F \leftrightarroweq_b G$. Choose, by the induction hypothesis for part (a), $\bar{F}, \bar{G} \in \mathcal{E}_{cc}$ such that $F \leftrightarroweq_b \bar{F}$ 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 $\bar{F} \leftrightarroweq_b \bar{G}$. 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 $AX^b \vdash \alpha \cdot F = \alpha \cdot \bar{F} = \alpha \cdot \bar{G} = \alpha \cdot G$. □

With Lemma 3.10 in place, we have by now gathered sufficient building blocks to provide a completeness proof for AX^b based on concrete processes.

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

Proof. Suppose $E, F \in \mathcal{E}$ and $E \leftrightarroweq_{rb} F$. 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, $\alpha_i, \beta_j \in \mathcal{A}$, $E_i, F_j \in \mathcal{E}$ (tacitly using theory AX). Since $E \leftrightarroweq_{rb} F$ we have that for all $i \in I$ there is a $j \in J$ such that $\alpha_i = \beta_j$ and $E_i \leftrightarroweq_b F_j$, and, symmetrically, that for all $j \in J$ there is an $i \in I$ such that $\alpha_i = \beta_j$ and $E_i \leftrightarroweq_b F_j$. Put $K = \{ (i,j) \in I \times J \mid (\alpha_i = \beta_j) \wedge (E_i \leftrightarroweq_b F_j) \}$. Define the processes $G, H \in \mathcal{E}$ by

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

where, for $i \in I$, $\gamma_k = \alpha_i$ and $G_k = E_i$ if $k = (i,j)$ for some $j \in J$, and, similarly for $j \in J$, $\zeta_k = \beta_j$ and $H_k = F_j$ 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 $G_k = E_i \leftrightarroweq_b F_j = H_k$, 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 $AX^b \vdash E = \sum_{i \in I} \alpha_i \cdot E_i = \sum_{k \in K} \gamma_k \cdot G_k = \sum_{k \in K} \zeta_k \cdot H_k = \sum_{j \in J} \beta_j \cdot F_j = F$ which concludes the proof of the theorem. □

In summary, in this section we describe a proof method for completeness, in particular, of an axiomatisation of branching bisimilarity in the setting of a simple non-deterministic process language. The key building blocks of the method are the completeness of strong bisimilarity and the lemma that every process has a branching bisimilar concrete counterpart. In the sequel of the paper we apply the proof method to obtain a complete axiomatisation of branching probabilistic bisimulation for a process language featuring both non-deterministic and probabilistic choice.

4. Probabilistic processes

In this section we define a syntax and a transition system semantics for probabilistic processes. Following [7], we start with adapting the syntax of the processes of Section 3, by mixing non-deterministic and probabilistic choice. Dependent on the top operator, a process is either a non-deterministic process $E \in \mathcal{E}$, for constant $\mathbf{0}$, prefix operators $\alpha\,\cdot$, and non-deterministic choice $+$, or a probabilistic process $P \in \mathcal{P}$, for the Dirac operator ∂ and probabilistic choices ${}_r\oplus$.

Definition 4.1 (Syntax). The classes $\mathcal{E}$ and $\mathcal{P}$ of non-deterministic and probabilistic processes, respectively, over the set of actions $\mathcal{A}$, 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 $r \in (0,1)$.

We use $E, F, G, \ldots$ to range over $\mathcal{E}$ and $P, Q, R, \ldots$ to range over $\mathcal{P}$. The probabilistic process $P_1 \,{}_{r}\!\oplus P_2$ executes the behaviour of P_1 with probability r and the behaviour P_2 with probability $1-r$. By convention, $P \;{}_{1}\!\oplus\; Q$ denotes P and $P \;{}_{0}\!\oplus\; Q$ denotes Q.

In the sequel we often write $\bigoplus_{i=1}^{n} p_i \cdot E_i$ for $n \geqslant 1$, $p_1, \ldots, p_n \geqslant 0$ such that $p_1 + \cdots + p_n = 1$ and $E_1, \ldots, E_n \in \mathcal{E}$ for the probabilistic process given by $\bigoplus_{i=1}^{n} p_i \cdot E_i = \partial(E_1)$ if $p_1 = 1$ and $\bigoplus_{i=1}^{n} p_i \cdot E_i = \partial(E_1) \;{}_{p_1}\!\oplus\; \big(\bigoplus_{i=2}^{n} \frac{p_i}{1-p_1} \cdot E_i\big)$ otherwise. For example, for non-deterministic processes E, F and G, we have that $\frac{1}{2} \cdot E \oplus \frac{1}{3} \cdot F \oplus \frac{1}{6} \cdot G$ is the probabilistic process $\partial(E) \;{}_{\frac{1}{2}}\!\oplus\; (\partial(F) \;{}_{\frac{2}{3}}\!\oplus\; \partial(G))$. Similarly we use the notation $\bigoplus_{i=1}^{n} p_i \cdot P_i$ where $n \geqslant 1$, $p_1, \ldots, p_n > 0$, $p_1 + \cdots + p_n = 1$ and $P_1, \ldots, P_n \in \mathcal{P}$, and also the notation $\bigoplus_{i \in I} p_i \cdot P_i$ for an ordered finite index set I. As a consequence, each non-deterministic process $E \in \mathcal{E}$ and each probabilistic process $P \in \mathcal{P}$ can be written as

$$E = \textstyle\sum_{i \in I} \alpha_i \cdot P_i \quad \text{and} \quad P = \bigoplus_{j \in J} p_j \cdot E_j$$

for suitable index sets I and J, $\alpha_i \in \mathcal{A}$, $P_i \in \mathcal{P}$ for $i \in I$, and $p_j > 0$, $E_j \in \mathcal{E}$ for $j \in J$ such that $\sum_{j \in J} p_j = 1$. The proof is straightforward by induction on the structure of terms.

Figure 2 presents a number of example pairs of (rooted branching probabilistic bisimilar) non-deterministic processes collected from the literature. The examples $\mathbf{H_1}$ and $\mathbf{H_2}$ are taken from [30]; $\mathbf{G_1}$ and $\mathbf{G_2}$ are taken from [20]. Examples $\mathbf{B_1}$ and $\mathbf{B_2}$ express the axiom called B in [22], cast to the setting of the present paper. The processes $\mathbf{I_1}$ and $\mathbf{I_2}$ are typical instances of $\mathbf{B_1}$ and $\mathbf{B_2}$. The two examples $\mathbf{E_1}$ and $\mathbf{E_2}$ are adapted from [15], while the new examples $\mathbf{T_1}$ and $\mathbf{T_2}$ further illustrate the intricacy of the mingling of probabilistic choice and action prefix.

As usual, the SOS semantics for $\mathcal{E}$ and $\mathcal{P}$ makes use of two types of transition relations [29, 7].

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 $\mu = \bigoplus_{i \in I} p_i \cdot E_i$, $\mu' = \bigoplus_{i \in I} p_i \cdot \mu'_i$, and $E_i \xrightarrow{\alpha} \mu'_i$ for all $i \in I$.

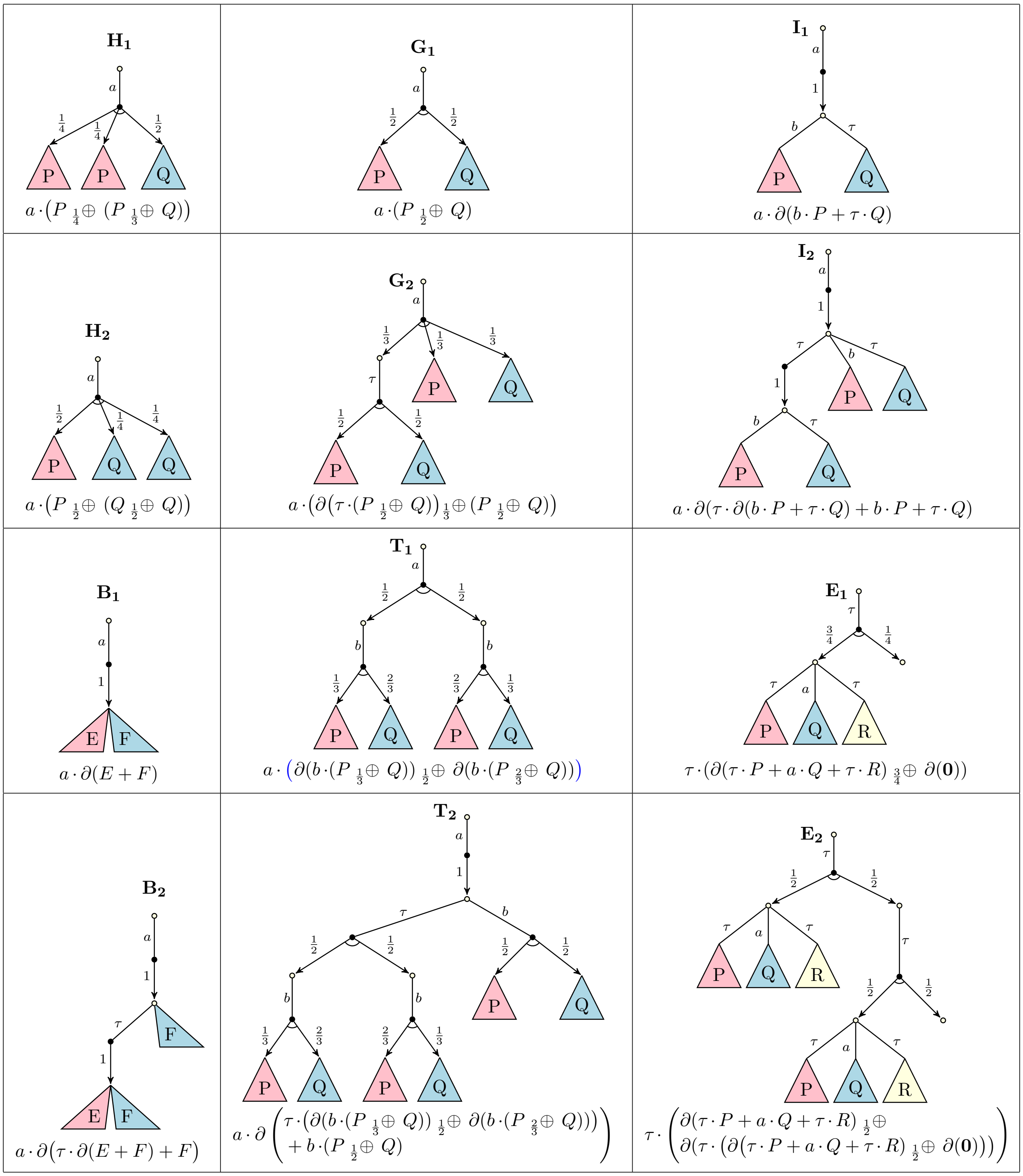


Figure 2: Pairwise rooted branching probabilistic bisimilar non-deterministic processes.

With $[\![P]\!]$, for $P \in \mathcal{P}$, we denote the unique distribution μ such that $P \mapsto \mu$. Thus, the probabilistic process $\bigoplus_{i\in I} p_i \cdot E_i$ corresponds to the distribution $[\![\bigoplus_{i\in I} p_i \cdot E_i]\!] = \bigoplus_{i\in I} p_i \cdot \delta(E_i)$. Similarly, for $\bigoplus_{i\in I} p_i \cdot P_i \in \mathcal{P}$ we have $[\![\bigoplus_{i\in I} p_i \cdot P_i]\!] = \bigoplus_{i\in I} p_i \cdot [\![P_i]\!]$.

Following [37, 36], the transition relation $\rightarrow$ on distributions as given by Definition 4.2b allows for a probabilistic combination of non-deterministic alternatives resulting in a so-called combined transition. For example, for the process $E = a \cdot (P \;{}_{\frac{1}{2}}\!\oplus\; Q) + a \cdot (P \;{}_{\frac{1}{3}}\!\oplus\; Q)$ of [7], we have that the Dirac process $\partial(E) = \partial(a \cdot (P \;{}_{\frac{1}{2}}\!\oplus\; Q) + a \cdot (P \;{}_{\frac{1}{3}}\!\oplus\; Q))$ provides an a-transition to $[\![P \;{}_{\frac{1}{2}}\!\oplus\; Q]\!]$ as well as an a-transition to $[\![P \;{}_{\frac{1}{3}}\!\oplus\; Q]\!]$. However, since we can represent the distribution $\delta(E)$ by $\delta(E) = \frac{1}{2}\delta(E) \oplus \frac{1}{2}\delta(E)$, the distribution $\delta(E)$ also has a combined transition

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

As noted in [38], the ability to combine transitions is crucial for obtaining transitivity of probabilistic process equivalences that take internal actions into account.

Example 4.3. Referring to some of the processes of Figure 2 we have, for example,

$$\begin{array}{rl}
\mathbf{H_1}: & \delta(a \cdot (P \;{}_{\frac{1}{4}}\!\oplus\; (P \;{}_{\frac{1}{3}}\!\oplus\; Q))) \xrightarrow{a} [\![P \;{}_{\frac{1}{4}}\!\oplus\; (P \;{}_{\frac{1}{3}}\!\oplus\; Q)]\!] = [\![P \;{}_{\frac{1}{2}}\!\oplus\; Q]\!] \\
\mathbf{H_2}: & \delta(a \cdot (P \;{}_{\frac{1}{2}}\!\oplus\; (Q \;{}_{\frac{1}{2}}\!\oplus\; Q))) \xrightarrow{a} [\![P \;{}_{\frac{1}{2}}\!\oplus\; (Q \;{}_{\frac{1}{2}}\!\oplus\; Q)]\!] = [\![P \;{}_{\frac{1}{2}}\!\oplus\; Q]\!] \\
\mathbf{E_1}: & \delta(\tau \cdot (\partial(\tau \cdot P + a \cdot Q + \tau \cdot R) \;{}_{\frac{3}{4}}\!\oplus\; \partial(\mathbf{0}))) \xrightarrow{\tau} \frac{3}{4}\delta(\tau \cdot P + a \cdot Q + \tau \cdot R) \oplus \frac{1}{4}\delta(\mathbf{0}).
\end{array}$$

In preparation to the definition of the notion of branching probabilistic bisimilarity in Section 5 we introduce some notation.

Definition 4.4. 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 $\mu' = \mu$, or (iii) $\alpha = \tau$ and there exist $\mu_1, \mu_2, \mu_1', \mu_2' \in \mathit{Distr}(\mathcal{E})$ such that $\mu = \mu_1 \;{}_r\!\oplus\; \mu_2$, $\mu' = \mu_1' \;{}_r\!\oplus\; \mu_2'$, $\mu_1 = \mu_1'$, and $\mu_2 \xrightarrow{\tau} \mu_2'$ for some $r \in (0,1)$.

Cases (i) and (ii) in the definition above correspond with the limits $r = 0$ and $r = 1$ of case (iii). Following [12], μ_1 and μ_2 are the fragments of the distribution μ that stay in place, respectively, go forward via a τ. We use $\Longrightarrow$ to denote the reflexive transitive closure of $\xrightarrow{(\tau)}$. A transition $\mu \xrightarrow{(\tau)} \mu'$ is called a partial transition, and a transition $\mu \Longrightarrow \mu'$ is called a weak transition.

Example 4.5.

(a) According to Definition 4.4 we have, for example,

$$\tfrac{1}{3}\delta(\tau \cdot (P \;{}_{\frac{1}{2}}\!\oplus\; Q)) \oplus \tfrac{2}{3}[\![P \;{}_{\frac{1}{2}}\!\oplus\; Q]\!] \xrightarrow{(\tau)} \tfrac{1}{3}[\![P \;{}_{\frac{1}{2}}\!\oplus\; Q]\!] \oplus \tfrac{2}{3}[\![P \;{}_{\frac{1}{2}}\!\oplus\; Q]\!] = [\![P \;{}_{\frac{1}{2}}\!\oplus\; Q]\!].$$

(b) There are typically multiple ways to construct a weak transition $\Longrightarrow$. Consider the weak transition $\frac{1}{2}\delta(\tau \cdot \partial(\tau \cdot P)) \oplus \frac{1}{3}\delta(\tau \cdot P) \oplus \frac{1}{6}[\![P]\!] \Longrightarrow [\![P]\!]$ which can be obtained, among uncountably many other possibilities, via

$$\begin{array}{l}
\tfrac{1}{2}\delta(\tau \cdot \partial(\tau \cdot P)) \oplus \tfrac{1}{3}\delta(\tau \cdot P) \oplus \tfrac{1}{6}[\![P]\!] \xrightarrow{(\tau)} \\
\qquad \tfrac{1}{2}\delta(\tau \cdot P)) \oplus \tfrac{1}{3}\delta(\tau \cdot P) \oplus \tfrac{1}{6}[\![P]\!] = \tfrac{5}{6}\delta(\tau \cdot P) \oplus \tfrac{1}{6}[\![P]\!] \xrightarrow{(\tau)} [\![P]\!]
\end{array}$$

or via

$$\tfrac{1}{2}\delta(\tau\cdot\partial(\tau\cdot P))\oplus\tfrac{1}{3}\delta(\tau\cdot P)\oplus\tfrac{1}{6}[\![P]\!]\xrightarrow{(\tau)}\tfrac{1}{2}\delta(\tau\cdot\partial(\tau\cdot P))\oplus\tfrac{1}{3}\delta(P)\oplus\tfrac{1}{6}[\![P]\!]=$$
$$\tfrac{1}{2}\delta(\tau\cdot\partial(\tau\cdot P))\oplus\tfrac{1}{2}\delta(P)\xrightarrow{(\tau)}\tfrac{1}{2}\delta(\tau\cdot P)\oplus\tfrac{1}{2}[\![P]\!]\xrightarrow{(\tau)}\tfrac{1}{2}[\![P]\!]\oplus\tfrac{1}{2}[\![P]\!]=[\![P]\!]$$

(c) The distribution $\frac{1}{2}\delta(\tau\cdot\partial(a\cdot\partial(\mathbf{0})+b\cdot\partial(\mathbf{0})))\oplus\frac{1}{2}\delta(a\cdot\partial(c\cdot\partial(\mathbf{0})))$ doesn't admit a τ-transition $\xrightarrow{\tau}$ nor an a-transition $\xrightarrow{a}$. However, we have

$$\tfrac{1}{2}\delta(\tau\cdot\partial(a\cdot\partial(\mathbf{0})+b\cdot\partial(\mathbf{0})))\oplus\tfrac{1}{2}\delta(a\cdot\partial(c\cdot\partial(\mathbf{0})))\xrightarrow{(\tau)}$$
$$\tfrac{1}{2}\partial(a\cdot\partial(\mathbf{0})+b\cdot\partial(\mathbf{0}))\oplus\tfrac{1}{2}\delta(a\cdot\partial(c\cdot\partial(\mathbf{0})))\xrightarrow{a}\tfrac{1}{2}\delta(\mathbf{0})\oplus\tfrac{1}{2}\delta(c\cdot\partial(\mathbf{0})).$$

The next lemma will play a crucial rôle in our forthcoming congruence proof. Its proof can be found in the appendix.

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 both $\xi=\bigoplus_{i\in I}p_i\cdot\mu_i$ and $\xi=\bigoplus_{j\in J}q_j\cdot\nu_j$. Then there are $r_{ij}\in[0,1]$ and $\varrho_{ij}\in \mathit{Distr}(\mathcal{E})$ such that $\sum_{j\in J}r_{ij}=p_i$ and $p_i\cdot\mu_i=\bigoplus_{j\in J}r_{ij}\cdot\varrho_{ij}$ for all $i\in I$, and $\sum_{i\in I}r_{ij}=q_j$ and $q_j\cdot\nu_j=\bigoplus_{i\in I}r_{ij}\cdot\varrho_{ij}$ for all $j\in J$.

The following lemma says that the transitions $\xrightarrow{\alpha}$, $\xrightarrow{(\alpha)}$ and $\Longrightarrow$ of Definitions 4.2b and 4.4 can be probabilistically composed.

Lemma 4.7. Let $\mu_i,\mu_i'\in \mathit{Distr}(\mathcal{E})$ for a finite index set I, and let $\sum_{i\in I}p_i=1$.

(a) If $\mu_i\xrightarrow{\alpha}\mu_i'$ for all $i\in I$, then $\bigoplus_{i\in I}p_i\cdot\mu_i\xrightarrow{\alpha}\bigoplus_{i\in I}p_i\cdot\mu_i'$.

(b) If $\mu_i\xrightarrow{(\tau)}\mu_i'$ for all $i\in I$, then $\bigoplus_{i\in I}p_i\cdot\mu_i\xrightarrow{(\tau)}\bigoplus_{i\in I}p_i\cdot\mu_i'$.

(c) If $\mu_i\Longrightarrow\mu_i'$ for all $i\in I$, then $\bigoplus_{i\in I}p_i\cdot\mu_i\Longrightarrow\bigoplus_{i\in I}p_i\cdot\mu_i'$.

Proof. Let $\mu:=\bigoplus_{i\in I}p_i\cdot\mu_i$ and $\mu':=\bigoplus_{i\in I}p_i\cdot\mu_i'$. Without loss of generality, we may assume that $p_i>0$ for all $i\in I$.

(a) Suppose $\mu_i\xrightarrow{\alpha}\mu_i'$ for all $i\in I$. Then, for all $i\in I$, by Definition 4.2b, exist index sets J_i, $p_{ij}\geqslant 0$, and processes $E_{ij}\in\mathcal{E}$, for $j\in J_i$, such that $\mu_i=\bigoplus_{j\in J_i}p_{ij}\cdot E_{ij}$, $\mu_i'=\bigoplus_{j\in J_i}p_{ij}\cdot\mu_{ij}'$, and $E_{ij}\xrightarrow{\alpha}\mu_{ij}'$ for all $j\in J_i$. Let $K:=\{\,(i,j)\mid i\in I,\ j\in J_i\,\}$ and $q_{(i,j)}:=p_i\cdot p_{ij}$ for all $(i,j)\in K$, so that $\sum_{k\in K}q_k=1$. Then $\mu=\bigoplus_{k\in K}q_k\cdot E_{ij}$ and $\mu'=\bigoplus_{k\in K}q_k\cdot\mu_{ij}$, so $\mu\xrightarrow{\alpha}\mu'$ by Definition 4.2b.

(b) Let $\mu_i\xrightarrow{(\tau)}\mu_i'$ for all $i\in I$. Then, for all $i\in I$, by Definition 4.4, there exists $r_i\in[0,1]$ and $\mu_i^{\text{stay}},\mu_i^{\text{go}},\mu_i''\in \mathit{Distr}(\mathcal{E})$ such that $\mu_i=\mu_i^{\text{stay}}\,{}_{r_i}{\oplus}\,\mu_i^{\text{go}}$, $\mu_i'=\mu_i^{\text{stay}}\,{}_{r_i}{\oplus}\,\mu_i''$, and either $r_i=1$ or $\mu_i^{\text{go}}\xrightarrow{\tau}\mu_i''$. In case $r_i=0$ for all $i\in I$, we have that $\mu_i\xrightarrow{\tau}\mu_i'$ for all $i\in I$, and thus $\mu\xrightarrow{\tau}\mu'$ by the first claim of the lemma, and $\mu\xrightarrow{(\tau)}\mu'$ by Definition 4.4i. In case $r_i=1$ for all $i\in I$, we have $\mu'=\mu$ and thus $\mu\xrightarrow{(\tau)}\mu'$ by Definition 4.4ii. Otherwise, let $I':=\{\,i\in I\mid r_i<1\,\}$, $r=\sum_{i\in I}p_i\cdot r_i$, $\mu^{\text{stay}}:=\bigoplus_{i\in I}\frac{p_i\cdot r_i}{r}\cdot\mu_i^{\text{stay}}$, $\mu^{\text{go}}:=\bigoplus_{i\in I'}\frac{p_i\cdot(1-r_i)}{1-r}\cdot\mu_i^{\text{go}}$ and $\mu'':=\bigoplus_{i\in I'}\frac{p_i\cdot(1-r_i)}{1-r}\cdot\mu_i''$. Then $\mu^{\text{go}}\xrightarrow{\tau}\mu''$ by the first claim of the lemma. Moreover, $\mu=\mu^{\text{stay}}\,{}_{r}{\oplus}\,\mu^{\text{go}}$, $\mu'=\mu^{\text{stay}}\,{}_{r}{\oplus}\,\mu''$ and $r\in(0,1)$. So $\mu\xrightarrow{(\tau)}\mu'$ by Definition 4.4iii.

(c) Let $\mu_i\Longrightarrow\mu_i'$ for all $i\in I$. As I is finite and $\Longrightarrow$ is reflexive, there exists an $n\in\mathbb{N}$ such that $\mu_i=\mu_i^{(0)}\xrightarrow{(\tau)}\mu_i^{(1)}\xrightarrow{(\tau)}\dots\xrightarrow{(\tau)}\mu_i^{(n)}=\mu_i'$ for all $i\in I$. Now $\mu\Longrightarrow\mu'$ follows by n applications of the second statement of the lemma. □

Likewise, the next lemma allows *probabilistic decomposition* of transitions $\xrightarrow{\alpha}$, $\xrightarrow{(\alpha)}$ and $\Longrightarrow$.

Lemma 4.8. Let $\mu, \mu' \in \mathit{Distr}(\mathcal{E})$ and $\mu = \bigoplus_{i\in I} p_i \cdot \mu_i$ with $p_i > 0$ for all $i \in I$.

(a) If $\mu \xrightarrow{\alpha} \mu'$, then there are μ'_i for $i \in I$ such that $\mu_i \xrightarrow{\alpha} \mu'_i$ for all $i \in I$ and $\mu' = \bigoplus_{i\in I} p_i \cdot \mu'_i$.

(b) If $\mu \xrightarrow{(\tau)} \mu'$, then there are μ'_i for $i \in I$ such that $\mu_i \xrightarrow{(\tau)} \mu'_i$ for all $i \in I$ and $\mu' = \bigoplus_{i\in I} p_i \cdot \mu'_i$.

(c) If $\mu \Longrightarrow \mu'$, then there are μ'_i for $i \in I$ such that $\mu_i \Longrightarrow \mu'_i$ for all $i \in I$ and $\mu' = \bigoplus_{i\in I} p_i \cdot \mu'_i$.

Proof. (a) Suppose $\mu \xrightarrow{\alpha} \mu'$. By Definition 4.2b $\mu = \bigoplus_{j\in J} q_j \cdot E_j$, $\mu' = \bigoplus_{j\in J} q_j \cdot \nu'_j$, and $E_j \xrightarrow{\alpha} \nu'_j$ for all $j \in J$, for suitable index set J, $q_j > 0$, $E_j \in \mathcal{E}$, and $\nu'_j \in \mathit{Distr}(\mathcal{E})$. By Lemma 4.6 there are $r_{ij} \in [0,1]$ and $\varrho_{ij} \in \mathit{Distr}(\mathcal{E})$ such that $\sum_{j\in J} r_{ij} = p_i$ and $\mu_i = \bigoplus_{j\in J} \frac{r_{ij}}{p_i} \cdot \varrho_{ij}$ for all $i \in I$, and $\sum_{i\in I} r_{ij} = q_j$ and $q_j \cdot \delta(E_j) = \bigoplus_{i\in I} r_{ij} \cdot \varrho_{ij}$ for all $j \in J$. It follows that $\varrho_{ij} = \delta(E_j)$ for all $i \in I$ and $j \in J$.

For all $i \in I$, let $\mu'_i := \bigoplus_{j\in J} \frac{r_{ij}}{p_i} \cdot \nu'_j$. Then $\mu_i \xrightarrow{\alpha} \mu'_i$, for all $i \in I$, by Lemma 4.7a. Moreover,

$$\textstyle\bigoplus_{i\in I} p_i \cdot \mu'_i = \bigoplus_{i\in I} p_i \cdot \bigoplus_{j\in J} \frac{r_{ij}}{p_i} \cdot \nu'_j = \bigoplus_{j\in J} \bigoplus_{i\in I} r_{ij} \cdot \nu'_j = \bigoplus_{j\in J} q_j \cdot \nu'_j = \mu' \ .$$

(b) Suppose $\mu \xrightarrow{(\tau)} \mu'$. By Definition 4.4, either (i) $\mu \xrightarrow{\tau} \mu'$, or (ii) $\mu' = \mu$, or (iii) there exist $\nu_1, \nu_2, \nu'_1, \nu'_2 \in \mathit{Distr}(\mathcal{E})$ such that $\mu = \nu_1 \ {}_r\!\oplus\ \nu_2$, $\mu' = \nu'_1 \ {}_r\!\oplus\ \nu'_2$, $\nu_1 = \nu'_1$, and $\nu_2 \xrightarrow{\tau} \nu'_2$ for some $r \in (0,1)$. In case (i), the required μ'_i exist by the first statement of this lemma. In case (ii) one can simply take $\mu'_i := \mu_i$ for all $i \in I$. Hence assume that case (iii) applies. Let $J := \{1,2\}$, $q_1 := r$ and $q_2 := 1-r$. By Lemma 4.6 there are $r_{ij} \in [0,1]$ and $\varrho_{ij} \in \mathit{Distr}(\mathcal{E})$ with $\sum_{j\in J} r_{ij} = p_i$ and $\mu_i = \bigoplus_{j\in J} \frac{r_{ij}}{p_i} \cdot \varrho_{ij}$ for all $i \in I$, and $\sum_{i\in I} r_{ij} = q_j$ and $\nu_j = \bigoplus_{i\in I} \frac{r_{ij}}{q_j} \cdot \varrho_{ij}$ for all $j \in J$.

Let $I' := \{\, i \in I \mid r_{i2} > 0 \,\}$. Since $\nu_2 = \bigoplus_{i\in I'} \frac{r_{i2}}{1-r} \cdot \varrho_{i2} \xrightarrow{\tau} \nu'_2$, it follows from the first statement of the lemma, for all $i \in I'$ there are ϱ'_{i2} such that $\varrho_{i2} \xrightarrow{\tau} \varrho'_{i2}$ and $\nu'_2 = \bigoplus_{i\in I'} \frac{r_{i2}}{1-r} \cdot \varrho'_{i2}$. For all $i \in I \backslash I'$, pick $\varrho'_{i2} \in \mathit{Distr}(\mathcal{E})$ arbitrarily. It follows that $\mu_i = \varrho_{i1} \ {}_{\frac{r_{i1}}{p_i}}\!\oplus\ \varrho_{i2} \xrightarrow{(\tau)} \varrho_{i1} \ {}_{\frac{r_{i1}}{p_i}}\!\oplus\ \varrho'_{i2} =: \mu'_i$ for all $i \in I$. Moreover,

$$\textstyle\bigoplus_{i\in I} p_i \cdot \mu'_i = \bigoplus_{i\in I} p_i \cdot (\varrho_{i1} \ {}_{\frac{r_{i1}}{p_i}}\!\oplus\ \varrho'_{i2}) = (\bigoplus_{i\in I} \frac{r_{i1}}{r} \cdot \varrho_{i1}) \ {}_r\!\oplus\ (\bigoplus_{i\in I} \frac{r_{i2}}{1-r} \cdot \varrho'_{i2}) = \nu_1 \ {}_r\!\oplus\ \nu'_2 = \mu' \ .$$

(c) The last statement follows by transitivity from the second one. □

5. Branching bisimilarity for probabilistic processes

We next define the notions of strong probabilistic bisimilarity and branching probabilistic bisimilarity. Note that the notion of strong probabilistic bisimilarity is the variant with combined transitions as defined in [37, 7].

Definition 5.1 (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 $\mu = \bigoplus_{i\in I} p_i \cdot \mu_i$, there are $\nu_i \in \mathit{Distr}(\mathcal{E})$, for $i \in I$, such that

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

(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 $\mu \mathrel{\mathcal{R}} \nu$ and $\mu \xrightarrow{\alpha} \mu'$ there is a $\nu' \in \mathit{Distr}(\mathcal{E})$ such that

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

(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 $\mu \mathrel{\mathcal{R}} \nu$ and $\mu = \bigoplus_{i \in I} p_i \cdot \mu_i$ there are $\bar{\nu}, \nu_i \in \mathit{Distr}(\mathcal{E})$, for $i \in I$, such that

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

(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 $\mu \mathrel{\mathcal{R}} \nu$ and $\mu \xrightarrow{\alpha} \mu'$, there are $\bar{\nu}, \nu' \in \mathit{Distr}(\mathcal{E})$ such that

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

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

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

Two non-deterministic processes are considered to be strongly or branching probabilistic bisimilar iff their Dirac distributions are, i.e., for $E, F \in \mathcal{E}$ we have $E \leftrightarroweq F$ iff $\delta(E) \leftrightarroweq \delta(F)$ and $E \leftrightarroweq_b F$ iff $\delta(E) \leftrightarroweq_b \delta(F)$. Two probabilistic processes are considered to be strongly or branching probabilistic bisimilar iff their associated distributions over $\mathcal{E}$ are, i.e., for $P, Q \in \mathcal{P}$ we have $P \leftrightarroweq Q$ iff $[\![P]\!] \leftrightarroweq [\![Q]\!]$ and $P \leftrightarroweq_b Q$ iff $[\![P]\!] \leftrightarroweq_b [\![Q]\!]$.

The notion of decomposability has been adopted from [30] and weak decomposability from [33]. The underlying idea stems from [12]. These notions provide a convenient dexterity to deal with the behaviour 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 $\partial(\mathbf{0})$, and to handle combined behaviour.

By comparison, on finite processes, as used in this paper, the notion of branching probabilistic bisimilarity of Segala & Lynch [37] 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 $\mathbf{G}_0$, $\mathbf{G}_1$, and $\mathbf{G}_2$ from the introduction.

Example 5.2.

(a) Since the distributions $\delta(\mathbf{H_1}) = \delta(a \cdot (P \,{}_{\frac{1}{4}}{\oplus}\, (P \,{}_{\frac{1}{3}}{\oplus}\, Q)))$ and $\delta(\mathbf{H_2}) = \delta(a \cdot (P \,{}_{\frac{1}{2}}{\oplus}\, (Q \,{}_{\frac{1}{2}}{\oplus}\, Q)))$ only have the transitions

$$\delta(a \cdot (P \,{}_{\frac{1}{4}}{\oplus}\, (P \,{}_{\frac{1}{3}}{\oplus}\, Q))) \xrightarrow{\alpha} \tfrac{1}{2}[\![P]\!] \oplus \tfrac{1}{2}[\![Q]\!] \quad \text{and} \quad \delta(a \cdot (P \,{}_{\frac{1}{2}}{\oplus}\, (Q \,{}_{\frac{1}{2}}{\oplus}\, Q))) \xrightarrow{\alpha} \tfrac{1}{2}[\![P]\!] \oplus \tfrac{1}{2}[\![Q]\!],$$

it follows that $\mathcal{R} = \{\langle\delta(\mathbf{H_1}), \delta(\mathbf{H_2})\rangle\}^\dagger \cup \{\ \langle\mu,\mu\rangle \mid \mu \in \mathit{Distr}(\mathcal{E})\ \}$ is a strong bisimulation relation. Here, for a relation $\mathcal{S} \subseteq \mathit{Distr}(\mathcal{E}) \times \mathit{Distr}(\mathcal{E})$, $\mathcal{S}^\dagger$ denotes its symmetric closure. Since $\mathcal{R}$ is a strong probabilistic bisimulation relation, it follows that $\mathbf{H_1}$ and $\mathbf{H_2}$ are strong probabilistic bisimilar, i.e., $\delta(\mathbf{H_1}) \leftrightarrow \delta(\mathbf{H_2})$.

(b) The distributions $\delta(\mathbf{G_1}) = \delta(a \cdot (P \,{}_{\frac{1}{2}}{\oplus}\, Q))$ and $\delta(\mathbf{G_2}) = \delta(a \cdot (\partial(\tau \cdot (P \,{}_{\frac{1}{2}}{\oplus}\, Q)) \,{}_{\frac{1}{3}}{\oplus}\, (P \,{}_{\frac{1}{2}}{\oplus}\, Q)))$ are not strong probabilistic bisimilar. Although the two distributions both admit an a-transition,

$$\delta(a \cdot (P \,{}_{\frac{1}{2}}{\oplus}\, Q)) \xrightarrow{a} \tfrac{1}{2}[\![P]\!] \oplus \tfrac{1}{2}[\![Q]\!]$$
$$\delta(a \cdot (\partial(\tau \cdot (P \,{}_{\frac{1}{2}}{\oplus}\, Q)) \,{}_{\frac{1}{3}}{\oplus}\, (P \,{}_{\frac{1}{2}}{\oplus}\, Q))) \xrightarrow{a} \tfrac{1}{3}\delta(\tau \cdot (P \,{}_{\frac{1}{2}}{\oplus}\, Q)) \oplus \tfrac{1}{3}[\![P]\!] \oplus \tfrac{1}{3}[\![Q]\!]$$

the resulting distributions at the right-hand side are not strong probabilistic bisimilar. However, the symmetric closure $\mathcal{R}^\dagger$ of the relation $\mathcal{R}$ containing the pairs

$$\langle\delta(\tau \cdot (P \,{}_{\frac{1}{2}}{\oplus}\, Q)), \tfrac{1}{2}[\![P]\!] \oplus \tfrac{1}{2}[\![Q]\!]\rangle \quad \text{and} \quad \langle\mu,\mu\rangle \text{ for } \mu \in \mathit{Distr}(\mathcal{E})$$

clearly is a branching probabilistic bisimulation relation. By Lemma 5.3 below, also its convex closure $cc(\mathcal{R}^\dagger)$ is a branching probabilistic bisimulation relation. Considering that $\mathcal{R}(\delta(\tau \cdot (P \,{}_{\frac{1}{2}}{\oplus}\, Q)), \tfrac{1}{2}[\![P]\!] \oplus \tfrac{1}{2}[\![Q]\!])$ and $\mathcal{R}(\tfrac{1}{2}[\![P]\!] \oplus \tfrac{1}{2}[\![Q]\!], \tfrac{1}{2}[\![P]\!] \oplus \tfrac{1}{2}[\![Q]\!])$, we have that

$$cc(\mathcal{R}^\dagger)(\tfrac{1}{3}\delta(\tau \cdot (P \,{}_{\frac{1}{2}}{\oplus}\, Q) \oplus \tfrac{2}{3}(\tfrac{1}{2}[\![P]\!] \oplus \tfrac{1}{2}[\![Q]\!]), \tfrac{1}{3}(\tfrac{1}{2}[\![P]\!] \oplus \tfrac{1}{2}[\![Q]\!]) \oplus \tfrac{2}{3}(\tfrac{1}{2}[\![P]\!] \oplus \tfrac{1}{2}[\![Q]\!]))) \ .$$

i.e., the distributions $\tfrac{1}{3}\delta(\tau \cdot (P \,{}_{\frac{1}{2}}{\oplus}\, Q)) \oplus \tfrac{2}{3}(\tfrac{1}{2}[\![P]\!] \oplus \tfrac{1}{2}[\![Q]\!])$ and $\tfrac{1}{2}[\![P]\!] \oplus \tfrac{1}{2}[\![Q]\!]$ are related by $cc(\mathcal{R}^\dagger)$. Adding the pair of processes $\langle\delta(a \cdot (P \,{}_{\frac{1}{2}}{\oplus}\, Q)), \delta(a \cdot (\partial(\tau \cdot (P \,{}_{\frac{1}{2}}{\oplus}\, Q)) \,{}_{\frac{1}{3}}{\oplus}\, (P \,{}_{\frac{1}{2}}{\oplus}\, Q)))\rangle$ (and closing for symmetry) then yields a branching probabilistic bisimulation relation relating $\delta(\mathbf{G_1})$ and $\delta(\mathbf{G_2})$.

(c) The a-derivatives of $\mathbf{I_1}$ and $\mathbf{I_2}$, i.e. the processes $I_1' = \partial(b \cdot P + \tau \cdot Q)$ and $I_2' = \partial(\tau \cdot \partial(b \cdot P + \tau \cdot Q) + b \cdot P + \tau \cdot Q)$, are branching probabilistic bisimilar. A τ-transition of I_2' partially based on its left branch, can be simulated by I_1' by a partial stand-still:

$$I_2' \;=\; r \cdot [\![I_2']\!] \oplus (1-r) \cdot [\![I_2']\!] \quad \xrightarrow{\tau} \quad r \cdot \delta(b \cdot P + \tau \cdot Q) \oplus (1-r) \cdot [\![Q]\!]$$
$$I_1' \;=\; r \cdot [\![I_1']\!] \oplus (1-r) \cdot [\![I_1']\!] \quad \xrightarrow{(\tau)} \quad r \cdot [\![I_1']\!] \oplus (1-r) \cdot [\![Q]\!] \;=\; r \cdot \delta(b \cdot P + \tau \cdot Q) \oplus (1-r) \cdot [\![Q]\!].$$

A τ-transition of I_1' can be directly simulated by I_2' of course. It follows that the relation $\mathcal{R} = \{\langle\delta(\mathbf{I_1}), \delta(\mathbf{I_2})\rangle, \langle I_1', I_2'\rangle\}^\dagger \cup \{\,\langle\mu,\mu\rangle \mid \mu \in \mathit{Distr}(\mathcal{E})\,\}$, the symmetric relation containing the pairs mentioned and the diagonal of $\mathit{Distr}(\mathcal{E})$, constitutes a branching probabilistic bisimulation relation containing $\mathbf{I_1}$ and $\mathbf{I_2}$.

(d) The a-derivatives of $\mathbf{T_1}$ and $\mathbf{T_2}$, say $T_1' = \partial(b \cdot (P \,{}_{\frac{1}{3}}{\oplus}\, Q)) \,{}_{\frac{1}{2}}{\oplus}\, \partial(b \cdot (P \,{}_{\frac{2}{3}}{\oplus}\, Q))$ and $T_2' = \partial(\tau \cdot (\partial(b \cdot (P \,{}_{\frac{1}{3}}{\oplus}\, Q)) \,{}_{\frac{1}{2}}{\oplus}\, \partial(b \cdot (P \,{}_{\frac{2}{3}}{\oplus}\, Q))) + b \cdot (P \,{}_{\frac{1}{2}}{\oplus}\, Q))$, are similarly related as in the above example. Here though, it is slightly more difficult to see that T_1' can simulate the b-transition of T_2' into $P \,{}_{\frac{1}{2}}{\oplus}\, Q$. We have

$$T_2' \xrightarrow{b} \quad [\![P \,{}_{\frac{1}{2}}{\oplus}\, Q]\!]$$
$$T_1' \xrightarrow{b} \tfrac{1}{2}[\![P \,{}_{\frac{1}{3}}{\oplus}\, Q]\!] \oplus \tfrac{1}{2}[\![P \,{}_{\frac{2}{3}}{\oplus}\, Q]\!] = \tfrac{1}{6}[\![P]\!] \oplus \tfrac{1}{3}[\![Q]\!] \oplus \tfrac{1}{3}[\![P]\!] \oplus \tfrac{1}{6}[\![Q]\!] = [\![P \,{}_{\frac{1}{2}}{\oplus}\, Q]\!].$$

In the axiomatisation presented in the sequel, axioms are included (the axioms P1 to P3) to express the above identification of the distributions in $\mathit{Distr}(\mathcal{E})$ in terms of probabilistic processes from $\mathcal{P}$.

(e) A similar recombination of distributions as for case (d) takes place for the examples $\mathbf{E_1}$ and $\mathbf{E_2}$. In this case

$$\begin{aligned}
\delta(\mathbf{E_1}) &\xrightarrow{\tau} \tfrac{3}{4}\delta(\tau\cdot P + a\cdot Q + \tau\cdot R) \oplus \tfrac{1}{4}\delta(\mathbf{0}) \\
\delta(\mathbf{E_2}) &\xrightarrow{\tau} \tfrac{1}{2}\delta(\tau\cdot P + a\cdot Q + \tau\cdot R) \oplus \tfrac{1}{2}\delta(\tau\cdot(\partial(P + a\cdot Q + \tau\cdot R) \;{}_{\frac{1}{2}}\!\oplus\; \partial(\mathbf{0}))) \\
&\xrightarrow{(\tau)} \tfrac{1}{2}\delta(\tau\cdot P + a\cdot Q + \tau\cdot R) \oplus \tfrac{1}{2}[\![\partial(P + a\cdot Q + \tau\cdot R) \;{}_{\frac{1}{2}}\!\oplus\; \partial(\mathbf{0})]\!] \\
&= \tfrac{1}{2}\delta(\tau\cdot P + a\cdot Q + \tau\cdot R) \oplus \tfrac{1}{4}\delta(P + a\cdot Q + \tau\cdot R) \oplus \tfrac{1}{4}\delta(\mathbf{0}) \\
&= \tfrac{3}{4}\delta(\tau\cdot P + a\cdot Q + \tau\cdot R) \oplus \tfrac{1}{4}\delta(\mathbf{0}).
\end{aligned}$$

Because for $\mathbf{E_2}$ the τ-moves can be combined, the branching probabilistic bisimulation relation relating $\mathbf{E_1}$ and $\mathbf{E_2}$ is a bit more extensive. Put $S = \tau\cdot P + a\cdot Q + \tau\cdot R$ and

$$\begin{aligned}
\mathcal{R} \;=\; &\{\, \langle \delta(\mathbf{E_1}), \delta(\mathbf{E_2}) \rangle \,\}^{\dagger} \cup \\
&\{\, \langle r\cdot[\![S]\!] \oplus \tfrac{1-r}{2}\cdot[\![S]\!] \oplus \tfrac{1-r}{2}\cdot\delta(\mathbf{0}), r\cdot[\![S]\!] \oplus (1-r)\cdot\delta(\tau\cdot(S \;{}_{\frac{1}{2}}\!\oplus\; \partial(\mathbf{0}))) \rangle \mid 0 \leqslant r \leqslant 1 \,\}^{\dagger} \cup \\
&\{\, \langle \mu, \mu \rangle \mid \mu \in \mathit{Distr}(\mathcal{E}) \,\}
\end{aligned}$$

where the pairs $\langle r\cdot[\![S]\!] \oplus \frac{(1-r)}{2}\cdot[\![S]\!] \oplus \frac{1-r}{2}\cdot\delta(\mathbf{0}), r\cdot[\![S]\!] \oplus (1-r)\cdot\delta(\tau\cdot(S \;{}_{\frac{1}{2}}\!\oplus\; \partial(\mathbf{0}))) \rangle$, for $r \neq \frac{1}{2}$, are needed for $\mathcal{R}$ to be weakly decomposable.

Similar to the non-deterministic case, transitions $E \xrightarrow{\tau} \nu$ and $\mu \xrightarrow{\tau} \nu$ are called *inert* iff $\delta(E) \leftrightarroweq_b \nu$ and $\mu \leftrightarroweq_b \nu$. Typical cases of inert transitions include

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

A transition $E \xrightarrow{\tau} \mu_1 \;{}_r\!\oplus\; \mu_2$ with $r \in (0,1]$ and $\delta(E) \leftrightarroweq_b \mu_1$ is called *partially inert*. An illustrative instance of partial inertness is

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

Here we have that $\delta(\tau\cdot(\partial(a\cdot P+\tau\cdot Q)\;{}_r\!\oplus\; Q)+a\cdot P+\tau\cdot Q) \leftrightarroweq_b \delta(a\cdot P+\tau\cdot Q)$, because in particular $\delta(a\cdot P + \tau\cdot Q) = \delta(a\cdot P + \tau\cdot Q) \;{}_r\!\oplus\; \delta(a\cdot P + \tau\cdot Q) \xrightarrow{(\tau)} \delta(a\cdot P + \tau\cdot Q) \;{}_r\!\oplus\; [\![Q]\!]$. Partially inert transitions play a central role in the remainder.

The following lemma is handy for constructing branching probabilistic bisimulation relations; it was used already in Example 5.2b above. The proof of the lemma, because of its technical nature, is delegated to the appendix.

Lemma 5.3. If $\mathcal{R}$ is a branching probabilistic bisimulation relation, then so is $cc(\mathcal{R})$.

The next lemma provides a witness for strong probabilistic bisimilarity; it is used in the proof of Lemma 6.13. The proof of the lemma itself is given in the appendix.

Lemma 5.4. 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 $\mu \leftrightarroweq \nu$.

With the help of Lemma 4.6 we show—in the appendix—that the operator ${}_r{\oplus}$ respects branching probabilistic bisimilarity of distributions.

Lemma 5.5. Let $\mu_1, \mu_2, \nu_1, \nu_2 \in \mathit{Distr}(\mathcal{E})$ and $r \in (0,1)$. If $\mu_1 \leftrightarroweq_b \nu_1$ and $\mu_2 \leftrightarroweq_b \nu_2$ then $\mu_1 \,{}_r{\oplus}\, \mu_2 \leftrightarroweq_b \nu_1 \,{}_r{\oplus}\, \nu_2$.

A direct consequence of the lemma is that, for probabilistic processes $P_1, P_2, Q_1, Q_2 \in \mathcal{P}$, we have that $P_1 \leftrightarroweq_b Q_1$ and $P_2 \leftrightarroweq_b Q_2$ implies $P_1 \,{}_r{\oplus}\, Q_1 \leftrightarroweq_b P_2 \,{}_r{\oplus}\, Q_2$, i.e. $[\![P_1 \,{}_r{\oplus}\, P_2]\!] \leftrightarroweq_b [\![Q_1 \,{}_r{\oplus}\, Q_2]\!]$ when $[\![P_1]\!] \leftrightarroweq_b [\![Q_1]\!]$ and $[\![P]\!]_2 \leftrightarroweq_b [\![Q]\!]_2$.

As we did for the non-deterministic setting, we introduce a notion of rooted branching probabilistic bisimilarity for non-deterministic processes. We do not need such a notion for probabilistic processes.

Definition 5.6. Two nondeterministic processes $E, F \in \mathcal{E}$ are *rooted branching probabilistic bisimilar*, notation $E \leftrightarroweq_{rb} F$, if for each transition $\delta(E) \xrightarrow{\alpha} \mu$ with $\alpha \in \mathcal{A}$ there is a transition $\delta(F) \xrightarrow{\alpha} \nu$ with $\mu \leftrightarroweq_b \nu$, and, vice versa, for each transition $\delta(F) \xrightarrow{\alpha} \nu$ there is a $\delta(E) \xrightarrow{\alpha} \mu$ with $\mu \leftrightarroweq_b \nu$.

To show that $\leftrightarroweq_b$ is an equivalence relation, we need the following useful property.

Lemma 5.7. Let $\mu, \nu \in \mathit{Distr}(\mathcal{E})$ such that $\mu \leftrightarroweq_b \nu$ and $\mu \Longrightarrow \mu'$ for some $\mu' \in \mathit{Distr}(\mathcal{E})$. Then exists $\nu' \in \mathit{Distr}(\mathcal{E})$ such that $\nu \Longrightarrow \nu'$ and $\mu' \leftrightarroweq_b \nu'$.

Proof. We check that a partial transition $\mu \xrightarrow{(\tau)} \mu'$ can be matched by ν given $\mu \leftrightarroweq_b \nu$. So, suppose $\mu = \mu_1 \,{}_r{\oplus}\, \mu_2$, $\mu_1 \xrightarrow{\tau} \mu_1'$, and $\mu' = \mu_1' \,{}_r{\oplus}\, \mu_2$. By weak decomposability of $\leftrightarroweq_b$ we can find distributions $\bar{\nu}, \nu_1, \nu_2$ such that $\nu \Longrightarrow \bar{\nu} = \nu_1 \,{}_r{\oplus}\, \nu_2$ and $\mu \leftrightarroweq_b \bar{\nu}$, $\nu_1 \leftrightarroweq_b \mu_1$, $\nu_2 \leftrightarroweq_b \mu_2$. Choose distributions $\bar{\nu}_1, \bar{\nu}_1'$ such that $\nu_1 \Longrightarrow \bar{\nu}_1 \xrightarrow{(\tau)} \nu_1'$ and $\bar{\nu}_1 \leftrightarroweq_b \mu_1$, $\nu_1' \leftrightarroweq_b \mu_1'$. Put $\nu' = \nu_1' \,{}_r{\oplus}\, \nu_2$. Then $\nu \Longrightarrow \nu'$, using Lemma 4.7c, and we have by Lemma 5.5: $\nu' = \nu_1' \,{}_r{\oplus}\, \nu_2 \leftrightarroweq_b \mu_1' \,{}_r{\oplus}\, \mu_2 = \mu'$ since $\nu_1' \leftrightarroweq_b \mu_1'$ and $\nu_2 \leftrightarroweq_b \mu_2$. $\square$

We are now in a position to show that the various bisimulation relations introduced in Definitions 5.1 and 5.6 are equivalence relations.

Lemma 5.8 (Equivalence). The relations $\leftrightarroweq$, $\leftrightarroweq_{rb}$, and $\leftrightarroweq_b$ on $\mathcal{E}$, as well as $\leftrightarroweq$ and $\leftrightarroweq_b$ on $\mathcal{P}$ are equivalence relations.

Proof. That these relations are reflexive and symmetric follows immediately from the definitions; for reflexivity one takes the identity relation between distributions as a witness. We show that $\underline{\leftrightarrow}_b$ is transitive by showing that the relation $\mathcal{R}$ given by

$$\mathcal{R} = \{ \langle \mu, \varrho \rangle \mid \exists \nu \colon \mu \;\underline{\leftrightarrow}_b\; \nu \wedge \nu \;\underline{\leftrightarrow}_b\; \varrho \},$$

i.e. $\mathcal{R} = \underline{\leftrightarrow}_b \cdot \underline{\leftrightarrow}_b$, is a branching probabilistic bisimulation relation. Symmetry of $\mathcal{R}$ follows from symmetry of $\underline{\leftrightarrow}_b$. As to weak decomposability, suppose $\mathcal{R}(\mu, \varrho)$ for distributions μ and ϱ such that $\mu = \bigoplus_{i \in I} p_i \cdot \mu_i$ for an index set I, and $\mu_i \in \mathit{Distr}(\mathcal{E})$. Choose $\nu \in \mathit{Distr}(\mathcal{E})$ such that $\mu \;\underline{\leftrightarrow}_b\; \nu$ and $\nu \;\underline{\leftrightarrow}_b\; \varrho$. Since $\nu \;\underline{\leftrightarrow}_b\; \mu$ we can find $\bar{\nu}, \nu_i \in \mathit{Distr}(\mathcal{E})$ for $i \in I$ such that $\nu \Longrightarrow \bar{\nu} = \bigoplus_{i \in I} p_i \cdot \nu_i$, $\mu \;\underline{\leftrightarrow}_b\; \bar{\nu}$, and $\mu_i \;\underline{\leftrightarrow}_b\; \nu_i$ for $i \in I$. By Lemma 5.7 we can find $\bar{\varrho} \in \mathit{Distr}(\mathcal{E})$ such that $\varrho \Longrightarrow \bar{\varrho}$ and $\bar{\varrho} \;\underline{\leftrightarrow}_b\; \bar{\nu}$. Hence, there exist distributions $\hat{\varrho}$ and ϱ_i for $i \in I$ such that $\bar{\varrho} \Longrightarrow \hat{\varrho} = \bigoplus_{i \in I} p_i \cdot \varrho_i$, $\bar{\nu} \;\underline{\leftrightarrow}_b\; \hat{\varrho}$ and $\nu_i \;\underline{\leftrightarrow}_b\; \varrho_i$ for $i \in I$. Thus, $\varrho \Longrightarrow \hat{\varrho} = \bigoplus_{i \in I} p_i \cdot \varrho_i$, where $\mu \;\underline{\leftrightarrow}_b\; \bar{\nu}$ and $\bar{\nu} \;\underline{\leftrightarrow}_b\; \hat{\varrho}$, hence $\mathcal{R}(\mu, \hat{\varrho})$, and likewise $\mu_i \;\underline{\leftrightarrow}_b\; \nu_i$ and $\nu_i \;\underline{\leftrightarrow}_b\; \varrho_i$, hence $\mathcal{R}(\mu_i, \varrho_i)$ for $i \in I$.

Finally, if $\mu \xrightarrow{\alpha} \mu'$ for some $\mu' \in \mathit{Distr}(\mathcal{E})$, then distributions $\bar{\nu}, \nu'$ exist such that $\nu \Longrightarrow \bar{\nu} \xrightarrow{(\alpha)} \nu'$ and $\bar{\nu} \;\underline{\leftrightarrow}_b\; \mu$, $\nu' \;\underline{\leftrightarrow}_b\; \mu'$. Again with appeal to Lemma 5.7 there exists $\bar{\varrho} \in \mathit{Distr}(\mathcal{E})$ such that $\varrho \Longrightarrow \bar{\varrho}$ and $\bar{\varrho} \;\underline{\leftrightarrow}_b\; \bar{\nu}$. Then there also exist $\hat{\varrho}, \varrho' \in \mathit{Distr}(\mathcal{E})$ such that $\bar{\varrho} \Longrightarrow \hat{\varrho} \xrightarrow{(\alpha)} \varrho'$, $\hat{\varrho} \;\underline{\leftrightarrow}_b\; \bar{\nu}$ and $\varrho' \;\underline{\leftrightarrow}_b\; \nu'$. So, we have $\varrho \Longrightarrow \hat{\varrho} \xrightarrow{(\alpha)} \varrho'$ and $\mathcal{R}(\mu, \hat{\varrho})$, $\mathcal{R}(\mu', \varrho')$. Thus $\mathcal{R}$ also satisfies the weak transfer condition and, consequently, is a branching probabilistic bisimulation relation.

The proof of $\underline{\leftrightarrow}$ being transitive is obtained by simplification of the above argument. The fact that $\underline{\leftrightarrow}_{rb}$ is transitive follows immediately from the definition. □

For more detail on transitivity proofs, in the setting of a slightly different notion of branching probabilistic bisimulation, see [9].

As argued in Section 3, for non-deterministic processes branching probabilistic bisimilarity is not a congruence with respect to non-deterministic choice. The argument holds true in the mixed non-deterministic and probabilistic setting of this section as well. This is the reason we use rooted branching bisimilarity instead.

Strong probabilistic bisimulation semantics employs strong probabilistic bisimilarity $\underline{\leftrightarrow}$ on $\mathcal{E}$ as well as $\mathcal{P}$. Here we propose a notion of *rooted branching probabilistic bisimulation semantics* that employs rooted branching probabilistic bisimilarity $\underline{\leftrightarrow}_{rb}$ on $\mathcal{E}$, and branching probabilistic bisimilarity $\underline{\leftrightarrow}_b$ on $\mathcal{P}$.

Lemma 5.9 (Congruence). Both strong probabilistic bisimulation semantics and rooted branching probabilistic bisimulation semantics induce a congruence relation.

Proof. Regarding rooted branching probabilistic bisimulation semantics we have to show four congruence properties:

1. if $P_i \;\underline{\leftrightarrow}_b\; Q_i$ for $i = 1, 2$ then $P_1 \;{}_r\!\oplus\; Q_1 \;\underline{\leftrightarrow}_b\; P_2 \;{}_r\!\oplus\; Q_2$,

2. if $P \;\underline{\leftrightarrow}_b\; Q$ then $\alpha \cdot P \;\underline{\leftrightarrow}_{rb}\; a \cdot Q$,

3. if $E_i \;\underline{\leftrightarrow}_{rb}\; F_i$ for $i = 1, 2$ then $E_1 + F_1 \;\underline{\leftrightarrow}_{rb}\; F_2 + F_2$, and

4. if $E \;\underline{\leftrightarrow}_{rb}\; F$ then $\partial(E) \;\underline{\leftrightarrow}_b\; \partial(F)$.

Property 1 was the subject of Lemma 5.5, whereas Properties 2 and 4 are trivial with Definition 5.6. We are left with Property 3. Suppose $\delta(E_1) \leftrightarrow_{rb} \delta(F_1)$ and $\delta(E_2) \leftrightarrow_{rb} \delta(F_2)$. 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. In that case, we can find $\nu'_1, \nu'_2 \in \mathit{Distr}(\mathcal{E})$ such that $\delta(F_1) \xrightarrow{\alpha} \nu'_1$, $\delta(F_2) \xrightarrow{\alpha} \nu'_2$, $\mu'_1 \leftrightarrow_b \nu'_1$, and $\mu'_2 \leftrightarrow_b \nu'_2$. From this it follows that $\delta(F_1 + F_2) \xrightarrow{\alpha} \nu'$ and $\mu' \leftrightarrow_b \nu'$ for $\nu' = \nu'_1 \,{}_r{\oplus}\, \nu'_2$ using Lemma 5.5.

The congruence properties for strong probabilistic bisimulation semantics are well-known, and can be obtained by simplification of the arguments above. □

Exactly as for the nondeterministic case [22], one can show that rooted branching probabilistic bisimulation semantics yields the coarsest, or largest, congruence included in $\leftrightarrow_b$.

We close this section with two fundamental properties of branching probabilistic bisimilarity that we need further on. We discuss the stuttering property, known from [22] for non-deterministic processes, and cancellativity of probabilistic choice with respect to $\leftrightarrow_b$.

Lemma 5.10 (Stuttering Property). For all $\mu, \nu, \varrho \in \mathit{Distr}(\mathcal{E})$, if $\mu \Rightarrow \nu$, $\nu \Rightarrow \varrho$ and $\mu \leftrightarrow_b \varrho$ then it holds that $\mu \leftrightarrow_b \nu$.

Proof. We show that the relation $\mathcal{R} = \{(\mu,\nu),(\nu,\mu)\} \cup \leftrightarrow_b$ is a branching probabilistic bisimulation relation.

Suppose $\mu \xrightarrow{\alpha} \mu'$ for some $\alpha \in \mathcal{A}$, $\mu' \in \mathit{Distr}(\mathcal{E})$. Since $\mu \leftrightarrow_b \varrho$ there exist $\hat{\varrho}, \varrho' \in \mathit{Distr}(\mathcal{E})$ such that $\varrho \Rightarrow \hat{\varrho} \xrightarrow{(\alpha)} \varrho'$ matches $\mu \xrightarrow{\alpha} \mu'$. In particular, $\hat{\varrho} \leftrightarrow_b \mu$ and $\varrho' \leftrightarrow_b \mu'$. Then, from $\nu \Rightarrow \varrho$ we obtain $\nu \Rightarrow \varrho'$. Hence $\nu \Rightarrow \hat{\varrho} \xrightarrow{(\alpha)} \varrho'$ matches $\mu \xrightarrow{\alpha} \mu'$.

Now suppose $\nu \xrightarrow{\alpha} \nu'$ for some $\alpha \in \mathcal{A}$, $\nu' \in \mathit{Distr}(\mathcal{E})$. Since $\mu \Rightarrow \nu$ by assumption, we see that $\mu \Rightarrow \nu \xrightarrow{\alpha} \nu'$ matches $\nu \xrightarrow{\alpha} \nu'$.

To verify weak decomposability of the relation $\mathcal{R}$, first suppose $\mu = \bigoplus_{i \in I} p_i \cdot \mu_i$ for some index set I and $\mu_i \in \mathit{Distr}(\mathcal{E})$ for $i \in I$. Since $\varrho \leftrightarrow_b \mu$, we obtain from weak decomposability of $\leftrightarrow_b$ that $\varrho \Rightarrow \bigoplus_{i \in I} p_i \cdot \varrho_i$ for $\varrho_i \in \mathit{Distr}(\mathcal{E})$ such that $\varrho_i \leftrightarrow_b \mu_i$ for $i \in I$. From $\nu \Rightarrow \varrho$ we then obtain for $\nu_i = \varrho_i$ for $i \in I$ that $\nu \Rightarrow \bigoplus_{i \in I} p_i \cdot \nu_i$ and $\nu_i \leftrightarrow_b \mu_i$ for $i \in I$. Second, suppose $\nu = \bigoplus_{i \in I} p_i \cdot \nu_i$ for some index set I and $\nu_i \in \mathit{Distr}(\mathcal{E})$ for $i \in I$. Since $\mu \Rightarrow \nu$ by assumption, we have for $\mu_i = \nu_i$ for $i \in I$ that $\mu \Rightarrow \bigoplus_{i \in I} p_i \cdot \mu_i$ and $\mu_i \leftrightarrow_b \nu_i$ for $i \in I$. □

The so-called *cancellativity law*, proven in [21], provides a partial reversal of Lemma 5.5: Suppose a convex combination of two distributions is branching probabilistic bisimilar to a similar convex combination of two other distributions. If one pair of corresponding components is branching probabilistic bisimilar, then so is the other.

Lemma 5.11 (Cancellativity). Let $\mu, \mu', \nu, \nu' \in \mathit{Distr}(\mathcal{E})$. If $\mu \,{}_r{\oplus}\, \nu \leftrightarrow_b \mu' \,{}_r{\oplus}\, \nu'$ with $r \in (0,1]$ and $\nu \leftrightarrow_b \nu'$, then $\mu \leftrightarrow_b \mu'$.

In this section we have introduced notions of strong, branching, and rooted branching probabilistic bisimilarity, and we derived various properties. In the next section we address how these notions of bisimilarity can be captured equationally.

6. Complete axiomatisation of probabilistic bisimulation

In this section we provide a sound and complete equational characterisation of strong probabilistic bisimulation semantics and rooted branching probabilistic bisimulation semantics. The completeness result for the latter is obtained along the same lines as the corresponding result for branching bisimilarity for non-deterministic processes in Section 3.

First, we extend and adapt the non-deterministic theory AX of Section 3 to the theory AX_p to cater for probabilistic choice and combined transitions.

Definition 6.1 (Axiomatization of $\leftrightarrow$). The equational theory AX_p is given by the axioms A1 to A4, the axioms P1 to P3, and the axiom C listed in Table 2.

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 it also holds that $(1{-}r)s = (1{-}\bar{r})\bar{s}$. In particular, the probability for subprocess 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 captures that any two non-deterministic transitions with the same label can be executed in a combined fashion: assigning probability r to the one transition and the complementary probability $1{-}r$ to the other. For the mixed setting of non-deterministic and probabilistic choice, the axioms A1–A4 and P1–P3, together with axiom C have been presented as an equational theory for probabilistic strong bisimulation elsewhere, e.g., in [7, 30, 17].

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. As explained in Section 5, we often denote such a process by $\bigoplus_{i\in I} p_i \cdot E_i$ with $p_i = r_i \prod_{j=1}^{i-1}(1{-}r_j)$. More specifically, if a probabilistic process P corresponds to a distribution $\bigoplus_{i\in I} p_i \cdot E_i$, i.e. $[\![P]\!] = \bigoplus_{i\in I} p_i \cdot E_i$, then we have that $AX_p \vdash P = \bigoplus_{i\in I} p_i \cdot E_i$, as can be shown by induction on the structure of P.

As noted, the equational characterisation of strong probabilistic bisimilarity has been addressed by various authors. The theory AX_p provides a sound and complete equational axiomatisation of strong probabilistic bisimilarity. For a proof, see [30], for example.

Theorem 6.2. The theory AX_p is sound and complete for strong probabilistic bisimilarity. □

Continuing with the axiomatisation of rooted branching probabilistic bisimulation semantics, we make use of an auxiliary relation $\sqsubseteq$ on $\mathcal{E} \times \mathcal{P}$, referred to as *inclusion* of a non-deterministic process in a probabilistic process—see Table 2.

Definition 6.3 (Probabilistic inclusion). The relation $\sqsubseteq\ \subseteq \mathcal{E} \times \mathcal{P}$ is such that

$$\begin{aligned} E \sqsubseteq P \ \text{ iff } \ & E \xrightarrow{\alpha} \mu \text{ for } \alpha \in \mathcal{A},\ \mu \in \mathit{Distr}(\mathcal{E}) \text{ implies} \\ & [\![P]\!] \xrightarrow{(\alpha)} \nu \text{ for some } \nu \in \mathit{Distr} \text{ such that } \nu \leftrightarrow \mu\,. \end{aligned}$$

Thus, for $E \sqsubseteq P$ to hold, we require that every transition of the non-deterministic process E can be directly matched by the probabilistic process P, possibly as a partial transition. The next lemma confirms that this matching of transitions extends to the Dirac process of E.

Lemma 6.4. 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 $\mu \leftrightarrow \nu$.

Proof. If $\delta(E) \xrightarrow{\alpha} \mu$, then $\mu = \bigoplus_{i\in I} p_i \cdot \mu_i$ and $E \xrightarrow{\alpha} \mu_i$ for suitable index set I, $p_i \geqslant 0$, and $\mu_i \in \mathit{Distr}(\mathcal{E})$. 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 $\mu_i \leftrightarrow \nu_i$. Hence $[\![P]\!] \xrightarrow{(\alpha)} \nu$ for $\nu = \bigoplus_{i\in I} p_i \cdot \nu_i$ by Lemma 4.7, and $\mu \leftrightarrow \nu$ by Lemma 5.5. □

The following lemma tells that the inclusion relation $\sqsubseteq$ is compatible with strong probabilistic bisimulation semantics.

Lemma 6.5. If $E \sqsubseteq P$, $E \leftrightarrow F$, and $P \leftrightarrow Q$, then $F \sqsubseteq Q$.

Proof. Suppose $E \sqsubseteq P$, $E \leftrightarrow F$, and $P \leftrightarrow Q$. Let $F \xrightarrow{\alpha} \mu$. Then $\delta(F) \xrightarrow{\alpha} \mu$, and by Definition 5.1b $\delta(E) \xrightarrow{\alpha} \mu'$ for some $\mu' \in \mathit{Distr}(\mathcal{E})$ such that $\mu \leftrightarrow \mu'$. So, by Lemma 6.4 exists $\nu' \in \mathit{Distr}(\mathcal{E})$ such that $[\![P]\!] \xrightarrow{(\alpha)} \nu'$ and $\mu' \leftrightarrow \nu'$. Again by application of Definition 5.1b, exists $\nu \in \mathit{Distr}(\mathcal{E})$ such that $[\![Q]\!] \xrightarrow{(\alpha)} \nu$ and $\nu' \leftrightarrow \nu$. By transitivity $\mu \leftrightarrow \nu$. □

However, $\sqsubseteq$ is not compatible with (rooted) branching probabilistic bisimulation semantics: we have $a.P \sqsubseteq \partial(a.P) \leftrightarrow_b \partial(\tau.\partial(a.P))$, yet $a.P \not\sqsubseteq \partial(\tau.\partial(a.P))$. Thus, if we have $AX_p \vdash P = Q$ and $E \sqsubseteq P$ we can conclude that $E \sqsubseteq Q$. However, with AX_p^b the equational theory capturing branching probabilistic bisimulation semantics discussed below, it is not allowed to infer $E \sqsubseteq Q$ from $E \sqsubseteq P$ and $AX_p^b \vdash P = Q$, i.e., after proving $P = Q$ by means of axioms that are merely sound for branching probabilistic bisimilarity.

We must be able to capture inclusion equationally. The axioms I1–I6, presented in Table 2, together with AX_p, constitute a complete axiomatisation of $\sqsubseteq$. We refer to the theory AX_p, I1–I6 as AX_p^I.

Axioms I1 and I2 for inclusion take care of matching by a standard transition and of matching by no transition, respectively. Matching of a partial transition is captured by axiom I3. Note that the variants of axiom I3 with $r = 0$ and $r = 1$ follow from I1 and I2, respectively. Probabilistic and non-deterministic composition are covered by axioms I4 and I5, respectively, deadlock by axiom I6.

Lemma 6.6. Let $E \in \mathcal{E}$ and $P \in \mathcal{P}$. Then $E \sqsubseteq P$ iff $AX_p^I \vdash E \sqsubseteq P$.

Proof. "If", soundness. In view of Theorem 6.2 and Lemma 6.5, it suffices to check the soundness of each of the axioms I1–I6. The soundness of the axioms I1, I2, and I6 follows immediately from the definition of $\sqsubseteq$.

For the soundness of I3, the transition $\tau \cdot (\partial(E + \tau \cdot P)\ {}_r\!\oplus\ P) \xrightarrow{\tau} \delta(E + \tau \cdot P)\ {}_r\!\oplus\ [\![P]\!]$ can be mimicked as $[\![\partial(E + \tau \cdot P)]\!] \xrightarrow{(\tau)} \delta(E + \tau \cdot P)\ {}_r\!\oplus\ [\![P]\!]$. Namely, $[\![\partial(E + \tau \cdot P)]\!] = \delta(E + \tau \cdot P)\ {}_r\!\oplus\ \delta(E + \tau \cdot P)$ and $\delta(E + \tau \cdot P) \xrightarrow{\tau} [\![P]\!]$.

For axiom I4, suppose $\alpha \cdot P_i \sqsubseteq Q_i$ for $i = 1, 2$. Since $\alpha \cdot P_i \xrightarrow{\alpha} [\![P_i]\!]$, one has $[\![Q_i]\!] \xrightarrow{(\alpha)} [\![P_i]\!]$ for $i = 1, 2$. So $[\![Q_1\ {}_r\!\oplus\ Q_2]\!] = [\![Q_1]\!]\ {}_r\!\oplus\ [\![Q_2]\!] \xrightarrow{(\alpha)} [\![P_1]\!]\ {}_r\!\oplus\ [\![P_2]\!] = [\![P_1\ {}_r\!\oplus\ P_2]\!]$ by Lemma 4.7. Hence, the transition $\alpha \cdot (P_1\ {}_r\!\oplus\ P_2) \xrightarrow{\alpha} [\![P_1\ {}_r\!\oplus\ P_2]\!]$ can be matched by $[\![Q_1\ {}_r\!\oplus\ Q_2]\!]$.

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 $\partial(E + \tau \cdot P) = P$
G	if $E \sqsubseteq \partial(F)$ then $\partial(E + F) = \partial(F)$
I1	$\alpha \cdot P \sqsubseteq \partial(E + \alpha \cdot P)$
I2	$\tau \cdot \partial(E) \sqsubseteq \partial(E)$
I3	$\tau \cdot (\partial(E + \tau \cdot P) \;{}_{r}{\oplus}\; P) \sqsubseteq \partial(E + \tau \cdot P)$
I4	if $\alpha \cdot P_1 \sqsubseteq Q_1$ and $\alpha \cdot P_2 \sqsubseteq Q_2$ then $\alpha \cdot (P_1 \;{}_{r}{\oplus}\; P_2) \sqsubseteq Q_1 \;{}_{r}{\oplus}\; Q_2$
I5	if $E_1 \sqsubseteq P$ and $E_2 \sqsubseteq P$ then $E_1 + E_2 \sqsubseteq P$
I6	$\mathbf{0} \sqsubseteq P$

Table 2: Axioms for strong and rooted branching probabilistic bisimilarity

For I5, suppose $E_i \sqsubseteq P$ for $i = 1, 2$, and $E_1 + E_2 \xrightarrow{\alpha} \mu$. Then either $E_1 \xrightarrow{\alpha} \mu$ or $E_2 \xrightarrow{\alpha} \mu$, so $[\![P]\!] \xrightarrow{(\alpha)} \nu$ for some $\nu \in \mathit{Distr}(\mathcal{E})$ such that $\mu \mathrel{\underline{\leftrightarrow}} \nu$.

"Only if", completeness. Suppose $E \sqsubseteq Q$. Using AX_p, process E can be brought in the form $\sum_{i \in I} \alpha_i \cdot P_i$, and Q in the form $\bigoplus_{j \in J} q_j \cdot F_j$ with $q_j > 0$ for all $j \in J$.

First consider the situation where $|I| = |J| = 1$, so $E = \alpha \cdot P$ and $Q = \partial(F)$ for suitable α, P, and F. Since $E \xrightarrow{\alpha} [\![P]\!]$ and $E \sqsubseteq \partial(F)$, one has $\delta(F) \xrightarrow{(\alpha)} \nu$ for some $\nu \in \mathit{Distr}(\mathcal{E})$ such that $\nu \mathrel{\underline{\leftrightarrow}} [\![P]\!]$. By Definition 4.4 either (i) $\delta(F) \xrightarrow{\alpha} \nu$, or (ii) $\alpha = \tau$ and $\nu = \delta(F)$, or (iii) $\alpha = \tau$ and $\nu = \delta(F) \;{}_{r}{\oplus}\; \nu_2$ for some $r \in (0,1)$ and $\nu_2 \in \mathit{Distr}(\mathcal{E})$ with $\delta(F) \xrightarrow{\alpha} \nu_2$. (i) In the first case we have $F \mathrel{\underline{\leftrightarrow}} F + \alpha \cdot P$, so $AX_p \vdash F = F + \alpha \cdot P$ by Theorem 6.2 and $AX_p \vdash \partial(F) = \partial(F + \alpha \cdot P)$. Application of axiom I1 yields $AX_p^I \vdash E = \alpha \cdot P \sqsubseteq \partial(F + \alpha \cdot P) = \partial(F) = Q$. (ii) In the second case, $AX_p \vdash P = \partial(F)$ by Theorem 6.2. Axiom I2 yields $AX_p^I \vdash E = \tau \cdot P = \tau \cdot \partial(F) \sqsubseteq \partial(F) = Q$. (iii) In the third case, decomposability required by Definition 5.1a yields $[\![P]\!] = \mu_1 \;{}_{r}{\oplus}\; \mu_2$ with $\mu_1 \mathrel{\underline{\leftrightarrow}} \delta(F)$ and $\mu_2 \mathrel{\underline{\leftrightarrow}} \nu_2$. Thus, by Theorem 6.2 we have $AX_p \vdash P = \partial(F) \;{}_{r}{\oplus}\; P_2$ with P_2 such that $[\![P_2]\!] \mathrel{\underline{\leftrightarrow}} \nu_2$. Now $F \mathrel{\underline{\leftrightarrow}} F + \tau \cdot P_2$, since $\delta(F) \xrightarrow{\tau} \nu_2 \mathrel{\underline{\leftrightarrow}} [\![P_2]\!]$. So $AX_p \vdash F = F + \tau \cdot P_2$ by Theorem 6.2. Therefore it holds that

$$AX_p^I \vdash E = \tau \cdot P = \tau \cdot \big(\partial(F) \;{}_{r}{\oplus}\; P_2\big) = \tau \cdot \big(\partial(F + \tau \cdot P_1) \;{}_{r}{\oplus}\; P_2\big) \sqsubseteq \partial(F + \tau \cdot P_2) = \partial(F) = Q$$

by help of axiom I3.

Next consider the situation where $|I| = 1$ and $|J| > 1$. So, $E = \alpha \cdot P$ for some α and P. Since $E \xrightarrow{\alpha} [\![P]\!]$ and $E \sqsubseteq \bigoplus_{j \in J} q_j \cdot F_j$, one has $\bigoplus_{j \in J} q_j \cdot \delta(F_j) \xrightarrow{(\alpha)} \nu$ for some $\nu \in \mathit{Distr}(\mathcal{E})$

such that $[\![P]\!] \leftrightarrow \nu$. By Lemma 4.8, $\nu = \bigoplus_{j\in J} q_j \cdot \nu_j$ for $\nu_j \in \mathit{Distr}(\mathcal{E})$ with $\delta(F_j) \xrightarrow{(\alpha)} \nu_j$ for all $j \in J$. By Definition 5.1a, $[\![P]\!] = \bigoplus_{j\in J} q_j \cdot \mu_j$ for $\mu_j \in \mathit{Distr}(\mathcal{E})$ with $\mu_j \leftrightarrow \nu_j$ for all $j \in J$. We have $AX_p \vdash P = \bigoplus_{j\in J} q_j \cdot P_j$ where $P_j \in \mathcal{P}$ is such that $[\![P_j]\!] = \mu_j$ for all $j \in J$. In addition, $\alpha \cdot P_j \sqsubseteq \partial(F_j)$, hence $AX_p^I \vdash \alpha \cdot P_j \sqsubseteq \partial(F_j)$ by the previous case of $|I| = 1$ and $|J| = 1$. Therefore it follows that

$$AX_p^I \vdash E = \alpha \cdot P = \alpha \cdot \big(\bigoplus_{j\in J} q_j \cdot P_j\big) \sqsubseteq \bigoplus_{j\in J} q_j \cdot F_j = Q$$

by application of axiom I4 specifically.

Finally, consider $E = \sum_{i\in I} \alpha_i \cdot P_i$ with $|I| > 1$. If $\alpha_i \cdot P_i \xrightarrow{\alpha_i} \mu$ for some $i \in I$ then $E \xrightarrow{\alpha_i} \mu$. Since $E \sqsubseteq Q$, this implies $Q \xrightarrow{(\alpha_i)} \nu$ for some $\nu \leftrightarrow \mu$. Hence $\alpha_i \cdot P_i \sqsubseteq Q$. Thus, by the above, we obtain $AX_p^I \vdash \alpha_i \cdot P_i \sqsubseteq Q$ for all $i \in I$. Axioms I5 and I6 then yield $AX_p^I \vdash E \sqsubseteq Q$. $\square$

Having introduced the notion of inclusion and its axiomatisation, we now introduce an axiomatisation for rooted branching probabilistic bisimulation semantics that we will show to be sound and complete. The theory involves the inclusion relation. At the end of this section we convert the conditional axioms BP and G to a purely equational form.

Definition 6.7 (Axiomatization of $\leftrightarrow_{rb}$). The theory AX_p^b contains AX_p together with the axioms BP and G. The preconditions $E \sqsubseteq P$ of BP and G are to be obtained from AX_p^I.

Axiom BP is an adaptation of axiom B of the theory AX^b presented in Section 3 to the probabilistic setting of AX_p^b. In the setting of non-deterministic processes the implication $F \xrightarrow{\alpha} F' \implies E \xrightarrow{\alpha} E' \wedge F' \leftrightarrow_b E'$ for some E' is captured by $E + F \leftrightarrow_{rb} E$. 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. In comparison, the action prefix α occurring in B, related to the root condition for rooted branching bisimulation, has been replaced in BP by the Dirac construction $\partial(\cdot)$.

As to BP, a non-deterministic alternative E that is also offered by a probabilistic process P after a τ-prefix can be dispensed with, together with the prefix τ. In a formulation retaining the τ-prefix on the right-hand side, the axiom BP shows similarity with axioms T2 and T3 in [17] which, in turn, are reminiscent of axioms T1 and T2 of [13]; these axioms stem from Milner's second τ-law [34].

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

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

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

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

An example illustrating partiality, i.e., the use of (τ), rather than τ 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

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

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

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

Before presenting concrete applications of AX_p^b we first discuss some derived laws, also as an illustration. The second equation is the B-axiom of [22] in the setting of AX_p^b. The axioms in a non-probabilistic setting are preceded by an action to deal with the rootedness issue. In the probabilistic setting it is enough to use only the Dirac operator. See the first equation. Clearly the second equation follows directly from the first. The last one is the pendant of Milner's first τ-law.

Lemma 6.8. The following equations are derivable from AX_p^b.

(a) $AX_p^b \vdash \partial(E + F) = \partial(\tau \cdot \partial(E + F) + F)$.

(b) $AX_p^b \vdash \alpha \cdot \partial(E + F) = \alpha \cdot \partial(\tau \cdot \partial(E + F) + F)$.

(c) $AX_p^b \vdash P = \partial(\tau \cdot P)$.

Proof. (a) The equation follows from axioms BP and A1 by taking $P := \partial(E + F)$, using that $F \sqsubseteq \partial(E + F)$.

(b) The equation follows directly from the previous item using congruence.

(c) The equation is yielded by the axioms BP, I6, A1, and A4, taking $E := \mathbf{0}$. ☐

We further illustrate the working of theory AX_p^b by showing the equivalence of the remaining example pairs of Figure 2.

Example 6.9.

(a) For the two examples taken from [30] we exploit associativity and splitting as provided by the axioms P2 and P3.

$$\begin{aligned} AX_p^b \vdash\ & \mathbf{H_1} \\ =\ & a \cdot \big(P \,{}_{\frac{1}{4}}\!\oplus\, (P \,{}_{\frac{1}{3}}\!\oplus\, Q)\big) \\ =\ & a \cdot \big((P \,{}_{\frac{1}{2}}\!\oplus\, P) \,{}_{\frac{1}{2}}\!\oplus\, Q\big) && \text{Axiom P2} \\ =\ & a \cdot \big(P \,{}_{\frac{1}{2}}\!\oplus\, Q\big) && \text{Axiom P3} \\ =\ & a \cdot \big(P \,{}_{\frac{1}{2}}\!\oplus\, (Q \,{}_{\frac{1}{2}}\!\oplus\, Q)\big) && \text{Axiom P3} \\ =\ & \mathbf{H_2}. \end{aligned}$$

(b) The partial inert expansion of the examples $\mathbf{G_1}$ and $\mathbf{G_2}$ is covered by a combination of axiom P3, allowing to split a distribution, and the axiom BP to introduce an inert transition in the proper context.

$$\begin{aligned}
AX_p^b \vdash\ & \mathbf{G_1} \\
=\ & a \cdot (P \,{}_{\frac{1}{2}}\!\oplus\, Q) \\
=\ & a \cdot \big((P \,{}_{\frac{1}{2}}\!\oplus\, Q) \,{}_{\frac{1}{3}}\!\oplus\, (P \,{}_{\frac{1}{2}}\!\oplus\, Q)\big) && \text{Axiom P3} \\
=\ & a \cdot \big(\partial(\tau \cdot (P \,{}_{\frac{1}{2}}\!\oplus\, Q)) \,{}_{\frac{1}{3}}\!\oplus\, (P \,{}_{\frac{1}{2}}\!\oplus\, Q)\big) && \text{Lemma 6.8c} \\
=\ & \mathbf{G_2}.
\end{aligned}$$

(c) To show equality of the processes $\mathbf{I_1}$ and $\mathbf{I_2}$ we make use of Lemma 6.8. We have

$$\begin{aligned}
AX_p^b \vdash\ & \mathbf{I_1} \\
=\ & a \cdot \partial(b \cdot P + \tau \cdot Q) \\
=\ & a \cdot \partial(b \cdot P + \tau \cdot Q + b \cdot P + \tau \cdot Q) && \text{Axiom A3} \\
=\ & a \cdot \partial(\tau \cdot \partial(b \cdot P + \tau \cdot Q + b \cdot P + \tau \cdot Q) + b \cdot P + \tau \cdot Q) && \text{Lemma 6.8a} \\
=\ & a \cdot \partial(\tau \cdot \partial(b \cdot P + \tau \cdot Q) + b \cdot P + \tau \cdot Q) && \text{Axiom A3} \\
=\ & \mathbf{I_2}.
\end{aligned}$$

(d) The equality of the process $\mathbf{T_1} = a \cdot \partial(b \cdot (P \,{}_{\frac{1}{3}}\!\oplus\, Q)) \,{}_{\frac{1}{2}}\!\oplus\, \partial(b \cdot (P \,{}_{\frac{2}{3}}\!\oplus\, Q))$ and the process $\mathbf{T_2} = a \cdot \partial(\tau \cdot \big(\partial(b \cdot (P \,{}_{\frac{1}{3}}\!\oplus\, Q)) \,{}_{\frac{1}{2}}\!\oplus\, \partial(b \cdot (P \,{}_{\frac{2}{3}}\!\oplus\, Q))\big) + b \cdot (P \,{}_{\frac{1}{2}}\!\oplus\, Q))$ modulo AX_p^b follows immediately from axiom BP once we have $b \cdot (P \,{}_{\frac{1}{2}}\!\oplus\, Q) \sqsubseteq \partial(b \cdot (P \,{}_{\frac{1}{3}}\!\oplus\, Q)) \,{}_{\frac{1}{2}}\!\oplus\, \partial(b \cdot (P \,{}_{\frac{2}{3}}\!\oplus\, Q))$. This follows from axioms I1 and I4, by writing $b \cdot (P \,{}_{\frac{1}{2}}\!\oplus\, Q)$ as $b \cdot ((P \,{}_{\frac{1}{3}}\!\oplus\, Q) \,{}_{\frac{1}{2}}\!\oplus\, (P \,{}_{\frac{2}{3}}\!\oplus\, Q))$, using axioms P1 to P3 as well.

(e) To formally prove that the processes $\mathbf{E_1}$ and $\mathbf{E_2}$ of [15] are equal with respect to AX_p^b we observe

$$\begin{aligned}
AX_p^b \vdash\ & \mathbf{E_1} \\
=\ & \tau \cdot (\partial(\tau \cdot P + a \cdot Q + \tau \cdot R) \,{}_{\frac{3}{4}}\!\oplus\, \partial(\mathbf{0})) \\
=\ & \tau \cdot (\partial(\tau \cdot P + a \cdot Q + \tau \cdot R) \,{}_{\frac{1}{2}}\!\oplus\, (\partial(\tau \cdot P + a \cdot Q + \tau \cdot R) \,{}_{\frac{1}{2}}\!\oplus\, \partial(\mathbf{0}))) && \text{Axioms P3, P2} \\
=\ & \tau \cdot (\partial(\tau \cdot P + a \cdot Q + \tau \cdot R) \,{}_{\frac{1}{2}}\!\oplus \\
& \qquad (\partial(\tau \cdot \partial(\tau \cdot P + a \cdot Q + \tau \cdot R) \,{}_{\frac{1}{2}}\!\oplus\, \partial(\mathbf{0})))) && \text{Lemma 6.8c} \\
=\ & \mathbf{E_2}.
\end{aligned}$$

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

Lemma 6.10 (Soundness). For all $P, Q \in \mathcal{P}$, if $AX_p^b \vdash P = Q$ then $P \leftrightarrow_b Q$. Likewise, for all $E, F \in \mathcal{E}$, if $AX_p^b \vdash E = F$ then $E \leftrightarrow_{rb} F$.

Proof. In view of Theorem 6.2 and Lemma 5.9 we only need to prove the soundness of the axioms BP and G. For BP we need to show that $\delta(E + \tau.P) \leftrightarrows_b [\![P]\!]$ when $E \sqsubseteq P$, and for G that $\delta(E + F) \leftrightarrows_b \delta(F)$ when $E \sqsubseteq \partial(F)$.

Both statements follow from the observation that the relations

$$\{ \langle \delta(E + \tau.P), [\![P]\!] \rangle \mid E \sqsubseteq P \}^\dagger \cup \leftrightarrows_b$$

and

$$\{ \langle \delta(E + F), \delta(F) \rangle \mid E \sqsubseteq \partial(F) \}^\dagger \cup \leftrightarrows_b$$

are branching probabilistic bisimulation relations, as can be straightforwardly checked. □

As for the process language with non-deterministic processes only, we aim at a completeness proof that is built on the completeness of strong bisimilarity and the notion of a concrete process. 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. Not only do we need to consider partially inert transitions, but we also want to exclude, for example, processes of the form

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

from being concrete, although they cannot perform a transition by themselves at all. To capture inertness of subprocesses we employ the following definition.

Definition 6.11.

(a) The *derivatives* $der(E), der(P) \subseteq \mathcal{E}$ of non-deterministic and probabilistic processes $E \in \mathcal{E}$ and $P \in \mathcal{P}$ are given by

$$\begin{aligned} der(\textstyle\sum_{i \in I} \alpha_i \cdot P_i) &= \{ \textstyle\sum_{i \in I} \alpha_i \cdot P_i \} \cup \textstyle\bigcup_{i \in I} der(P_i) \\ der(\textstyle\bigoplus_{i \in I} p_i \cdot E_i) &= \textstyle\bigcup_{i \in I} der(E_i). \end{aligned}$$

(b) A process $\bar{E} \in \mathcal{E}$ or $\bar{P} \in \mathcal{P}$ is said to be *concrete* if none of its derivatives can perform a partially inert transition, i.e., there is no $E \in der(\bar{E})$ or $E \in der(\bar{P})$, respectively, that has a transition of the form $E \xrightarrow{\tau} \mu_1 \;{}_r{\oplus}\; \mu_2$ with $r > 0$ and $\delta(E) \leftrightarrows_b \mu_1$.

(c) A process $E \in \mathcal{E}$ is called *rigid* if it has no inert transition, i.e., a transition $E \xrightarrow{\tau} \mu$ such that $\delta(E) \leftrightarrows_b \mu$.

(d) The sets $\mathcal{E}_{cc}$ and $\mathcal{P}_{cc}$ of concrete non-deterministic processes and concrete probabilistic processes are given by

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

The set $\mathcal{E}_r$ of non-deterministic processes that are rigid is given by $\mathcal{E}_r = \{ E \in \mathcal{E} \mid E \text{ is rigid} \}$.

A concrete process has no derivative that can perform a partially inert transition. Thus, a non-deterministic process is concrete if it has no partially inert transition and all its derivatives are are concrete. A probabilistic process is concrete if it is a probabilistic choice of concrete non-deterministic processes. Clearly, $\mathcal{E}_{cc} \subseteq \mathcal{E}_r$. We use concrete and rigid processes to build the completeness proof for rooted branching probabilistic bisimilarity on top of the completeness proof of strong probabilistic bisimilarity. The following lemma lists all the properties of concrete and rigid processes that we need for this.

Lemma 6.12.

(a) Let $E = \sum_{i \in I} \alpha_i \cdot P_i$ with $P_i \in \mathcal{P}_{cc}$ for $i \in I$. If, for all $i \in I$, (i) $\alpha_i \neq \tau$, or (ii) $[\![P_i]\!]$ cannot be written as $\mu_1 \,{}_r\!\oplus\, \mu_2$ where $r > 0$ and $\delta(E) \leftrightarroweq_b \mu_1$, 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 $\mu = \bigoplus_{i \in I} p_i \cdot \mu_i \in \mathit{Distr}(\mathcal{E}_{cc})$ where $p_i > 0$ for all $i \in I$, then $\mu_i \in \mathit{Distr}(\mathcal{E}_{cc})$ for all $i \in I$.

(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 $\mu \Longrightarrow \mu'$ with $\mu \leftrightarroweq_b \mu'$, then $\mu = \mu'$.

(f) If $\mu \leftrightarroweq_b \bigoplus_{i \in I} p_i \cdot \nu_i$ for $\mu \in \mathit{Distr}(\mathcal{E}_r)$, then $\mu = \bigoplus_{i \in I} p_i \cdot \mu_i$ for certain $\mu_i \leftrightarroweq_b \nu_i$ with $i \in I$.

(g) If $E \in \mathcal{E}_r$ and $\delta(E) \leftrightarroweq_b \nu$, then $E \leftrightarroweq_b F$ for all $F \in \mathrm{spt}(\nu)$.

(h) If $E \in \mathcal{E}_{cc}$ and $\delta(E) \xrightarrow{\tau} \mu_1 \,{}_r\!\oplus\, \mu_2$ with $\delta(E) \leftrightarroweq_b \mu_1$, then $r = 0$.

(i) Let $E \in \mathcal{E}_{cc}$ and $F \in \mathcal{E}$ such that $\delta(E) \leftrightarroweq_b \delta(F)$. If $\delta(E) \xrightarrow{\alpha} \mu$, $\delta(F) \xrightarrow{(\alpha)} \nu$, and $\mu \leftrightarroweq_b \nu$ for $\mu, \nu \in \mathit{Distr}(\mathcal{E})$, then $\delta(F) \xrightarrow{\alpha} \nu$ and there is no $G \in \mathrm{spt}(\nu)$ with $E \leftrightarroweq_b G$.

Proof. For property (a) it suffices to show that E cannot perform a partially inert transition. So suppose, to the contrary, that $E \xrightarrow{\tau} \mu_1 \,{}_r\!\oplus\, \mu_2$ with $r > 0$ and $\delta(E) \leftrightarroweq_b \mu_1$. Then there is an index $i \in I$ with $\alpha_i = \tau$ and $[\![P_i]\!] = \mu_1 \,{}_r\!\oplus\, \mu_2$, contradicting the assumption.

Property (b) follows directly from the observation that following Definition 6.11 it holds that $\mathit{der}(P_1 \,{}_r\!\oplus\, P_2) = \mathit{der}(P_1) \cup \mathit{der}(P_2)$.

To see property (c), we observe that, for $i \in I$, $\mathrm{spt}(\mu_i) \subseteq \mathrm{spt}(\mu)$, and therefore $\mathrm{spt}(\mu) \subseteq \mathcal{E}_{cc}$ implies $\mathrm{spt}(\mu_i) \subseteq \mathcal{E}_{cc}$.

As to property (d), we can assume $\mathrm{spt}(\mu) = \{ E_i \mid i \in I \}$ and $\mu' = \bigoplus_{i \in I} p_i \cdot \mu'_i$ where $E_i \xrightarrow{\alpha} \mu'_i$ or $\mu'_i = \delta(E_i)$ for $i \in I$. So, we have $\mathrm{spt}(\mu'_i) \subseteq \mathit{der}(E_i) \subseteq \mathcal{E}_{cc}$ or $\mathrm{spt}(\mu'_i) = E_i \in \mathrm{spt}(\mu) \subseteq \mathcal{E}_{cc}$, respectively, for $i \in I$. Therefore, $\mathrm{spt}(\mu'_i) \subseteq \mathcal{E}_{cc}$ for $i \in I$ and $\mathrm{spt}(\mu') \subseteq \mathcal{E}_{cc}$.

For (e), let $\mu \in \mathit{Distr}(\mathcal{E}_r)$ and $\mu \Longrightarrow \mu'$ with $\mu \leftrightarroweq_b \mu'$. 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 $\bar{\mu} \Longrightarrow \mu'$. We may even choose $\bar{\mu}$ such that the transition $\mu \xrightarrow{(\tau)} \bar{\mu}$ acts on only one element of the support of μ, i.e. there are $E \in \mathcal{E}$, $r \in (0,1]$ and $\hat{\mu}, \varrho \in \mathit{Distr}(\mathcal{E})$ such that $\mu = \delta(E) \,{}_r\!\oplus\, \varrho$, $E \xrightarrow{\tau} \hat{\mu}$ and $\bar{\mu} = \hat{\mu} \,{}_r\!\oplus\, \varrho$. By the stuttering property of Lemma 5.10, $\mu \leftrightarroweq_b \bar{\mu}$, thus $\delta(E) \,{}_r\!\oplus\, \varrho = \mu \leftrightarroweq_b \bar{\mu} = \hat{\mu} \,{}_r\!\oplus\, \varrho$. Hence, by cancellativity of Lemma 5.11, we obtain $\delta(E) \leftrightarroweq_b \hat{\mu}$. So, the transition $E \xrightarrow{\tau} \hat{\mu}$ is inert, contradicting $E \in \mathcal{E}_r$.

Regarding (f), if $\mu \leftrightarrow_b \bigoplus_{i\in I} p_i \cdot \nu_i$ for $\mu \in Distr(\mathcal{E}_r)$, then $\mu \Rightarrow \bar{\mu} := \bigoplus_{i\in I} p_i \cdot \mu_i$ with $\mu \leftrightarrow_b \bar{\mu}$ and $\mu_i \leftrightarrow_b \nu_i$ by weak decomposability of $\leftrightarrow_b$. By case (e) of the lemma we have $\bar{\mu} = \mu$.

For (g), suppose $E \in \mathcal{E}_r$ and $\delta(E) \leftrightarrow_b \nu$. Let $\nu = \bigoplus_{i\in I} p_i \cdot F_i$. Then $\delta(E) = \bigoplus_{i\in I} p_i \cdot \mu_i$ for certain $\mu_i \leftrightarrow_b \delta(F_i)$, using case (f). Now $\mu_i = \delta(E)$ for all $i \in I$ and hence $F_i \leftrightarrow_b E$ for all $i \in I$.

For (h), suppose $E \in \mathcal{E}_{cc}$ and $\delta(E) \xrightarrow{\tau} \mu_1 \,{}_r\!\oplus\, \mu_2$ with $\delta(E) \leftrightarrow_b \mu_1$ and $r > 0$. Say, $\mu_1 \,{}_r\!\oplus\, \mu_2 = \bigoplus_{i\in I} p_i \cdot \nu_i$ where $E \xrightarrow{\tau} \nu_i$ for $i \in I$. Since $r > 0$, for some $i \in I$ we have that $\mathrm{spt}(\mu_1) \cap \mathrm{spt}(\nu_i) \neq \emptyset$. By case (g) of the lemma it holds that $F \leftrightarrow_b E$ for $F \in \mathrm{spt}(\mu_1)$. Thus, the transition $E \xrightarrow{\tau} \nu_i$ is partially inert. This contradicts the assumption $E \in \mathcal{E}_{cc}$.

To establish (i), suppose $E \in \mathcal{E}_{cc}$, $F \in \mathcal{E}$, and $\mu, \nu \in Distr(\mathcal{E})$ are such that $\delta(E) \leftrightarrow_b \delta(F)$, $\delta(E) \xrightarrow{\alpha} \mu$, $\delta(F) \xrightarrow{(\alpha)} \nu$ and $\mu \leftrightarrow_b \nu$. Assume, for proving the first conclusion of case (i), that $\alpha = \tau$, for otherwise the statement is trivial. Then, for some $\nu_1, \nu_2 \in Distr(\mathcal{E})$ and $r \in [0,1]$, $\nu = \nu_1 \,{}_r\!\oplus\, \nu_2$, $\nu_1 = \delta(F)$ and either $r = 1$ or $\delta(F) \xrightarrow{\tau} \nu_2$. Since $\mu \leftrightarrow_b \nu$ and $\leftrightarrow_b$ is weakly decomposable, there are $\bar{\mu}, \mu_1, \mu_2 \in Distr(\mathcal{E})$ such that $\mu \Longrightarrow \bar{\mu} = \mu_1 \,{}_r\!\oplus\, \mu_2$, $\mu \leftrightarrow_b \bar{\mu}$, $\mu_1 \leftrightarrow_b \nu_1$ and $\mu_2 \leftrightarrow_b \nu_1$. Because $\mu \in Distr(\mathcal{E}_{cc})$ by case (d) of the lemma, it follows that $\bar{\mu} = \mu$ by case (e) of the lemma. Thus $\delta(E) \xrightarrow{\tau} \mu_1 \,{}_r\!\oplus\, \mu_2$ and $\delta(E) \leftrightarrow_b \delta(F) = \nu_1 \leftrightarrow_b \mu_1$. Since E is concrete and $\delta(E) \xrightarrow{\tau} \mu_1 \,{}_r\!\oplus\, \mu_2$, case (h) of the lemma yields $r = 0$. It follows that $\nu = \nu_2$ and $\delta(F) \xrightarrow{\tau} \nu$.

For the second conclusion of case (i), suppose $E \leftrightarrow_b G$ for some $G \in \mathrm{spt}(\nu)$. Then $\nu = \delta(G) \,{}_r\!\oplus\, \nu'$ for some $\nu' \in Distr(\mathcal{E})$ and $r > 0$. Exactly as above we find $\mu_1, \mu_2 \in Distr(\mathcal{E})$ such that $\mu = \mu_1 \,{}_r\!\oplus\, \mu_2$, $\delta(E) \xrightarrow{\tau} \mu_1 \,{}_r\!\oplus\, \mu_2$ and $\delta(E) \leftrightarrow_b \delta(G) \leftrightarrow_b \mu_1$, contradicting case (h) of the lemma. □

Because in concrete probabilistic processes partially inert transitions are absent, branching bisimilarity and strong bisimilarity coincide for concrete processes. As mentioned, this will help us to lift the completeness of the theory AX_p for strong probabilistic bisimulation to the completeness of the theory AX_p^b for branching probabilistic bisimulation.

Lemma 6.13. For all $\mu, \nu \in Distr(\mathcal{E}_{cc})$, if $\mu \leftrightarrow_b \nu$ then $\mu \leftrightarrow \nu$.

Proof. Let $\mu, \nu \in Distr(\mathcal{E}_{cc})$ be such that $\mu \leftrightarrow_b \nu$. Define the relation $\mathcal{R}$ by

$$\mathcal{R} = \leftrightarrow_b \cap \, (Distr(\mathcal{E}_{cc}) \times Distr(\mathcal{E}_{cc})) \; .$$

Then, by Lemma 6.12cd, $\mathcal{R}$ is a branching probabilistic bisimulation relation relating μ and ν. We show that $\mathcal{R}$ moreover satisfies the conditions of Lemma 5.4.

That $\mathcal{R}$ is decomposable follows by Lemma 6.12e since $\mathcal{R}$ is weakly decomposable. Condition (2) of Lemma 5.4 is a direct consequence of the congruence result of Lemma 5.5 and the observation that $\mu_1 \,{}_r\!\oplus\, \mu_2, \nu_1 \,{}_r\!\oplus\, \nu_2 \in Distr(\mathcal{E}_{cc})$ if $\mu_1, \mu_2, \nu_1, \nu_2 \in Distr(\mathcal{E}_{cc})$. Now, in order to verify condition (3) of the lemma, suppose $\delta(E), \delta(F) \in Distr(\mathcal{E}_{cc})$ are such that $\delta(E) \,\mathcal{R}\, \delta(F)$ and $E \xrightarrow{\alpha} \mu'$. Then $\delta(F) \Rightarrow \bar{\nu} \xrightarrow{(\alpha)} \nu'$ for some $\bar{\nu}, \nu' \in Distr(\mathcal{E})$ such that $\delta(E) \,\mathcal{R}\, \bar{\nu}$ and $\mu' \,\mathcal{R}\, \nu'$. By Lemma 6.12e we have $\bar{\nu} = \delta(F)$. Thus $\delta(F) \xrightarrow{(\alpha)} \nu'$. Using Lemma 6.12i it follows that $\delta(F) \xrightarrow{\alpha} \nu'$. With $\mathcal{R}$ being decomposable and satisfying conditions (2) and (3), Lemma 5.4 yields $\mu \leftrightarrow \nu$. □

Lemma 6.13 has a partial completeness result as an immediate consequence: branching bisimilarity for concrete probabilistic processes implies equality modulo AX_p^b, in fact modulo AX_p.

Corollary 6.14. For all $\bar{P}, \bar{Q} \in \mathcal{P}_{cc}$, if $\bar{P} \leftrightarrow_b \bar{Q}$ then $AX_p \vdash \bar{P} = \bar{Q}$.

Proof. For $\bar{P}, \bar{Q} \in \mathcal{P}_{cc}$ such that $\bar{P} \leftrightarrow_b \bar{Q}$, Lemma 6.13 above yields $\bar{P} \leftrightarrow \bar{Q}$. By Theorem 6.2 it then follows that $AX_p \vdash \bar{P} = \bar{Q}$, hence $AX_p^b \vdash \bar{P} = \bar{Q}$. □

The following lemma plays a crucial rôle in our completeness proof. It describes exactly the precondition $E \sqsubseteq \partial(F)$ that is needed for application of the axiom G in the proof.

Lemma 6.15. Let $F, H \in \mathcal{E}_{cc}$, $P \in \mathcal{P}_{cc}$, $r \in (0,1)$, and let $E := \tau \cdot (\partial(F)\,{}_r\!\oplus\, P) + H \in \mathcal{E}_r$ be such that $E \leftrightarrow_b F$. Suppose $G \leftrightarrow_b E$ for no $G \in \mathrm{spt}([\![P]\!])$. Then $\tau \cdot (\partial(F)\,{}_r\!\oplus\, P) \sqsubseteq \partial(H)$.

Proof. It suffices to show that $\delta(H) \xrightarrow{(\tau)} \nu$ for some $\nu \leftrightarrow \delta(F)\,{}_r\!\oplus\, [\![P]\!]$. To this end we prove three claims.

(a) $\delta(F) \xrightarrow{\tau} \mu$ for some $\mu \in \mathit{Distr}(\mathcal{E})$ with $\mu \leftrightarrow_b [\![P]\!]$.

(b) If $\delta(F) \xrightarrow{\alpha} \varrho$ then $\delta(H) \xrightarrow{\alpha} \eta$ for some $\eta \in \mathit{Distr}(\mathcal{E})$ with $\eta \leftrightarrow_b \varrho$.

(c) $H \leftrightarrow_b F$.

From claims (a) and (b) we derive $\delta(H) \xrightarrow{\tau} \eta$ for some η with $\eta \leftrightarrow_b [\![P]\!]$. Now take $\nu := \delta(H)\,{}_r\!\oplus\, \eta$. Then $\delta(H) \xrightarrow{(\tau)} \nu$. By claim (c) and Lemma 5.5 we obtain $\nu \leftrightarrow_b \delta(F)\,{}_r\!\oplus\, [\![P]\!]$. By Lemma 6.12d we have $\eta \in \mathit{Distr}(\mathcal{E}_{cc})$, and thus $\delta(H)\,{}_r\!\oplus \eta$, $\delta(F)\,{}_r\!\oplus [\![P]\!] \in \mathit{Distr}(\mathcal{E}_{cc})$ by the assumptions for H, F, and P being concrete. Hence $\nu \leftrightarrow \delta(F)\,{}_r\!\oplus\, [\![P]\!]$ by Lemma 6.13.

Proof of claim (a). Since $E \xrightarrow{\tau} \delta(F)\,{}_r\!\oplus\, [\![P]\!]$ and $E \leftrightarrow_b F$, we have $\delta(F) \Longrightarrow \bar{\mu} \xrightarrow{(\tau)} \mu$ for some $\bar{\mu} \leftrightarrow_b \delta(F)$ and $\mu \leftrightarrow_b \delta(F)\,{}_r\!\oplus\, [\![P]\!]$. By Lemma 6.12e it follows that $\bar{\mu} = \delta(F)$, using that F is rigid. By Lemma 6.12d we have $\mu \in \mathit{Distr}(\mathcal{E}_{cc}) \subseteq \mathit{Distr}(\mathcal{E}_r)$. So by Lemma 6.12f, $\mu = \mu_1\,{}_r\!\oplus\, \mu_2$ with $\mu_1 \leftrightarrow_b \delta(F)$ and $\mu_2 \leftrightarrow_b [\![P]\!]$. On the other hand, as $\delta(F) \xrightarrow{(\tau)} \mu$, we obtain $\mu = \delta(F)\,{}_s\!\oplus\, \mu'$ for some $s \in [0,1]$ and μ' with either $s = 1$ or $\delta(F) \xrightarrow{\tau} \mu'$. Thus, we have two divisions of the same distribution μ in two parts. We proceed to show that these divisions are actually the same.

By Lemma 6.12g $F \leftrightarrow_b G'$ for each $G' \in \mathrm{spt}(\mu_1)$. Furthermore, we claim that $F \leftrightarrow_b G'$ for no $G' \in \mathrm{spt}(\mu_2)$. Namely, if $G' \in \mathrm{spt}(\mu_2)$ with $F \leftrightarrow_b G'$, then $\mu_2 = \delta(G')\,{}_p\!\oplus\, \mu_2'$ for some $p > 0$, and by Lemma 6.12f, using that $[\![P]\!] \subseteq \mathit{Distr}(\mathcal{E}_{cc}) \subseteq \mathit{Distr}(\mathcal{E}_r)$, $[\![P]\!] = \nu_1\,{}_p\!\oplus\, \nu_2$ for some $\nu_1 \leftrightarrow_b \delta(G')$ and $\nu_2 \leftrightarrow_b \mu_2'$. Since $\nu_1 \leftrightarrow_b \delta(G') \leftrightarrow_b \delta(F)$ and F is rigid, by Lemma 6.12g one obtains $G \leftrightarrow_b F \leftrightarrow_b E$ for some, in fact all, $G \in \mathrm{spt}(\nu_1) \subseteq \mathrm{spt}([\![P]\!])$, contradicting our assumption.

Since $\mathrm{spt}(\delta(F)) = F$ it follows that $s \leqslant r < 1$. Thus $\delta(F) \xrightarrow{\tau} \mu'$. Since $F \in \mathcal{E}_{cc}$, by Lemma 6.12h we have that no $G' \in \mathrm{spt}(\mu')$ satisfies $F \leftrightarrow_b G'$. Hence $s = r$ and $\mu' = \mu_2 \leftrightarrow_b [\![P]\!]$. This proves that $\delta(F) \xrightarrow{\tau} \mu'$ for some μ' with $\mu' \leftrightarrow_b [\![P]\!]$, as claimed.

Proof of claim (b). Assume $\delta(F) \xrightarrow{\alpha} \varrho$. Since $E \leftrightarrow_b F$, we have $\delta(E) \Longrightarrow \bar{\eta} \xrightarrow{(\alpha)} \eta$ for some $\bar{\eta} \leftrightarrow_b \delta(E)$ and $\eta \leftrightarrow_b \varrho$. By Lemma 6.12e $\bar{\eta} = \delta(E)$, using that E is rigid. Since F is concrete and $\delta(E) \xrightarrow{(\alpha)} \eta$, we have $\delta(E) \xrightarrow{\alpha} \eta$ by Lemma 6.12i. Lemma 6.12i also says that $F \notin \sup(\eta)$. Hence no fraction of the transition $\delta(E) \xrightarrow{\alpha} \eta$ can stem from the transition $E \xrightarrow{\tau} \delta(F)\,{}_r\!\oplus\, [\![P]\!]$. It follows that $\delta(H) \xrightarrow{\alpha} \eta$ with $\eta \leftrightarrow_b \varrho$.

Proof of claim (c). Let $\mathcal{R} = \{\langle \delta(H), \delta(F) \rangle\}^\dagger \cup \leftrightarrow_b$. It suffices to show that $\mathcal{R}$ is a branching probabilistic bisimulation relation. That $\mathcal{R}$ is weakly decomposable is straightforward. So it suffices to check the transfer condition for the pairs $\langle \delta(H), \delta(F) \rangle$ and $\langle \delta(F), \delta(H) \rangle$. Assume $\delta(H) \xrightarrow{\alpha} \varrho$. Then also $\delta(E) \xrightarrow{\alpha} \varrho$, and since $E \leftrightarrow_b F$ this move can be matched by $\delta(F)$. The other case follows by (b) above. □

We have now arrived at the main lemma that we need for a proof of completeness of the axioms of Table 2 with respect to rooted probabilistic branching bisimulation semantics. In its proof we reason by induction on the complexity of processes as captured by the complexity measure c below. Roughly speaking, the complexity measure counts the number of transitions of a process.

Definition 6.16. The complexity function $c : \mathcal{E} \cup \mathcal{P} \to \mathbb{N}$ is defined as follows:

$$c(\mathbf{0}) = 0 \qquad c(\alpha \cdot P) = 1 + c(P) \qquad c(E_1 + E_2) = c(E_1) + c(E_2)$$
$$c(\partial(E)) = c(E) \qquad c(P_1 \,{}_r\!\oplus\, P_2) = c(P_1) + c(P_2).$$

Note, the application of axiom A1, A2, A4, P1 and P2 does not change the complexity of a term.

Lemma 6.17.

(a) For each non-deterministic process $E \in \mathcal{E}$ there is a concrete probabilistic process $\bar{P} \in \mathcal{P}_{cc}$ such that $[\![\bar{P}]\!] \leftrightarrow_b \delta(E)$ and $AX_p^b \vdash \bar{P} = \partial(E)$.

(b) For each probabilistic process $P \in \mathcal{P}$ there is a concrete probabilistic process $\bar{P} \in \mathcal{P}_{cc}$ such that $[\![\bar{P}]\!] \leftrightarrow_b [\![P]\!]$ and $AX_p^b \vdash \bar{P} = P$.

(c) For all probabilistic processes $P, Q \in \mathcal{P}$, if $[\![P]\!] \leftrightarrow_b [\![Q]\!]$ then $AX_p^b \vdash P = Q$.

Proof. We prove items (a) to (c) by simultaneous induction on $c(E)$, $c(P)$, and $\max\{c(P), c(Q)\}$.

Basis If $c(E) = 0$, then E is provably equal to $\mathbf{0}$. Hence, choosing $\bar{P} = \partial(\mathbf{0}) \in \mathcal{P}_{cc}$ suffices. If $c(P) = 0$, then $AX_p \vdash P = \bigoplus_{i \in I} p_i \cdot \partial(\mathbf{0})$ for a suitable index set I and $p_i > 0$ for $i \in I$. Hence $AX_p \vdash P = \partial(\mathbf{0})$ and choosing $\bar{P} = \partial(\mathbf{0}) \in \mathcal{P}_{cc}$ suffices here. If $\max\{c(P), c(Q)\} = 0$, then $AX_p \vdash P = \partial(\mathbf{0})$, $Q = \partial(\mathbf{0})$ by the above, from which $AX_p^b \vdash P = Q$ follows directly.

Induction step As to case (a), suppose $c(E) > 0$. Using axiom A1, A2, and A4 we can rewrite E such that $AX_p \vdash E = \sum_{i \in I} \alpha_i \cdot P_i$ for some index set I and suitable $\alpha_i \in \mathcal{A}$ and $P_i \in \mathcal{P}$. Note that, for all $i \in I$, $c(P_i) < c(E)$. Choose for each $i \in I$, by the induction hypothesis for part (b), $\bar{P}_i \in \mathcal{P}_{cc}$ such that $[\![\bar{P}_i]\!] \leftrightarrow_b [\![P_i]\!]$ and $AX_p^b \vdash \bar{P}_i = P_i$. Now $AX_p^b \vdash E = \bar{E}$ 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 $\bar{P}_{i_0} \leftrightarrow_b \partial(\bar{E})$, so that the summand $\alpha_{i_0} \cdot \bar{P}_{i_0}$ of $\bar{E}$ represents an inert τ-step. Then $AX_p^b \vdash E = H + \tau \cdot \bar{P}_{i_0}$, where $H := \sum_{i \in I \setminus \{i_0\}} \alpha_i \cdot \bar{P}_i$. It suffices to show that $H \sqsubseteq \bar{P}_{i_0}$, because then axiom BP yields $AX_p^b \vdash \partial(E) = \partial(H + \tau \cdot \bar{P}_{i_0}) = \bar{P}_{i_0}$.
So, suppose $H \xrightarrow{\alpha} \mu$. Then $\mu = [\![\bar{P}_i]\!]$ for some $i \in I \setminus \{i_0\}$. Since $\bar{E} \xrightarrow{\alpha} [\![\bar{P}_i]\!]$ and $\partial(\bar{E}) \leftrightarrow_b \bar{P}_{i_0}$, we have $[\![\bar{P}_{i_0}]\!] \Rightarrow \bar{\nu} \xrightarrow{(\alpha)} \nu$ where $\delta(\bar{E}) \leftrightarrow_b \bar{\nu}$ and $[\![\bar{P}_i]\!] \leftrightarrow_b \nu$. Because $\bar{P}_{i_0}$ is concrete, $[\![\bar{P}_{i_0}]\!] = \bar{\nu}$ by Lemma 6.12e. Thus $[\![\bar{P}_{i_0}]\!] \xrightarrow{(\alpha)} \nu$. Since $[\![\bar{P}_i]\!] \in \mathit{Distr}(\mathcal{E}_{cc})$, $\nu \in \mathit{Distr}(\mathcal{E}_{cc})$ by Lemma 6.12d, and $[\![\bar{P}_i]\!] \leftrightarrow_b \nu$, Lemma 6.13 yields $[\![\bar{P}_i]\!] \leftrightarrow \nu$, which was to be shown.

(ii) Next suppose that $\alpha_i \neq \tau$ or $\bar{P}_i \not\leftrightarrow_b \partial(\bar{E})$ for all $i \in I$, i.e., $\bar{E}$ is rigid. We will show that there is a concrete process $C \in \mathcal{E}_{cc}$ such that $AX_p^b \vdash \partial(\bar{E}) = \partial(C)$. We proceed by induction on the number of indices $k \in I$ such that $\alpha_k = \tau$ and $[\![\bar{P}_k]\!]$ can be written as $\mu_1 \,{}_r\!\oplus\, \mu_2$ for some $r \in (0,1]$ and $\delta(\bar{E}) \leftrightarroweq_b \mu_1$. *Basis* If there are no such k, then $C := \bar{E} \in \mathcal{E}_{cc}$ by Lemma 6.12a.

Induction step Let $i_0 \in I$ be an index such that $\alpha_{i_0} = \tau$ and $[\![\bar{P}_{i_0}]\!]$ can be written as $\mu_1 \,{}_r\!\oplus\, \mu_2$ with $r \in (0,1]$ and $\delta(\bar{E}) \leftrightarroweq_b \mu_1$. Without loss of generality we can assume that $[\![\bar{P}_{i_0}]\!] = \mu_1 \,{}_r\!\oplus\, \mu_2$ with $r \in (0,1]$, $\delta(\bar{E}) \leftrightarroweq_b \mu_1$, and $G \leftrightarroweq_b \bar{E}$ for no $G \in \mathrm{spt}(\mu_2)$, for each such $G \in \mathrm{spt}(\mu_2)$ can be shifted to $\mathrm{spt}(\mu_1)$. As $\bar{E}$ is rigid, it follows that $r < 1$.

Let again $H := \sum_{i \in I \setminus \{i_0\}} \alpha_i \cdot \bar{P}_i$. Then $AX_p \vdash \bar{E} = \tau \cdot \bar{P}_{i_0} + H$. By induction, exists $C \in \mathcal{E}_{cc}$ with $AX_p^b \vdash \partial(H) = \partial(C)$. So, $AX_p^b \vdash \bar{E} = \tau \cdot \bar{P}_{i_0} + C$. It suffices to show that $AX_p^b \vdash \partial(\bar{E}) = \partial(C)$. This will follow from axiom G once we obtain $\tau \cdot \bar{P}_{i_0} \sqsubseteq \partial(C)$.

By axioms P1–3, there are $P, P' \in \mathcal{P}_{cc}$, such that $AX_p \vdash \bar{P}_{i_0} = P' \,{}_r\!\oplus\, P$ with $[\![P']\!] = \mu_1$ and $[\![P]\!] = \mu_2$. For all $F \in spt([\![P']\!])$ we have $F \leftrightarroweq_b \bar{E}$ by Lemma 6.12g. So, for each $F \in \mathrm{spt}([\![P']\!])$, we have $P' \leftrightarroweq_b \partial(F)$ and $AX_p \vdash P' = \partial(F)$ by Corollary 6.14. Hence, $AX_p \vdash \bar{P}_{i_0} = \partial(F) \,{}_r\!\oplus\, P$. Moreover, $\widehat{E} := \tau \cdot (\partial(F) \,{}_r\!\oplus\, P) + C \leftrightarroweq_b \tau \cdot \bar{P}_{i_0} + C \leftrightarroweq_b \bar{E}$.

We analyse the τ-transitions of $\widehat{E}$ in order to show that it is rigid. Regarding the transition $\widehat{E} = \tau \cdot (\partial(F) \,{}_r\!\oplus\, P) + C \xrightarrow{\tau} [\![\partial(F) \,{}_r\!\oplus\, P]\!]$ we observe that $\partial(F) \,{}_r\!\oplus\, P \leftrightarroweq_b \bar{P}_{i_0}$, $\bar{P}_{i_0} \not\leftrightarroweq_b \partial(\bar{E})$ by assumption, and $\bar{E} \leftrightarroweq_b \widehat{E}$. So, $[\![\partial(F) \,{}_r\!\oplus\, P]\!] \not\leftrightarroweq_b \widehat{E}$. Now assume, to arrive at a contradiction, that $C \xrightarrow{\tau} \gamma$ and $\gamma \leftrightarroweq_b \delta(\widehat{E})$ for some $\gamma \in \mathit{Distr}(\mathcal{E})$. By Lemma 6.12d $\gamma \in \mathit{Distr}(\mathcal{E}_{cc})$. We claim that, given the assumption, it holds that $C \leftrightarroweq_b \widehat{E}$: Clearly, any transition $\delta(C) \xrightarrow{\alpha} \varrho$ can be matched by $\delta(\widehat{E}) = \delta(\tau \cdot (\partial(F) \,{}_r\!\oplus\, P) + C)$. Conversely, if $\delta(\widehat{E}) \xrightarrow{\alpha} \varrho$, then $\gamma \Rightarrow \bar{\nu} \xrightarrow{(\alpha)} \nu$ for some $\bar{\nu}, \nu \in \mathit{Distr}(\mathcal{E})$ with $\bar{\nu} \leftrightarroweq_b \delta(\widehat{E})$ and $\nu \leftrightarroweq_b \varrho$, and therefore $\delta(C) \Rightarrow \bar{\nu} \xrightarrow{(\alpha)} \nu$. So, we have $C \xrightarrow{\tau} \gamma$ and $\gamma \leftrightarroweq_b \delta(\widehat{E}) \leftrightarroweq_b \delta(C)$, which contradicts C being concrete. We conclude that $\tau \cdot (\partial(F) \,{}_r\!\oplus\, P)$ nor C yields an inert transition and that $\widehat{E} = \tau \cdot (\partial(F) \,{}_r\!\oplus\, P) + C$ is rigid.

Since F, P, and C are concrete, $r \in (0,1)$, $\widehat{E} = \tau \cdot (\partial(F) \,{}_r\!\oplus\, P) + C$ is rigid, $F \leftrightarroweq_b \bar{E} \leftrightarroweq_b \widehat{E}$ and $G \leftrightarroweq_b \widehat{E}$ for no $G \in \mathrm{spt}([\![P]\!])$, we obtain $\tau \cdot (\partial(F) \,{}_r\!\oplus\, P) \sqsubseteq \partial(C)$ by Lemma 6.15. Above we have shown that $AX_p \vdash \bar{P}_{i_0} = \partial(F) \,{}_r\!\oplus\, P$, hence $\partial(F) \,{}_r\!\oplus\, P \leftrightarroweq \bar{P}_{i_0}$. Therefore Lemma 6.5 gives $\tau \cdot \bar{P}_{i_0} \sqsubseteq \partial(C)$ as desired, closing the induction step for part (a).

As to the induction step for part (b), let $P = \bigoplus_{i \in I} p_i \cdot E_i$ where $p_i > 0$, $E_i \in \mathcal{E}$ for $i \in I$. Note, $c(E_i) \leqslant c(P)$, for $i \in I$. By part (a), for all $i \in I$, concrete processes $\bar{P}_i \in \mathcal{P}_{cc}$ exist such that $[\![\bar{P}_i]\!] \leftrightarroweq_b \delta(E_i)$ and $AX_p^b \vdash \bar{P}_i = \partial(E_i)$. Put $\bar{P} = \bigoplus_{i \in I} p_i \cdot \bar{P}_i$. Then $\bar{P} \in \mathcal{P}_{cc}$ by Lemma 6.12b. We have that $[\![\bar{P}]\!] = [\![\bigoplus_{i \in I} p_i \cdot \bar{P}_i]\!] \leftrightarroweq_b [\![\bigoplus_{i \in I} p_i \cdot E_i]\!] = [\![P]\!]$, since $[\![\bar{P}_i]\!] \leftrightarroweq_b \delta(E_i)$ for $i \in I$. Moreover, it holds that $AX_p^b \vdash \bar{P} = \bigoplus_{i \in I} p_i \cdot \bar{P}_i = \bigoplus_{i \in I} p_i \cdot E_i = P$, because $AX_p^b \vdash \bar{P}_i = \partial(E_i)$ for $i \in I$. This concludes the induction step for part (b).

For the induction step of part (c), let $P, Q \in \mathcal{P}$ be such that $\max\{c(P), c(Q)\} > 0$ and assume $[\![P]\!] \leftrightarroweq_b [\![Q]\!]$. By part (b) exist concrete processes $\bar{P}, \bar{Q} \in \mathcal{P}_{cc}$ such that $[\![\bar{P}]\!] \leftrightarroweq_b [\![P]\!]$ and $AX_p^b \vdash \bar{P} = P$, on the one hand, and $[\![\bar{Q}]\!] \leftrightarroweq_b [\![Q]\!]$ and $AX_p^b \vdash \bar{Q} = Q$, on the other hand. Thus $[\![\bar{P}]\!] \leftrightarroweq_b [\![P]\!] \leftrightarroweq_b [\![Q]\!] \leftrightarroweq_b [\![\bar{Q}]\!]$. Since $\bar{P}, \bar{Q} \in \mathcal{P}_{cc}$, it follows that $AX_p \vdash \bar{P} = \bar{Q}$ using Corollary 6.14. Combination of this gives $AX_p^b \vdash P = \bar{P} = \bar{Q} = Q$ and settles the induction step for part (c) and the proof of the lemma. □

By now we have gathered all ingredients to prove that the theory AX_p^b is a complete axiomatisation of rooted probabilistic branching bisimulation semantics. In the proof of this theorem we exploit axiom C.

Theorem 6.18 (AX_p^b **is sound and complete for** $\leftrightarroweq_{rb}$**).** For all non-deterministic processes $E, F \in \mathcal{E}$ and all probabilistic processes $P, Q \in \mathcal{P}$ it holds that $E \leftrightarroweq_{rb} F$ iff $AX_p^b \vdash E = F$ and $[\![P]\!] \leftrightarroweq_b [\![Q]\!]$ iff $AX_p^b \vdash P = Q$.

Proof. Lemma 6.10 settles the soundness of AX_p^b. Therefore it remains to show that the theory AX_p^b is complete. The completeness result for probabilistic processes was already delivered as Lemma 6.17c.

So, choose non-deterministic processes $E, F \in \mathcal{E}$ such that $E \leftrightarroweq_{rb} F$. 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, for $i \in I$, $j \in J$. For each $j \in J$ we have $F \xrightarrow{\beta_j} [\![Q_j]\!]$. Since $E \leftrightarroweq_{rb} F$, we can find, for each $j \in J$, a non-empty subset $I_j \subseteq I$ and $p_{ij} \geqslant 0$ such that $\alpha_i = \beta_j$ for $i \in I_j$, $\delta(E) \xrightarrow{\beta_j} \bigoplus_{i \in I_j} p_{ij} \cdot P_i$ and $[\![\bigoplus_{i \in I_j} p_{ij} \cdot P_i]\!] \leftrightarroweq_b [\![Q_j]\!]$. By Lemma 6.17c we have $AX_p^b \vdash \big(\bigoplus_{i \in I_j} p_{ij} \cdot P_i \big) = Q_j$. Thus, for each $j \in J$, it holds that

$$\begin{aligned}
AX_p^b \vdash\ & \textstyle\sum_{i \in I} \alpha_i \cdot P_i \\
&= \textstyle\sum_{i \in I} \alpha_i \cdot P_i + \sum_{i \in I_j} \alpha_i \cdot P_i && \text{Axioms A1–A3} \\
&= \textstyle\sum_{i \in I} \alpha_i \cdot P_i + \sum_{i \in I_j} \beta_j \cdot P_i && \alpha_i = \beta_j \text{ for } i \in I_j \\
&= \textstyle\sum_{i \in I} \alpha_i \cdot P_i + \sum_{i \in I_j} \beta_j \cdot P_i + \beta_j \cdot \big(\bigoplus_{i \in I_j} p_{ij} \cdot P_i \big) && \text{Axiom C} \\
&= \textstyle\sum_{i \in I} \alpha_i \cdot P_i + \sum_{i \in I_j} \beta_j \cdot P_i + \beta_j \cdot Q_j && \text{Since } AX_p^b \vdash \bigoplus_{i \in I_j} p_{ij} \cdot P_i = Q_j \\
&= \textstyle\sum_{i \in I} \alpha_i \cdot P_i + \beta_j \cdot Q_j . && \text{Reversing two steps above}
\end{aligned}$$

Exploiting this equality for each $j \in J$, as well as axioms A1 and A2, we obtain

$$E = \textstyle\sum_{i \in I} \alpha_i \cdot P_i = \sum_{i \in I} \alpha_i \cdot P_i + \sum_{j \in J} \beta_j \cdot Q_j .$$

Symmetrically, we derive

$$F = \textstyle\sum_{j \in J} \beta_j \cdot Q_j = \sum_{j \in J} \beta_j \cdot Q_j + \sum_{i \in I} \alpha_i \cdot P_i .$$

Combination of the two equations yields, again with help of axioms A1 and A2,

$$\begin{aligned}
AX_p^b \vdash E = \textstyle\sum_{i \in I} \alpha_i \cdot P_i &= \textstyle\sum_{i \in I} \alpha_i \cdot P_i + \sum_{j \in J} \beta_j \cdot Q_j \\
&= \textstyle\sum_{j \in J} \beta_j \cdot Q_j + \sum_{i \in I} \alpha_i \cdot P_i = \sum_{j \in J} \beta_j \cdot Q_j = F
\end{aligned}$$

which was to be shown. □

The axiomatisation AX_p^b, whose soundness and completeness has been proven above, involves the auxiliary relation $\sqsubseteq \subseteq \mathcal{E} \times \mathcal{P}$. This relation does not satisfy the law

$$\frac{F = E \qquad E \sqsubseteq P \qquad P = Q}{F \sqsubseteq Q} \tag{4}$$

when equality denotes provability with respect to AX_p^b. However, it satisfies (4) when equality denotes provability with respect to AX_p. See Lemma 6.5. This could be considered better, as it tells us that we never need to use the axioms BP and G to prove the inclusions $E \sqsubseteq P$ that are needed as premises of BP and G. However, if seen as a shortcoming of the relation $\sqsubseteq$, this can be easily repaired. Define the relation $\sqsubseteq' \subseteq \mathcal{E} \times \mathcal{P}$ by

$$F \sqsubseteq' Q \quad \text{iff} \quad \exists E \in \mathcal{E}, P \in \mathcal{P}.\ F \leftrightarroweq_{rb} E \wedge E \sqsubseteq P \wedge P \leftrightarroweq_b Q\ .$$

As can be directly obtained, this relation satisfies (4), i.e. $F \leftrightarroweq_{rb} E$, $E \sqsubseteq' P$, and $P \leftrightarroweq_b Q$ implies $F \sqsubseteq' Q$. It also satisfies axioms I1–I6, as can be straightforwardly verified. In addition, the axioms BP and G trivially remain sound when using $\sqsubseteq'$ in the precondition instead of $\sqsubseteq$. Thus, replacing $\sqsubseteq$ by $\sqsubseteq'$ in Table 2 yields the same axiomatisation, which is therefore sound and complete for rooted branching probabilistic bisimulation semantics, and now also satisfies (4).

We now proceed to convert the axioms BP and G into equations.

Lemma 6.19. Through application of AX_p, each true statement of the form $E \sqsubseteq P$ can be written in the form

$$\textstyle\sum_{i\in I} \tau \cdot \Big(\bigoplus_{k\in K} p_k \cdot \big(\partial(F_k)\ {}_{r_{ik}}\!\oplus\ P_{ik}\big)\Big) + \sum_{j\in J} a_j \cdot \big(\bigoplus_{k\in K} p_k \cdot P_{jk}\big) \sqsubseteq \bigoplus_{k\in K} p_k \cdot F_k$$

with

$$F_k = E_k + \textstyle\sum_{i\in I_k} \tau \cdot P_{ik} + \sum_{j\in J} a_j \cdot P_{jk}\ ,$$

where I, J, K are finite index sets, $I \cap J = \emptyset$, $E_k \in \mathcal{E}$ and $p_k \in (0,1]$ for all $k \in K$ such that $\sum_{k\in K} p_k = 1$, $P_{ik} \in \mathcal{P}$ and $r_{ik} \in [0,1]$ for $i \in I$ and $k \in K$, $P_{jk} \in \mathcal{P}$ for $j \in J$ and $k \in K$, $a_j \in \mathcal{A} \backslash \{\tau\}$ for $j \in J$, and $I_k = \{\, i \in I \mid r_{ik} < 1 \,\}$.

Proof. Suppose that E and P have the above form. We need to show that $E \sqsubseteq P$. So, suppose $E \xrightarrow{\alpha} \mu$ for some $\alpha \in \mathcal{A}$ and $\mu \in \mathit{Distr}(\mathcal{E})$.

First assume that $\alpha \neq \tau$. Then $\mu = \bigoplus_{k\in K} p_k \cdot [\![P_{jk}]\!]$ for some $j \in J$ with $a_j = \alpha$. For each $k \in K$ one has $F_k \xrightarrow{\alpha} [\![P_{jk}]\!]$. Hence $[\![P]\!] = \bigoplus_{k\in K} p_k \cdot \delta(F_k) \xrightarrow{\alpha} \bigoplus_{k\in K} p_k \cdot [\![P_{jk}]\!] = \mu$ by Lemma 4.7a. Next assume that $\alpha = \tau$. Then $\mu = \bigoplus_{k\in K} p_k \cdot (\delta(F_k)\ {}_{r_{ik}}\!\oplus\ [\![P_{ik}]\!])$ for some $i \in I$. For each $k \in K$ one has $\delta(F_k) \xrightarrow{(\tau)} \delta(F_k)\ {}_{r_{ik}}\!\oplus\ [\![P_{ik}]\!]$. Hence $[\![P]\!] \xrightarrow{(\tau)} \mu$ by Lemma 4.7b.

Now suppose $E \sqsubseteq P$. We need to show that using AX_p the expressions E and P can be written in the required form. Let E have the form $\sum_{i\in I} \tau \cdot P_i + \sum_{j\in J} a_j \cdot P_j$ for finite index sets I, J with $I \cap J = \emptyset$, $a_j \in \mathcal{A} \backslash \{\tau\}$ for $j \in J$, and $P_i \in \mathcal{P}$ for $i \in I \cup J$. Moreover, let P have the form $\bigoplus_{k\in K} p_k \cdot F_k$ for a finite index set K, $F_k \in \mathcal{E}$ and $p_k \in (0,1]$ for all $k \in K$, with $\sum_{k\in K} p_k = 1$.

For each $j \in J$ one has $E \xrightarrow{a_j} [\![P_j]\!]$ and thus $P \xrightarrow{a_j} \nu_j$ for some $\nu_j \in \mathit{Distr}(\mathcal{E})$ with $\nu_j \leftrightarroweq [\![P_j]\!]$. Lemma 4.8a implies that $\delta(F_k) \xrightarrow{a_j} \nu_{jk}$ for certain $\nu_{jk} \in \mathit{Distr}(\mathcal{E})$ such that $\nu_j = \bigoplus_{k\in K} p_k \cdot \nu_{jk}$. Let $P_{jk} \in \mathcal{P}$ be such that $[\![P_{jk}]\!] = \nu_{jk}$ for all $j \in J$ and $k \in K$. Then $F_k \leftrightarroweq F_k + a_j \cdot P_{jk}$ for all $j \in J$ and $k \in K$, and thus $AX_p \vdash F_k = F_k + a_j \cdot P_{jk}$ for all $j \in J$ and $k \in K$, by Theorem 6.2. Moreover, $P_j \leftrightarroweq \bigoplus_{k\in K} p_k \cdot P_{jk}$, and thus $AX_p \vdash P_j = \bigoplus_{k\in K} p_k \cdot P_{jk}$ by Theorem 6.2.

For each $i \in I$ one has $E \xrightarrow{\tau} [\![P_i]\!]$ and thus $[\![P]\!] \xrightarrow{(\tau)} \nu_i$ for some $\nu_i \in \mathit{Distr}(\mathcal{E})$ with $\nu_i \leftrightarroweq [\![P_i]\!]$.

Lemma 4.8b implies that $\delta(F_k) \xrightarrow{(\tau)} \nu_{ik}$ for certain $\nu_{ik} \in \mathit{Distr}(\mathcal{E})$ such that $\nu_i = \bigoplus_{k\in K} p_k{\cdot}\nu_{ik}$. By Definition 4.4, for each $i \in I$ and $k \in K$, either (i) $\delta(F_k) \xrightarrow{\tau} \nu_{ik}$, or (ii) $\nu_{ik} = \delta(F_k)$, or (iii) there exists a $\nu'_{ik} \in \mathit{Distr}(\mathcal{E})$ such that $\nu_{ik} = \delta(F_k)\ {}_{r_{ik}}\!\oplus\ \nu'_{ik}$ and $\delta(F_k) \xrightarrow{\tau} \nu'_{ik}$ for some $r_{ik} \in (0,1)$. Let $P_{ik} \in \mathcal{P}$ be such that $[\![P_{ik}]\!] = \nu_{ik}$ for all $(i,k) \in I \times K$ for which possibility (i) applies, and $[\![P_{ik}]\!] = \nu'_{ik}$ for all $(i,k) \in I \times K$ for which possibility (iii) applies. Pick $P_{ik} \in \mathcal{P}$ arbitrary in case possibility (ii) applies. Let $r_{ik} := 0$ for all $(i,k) \in I \times K$ for which possibility (i) applies, and $r_{ik} := 1$ for all $(i,k) \in I \times K$ for which possibility (ii) applies. Then $P_i \leftrightarrows \bigoplus_{k\in K} p_k{\cdot}\big(\partial(F_k)\ {}_{r_{ik}}\!\oplus\ P_{ik}\big)$ for all $(i,k) \in I \times K$, and thus $AX_p \vdash P_i = \bigoplus_{k\in K}(\partial(F_k)\ {}_{r_{ik}}\!\oplus\ P_{ik})$ for all $(i,k) \in I \times K$ by Theorem 6.2. Moreover, putting $I_k = \{\, i \in I \mid r_{ik} < 1 \,\}$, $F_k \leftrightarrows F_k + \tau \cdot P_{ik}$ for all $k \in K$ and $i \in I_k$, and thus $AX_p \vdash F_k = F_k + \tau \cdot P_{ik}$ for all $k \in K$ and $i \in I_k$, by Theorem 6.2.

Thus, for all $k \in K$ there are $E_k \in \mathcal{E}$ such that $AX_p \vdash F_k = E_k + \sum_{i\in I_k} \tau \cdot P_{ik} + \sum_{j\in J} a_j \cdot P_{jk}$. It follows that using AX_p the expressions E and P can be written in the form given by the lemma. □

It follows that an equational form of axiom BP can be obtained by skipping the precondition $E \sqsubseteq P$, and instead filling in the general forms of Lemma 6.19 for E and P. Thus, BP can be rendered as

$$\partial\Big(\textstyle\sum_{i\in I}\ \tau\cdot\big(\bigoplus_{k\in K} p_k \cdot \big(\partial(F_k)\ {}_{r_{ik}}\!\oplus\ P_{ik}\big)\big) + \sum_{j\in J} a_j \cdot \big(\bigoplus_{k\in K} p_k \cdot P_{jk}\big) + \tau \cdot \bigoplus_{k\in K} p_k \cdot F_k\Big) \ = \ \bigoplus_{k\in K} p_k \cdot F_k$$

with

$$F_k = E_k + \textstyle\sum_{i\in I_k}\ \tau \cdot P_{ik}\ + \sum_{j\in J} a_j \cdot P_{jk}\ ,$$

and where I, J, K are finite index sets, $I \cap J = \emptyset$, $E_k \in \mathcal{E}$ and $p_k \in (0,1)$ for all $k \in K$, $\sum_{k\in K} p_k = 1$, $P_{ik} \in \mathcal{P}$ and $r_{ik} \in [0,1]$ for $i \in I$ and $k \in K$, $P_{jk} \in \mathcal{P}$ for $j \in J$ and $k \in K$, $a_j \in \mathcal{A}\backslash\{\tau\}$ for $j \in J$, and $I_k = \{\, i \in I \mid r_{ik} < 1 \,\}$.

In the same way, axiom G can be transformed to a purely equational form. Since its precondition has the form $E \sqsubseteq \partial(F)$, we may restrict attention to the special case of the form for Lemma 6.19 with $|K| = 1$. This yields

$$\partial\Big(\textstyle\sum_{i\in I} \tau \cdot \big(\partial(F)\ {}_{r_i}\!\oplus\ P_i\big) + \sum_{j\in J} a_j \cdot P_j + F\Big) = \partial(F)$$

with

$$F = E + \textstyle\sum_{i\in I'}\ \tau \cdot P_i\ + \sum_{j\in J} a_j \cdot P_j\ ,$$

where I, J are finite index sets, $I \cap J = \emptyset$, $E \in \mathcal{E}$, $P_i \in \mathcal{P}$ and $r_i \in [0,1]$ for $i \in I$, $P_j \in \mathcal{P}$ and $a_j \in \mathcal{A}\backslash\{\tau\}$ for $j \in J$, and $I' = \{\, i \in I \mid r_i < 1 \,\}$. By application of axiom A3 the above axiom scheme can be simplified by restricting to the case $J = \emptyset$. Another application of A3 allows restriction to the cases that $I' = I$ or $|I\backslash I'| = 1$. The latter case can already be obtained as an instance of BP. Hence G can be rendered equationally as

$$\partial\Big(\ \textstyle\sum_{i\in I} \tau \cdot \big(P_i\ {}_{r_i}\!\oplus\ \partial\big(E + \sum_{i\in I} \tau \cdot P_i\big)\big) + E + \sum_{i\in I} \tau \cdot P_i\Big) \ = \ \partial\big(E + \sum_{i\in I} \tau \cdot P_i\big)$$

with I a finite index set, $E \in \mathcal{E}$, $P_i \in \mathcal{P}$ and $r_i \in [0,1]$ for all $i \in I$.

7. Concluding remarks

We presented an axiomatisation 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 axiomatisation of rooted branching bisimilarity for non-deterministic processes that employed concrete processes, 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 [14]. 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 [13, 17] is a clear direction for further research.

Also, we want to develop a minimisation algorithm for probabilistic processes modulo probabilistic branching bisimilarity. Eisentraut et al. propose in [15] an algorithm for deciding equivalence with respect to weak distribution bisimilarity relying on a state-based characterisation, a result presently not available in our setting. Other work and proposals for weak bisimilarity include [10, 16, 39], but these do not fit well with the installed base of our toolset [8]. For the case of strong probabilistic bisimilarity without combined transitions we recently developed in [27] an algorithm improving upon the early results of [6]. In [39] 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 [40, 41, 39] and of [26, 23].

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.

[5] C. Baier, P.R. D'Argenio, and H. Hermanns. On the probabilistic bisimulation spectrum with silent moves. *Acta Informatica*, 57:465–512, 2020.

[6] 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.

[7] E. Bandini and R. Segala. Axiomatizations for probabilistic bisimulation. In F. Orejas et al., editor, *Proc. ICALP 2001*, pages 370–381. LNCS 2076, 2001.

[8] 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.

[9] V. Castiglione and S. Tini. Raiders of the lost equivalence: Probabilistic branching bisimilarity. *Information Processing Letters*, 159–160:105947, 2020.

[10] 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.

[11] R. De Nicola and F.W. Vaandrager. Three logics for branching bisimulation. *Journal of the ACM*, 42(2):458–487, 1995.

[12] 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.

[13] Y. Deng and C. Palamidessi. Axiomatizations for probabilistic finite-state behaviors. *Theoretical Computer Science*, 373:92–114, 2007.

[14] 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.

[15] 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.

[16] 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.

[17] N. Fischer 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.

[18] W.J. Fokkink. *Introduction to Process Algebra.* Texts in Theoretical Computer Science: An EATCS Series. Springer, 2000.

[19] L.J. Ford Jr. and D.R. Fulkerson. Maximal flow through a network. *Canadian Journal of Mathematics*, 8:399–404, 1956.

[20] 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.A. Alvim et al., editor, *The Art of Modelling Computational Systems: A Journey from Logic and Concurrency to Security and Privacy*, pages 139–162. LNCS 11760, 2019.

[21] R.J. van Glabbeek, J.F. Groote, and E.P. de Vink. A cancellation law for probabilistic processes. In C. Antares Mezzina and G. Caltais, editors, *Proc. EXPRESS/SOS 2023*, pages 42–58. EPTCS 387, 2023.

[22] R.J. van Glabbeek and W.P. Weijland. Branching time and abstraction in bisimulation semantics. *Journal of the ACM*, 43:555–600, 1996.

[23] 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.

[24] J.F. Groote and S.P. Luttik. Undecidability and completeness results for process algebra with alternative quantification over data. Technical Report SEN-R21, CWI, 1998.

[25] J.F. Groote and M.R. Mousavi. *Modeling and Analysis of Communicating Systems*. The MIT Press, 2014.

[26] 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.

[27] 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.

[28] 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.

[29] H. Hansson and B. Jonsson. A calculus for communicating systems with time and probabilities. In *Proc. RTSS 1990*, pages 278–287. IEEE, 1990.

[30] M. Hennessy. Exploring probabilistic bisimulations, part I. *Formal Aspects of Computing*, 24:749–768, 2012.

[31] 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.

[32] H. Hermanns and A. Turrini. Deciding probabilistic automata weak bisimulation in polynomial time. In D. D'Souza, T. Kavitha, and J. Radhakrishnan, editors, *Proc. FSTTCS*, volume 18 of *LIPIcs*, pages 435–447, 2012.

[33] 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.

[34] R. Milner. *Communication and Concurrency*. Prentice Hall, 1989.

[35] R. Milner. A complete axiomatization for observational congruence of finite-state behaviours. *Information and Computation*, 81(2):227–247, 1989.

[36] R. Segala. *Modeling and Verification of Randomized Distributed Real-Time Systems*. PhD thesis, MIT, 1995. Technical Report MIT/LCS/TR–676.

[37] R. Segala and N.A. Lynch. Probabilistic simulations for probabilistic processes. In B. Jonsson and J. Parrow, editors, *Proc. CONCUR 94*, pages 481–496. LNCS 836, 1994.

[38] M. Stoelinga. Alea Jacta est*: Verification of probabilistic, real-time and parametric systems.* PhD thesis, Radboud Universiteit, 2002.

[39] A. Turrini and H. Hermanns. Polynomial time decision algorithms for probabilistic automata. *Information and Computation*, 244:134–171, 2015.

[40] A. Valmari. Simple bisimilarity minimization in $O(m \log n)$ time. *Fundamenta Informaticae*, 105(3):319–339, 2010.

[41] 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.

Appendix

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

Proof. Put $r_{ij} = \sum_{E\in spt(\xi)} \dfrac{p_i\mu_i(E) \cdot q_j\nu_j(E)}{\xi(E)}$ for all $i \in I$ and $j \in J$. In case $r_{ij} = 0$, choose $\varrho_{ij} \in Distr(\mathcal{E})$ arbitrarily. In case $r_{ij} \neq 0$, define $\varrho_{ij} \in Distr(\mathcal{E})$, for $i \in I$ and $j \in J$, by

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

for all $E \in \mathcal{E}$. By definition of r_{ij} and ϱ_{ij} it holds that $\sum\{\, \varrho_{ij}(E) \mid E \in \mathcal{E} \,\} = 1$. So, $\varrho_{ij} \in Distr(\mathcal{E})$ indeed.

We verify $\sum_{j\in J} r_{ij} = p_i$ and $p_i \cdot \mu_i = \bigoplus_{j\in J} r_{ij} \cdot \varrho_{ij}$ for $i \in I$.

$$\begin{aligned} \textstyle\sum_{j\in J} r_{ij} &= \textstyle\sum_{j\in J} \sum\limits_{E\in spt(\xi)} p_i\mu_i(E) \cdot q_j\nu_j(E)/\xi(E) \\ &= \textstyle\sum_{E\in spt(\xi)} p_i\mu_i(E) \cdot \sum_{j\in J} q_j\nu_j(E)/\xi(E) \\ &= \textstyle\sum_{E\in spt(\xi)} p_i\mu_i(E) && \text{Since } \xi = \textstyle\bigoplus_{j\in J} q_j \cdot \nu_j. \\ &= p_i \textstyle\sum_{E\in spt(\xi)} \mu_i(E) \\ &= p_i. \end{aligned}$$

Next, pick $F \in \mathcal{E}$ and $i \in I$. If $\xi(F) = 0$, then $p_i\mu_i(F) = 0$, since $\xi(F) = \sum_{i\in I} p_i\mu_i(F)$, and $r_{ij} = 0$ or $\varrho_{ij}(F) = 0$ for all $j \in J$, by the various definitions, thus $\sum_{j\in J} r_{ij}\varrho_{ij}(F) = 0$ as well.

Suppose $\xi(F) > 0$. Put $J_i = \{\, j \in J \mid r_{ij} > 0 \,\}$. Note, if $j \in J \backslash J_i$, i.e. if $r_{ij} = 0$, then $p_i\mu_i(F)q_j\nu_j(F)/\xi(F) = 0$ by definition of r_{ij}. Therefore we have

$$\begin{aligned} \textstyle\sum_{j\in J} r_{ij}\varrho_{ij}(F) &= \textstyle\sum_{j\in J_i} r_{ij}\varrho_{ij}(F) \\ &= \textstyle\sum_{j\in J_i} r_{ij}p_i\mu_i(F) \cdot q_j\nu_j(F)/(r_{ij}\xi(F)) \\ &= \textstyle\sum_{j\in J_i} p_i\mu_i(F) \cdot q_j\nu_j(F)/\xi(F) \\ &= \textstyle\sum_{j\in J} p_i\mu_i(F) \cdot q_j\nu_j(F)/\xi(F) && \text{Summand zero for } j \in J\backslash J_i. \\ &= p_i\mu_i(F)/\xi(F) \cdot \textstyle\sum_{j\in J} q_j\nu_j(F) \\ &= p_i\mu_i(F) && \text{Since } \xi = \textstyle\bigoplus_{j\in J} q_j \cdot \nu_j. \end{aligned}$$

The statements $\sum_{i\in I} r_{ij} = q_j$ and $q_j \cdot \nu_j = \bigoplus_{i\in I} r_{ij} \cdot \varrho_{ij}$ for $j \in J$, follow by symmetry. □

Lemma 5.3 If $\mathcal{R}$ is a branching probabilistic bisimulation relation, then so is $cc(\mathcal{R})$.

Proof. We first verify that $cc(\mathcal{R})$ is weakly decomposable. Suppose $\mu\ cc(\mathcal{R})\ \nu$ for $\mu, \nu \in \mathit{Distr}(\mathcal{E})$. Say $\mu = \bigoplus_{i \in I} p_i \cdot \mu_i$ and $\nu = \bigoplus_{i \in I} p_i \cdot \nu_i$ for a suitable index set I and $p_i > 0$, $\mu_i, \nu_i \in \mathit{Distr}(\mathcal{E})$ such that $\mu_i \,\mathcal{R}\, \nu_i$ for $i \in I$. For $i \in I$, we have $\mu_i = \bigoplus_{E \in \mathrm{spt}(\mu)} \mu_i(E) \cdot E$. Since $\mathcal{R}$ is weakly decomposable and $\mu_i \,\mathcal{R}\, \nu_i$, there exist distributions $\bar{\nu}_i$ and $\nu_{i,E}$ for $i \in I$, $E \in \mathrm{spt}(\mu)$, such that $\nu_i \Rightarrow \bar{\nu}_i$, $\bar{\nu}_i = \bigoplus_{E \in \mathrm{spt}(\mu)} \mu_i(E) \cdot \nu_{i,E}$, and $\delta(E) \,\mathcal{R}\, \nu_{i,E}$. Let $\bar{\nu} := \bigoplus_{i \in I} p_i \cdot \bar{\nu}_i$ and $\nu_E := \bigoplus_{i \in I} p_i \cdot \nu_{i,E}$. Then $\nu = \bigoplus_{i \in I} p_i \cdot \nu_i \Rightarrow \bigoplus_{i \in I} p_i \cdot \bar{\nu}_i = \bar{\nu}$ because $\nu_i \Rightarrow \bar{\nu}_i$ for $i \in I$. Moreover, $\delta(E)\ cc(\mathcal{R})\ \nu_E$, because $\delta(E) \,\mathcal{R}\, \nu_{i,E}$ for $i \in I$.

Let $\bigoplus_{j \in J} q_j \cdot \mu'_j$ be an arbitrary decomposition of μ. It suffices to find distributions $\bar{\nu}'$ and ν'_j for $j \in J$ such that (i) $\nu \Rightarrow \bar{\nu}'$, (ii) $\bar{\nu}' = \bigoplus_{j \in J} q_j \cdot \nu'_j$, and (iii) $\mu'_j\ cc(\mathcal{R})\ \nu'_j$ for $j \in J$. In fact, we choose $\bar{\nu}' := \bar{\nu}$, thus independently of the given decomposition of μ. Without limitation of generality we may assume that $q_i > 0$ for all $j \in J$.

Because, for each $E \in \mathrm{spt}(\mu)$, $\sum_{i \in I} p_i \cdot \mu_i(E) = \mu(E) = \sum_{j \in J} q_j \cdot \mu'_j(E)$ there are $r^E_{i,j} \geqslant 0$ for $i \in I$ and $j \in J$, such that $\sum_{j \in J} r^E_{i,j} = p_i \cdot \mu_i(E)$ and $\sum_{i \in I} r^E_{i,j} = q_j \cdot \mu'_j(E)$. Define $\nu'_j = \bigoplus_{E \in \mathrm{spt}(\mu)} \bigoplus_{i \in I} r^E_{i,j}/q_j \cdot \nu_{i,E}$ for $j \in J$. Note that ν'_j is well-defined since

$$\textstyle\sum_{E \in \mathrm{spt}(\mu)} \sum_{i \in I} r^E_{i,j}/q_j = \sum_{E \in \mathrm{spt}(\mu)} q_j \mu'_j(E)/q_j = \sum_{E \in \mathrm{spt}(\mu)} \mu'_j(E) = 1.$$

We verify the remaining requirements (ii) and (iii) listed above. Regarding requirement (ii) we calculate

$$\begin{aligned}
\textstyle\bigoplus_{j \in J} q_j \cdot \nu'_j &= \textstyle\bigoplus_{j \in J} q_j \cdot \big(\bigoplus_{E \in \mathrm{spt}(\mu)} \bigoplus_{i \in I} r^E_{i,j}/q_j \cdot \nu_{i,E}\big) \\
&= \textstyle\bigoplus_{E \in \mathrm{spt}(\mu)} \bigoplus_{i \in I} \big(\sum_{j \in J} r^E_{i,j}\big) \cdot \nu_{i,E} \\
&= \textstyle\bigoplus_{E \in \mathrm{spt}(\mu)} \bigoplus_{i \in I} p_i \cdot \mu_i(E) \cdot \nu_{i,E} \\
&= \textstyle\bigoplus_{i \in I} p_i \cdot \big(\bigoplus_{E \in \mathrm{spt}(\mu)} \mu_i(E) \cdot \nu_{i,E}\big) \\
&= \textstyle\bigoplus_{i \in I} p_i \cdot \bar{\nu}_i \\
&= \bar{\nu}
\end{aligned}$$

Regarding requirement (iii) we have

$$\begin{aligned}
\mu'_j &= \textstyle\bigoplus_{E \in \mathrm{spt}(\mu)} \mu'_j(E) \cdot E \\
&= \textstyle\bigoplus_{E \in \mathrm{spt}(\mu)} \big(\sum_{i \in I} r^E_{i,j}/q_j\big) \cdot E && \text{Choice of } r^E_{i,j} \text{ for } i \in I,\ j \in J,\ E \in \mathrm{spt}(\mu) \\
&= \textstyle\bigoplus_{E \in \mathrm{spt}(\mu)} \bigoplus_{i \in I} r^E_{i,j}/q_j \cdot \delta(E) \\
&\ cc(\mathcal{R}) \textstyle\bigoplus_{E \in \mathrm{spt}(\mu)} \bigoplus_{i \in I} r^E_{i,j}/q_j \cdot \nu_{i,E} && \delta(E) \,\mathcal{R}\, \nu_{i,E} \text{ for } i \in I \\
&= \nu'_j && \text{Definition of } \nu'_j
\end{aligned}$$

Thus $\mu = \bigoplus_{j \in J} q_j \cdot \mu'_j\ cc(\mathcal{R}) \bigoplus_{j \in J} q_j \cdot \nu'_j = \bar{\nu}$ as was to be checked.

Next we check that $cc(\mathcal{R})$ satisfies the transfer condition of Definition 5.1d. Suppose $\mu\ cc(\mathcal{R})\ \nu$ for $\mu, \nu \in \mathit{Distr}(\mathcal{E})$. Say $\mu = \bigoplus_{i \in I} p_i \cdot \mu_i$ and $\nu = \bigoplus_{i \in I} p_i \cdot \nu_i$ for a suitable index set I and $p_i > 0$, $\mu_i, \nu_i \in \mathit{Distr}(\mathcal{E})$ such that $\mu_i \,\mathcal{R}\, \nu_i$ for $i \in I$. Furthermore, suppose $\mu \xrightarrow{\alpha} \mu'$, that is,

$\mu = \bigoplus_{j\in J} q_j \cdot E_j$, $\mu' = \bigoplus_{j\in J} q_j \cdot \mu'_i$ and $E_j \xrightarrow{\alpha} \mu'_j$ for all $j \in I$. By Lemma 4.6 there are $r_{ij} \in [0,1]$ and $\varrho_{ij} \in \mathit{Distr}(\mathcal{E})$ such that $\sum_{j\in J} r_{ij} = p_i$ and $p_i \cdot \mu_i = \bigoplus_{j\in J} r_{ij} \cdot \varrho_{ij}$ for all $i \in I$, and $\sum_{i\in I} r_{ij} = q_j$ and $q_j \cdot E_j = \bigoplus_{i\in I} r_{ij} \cdot \varrho_{ij}$ for all $j \in J$; naturally $\varrho_{ij} = \delta(E_j)$ for all $i \in I$ and $j \in J$. Write s_{ij} for r_{ij}/p_i, so that $\sum_{j\in J} s_{ij} = 1$ and $\mu_i = \bigoplus_{j\in J} s_{ij} \cdot E_j$ for all $i \in I$. For all $i \in I$ let $\hat{\mu}'_i := \bigoplus_{j\in J} s_{ij} \cdot \mu'_j$, so that $\bigoplus_{i\in I} p_i \cdot \hat{\mu}'_i = \bigoplus_{j\in J} (\sum_{i\in I} r_{ij}) \cdot \mu'_j = \bigoplus_{j\in J} q_j \cdot \mu'_i = \mu'$.

Since $\mathcal{R}$ is weakly decomposable, $\mu_i \mathrel{\mathcal{R}} \nu_i$ and $\mu_i = \bigoplus_{j\in J} s_{ij} \cdot E_j$, there exist distributions $\bar{\nu}_i$ and ν_{ij} for $i \in I$, $j \in J$, such that $\nu_i \Rightarrow \bar{\nu}_i$, $\bar{\nu}_i = \bigoplus_{j\in J} s_{ij} \cdot \nu_{ij}$, and $\delta(E_j) \mathrel{\mathcal{R}} \nu_{ij}$. Moreover, since $E_j \xrightarrow{\alpha} \mu'_j$, for each $i \in J$ and $j \in J$ there are $\bar{\nu}'_{ij}, \nu'_{ij} \in \mathit{Distr}(\mathcal{E})$ such that

$$\nu_{ij} \Rightarrow \bar{\nu}'_{ij},\ \bar{\nu}'_{ij} \xrightarrow{(\alpha)} \nu'_{ij},\ \delta(E_j) \mathrel{\mathcal{R}} \bar{\nu}'_{ij}, \text{ and } \mu'_j \mathrel{\mathcal{R}} \nu'_{ij}.$$

Let $\bar{\nu}'_i := \bigoplus_{j\in J} s_{ij} \cdot \bar{\nu}'_{ij}$ and $\nu'_i := \bigoplus_{j\in J} s_{ij} \cdot \nu'_{ij}$. Then $\bar{\nu}_i \Rightarrow \bar{\nu}'_i$ and $\bar{\nu}'_i \xrightarrow{(\alpha)} \nu'_i$ because $\nu_{ij} \Rightarrow \bar{\nu}'_{ij}$ and $\bar{\nu}'_{ij} \xrightarrow{(\alpha)} \nu'_{ij}$ for $j \in J$. Moreover, $\mu_i \ cc(\mathcal{R})\ \bar{\nu}'_i$ and $\hat{\mu}'_i \ cc(\mathcal{R})\ \nu'_i$, because $\delta(E_j) \mathrel{\mathcal{R}} \bar{\nu}'_{ij}$ and $\mu'_j \mathrel{\mathcal{R}} \nu'_{ij}$ for $j \in J$. Let $\bar{\nu}' := \bigoplus_{i\in I} p_i \cdot \bar{\nu}'_i$ and $\nu' := \bigoplus_{i\in I} p_i \cdot \nu'_i$. Then $\nu = \bigoplus_{i\in I} p_i \cdot \nu_i \Rightarrow \bigoplus_{i\in I} p_i \cdot \bar{\nu}'_i = \bar{\nu}'$ because $\nu_i \Rightarrow \bar{\nu}_i \Rightarrow \bar{\nu}'_i$ for $i \in I$. Also, $\mu \ cc(\mathcal{R})\ \bar{\nu}'$ and $\mu' \ cc(\mathcal{R})\ \nu'$, as $\mu_i \ cc(\mathcal{R})\ \bar{\nu}'_i$ and $\hat{\mu}'_i \ cc(\mathcal{R})\ \nu'_i$ for $i \in I$, which finishes the proof. □

Lemma 5.4 Let $\mathcal{R} \subseteq \mathit{Distr}(\mathcal{E}) \times \mathit{Distr}(\mathcal{E})$ be a decomposable relation such that

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

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

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

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

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

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

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

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

Here $\mu_{ij} = \delta(E_i)$. Writing $E_{ij} := E_i$, $q_{ij} := p_i \cdot p_{ij}$ and $K = \{\, (i,j) \mid i \in I,\ j \in J_i \,\}$ we obtain (with $q_k = q_{ij}$, $E_k = E_{ij}$, and $F_k = F_{ij}$ for $k \in K$ such that $k = (i,j)$) that

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

Let $\mu'_{ij} := \mu'_i$ for all $i \in I$ and $j \in J_i$. Then $\mu' = \bigoplus_{k\in K} q_k \cdot \mu'_k$. Using that $E_k \xrightarrow{\alpha} \mu'_k$ for all $k \in K$, by (3) there must be distributions ν'_k for $k \in K$ such that

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

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

Lemma 5.5 Let $\mu_1, \mu_2, \nu_1, \nu_2 \in \mathit{Distr}(\mathcal{E})$ and $r \in (0,1)$. If $\mu_1 \leftrightarroweq_b \nu_1$ and $\mu_2 \leftrightarroweq_b \nu_2$ then $\mu_1 \, {}_r\!\oplus \, \mu_2 \leftrightarroweq_b \nu_1 \, {}_r\!\oplus \, \nu_2$.

Proof. Suppose $\mu_1 \leftrightarroweq_b \nu_1$ and $\mu_2 \leftrightarroweq_b \nu_2$ 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 first show that $\mathcal{R}$ is weakly decomposable. So, assume $\xi \, \mathcal{R} \, \eta$ and $\xi = \bigoplus_{i \in I} p_i \cdot \xi_i$ with all $p_i > 0$. 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 $\xi', \xi'', \eta', \eta'' \in \mathit{Distr}(\mathcal{E})$. Since $\xi' \, {}_s\!\oplus \, \xi'' = \bigoplus_{i \in I} p_i \cdot \xi_i$, we have by Lemma 4.6 that 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

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

and $\sum_{i \in I} s_i' = s$, $\sum_{i \in I} s_i'' = 1-s$, and $s_i' + s_i'' = p_i$ for all $i \in I$. Thus $\xi' = \bigoplus_{i \in I} s_i'/s \cdot \xi_i'$ and $\xi'' = \bigoplus_{i \in I} s_i''/(1-s) \cdot \xi_i''$. Since the relations $\mathcal{R}_1$ 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

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

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,

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

Thus, for $\bar{\eta} = \bar{\eta}' \, {}_s\!\oplus \, \bar{\eta}''$ and $\eta_i = \eta_i' \, {}_{s_i'/p_i}\!\oplus \, \eta_i''$ for $i \in I$, we have that $\eta = \eta' \, {}_s\!\oplus \, \eta'' \Rightarrow \bar{\eta}' \, {}_s\!\oplus \, \bar{\eta}'' = \bar{\eta}$, $\xi = (\xi' \, {}_s\!\oplus \, \xi'') \, \mathcal{R} \, (\bar{\eta}' \, {}_s\!\oplus \, \bar{\eta}'') = \bar{\eta}$, $\bar{\eta} = \bigoplus_{i \in I} \eta_i$, and $\xi_i = (\xi_i' \, {}_{s_i'/p_i}\!\oplus \, \xi_i'') \, \mathcal{R} \, (\eta_i' \, {}_{s_i'/p_i}\!\oplus \, \eta_i'') = \eta_i$ 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 branching bisimulations. Suppose $\xi \, \mathcal{R} \, \eta$. We have $\xi = \xi_1 \, {}_r\!\oplus \, \xi_2$, $\eta = \eta_1 \, {}_r\!\oplus \, \eta_2$ for distributions $\xi_1, \xi_2, \eta_1, \eta_2$ such that $\xi_1 \, \mathcal{R}_1 \, \eta_1$ and $\xi_2 \, \mathcal{R}_2 \, \eta_2$. If $\xi \xrightarrow{\alpha} \xi'$, then $\xi' = \xi_1' \, {}_r\!\oplus \, \xi_2'$ for distributions ξ_1', ξ_2' with $\xi_1 \xrightarrow{\alpha} \xi_1'$, $\xi_2 \xrightarrow{\alpha} \xi_2'$ and $\xi' = \xi_1' \, {}_r\!\oplus \, \xi_2'$. By assumption, $\bar{\eta}_1$, η_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 for $\bar{\eta} = \bar{\eta}_1 \, {}_r\!\oplus \, \bar{\eta}_2$, $\eta' = \eta_1' \, {}_r\!\oplus \, \eta_2'$ that $\xi = (\xi_1 \, {}_r\!\oplus \, \xi_2) \, \mathcal{R} \, (\bar{\eta}_1 \, {}_r\!\oplus \, \bar{\eta}_2) = \bar{\eta}$, $\eta = \eta_1 \, {}_r\!\oplus \, \eta_2 \Rightarrow \bar{\eta}_1 \, {}_r\!\oplus \, \bar{\eta}_2 = \bar{\eta} \xrightarrow{(\alpha)} \eta'$, and $\xi' = (\xi_1' \, {}_r\!\oplus \, \xi_2') \, \mathcal{R} \, (\beta_1' \, {}_r\!\oplus \, \eta_2') = \eta'$, as required for $\mathcal{R}$ to satisfy the transfer property of Definition 5.1d. Since $\mathcal{R}$ clearly relates $\mu_1 \, {}_r\!\oplus \, \mu_2$ and $\nu_1 \, {}_r\!\oplus \, \nu_2$, this finishes the proof. $\square$