Compositional Reasoning for Probabilistic Finite-State Behaviors

Yuxin Deng[1] ⋆, Catuscia Palamidessi[2] ⋆⋆, and Jun Pang[2]

[1] INRIA Sophia-Antipolis and Université Paris 7, France
[2] INRIA Futurs and LIX, École Polytechnique, France

Abstract. We study a process algebra which combines both nondeterministic and probabilistic behavior in the style of Segala and Lynch's simple probabilistic automata. We consider strong bisimulation and observational equivalence, and provide complete axiomatizations for a language that includes a restricted form of parallel composition and (guarded) recursion. The presence of the parallel composition, in particular, introduces various technical difficulties, but we believe that a "good" compositional semantics should take it into account since it is an essential operator to specify concurrent systems.

1 Introduction

Process algebras, also known as process calculi, are a powerful mathematical model for the specification and verification of concurrent systems. They provide a formal apparatus for representing and reasoning about the behaviors of distributed systems, algorithms and protocols in a compositional way. Some of the most prominent representants of these formalisms are CCS [26], ACP [8, 6], and CSP [21].

The axiomatic theories of process algebra provide an elegant way for proving properties of systems. Both a system and its desired external behavior can be expressed as process terms. The correctness of the system can then be verified by proving that these two terms are equivalent.

In a process algebra typically there are only a few operators, such as action prefix, summation (nondeterministic choice), recursion and parallel composition. The latter is particularly important for concurrency, as it allows to specify the structural properties of systems composed of several interacting parts. For example, a typical communication protocol for data transferring involves two agents S and R, representing the sender and the receiver, and two lossy channels K and L between them (see Figure 1). The behavior of each of these four components can be described as a process term in a chosen process algebra, and then they are all put together in parallel to form the complete view of the protocol. The parallel composition operator captures both the interleaving behaviors and

⋆ Supported by the EU project PROFUNDIS.
⋆⋆ Partially supported by the projet Rossignol of the ACI Sécurité Informatique (Ministère de la recherche et nouvelles technologies).

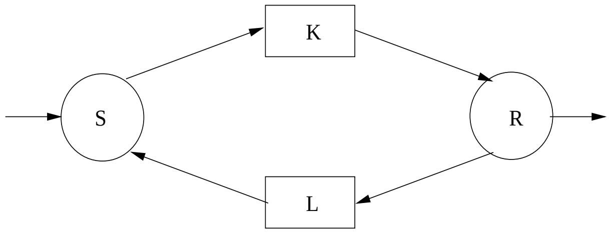

Fig. 1. A communication protocol

the possible synchronization of the components. The external behavior of the protocol can be specified as a FIFO queue. The equivalence proof between the protocol and its external behavior is established by equational reasoning based on axiomatization, hiding internal behavior, using fairness assumption, and the other feasible methods (see e.g. [9, 17]).

Developing a both complete and sound axiomatization for a chosen bisimulation relation over a process algebra expressing finite-state processes has been a research focus for the process algebra community. This led to a wealth of classical results in the literature. Milner [25, 27] gave complete axiomatizations of both strong bisimilarity and observational equivalence for a core CCS (not containing the parallel composition operator) with both unguarded and guarded recursion. Bergstra and Klop [10] axiomatized observational equivalence in an alternative way by using an interesting graph rewriting technique. Hennessy and Milner [20] offered a complete equational axiomatization of strong bisimulation over the recursion free fragment of CCS. To deal with parallel composition, they used the so-called *expansion law*, which is an equation schema with a countably infinite number of instances. Bergstra and Klop [8] gave a finite equational axiomatization of the merge operator (as the parallel composition in CCS) using the auxiliary left merge and communication merge operators. An interesting essay on equational axiomatizations of parallel composition can be found in [2].

Having both recursion and parallel composition in a process algebra complicates the matters to establish a complete axiomatization, mostly because this can give rise to infinite-state systems even with the guardedness condition. For example, let E be the expression $\mu_X(a.(X \mid b))$, then we have the infinite transition graph starting from E in Figure 2. Milner pointed out in [27] that in order to have a complete axiomatization for CCS with both recursion and parallel composition, a sufficient condition is that the parallel composition does not occur in the body of any recursive expression.

In this paper we relax this restriction by requiring, instead, that free variables do not appear in the scope of parallel composition. A similar restriction was adopted, independently, in [5]. In that paper, Baeten and Bravetti considered a generic process algebra of which CCS, CSP and ACP are subalgebras. Finite-stateness is achieved by requiring that recursion variables do not occur in the scope of *static operators*, which include the parallel composition. Our work and

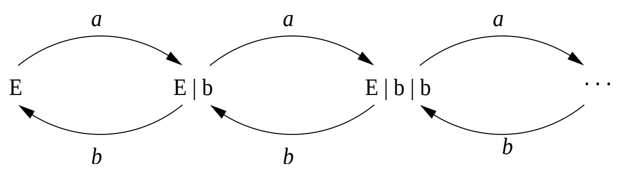

Fig. 2. The transition graph of E.

[5] are, in a sense, incomparable, because we consider a probabilistic and nondeterministic framework (as explained in the rest of this introduction) with CCS-like communication, while [5] considers a purely nondeterministic paradigm, but more general than our nondeterministic fragment. The same restriction already appeared in [11], for a nondeterministic process algebra with CSP multiway synchronization.

Recently there has been an increasing interest in the area of formal methods for the specification and analysis of probabilistic behaviors, as exhibited for instance in randomized, distributed and fault-tolerant systems. The notion of probabilistic bisimulation is introduced first by Larsen and Skou [22]. Later many variant behavioural equivalences have been defined for various probabilistic models. A representative model for analyzing probabilistic systems is provided by Segala and Lynch's simple probabilistic automata [29], which take into account both probabilistic and nondeterministic behavior and which have been successfully adopted in the studies of distributed algorithms [23, 28] and practical communication protocols [32]. An axiomatization for the finite sequential fragment of simple probabilistic automata has been provided by Bandini and Segala in [7]. Following this line of research, Deng and Palamidessi [16, 15] have given a sound and complete axiomatization for a larger language, which includes the recursion operator.

In this paper, we improve on [16, 15] by considering also the parallel composition. To our knowledge, it is the first time that an axiomatization for a probabilistic and nondeterministic process algebra with both recursion and parallel operator has been attempted. Similar to the case of classical process algebra, once we have both parallel composition and recursion, the equational axiomatization of strong bisimulation and observational equivalence turns out to be quite complicated to achieve.

To obtain the completeness of the axiomatizations, we develop a probabilistic version of the expansion law to eliminate all occurrences of parallel composition. In order to do that, we heavily rely on the condition that only closed terms are put in parallel (cf. Theorem 3).

Concerning soundness, it turns out to be particularly difficult to prove that strong and weak bisimilarities are closed under the parallel composition operator. Our approach is to manipulate equivalences of distributions on terms. An important property that we exploit in our proofs is Lemma 2, which says that if two distributions are equivalent with respect to an equivalence relation $\mathcal{R}$, then there is a uniform way to extend them so that the resulting distributions in parallel contexts are equivalent with respect to another equivalence relation $\mathcal{R}^{\lceil}$. It turns out that if $\mathcal{R}$ is instantiated as strong or weak bisimilarity then $\mathcal{R}^{\lceil}$ is a subset of $\mathcal{R}$, thus $\mathcal{R}^{\lceil}$ also relates bisimilar expressions.

Structure of the paper. In the next section we briefly recall some basic concepts and definitions about probabilistic distributions. In Section 3, we present the syntax and operational semantics of a probabilistic process calculus. Next, we give the notions of strong and weak behavioral equivalences in Section 4. We provide complete axiomatizations for strong bisimilarity and observational equivalence in Sections 5 and 6 respectively, restricted to guarded expressions in the second case. In Section 7, we conclude and discuss some related work not yet mentioned in the introduction. Detailed proofs of the main propositions in Section 4 are in the Appendix.

2 Preliminaries

Let S be a set. A function $\eta : S \mapsto [0,1]$ is called a *discrete probability distribution*, or *distribution* for short, on S if the *support* of η, defined as $spt(\eta) = \{x \in S \mid \eta(x) > 0\}$, is finite or countably infinite and $\sum_{x\in S}\eta(x) = 1$. We denote by $\mathcal{P}(S)$ the set of distributions over S. If η is a distribution with finite support and $V \subseteq spt(\eta)$ we use the set $\{s_i : \eta(s_i)\}_{s_i\in V}$ to enumerate the probability associated with each element of V. The constructor $\uplus$ on this kind of sets is defined as follows.

$$\{s_i : p_i\}_{i\in I} \uplus \{s : p\} = \begin{cases} \{s_i : p_i\}_{i\in I\setminus j} \cup \{s_j : (p_j + p)\} & \text{if } s = s_j \text{ for some } j \in I \\ \{s_i : p_i\}_{i\in I} \cup \{s : p\} & \text{otherwise.} \end{cases}$$

$$\{s_i : p_i\}_{i\in I} \uplus \{t_j : p_j\}_{j\in 1..n} = (\{s_i : p_i\}_{i\in I} \uplus \{t_1 : p_1\}) \uplus \{t_j : p_j\}_{j\in 2..n}$$

Given some distributions $\eta_1, ..., \eta_n$ on S and some real numbers $r_1, ..., r_n \in [0,1]$ with $\sum_{i\in 1..n} r_i = 1$, we define the *convex combination* $r_1\eta_1 + ... + r_n\eta_n$ of $\eta_1, ..., \eta_n$ to be the distribution η such that $\eta(s) = \sum_{i\in 1..n} r_i\eta_i(s)$, for each $s \in S$.

A *simple probabilistic automaton* is a tuple $(S, s, \Sigma, \mathcal{T})$, where S is a set of *states*, $s \in S$ is a *start state*, Σ is a set of *actions*, and $\mathcal{T} \subseteq S \times \Sigma \times \mathcal{P}(S)$ is a *transition relation*. Informally, a simple probabilistic automaton is like an ordinary automaton except that a labeled transition leads to a probabilistic distribution over a set of states instead of a single state. Simple probabilistic automata are used in this paper to give operational semantics of our probabilistic process calculus.

3 Probabilistic process calculus

We assume a countable set of variables, $Var = \{X, Y, ...\}$, and a countable set of atomic actions, $\mathcal{A} = \{a, b, ...\}$. Given a special action τ not in $\mathcal{A}$, we let $u, v, ...$

range over the set of *actions*, $Act = \mathcal{A} \cup \overline{\mathcal{A}} \cup \{\tau\}$, and let $\alpha, \beta, ...$ range over the set $Var \cup Act$. The class of expressions $\mathcal{E}$ is defined by the following syntax:

$$E, F ::= u. \bigoplus_{i \in 1..n} p_i E_i \;\Big|\; \sum_{i \in 1..m} E_i \;\Big|\; E \mid F \;\Big|\; X \;\Big|\; \mu_X E$$

Here $\bigoplus_{i \in 1..n} p_i E_i$ stands for a *probabilistic choice* operator, where the p_i's represent positive probabilities, i.e., they satisfy $p_i \in (0,1]$ and $\sum_{i \in 1..n} p_i = 1$. When $n = 0$ we abbreviate the probabilistic choice as $\mathbf{0}$; when $n = 1$ we abbreviate it as E_1. Sometimes we are interested in certain branches of the probabilistic choice; in this case we write $\bigoplus_{i \in 1..n} p_i E_i$ as $p_1 E_1 \oplus ... \oplus p_n E_n$ or $(\bigoplus_{i \in 1..(n-1)} p_i E_i) \oplus p_n E_n$ where $\bigoplus_{i \in 1..(n-1)} p_i E_i$ abbreviates (with a slight abuse of notation) $p_1 E_1 \oplus ... \oplus p_{n-1} E_{n-1}$. The second construction $\sum_{i \in 1..m} E_i$ stands for *nondeterministic choice*, and occasionally we may write it as $E_1 + ... + E_m$. As in CCS we let variables range over process expressions. The notation μ_X stands for a recursion which binds the variable X. We shall use $fv(E)$ for the set of free variables (i.e., not bound by any μ_X) in E. As explained in the introduction, we require that only closed expressions are put in parallel composition, i.e., in $E \mid F$ we have $fv(E \mid F) = \emptyset$. As usual we identify expressions which differ only by a change of bound variables. We shall write $E\{F_1, ..., F_n / X_1, ..., X_n\}$ or $E\{\widetilde{F}/\widetilde{X}\}$ for the result of simultaneously substituting F_i for each occurrence of X_i in E $(1 \leq i \leq n)$, renaming bound variables if necessary.

Definition 1. *The variable X is* weakly guarded *(resp.* guarded*) in E if every free occurrence of X in E occurs within some subexpression $u.F$ (resp. $a.F$ or $\bar{a}.F$), otherwise X is* weakly unguarded *(resp.* unguarded*) in E.*

The operational semantics of an expression E is defined as a simple probabilistic automaton whose states are the expressions reachable from E and the transition relation is defined by the axioms and inference rules in Table 1, where $E \xrightarrow{\alpha} \eta$ describes a transition that, by performing an action or exposing a free variable, leaves from E and leads to a distribution η over $\mathcal{E}$. The symmetric rules of par and com are omitted.

var	$X \xrightarrow{X} \{\mathbf{0} : 1\}$	psum	$u. \bigoplus_{i \in 1..n} p_i E_i \xrightarrow{u} \biguplus_{i \in 1..n} \{E_i : p_i\}$
rec	$\dfrac{E\{\mu_X E/X\} \xrightarrow{\alpha} \eta}{\mu_X E \xrightarrow{\alpha} \eta}$	nsum	$\dfrac{E_j \xrightarrow{\alpha} \eta}{\sum_{i \in 1..m} E_i \xrightarrow{\alpha} \eta}$ for some $j \in 1..m$
par	$\dfrac{E \xrightarrow{\alpha} \{E_i : p_i\}_i}{E \mid F \xrightarrow{\alpha} \{E_i \mid F : p_i\}_i}$	com	$\dfrac{E \xrightarrow{a} \{E_i : p_i\}_{i \in I} \quad F \xrightarrow{\bar{a}} \{F_j : q_j\}_{j \in J}}{E \mid F \xrightarrow{\tau} \{E_i \mid F_j : p_i q_j\}_{i \in I, j \in J}}$

Table 1. Strong transitions

Finitary weak transitions are defined as in [7]. We abstract away finitely many invisible actions that occur before or after the appearance of a single visible action or a variable. It is easy to see that if $E \stackrel{X}{\Longrightarrow} \eta$ then $\eta = \{\mathbf{0} : 1\}$. We use the notation $\stackrel{\hat{\alpha}}{\Longrightarrow}$ to stand for $\stackrel{\alpha}{\Longrightarrow}$ if $\alpha \neq \tau$, for $\Longrightarrow$ otherwise. We also define a *weak combined transition*: $E \stackrel{\hat{\alpha}}{\Longrightarrow}_c \eta$ if there exists a collection $\{\eta_i, r_i\}_{i \in 1..n}$ of distributions and probabilities such that $\sum_{i \in 1..n} r_i = 1$, $\eta = r_1\eta_1 + ... + r_n\eta_n$ and $E \stackrel{\hat{\alpha}}{\Longrightarrow} \eta_i$ for each $i \in 1..n$. Similarly we write $E \stackrel{\alpha}{\Longrightarrow}_c \eta$ if every component is a "normal" (i.e., non-virtual) weak transition, namely, $E \stackrel{\alpha}{\Longrightarrow} \eta_i$ for all $i \leq n$.

$$\textsf{wea1}\ E \Longrightarrow \{E:1\} \qquad \textsf{wea2}\ \frac{E \stackrel{\tau}{\longrightarrow} \eta}{E \Longrightarrow \eta} \qquad \textsf{wea3}\ \frac{E \stackrel{\alpha}{\longrightarrow} \eta}{E \stackrel{\alpha}{\Longrightarrow} \eta}$$

$$\textsf{wea4}\ \frac{E \stackrel{\alpha}{\Longrightarrow} \{E_i : p_i\}_{i \in I} \quad \forall i \in I : E_i \Longrightarrow \{E_{ij} : p_{ij}\}_{j \in J_i}}{E \stackrel{\alpha}{\Longrightarrow} \{E_{ij} : p_i p_{ij}\}_{i \in I, j \in J_i}}$$

$$\textsf{wea5}\ \frac{E \Longrightarrow \{E_i : p_i\}_{i \in I} \quad \forall i \in I : E_i \stackrel{\alpha}{\Longrightarrow} \{E_{ij} : p_{ij}\}_{j \in J_i}}{E \stackrel{\alpha}{\Longrightarrow} \{E_{ij} : p_i p_{ij}\}_{i \in I, j \in J_i}}$$

Table 2. Weak transitions

4 Behavioral equivalences

To define behavioral equivalences in probabilistic process algebra, it is customary to consider equivalence of distributions with respect to equivalence relations on expressions.

4.1 Equivalence of distributions

If η is a distribution on S and $V \subseteq S$, we write $\eta(V)$ for $\sum_{s \in V} \eta(s)$. We lift an equivalence relation on $\mathcal{E}$ to an equivalence relation between distributions over $\mathcal{E}$ in the following way.

Definition 2. *Given two distributions η_1 and η_2 over $\mathcal{E}$, we say that they are equivalent w.r.t. an equivalence relation $\mathcal{R}$ on $\mathcal{E}$, written $\eta_1 \equiv_{\mathcal{R}} \eta_2$, if*

$$\forall V \in \mathcal{E}/\mathcal{R} : \eta_1(V) = \eta_2(V).$$

The following property is simple but important as it underpins many other results in the rest of the paper.

Lemma 1. *If $\eta_1 \equiv_{\mathcal{R}_1} \eta_2$ and $\mathcal{R}_1 \subseteq \mathcal{R}_2$ then $\eta_1 \equiv_{\mathcal{R}_2} \eta_2$.*

Given an equivalence relation $\mathcal{R}$, we construct two relations:

$$\begin{aligned}\mathcal{R}_G &\stackrel{\text{def}}{=} \{(E \mid G,\ F \mid G) \;\big|\; E\ \mathcal{R}\ F\}\\ \mathcal{R}^{\mid} &\stackrel{\text{def}}{=} \bigcup\{\mathcal{R}_G \;\big|\; G \in \mathcal{E}\}.\end{aligned}$$

Clearly $\mathcal{R}_G$ and $\mathcal{R}^{\mid}$ are also equivalence relations. If $V \in \mathcal{E}/_{\mathcal{R}_G}$ then we write $V^{\setminus G}$ for the set $\{E \;\big|\; E \mid G \in V\}$. It is easy to see that if $V \in \mathcal{E}/_{\mathcal{R}^{\mid}}$ then there exists some expression G such that $V \in \mathcal{E}/_{\mathcal{R}_G}$. Furthermore, we observe that $V \in \mathcal{E}/_{\mathcal{R}_G}$ iff $V^{\setminus G} \in \mathcal{E}/_{\mathcal{R}}$. Suppose $\theta_1 = \{E_i : p_i\}_{i\in I}$ and $\theta_2 = \{F_j : q_j\}_{j\in J}$, we introduce the following notation:

$$\theta_1 \mid \theta_2 \ \stackrel{\text{def}}{=}\ \{E_i \mid F_j : p_i q_j\}_{i\in I, j\in J}.$$

The following lemma is crucial for showing the congruence property of strong bisimilarity and observational equivalence (cf. Section 4.4). It says that if two distributions θ_1 and θ_2 are equivalent w.r.t. an equivalence relation $\mathcal{R}$, then there is a uniform way to extend the two distributions so that the resulting distributions on composed terms are equivalent w.r.t. another equivalence relation $\mathcal{R}^{\mid}$.

Lemma 2. *If $\theta_1 \equiv_{\mathcal{R}} \theta_2$ then $(\theta_1 \mid \theta) \ \equiv_{\mathcal{R}^{\mid}}\ (\theta_2 \mid \theta)$.*

Proof. Let $\theta = \{G_k : p_k\}_{k\in K}$. Without loss of generality, we assume that if $i, j \in K$ and $i \neq j$ then $G_i \neq G_j$. For any $V \in \mathcal{E}/_{\mathcal{R}^{\mid}}$ there exists some expression G such that $V \in \mathcal{E}/_{\mathcal{R}_G}$. There are two cases:

1. if $G \neq G_k$ for all $k \in K$, then $(\theta_1 \mid \theta)(V) = 0 = (\theta_2 \mid \theta)(V)$;
2. if $G = G_k$ for some $k \in K$, then $(\theta_1 \mid \theta)(V) = r_k\theta_1(V^{\setminus G_k}) = r_k\theta_2(V^{\setminus G_k}) = (\theta_2 \mid \theta)(V)$.

In summary, $(\theta_1 \mid \theta)(V) = (\theta_2 \mid \theta)(V)$ for any $V \in \mathcal{E}/_{\mathcal{R}^{\mid}}$, i.e., $(\theta_1 \mid \theta) \ \equiv_{\mathcal{R}^{\mid}}\ (\theta_2 \mid \theta)$, which is the required result. $\square$

Corollary 1. *If $\theta_1 \equiv_{\mathcal{R}} \theta_2$, $\theta_1' \equiv_{\mathcal{R}} \theta_2'$ and $\mathcal{R}$ is closed under parallel composition, then $(\theta_1 \mid \theta_1') \ \equiv_{\mathcal{R}}\ (\theta_2 \mid \theta_2')$.*

Proof. If $\mathcal{R}$ is closed under parallel composition, then $\mathcal{R}^{\mid} \subseteq \mathcal{R}$. By Lemma 1, we can state Lemma 2 as: if $\theta_1 \equiv_{\mathcal{R}} \theta_2$ then $(\theta_1 \mid \theta) \ \equiv_{\mathcal{R}}\ (\theta_2 \mid \theta)$. Similarly we can establish a symmetric property: if $\theta_1 \equiv_{\mathcal{R}} \theta_2$ then $(\theta \mid \theta_1) \ \equiv_{\mathcal{R}}\ (\theta \mid \theta_2)$. As a consequence we have $(\theta_1 \mid \theta_1') \ \equiv_{\mathcal{R}}\ (\theta_2 \mid \theta_1') \ \equiv_{\mathcal{R}}\ (\theta_2 \mid \theta_2')$. $\square$

4.2 Behavioral equivalences

Strong bisimulation is defined by requiring equivalence of distributions at every step. Because of the way equivalence of distributions is defined, we need to restrict to bisimulations which are equivalence relations.

Definition 3. *An equivalence relation $\mathcal{R} \subseteq \mathcal{E} \times \mathcal{E}$ is a* strong bisimulation *if $E\ \mathcal{R}\ F$ implies:*

– *whenever* $E \xrightarrow{\alpha} \eta_1$*, there exists* η_2 *such that* $F \xrightarrow{\alpha} \eta_2$ *and* $\eta_1 \equiv_{\mathcal{R}} \eta_2$*.*

Two expressions E, F *are* strong bisimilar*, written* $E \sim F$*, if there exists a strong bisimulation* $\mathcal{R}$ *s.t.* $E \mathcal{R} F$*.*

We have shown in [16, 15] that to define weak equivalences it is necessary to use weak combined transitions[3], so weak probabilistic bisimulation is given in the following way.

Definition 4. *An equivalence relation* $\mathcal{R} \subseteq \mathcal{E} \times \mathcal{E}$ *is a* weak probabilistic bisimulation *if* $E \mathcal{R} F$ *implies:*

– *whenever* $E \xrightarrow{\alpha} \eta_1$*, there exists* η_2 *such that* $F \overset{\hat{\alpha}}{\Longrightarrow}_c \eta_2$ *and* $\eta_1 \equiv_{\mathcal{R}} \eta_2$*.*

We write $E \approx F$ *whenever there exists a weak probabilistic bisimulation* $\mathcal{R}$ *s.t.* $E \mathcal{R} F$*.*

As usual, observational equivalence is defined in terms of weak probabilistic bisimulation.

Definition 5. *Two expressions* E, F *are* observationally equivalent*, written* $E \simeq F$*, if*

1. *whenever* $E \xrightarrow{\alpha} \eta_1$*, there exists* η_2 *such that* $F \overset{\alpha}{\Longrightarrow}_c \eta_2$ *and* $\eta_1 \equiv_{\approx} \eta_2$*.*
2. *whenever* $F \xrightarrow{\alpha} \eta_2$*, there exists* η_1 *such that* $E \overset{\alpha}{\Longrightarrow}_c \eta_1$ *and* $\eta_1 \equiv_{\approx} \eta_2$*.*

One can check that all the relations defined above are indeed equivalence relations and we have the inclusion ordering: $\sim \subsetneq \simeq \subsetneq \approx$.

Example 1. Consider the following expressions:

$$\begin{aligned} E_1 &\overset{\text{def}}{=} \mu_X(a.X + X) \\ E_2 &\overset{\text{def}}{=} \mu_X(\tfrac{1}{2}X \oplus \tfrac{1}{2}(X + X)) \\ F_1 &\overset{\text{def}}{=} a.b + \tau.c \\ F_2 &\overset{\text{def}}{=} F_1 + \tau.(\tfrac{1}{3}F_1 \oplus \tfrac{2}{3}c) \end{aligned}$$

It can be checked that $E_1 \sim E_2$, $F_1 \approx F_2$, and $\tau.F_1 \simeq \tau.F_2$. Note that $F_1 \not\simeq F_2$ because the transition $F_2 \xrightarrow{\tau} \{F_1 : \frac{1}{3},\ c : \frac{2}{3}\}$ cannot be matched up by the transition $F_1 \xrightarrow{\tau} \{c : 1\}$, which is the only normal transition from F_1 with action τ. $\square$

[3] The example given in [16, 15] for supporting this argument is built in probabilistic automata [29], but it is easy to write a similar example in simple probabilistic automata (see Appendix A).

4.3 Probabilistic "bisimulation up to" techniques

A natural way for showing $E \sim F$ in a probabilistic process calculus is to construct an equivalence relation $\mathcal{R}$ which includes the pair (E, F), and then to check that $\mathcal{R}$ is a bisimulation. However, it is often difficult to ensure that the relation $\mathcal{R}$ one constructs is indeed an equivalence relation. In this case we use "bisimulation up to" techniques. The idea is that we extend $\mathcal{R}$ to be $\mathcal{R}'$ such that $\mathcal{R} \subseteq \mathcal{R}'$ and $\mathcal{R}'$ is easily shown to be a bisimulation.

Given a binary relation $\mathcal{R}$ we denote by $\mathcal{R}_\sim$ the relation $(\mathcal{R} \cup \sim)^*$, the equivalence closure of $\mathcal{R} \cup \sim$. Similarly for the notation $\mathcal{R}_\approx$.

Definition 6. *A binary relation $\mathcal{R}$ is a* strong bisimulation up to $\sim$ *if $E \mathcal{R} F$ implies:*

1. *whenever $E \xrightarrow{\alpha} \eta_1$, there exists η_2 such that $F \xrightarrow{\alpha} \eta_2$ and $\eta_1 \equiv_{\mathcal{R}_\sim} \eta_2$.*
2. *whenever $F \xrightarrow{\alpha} \eta_2$, there exists η_1 such that $E \xrightarrow{\alpha} \eta_1$ and $\eta_1 \equiv_{\mathcal{R}_\sim} \eta_2$.*

A strong bisimulation up to $\sim$ is not necessarily an equivalence relation. It is just an ordinary binary relation included in $\sim$, as shown by the next proposition.

Proposition 1. *If $\mathcal{R}$ is a strong bisimulation up to $\sim$, then $\mathcal{R} \subseteq \sim$.*

For weak probabilistic bisimulation, the "up to" relation can be defined as well, but we need to be careful.

Definition 7. *A binary relation $\mathcal{R}$ is a* weak probabilistic bisimulation up to $\approx$ *if $E \mathcal{R} F$ implies:*

1. *whenever $E \stackrel{\alpha}{\Longrightarrow} \eta_1$, there exists η_2 such that $F \stackrel{\hat{\alpha}}{\Longrightarrow}_c \eta_2$ and $\eta_1 \equiv_{\mathcal{R}_\approx} \eta_2$.*
2. *whenever $F \stackrel{\alpha}{\Longrightarrow} \eta_2$, there exists η_1 such that $E \stackrel{\hat{\alpha}}{\Longrightarrow}_c \eta_1$ and $\eta_1 \equiv_{\mathcal{R}_\approx} \eta_2$.*

In the above definition, we are not able to replace the first double arrow in each clause by a simple arrow. Otherwise, the resulting relation would not be included in $\approx$.

Proposition 2. *If $\mathcal{R}$ is a weak probabilistic bisimulation up to $\approx$, then $\mathcal{R} \subseteq \approx$.*

In a way similar to Definition 7, we introduce an "up to $\simeq$" relation.

Definition 8. *A binary relation $\mathcal{R}$ is an* observational equivalence up to $\simeq$ *if $E \mathcal{R} F$ implies:*

1. *whenever $E \stackrel{\alpha}{\Longrightarrow} \eta_1$, there exists η_2 such that $F \stackrel{\alpha}{\Longrightarrow}_c \eta_2$ and $\eta_1 \equiv_{\mathcal{R}_\approx} \eta_2$.*
2. *whenever $F \stackrel{\alpha}{\Longrightarrow} \eta_2$, there exists η_1 such that $E \stackrel{\alpha}{\Longrightarrow}_c \eta_1$ and $\eta_1 \equiv_{\mathcal{R}_\approx} \eta_2$.*

As expected, observational equivalence up to $\simeq$ is useful because of the following property.

Proposition 3. *If $\mathcal{R}$ is an observational equivalence up to $\simeq$, then $\mathcal{R} \subseteq \simeq$.*

4.4 Some properties of behavioral equivalences

By using the "bisimulation up to" techniques introduced in the previous section, together with Lemma 2, we can prove the following results. Their detailed proofs are in Appendices B and C, respectively.

Proposition 4 (Properties of $\sim$).

1. *$\sim$ is a congruence relation;*
2. *$\mu_X E \sim E\{\mu_X E/X\}$;*
3. *$\mu_X(E+X) \sim \mu_X E$;*
4. *If $E \sim F\{E/X\}$ and X is weakly guarded in F, then $E \sim \mu_X F$.*

Proposition 5 (Properties of $\simeq$).

1. *$\simeq$ is a congruence relation;*
2. *If $\tau.E \simeq \tau.E + F$ and $\tau.F \simeq \tau.F + E$ then $\tau.E \simeq \tau.F$;*
3. *If $E \simeq F\{E/X\}$ and X is guarded in F then $E \simeq \mu_X F$.*

5 Axiomatizing strong bisimilarity

We present in this section the axiom system $\mathcal{A}_s$ for $\sim$, which includes all axioms and rules displayed in Table 3. We assume the usual rules for equality (reflexivity, symmetry, transitivity and substitutivity), and the alpha-conversion of bound variables. If we omit all the axioms involving probabilities, we obtain the system composed by **S1-3** and **R1-3**, which characterizes exactly the class of nonprobabilistic finite-state behaviors studied in [25]. The two axioms **S4-5** allow us to permute and merge probabilistic branches in a probabilistic choice. **E** is a probabilistic version of the expansion law in CCS.

The notation $\mathcal{A}_s \vdash E = F$ (and $\mathcal{A}_s \vdash \widetilde{E} = \widetilde{F}$ for a finite sequence of equations) means that the equation $E = F$ is derivable by applying the axioms and rules from $\mathcal{A}_s$. The following theorem shows that $\mathcal{A}_s$ is sound with respect to $\sim$.

Theorem 1 (Soundness of $\mathcal{A}_s$). *If $\mathcal{A}_s \vdash E = E'$ then $E \sim E'$.*

Proof. The soundness of the recursion axioms **R1-3** is shown in Section 4.4; the soundness of **S1-4** and **E** is obvious, and **S5** is a consequence of Definition 2. □

For the completeness proof, the basic points are: (1) if two expressions are bisimilar then we can construct an equation set in a certain format (standard format) that they both satisfy; (2) if two expressions satisfy the same standard equation set, then they can be proved equal by $\mathcal{A}_s$. This schema is inspired by [25, 31], but in our case the definition of standard format and the proof itself are more complicated due to the presence of both probabilistic and nondeterministic dimensions.

S1 $E + \mathbf{0} = E$
S2 $E + E = E$
S3 $\sum_{i\in I} E_i = \sum_{i\in I} E_{\rho(i)}$ $\quad\rho$ is any permutation on I
S4 $u.\bigoplus_{i\in I} p_i E_i = u.\bigoplus_{i\in I} p_{\rho(i)} E_{\rho(i)}$ $\quad\rho$ is any permutation on I
S5 $u.((\bigoplus_i p_i E_i) \oplus pE \oplus qE) = u.((\bigoplus_i p_i E_i) \oplus (p+q)E)$

R1 $\mu_X E = E\{\mu_X E/X\}$
R2 If $E = F\{E/X\}$, X weakly guarded in F, then $E = \mu_X F$
R3 $\mu_X(E + X) = \mu_X E$

E Assume $E \equiv \sum_i u_i.\bigoplus_j p_{ij} E_{ij}$ and $F \equiv \sum_k v_k.\bigoplus_l q_{kl} F_{kl}$. Then infer:

$$\begin{aligned} E \mid F = &\textstyle\sum_i u_i.\bigoplus_j p_{ij}(E_{ij} \mid F) + \sum_k v_k.\bigoplus_l q_{kl}(E \mid F_{kl}) \\ &+ \textstyle\sum_{u_i\ opp\ v_k} \tau.\bigoplus_{j,l}(p_{ij}q_{kl})(E_{ij} \mid F_{kl}) \end{aligned}$$

where u_i *opp* v_k means that u_i and v_k are complementary actions, i.e., $\bar{u}_i = v_k$.

Table 3. The axiom system $\mathcal{A}_s$

Definition 9. *Let $\widetilde{X} = \{X_1, ..., X_m\}$ and $\widetilde{W} = \{W_1, W_2, ...\}$ be disjoint sets of variables. Let $\widetilde{H} = \{H_1, ..., H_m\}$ be expressions with free variables in $\widetilde{X} \cup \widetilde{W}$. In the equation set $S : \widetilde{X} = \widetilde{H}$, we call $\widetilde{X}$* formal variables *and $\widetilde{W}$* free variables. *We say S is* standard *if each H_i takes the form $\sum_j E_{f(i,j)} + \sum_l W_{h(i,l)}$ where $E_{f(i,j)} = u_{f(i,j)}.\bigoplus_k p_{f(i,j,k)} X_{g(i,j,k)}$. We call S* weakly guarded *if there is no H_i s.t. $H_i \xrightarrow{X_i} \{\mathbf{0} : 1\}$. We say that E* provably satisfies *S if there are expressions $\widetilde{E} = \{E_1, ..., E_m\}$, with $E_1 \equiv E$ and $fv(\widetilde{E}) \subseteq \widetilde{W}$, such that $\mathcal{A}_s \vdash \widetilde{E} = \widetilde{H}\{\widetilde{E}/\widetilde{X}\}$.*

We first recall the theorem of unique solution of equations originally appeared in [25]. Adding probabilistic choice does not affect the validity of this theorem.

Theorem 2 (Unique solution of equations I). *If S is a weakly guarded equation set with free variables in $\widetilde{W}$, then there is an expression E which provably satisfies S. Moreover, if F provably satisfies S and has free variables in $\widetilde{W}$, then $\mathcal{A}_s \vdash E = F$.*

Proof. Exactly as in [25]. □

Below we give an extension of Milner's equational characterization theorem by accommodating probabilistic choice.

Theorem 3 (Equational characterization I). *For any expression E, with free variables in $\widetilde{W}$, there exist some expressions $\widetilde{E} = \{E_1, ..., E_m\}$, with $E_1 \equiv E$ and $fv(\widetilde{E}) \subseteq \widetilde{W}$, satisfying m equations*

$$\mathcal{A}_s \vdash E_i = \sum_{j\in 1..n(i)} E_{f(i,j)} + \sum_{j\in 1..l(i)} W_{h(i,j)} \qquad (i \leq m)$$

where $E_{f(i,j)} \equiv u_{f(i,j)}.\bigoplus_{k\in 1..o(i,j)} p_{f(i,j,k)} E_{g(i,j,k)}$.

Proof. By induction on the structure of E. We only consider the case that $E \equiv F \mid F'$; all other cases are similar to the proof in [25]. By definition F and F' are closed terms. By induction we have closed terms $F_1, .., F_m$ satisfying m equations

$$\mathcal{A}_s \vdash F_i = \sum_{j\in 1..n(i)} F_{f(i,j)} \qquad (i \le m)$$

where $F_{f(i,j)} \equiv u_{f(i,j)}.\bigoplus_{k\in 1..o(i,j)} p_{f(i,j,k)} F_{g(i,j,k)}$. Similarly we have closed expressions $F'_1, ..., F'_{m'}$ satisfying m' equations

$$\mathcal{A}_s \vdash F'_{i'} = \sum_{j'\in 1..n'(i')} F'_{f'(i',j')} \qquad (i \le m')$$

where $F'_{f'(i',j')} \equiv u'_{f'(i',j')}.\bigoplus_{k'\in 1..o'(i',j')} p'_{f'(i',j',k')} F'_{g'(i',j',k')}$. Now set $E_{i,i'} \equiv F_i \mid F'_{i'}$. By the expansion law **E** we obtain the equations

$$\begin{aligned}\mathcal{A}_s \vdash E_{i,i'} = &\textstyle\sum_{j\in 1..n(i)} u_{f(i,j)}.\bigoplus_{k\in 1..o(i,j)} p_{f(i,j,k)} E_{g(i,j,k),i'} \\ &+ \textstyle\sum_{j'\in 1..n'(i')} u'_{f'(i',j')}.\bigoplus_{k'\in 1..o'(i',j')} p'_{f'(i',j',k')} E_{i,g'(i',j',k')} \\ &+ \textstyle\sum_{u_{f(i,j)}\ opp\ u'_{f'(i',j')}} \tau.\bigoplus_{k\in 1..o(i,j), k'\in 1..o'(i',j')} (p_{f(i,j,k)} p'_{f'(i',j',k')}) \\ &E_{f(i,j,k), f'(i',j',k')}\end{aligned}$$

where $i \le m,\ i' \le m'$ and $u_{f(i,j)}\ opp\ u'_{f'(i',j')}$ means that $u_{f(i,j)}$ and $u'_{f'(i',j')}$ are complementary actions, i.e., they are a and $\bar{a}$ respectively, for some a, or the inverse.

Moreover, we have $E \equiv F_1 \mid F'_1 \equiv E_{1,1}$. □

The following completeness proof is closely analogous to that of [31]. It is complicated somewhat by the presence of nondeterministic choice. For example, to construct the formal equations, we need to consider a more refined relation $L_{iji'j'}$ underneath the relation $K_{ii'}$ while in [25, 31] it is sufficient to just use $K_{ii'}$.

Theorem 4 (Completeness of $\mathcal{A}_s$). *If $E \sim E'$ then $\mathcal{A}_s \vdash E = E'$.*

Proof. Let E and E' have free variables in $\widetilde{W}$. By Theorem 3 there are provable equations such that $E \equiv E_1$, $E' \equiv E'_1$ and

$$\mathcal{A}_s \vdash E_i = \sum_{j\in 1..n(i)} E_{f(i,j)} + \sum_{j\in 1..l(i)} W_{h(i,j)} \qquad (i \le m)$$

$$\mathcal{A}_s \vdash E'_{i'} = \sum_{j'\in 1..n'(i')} E'_{f'(i',j')} + \sum_{j'\in 1..l'(i')} W_{h'(i',j')} \qquad (i' \le m')$$

with

$$E_{f(i,j)} \equiv u_{f(i,j)}.\bigoplus_{k\in 1..o(i,j)} p_{f(i,j,k)} E_{g(i,j,k)}$$

$$E'_{f'(i',j')} \equiv u'_{f'(i',j')}.\bigoplus_{k'\in 1..o'(i',j')} p'_{f'(i',j',k')}E'_{g'(i',j',k')}.$$

Let $I = \{\langle i,i'\rangle \mid E_i \sim E'_{i'}\}$. By hypothesis we have $E_1 \sim E'_1$, so $\langle 1,1\rangle \in I$. Moreover, for each $\langle i,i'\rangle \in I$, the following holds, by the definition of strong bisimilarity:

1. There exists a total surjective relation $K_{ii'}$ between $\{1,...,n(i)\}$ and $\{1,...,n'(i')\}$, given by
$$K_{ii'} = \{\langle j,j'\rangle \mid \langle f(i,j), f'(i',j')\rangle \in I\}.$$
Furthermore, for each $\langle j,j'\rangle \in K_{ii'}$, we have $u_{f(i,j)} = u'_{f'(i',j')}$ and there exists a total surjective relation $L_{iji'j'}$ between $\{1,...,o(i,j)\}$ and $\{1,...,o'(i',j')\}$, given by
$$L_{iji'j'} = \{\langle k,k'\rangle \mid \langle g(i,j,k), g'(i',j',k')\rangle \in I\}.$$
2. $\mathcal{A}_s \vdash \sum_{j\in 1..l(i)} W_{h(i,j)} = \sum_{j'\in 1..l'(i')} W_{h'(i',j')}$.

Now, let $L_{iji'j'}(k)$ denote the image of $k \in \{1,...,o(i,j)\}$ under $L_{iji'j'}$ and $L^{-1}_{iji'j'}(k')$ the preimage of $k' \in \{1,...,o'(i',j')\}$ under $L_{iji'j'}$. We write $[k]_{iji'j'}$ for the set $L^{-1}_{iji'j'}(L_{iji'j'}(k))$ and $[k']_{iji'j'}$ for $L_{iji'j'}(L^{-1}_{iji'j'}(k'))$. It follows from the definitions that

1. If $\langle i,i'_1\rangle \in I$, $\langle i,i'_2\rangle \in I$, $\langle j,j'_1\rangle \in K_{ii'_1}$ and $\langle j,j'_2\rangle \in K_{ii'_2}$, then $[k]_{iji'_1j'_1} = [k]_{iji'_2j'_2}$.
2. If $q_1 \in [k]_{iji'j'}$ and $q_2 \in [k]_{iji'j'}$, then $E_{g(i,j,q_1)} \sim E_{g(i,j,q_2)}$.

Define $\nu_{ijk} = \sum_{q\in[k]_{iji'j'}} p_{f(i,j,q)}$ for any i',j' such that $\langle i,i'\rangle \in I$ and $\langle j,j'\rangle \in K_{ii'}$; define $\nu'_{i'j'k'} = \sum_{q'\in[k']_{iji'j'}} p'_{f'(i',j',q')}$ for any i,j such that $\langle i,i'\rangle \in I$ and $\langle j,j'\rangle \in K_{ii'}$. It is easy to see that whenever $\langle i,i'\rangle \in I$, $\langle j,j'\rangle \in K_{ii'}$ and $\langle k,k'\rangle \in L_{iji'j'}$ then $\nu_{ijk} = \nu'_{i'j'k'}$.

We now consider the formal equations, one for each $\langle i,i'\rangle \in I$:

$$X_{i,i'} = \sum_{\langle j,j'\rangle\in K_{ii'}} H_{f(i,j),f'(i',j')} + \sum_{j\in 1..l(i)} W_{h(i,j)}$$

where

$$H_{f(i,j),f'(i',j')} \equiv u_{f(i,j)}.\bigoplus_{\langle k,k'\rangle\in L_{iji'j'}} (\frac{p_{f(i,j,k)}p'_{f'(i',j',k')}}{\nu_{ijk}})X_{g(i,j,k),g'(i',j',k')}.$$

These equations are provably satisfied when each $X_{i,i'}$ is instantiated to E_i, since $K_{ii'}$ and $L_{iji'j'}$ are total and the right-hand side differs at most by repeated summands from that of the already proved equation for E_i. Note that each probabilistic branch $p_{f(i,j,k)}E_{g(i,j,k)}$ in the subterm $E_{f(i,j)}$ of E_i becomes the probabilistic summation of several branches like

$$\bigoplus_{q'\in[k']_{iji'j'}} (\frac{p_{f(i,j,k)}p'_{f'(i',j',q')}}{\nu_{ijk}})E_{g(i,j,k)}$$

in $H_{f(i,j),f'(i',j')}\{E_i/X_{i,i'}\}_i$, where $\langle i,i'\rangle \in I$, $\langle j,j'\rangle \in K_{ii'}$ and $\langle k,k'\rangle \in L_{iji'j'}$. But they are provably equal because

$$\begin{aligned}\textstyle\sum_{q'\in[k']_{iji'j'}}\left(\frac{p_{f(i,j,k)}p'_{f'(i',j',q')}}{\nu_{ijk}}\right) &= \tfrac{p_{f(i,j,k)}}{\nu_{ijk}}\cdot\textstyle\sum_{q'\in[k']_{iji'j'}} p'_{f'(i',j',q')}\\ &= \tfrac{p_{f(i,j,k)}}{\nu_{ijk}}\cdot \nu'_{i'j'k'} = p_{f(i,j,k)}\end{aligned}$$

and then the axiom **S5** can be used. Symmetrically, the equations are provably satisfied when each $X_{i,i'}$ is instantiated to $E'_{i'}$; this depends on the surjectivity of $K_{ii'}$ and $J_{iji'j'}$.

Finally, we note that each $X_{i,i'}$ is weakly guarded in the right-hand sides of the formal equations. It follows from Theorem 2 that $\vdash E_i = E'_{i'}$ for each $\langle i,i'\rangle \in I$, and hence $\vdash E = E'$. □

6 Axiomatizing observational equivalence

In this section we axiomatize the observational equivalence $\simeq$. We are not able to give a complete axiomatization for the whole set of expressions (and we conjecture that it is not possible), so we restrict to the subset of $\mathcal{E}$ consisting of *guarded expressions* only. An expression is guarded if for each of its subexpression of the form $\mu_X F$, the variable X is guarded in F (cf. Definition 1).

First let us analyze the system $\mathcal{A}_s$. All axioms except for **R2-3** are still valid for $\simeq$. **R3** is not needed because it deals with unguarded expressions. We can reuse **R2** by requiring X to be (strongly) guarded, so we get **R2′** in Table 4. To establish the system $\mathcal{A}_o$ for $\simeq$, we use five τ-laws, **T1-5** in Table 4, to abstract away invisible actions. Note that **T1** and **T2** together constitute the probabilistic version of Milner's second τ-law ([27] page 231). **T3** and **T4** are the probabilistic extensions of Milner's third and first τ-laws, respectively. The extra rule **T5** has no nonprobabilistic counterpart in CCS, but it plays an important role in the proof of Theorem 8. As in [7] the axiom **C** is needed because we use combined transitions when defining observational equivalence.

Theorem 5 (Soundness of $\mathcal{A}_o$). *If $\mathcal{A}_o \vdash E = F$ then $E \simeq F$.*

Proof. The rules **R2′** and **T5** are proved to be sound in Proposition 5 (its proof is detailed in Appendix C). The soundness of **C** and **T1-4** is straightforward. □

For the completeness proof, it is convenient to use the following saturation property, which relates operational semantics to term transformation, and which can be shown by using the probabilistic τ-laws **T1-4** and the axiom **C**.

Lemma 3 (Saturation). *Suppose there is no parallel composition in E.*

1. *If $E \stackrel{u}{\Longrightarrow} \eta$ with $\eta = \{E_i : p_i\}_i$, then $\mathcal{A}_o \vdash E = E + u.\bigoplus_i p_i E_i$;*
2. *If $E \stackrel{u}{\Longrightarrow}_c \eta$ with $\eta = \{E_i : p_i\}_i$, then $\mathcal{A}_o \vdash E = E + u.\bigoplus_i p_i E_i$;*
3. *If $E \stackrel{X}{\Longrightarrow} \{\mathbf{0} : 1\}$ then $\mathcal{A}_o \vdash E = E + X$.*

T1	$\tau.\bigoplus_i p_i(E_i + X) = X + \tau.\bigoplus_i p_i(E_i + X)$
T2	$\tau.\bigoplus_i p_i(E_i + u.\bigoplus_j p_{ij}.E_{ij}) + u.\bigoplus_{i,j} p_i p_{ij}.E_{ij}$ $= \tau.\bigoplus_i p_i(E_i + u.\bigoplus_j p_{ij}.E_{ij})$
T3	$u.\bigoplus_i p_i(E_i + \tau.\bigoplus_j p_{ij}.E_{ij}) + u.\bigoplus_{i,j} p_i p_{ij}.E_{ij}$ $= u.\bigoplus_i p_i(E_i + \tau.\bigoplus_j p_{ij}.E_{ij})$
T4	$u.(p\tau.E \oplus \bigoplus_i p_i E_i) = u.(pE \oplus \bigoplus_i p_i E_i)$
T5	If $\tau.E = \tau.E + F$ and $\tau.F = \tau.F + E$ then $\tau.E = \tau.F$.
R2′	If $E = F\{E/X\}$, X guarded in F, then $E = \mu_X F$
C	$\sum_{i\in 1..n} u.\bigoplus_j p_{ij}E_{ij} = \sum_{i\in 1..n} u.\bigoplus_j p_{ij}E_{ij} + u.\bigoplus_{i\in 1..n}\bigoplus_j r_i p_{ij}E_{ij}$ with $\sum_{i\in 1..n} r_i = 1$.

Table 4. Some laws for the axiom system $\mathcal{A}_o$

Proof. The first and third clauses are proved by transition induction on the inference $E \stackrel{u}{\Longrightarrow} \eta$; the second clause is a corollary of the first one. □

Below we state two simple properties of weak combined transitions. They will be used in proving Theorem 8.

Lemma 4. *1. If $E \stackrel{\hat{u}}{\Longrightarrow}_c \eta$ then $\tau.E \stackrel{u}{\Longrightarrow}_c \eta$;*
2. If $E \stackrel{X}{\Longrightarrow}_c \{\mathbf{0}:1\}$ then $E \stackrel{X}{\Longrightarrow} \{\mathbf{0}:1\}$.

Proof. Trivial. □

Lemma 5. *If $E \stackrel{\hat{u}}{\Longrightarrow}_c \{E_i : p_i\}_i$ then $\mathcal{A}_o \vdash \tau.E = \tau.E + u.\bigoplus_i p_i E_i$.*

Proof. It follows from Lemma 4 and Lemma 3. □

To show the completeness of $\mathcal{A}_o$, we need some notations. Given a standard equation set $S : \widetilde{X} = \widetilde{H}$, which has free variables $\widetilde{W}$, we define the relations $\stackrel{\alpha}{\longrightarrow}_S \subseteq \widetilde{X} \times \mathcal{P}(\widetilde{X})$ (recall that the notation $\mathcal{P}(V)$ represents all distributions on V) as $X_i \stackrel{\alpha}{\longrightarrow}_S \eta$ iff $H_i \stackrel{\alpha}{\longrightarrow} \eta$. From $\stackrel{\alpha}{\longrightarrow}_S$ we can define the weak transition $\stackrel{\alpha}{\Longrightarrow}_S$ in the same way as in Section 3. We shall call S *guarded* if there is no X_i s.t. $X_i \stackrel{X_i}{\Longrightarrow}_S \{\mathbf{0}:1\}$. The variable W is *guarded* in S if it is not the case that $X_1 \stackrel{W}{\Longrightarrow}_S \{\mathbf{0}:1\}$.

For guarded expressions, the equational characterization theorem and the unique solution theorem given in last section can now be refined, as done in [27].

Theorem 6 (Equational characterization II). *Each guarded expression E with free variables in $\widetilde{W}$ provably satisfies a standard guarded equation set S with free variables in $\widetilde{W}$. Moreover, if W is guarded in E then W is guarded in S.*

Proof. By induction on the structure of E. Consider the case that $E \equiv u.\bigoplus_{i\in I} p_i E_i$. For each $i \in I$, let X_i be the distinguished variable of the equation set S_i for E_i. We can define S as $\{X = u.\bigoplus_{i\in I} p_i X_i\} \cup \bigcup_{i\in I} S_i$, with the new variable X distinguished. All other cases are the same as in [27]. For the case that $E \equiv F \mid F'$, the arguments are similar to those in Theorem 3. $\square$

Theorem 7 (Unique solution of equations II). *If S is a guarded equation set with free variables in $\widetilde{W}$, then there is an expression E which provably satisfies S. Moreover, if F provably satisfies S and has free variables in $\widetilde{W}$, then $\mathcal{A}_o \vdash E = F$.*

Proof. Nearly the same as the proof of Theorem 2, just replacing the recursion rule **R2** with **R2′**. $\square$

The following theorem plays a crucial role in proving the completeness of $\mathcal{A}_o$.

Theorem 8. *Let E provably satisfy S and F provably satisfy T, where both S and T are standard, guarded equation sets, and let $E \simeq F$. Then there is a standard, guarded equation set U satisfied by both E and F.*

Proof. Suppose that $\widetilde{X} = \{X_1, ..., X_m\}$, $\widetilde{Y} = \{Y_1, ..., Y_n\}$ and $\widetilde{W} = \{W_1, W_2, ...\}$ are disjoint sets of variables. Let

$$S : \widetilde{X} = \widetilde{H}$$

$$T : \widetilde{Y} = \widetilde{J}$$

with $fv(\widetilde{H}) \subseteq \widetilde{X} \cup \widetilde{W}$, $fv(\widetilde{J}) \subseteq \widetilde{Y} \cup \widetilde{W}$, and that there are expressions $\widetilde{E} = \{E_1, ..., E_m\}$ and $\widetilde{F} = \{F_1, ..., F_n\}$ with $E_1 \equiv E$, $F_1 \equiv F$, and $fv(\widetilde{E}) \cup fv(\widetilde{F}) \subseteq \widetilde{W}$, so that

$$\mathcal{A}_o \vdash \widetilde{E} = \widetilde{H}\{\widetilde{E}/\widetilde{X}\}$$

$$\mathcal{A}_o \vdash \widetilde{F} = \widetilde{J}\{\widetilde{F}/\widetilde{Y}\}.$$

Consider the least equivalence relation $\mathcal{R} \subseteq (\widetilde{X} \cup \widetilde{Y}) \times (\widetilde{X} \cup \widetilde{Y})$ such that

1. whenever $(Z, Z') \in \mathcal{R}$ and $Z \xrightarrow{\alpha} \eta$, then there exists η' s.t. $Z' \stackrel{\hat{\alpha}}{\Longrightarrow}_c \eta'$ and $\eta \equiv_{\mathcal{R}} \eta'$;
2. $(X_1, Y_1) \in \mathcal{R}$ and if $X_1 \xrightarrow{\alpha} \eta$ then there exists η' s.t. $Y_1 \stackrel{\alpha}{\Longrightarrow}_c \eta'$ and $\eta \equiv_{\mathcal{R}} \eta'$.

Clearly $\mathcal{R}$ is a weak probabilistic bisimulation on the transition system over $\widetilde{X} \cup \widetilde{Y}$, determined by $\rightarrow \stackrel{\text{def}}{=} \rightarrow_S \cup \rightarrow_T$. Now for two given distributions $\eta = \{X_i : p_i\}_{i\in I}$, $\eta' = \{Y_j : q_j\}_{j\in J}$, with $\eta \equiv_{\mathcal{R}} \eta'$, we introduce the following notations:

$$\begin{array}{rll} K_{\eta,\eta'} = & \{(i,j) \mid i \in I,\ j \in J,\ \text{and } (X_i, Y_j) \in \mathcal{R}\} & \\ \nu_i = & \sum\{p_{i'} \mid i' \in I,\ \text{and } (X_i, X_{i'}) \in \mathcal{R}\} & \text{for } i \in I \\ \nu_j = & \sum\{p_{j'} \mid j' \in J,\ \text{and } (Y_j, Y_{j'}) \in \mathcal{R}\} & \text{for } j \in J \end{array}$$

Since $\eta \equiv_{\mathcal{R}} \eta'$ it follows by definition that if $(i,j) \in K_{\eta,\eta'}$, for some η, η', then $\nu_i = \nu_j$. Thus we can define the expression

$$G_{\eta,\eta'} \stackrel{\text{def}}{=} \bigoplus_{(i,j)\in K_{\eta,\eta'}} \frac{p_i q_j}{\nu_i} Z_{ij}$$

which will play the same role as the expression $H_{f(i,j),f'(i',j')}$ in the proof of Theorem 4.

Based on the above $\mathcal{R}$ we choose a new set of variables $\widetilde{Z}$ such that

$$\widetilde{Z} = \{Z_{ij} \mid X_i \in \widetilde{X},\ Y_j \in \widetilde{Y} \text{ and } (X_i, Y_j) \in \mathcal{R}\}.$$

Furthermore, for each $Z_{ij} \in \widetilde{Z}$ we construct three auxiliary finite sets of expressions, denoted by A_{ij}, B_{ij} and C_{ij}, by the following procedure.

1. Initially the three sets are empty.
2. For each η with $X_i \xrightarrow{\alpha} \eta$, arbitrarily choose one (and only one — the same principle applies in other cases too) η' (if it exists) satisfying $\eta \equiv_{\mathcal{R}} \eta'$ and $Y_j \stackrel{\alpha}{\Longrightarrow}_c \eta'$. If $\alpha \in Act$ then we construct the expression $G_{\eta,\eta'}$ and update A_{ij} to be $A_{ij} \cup \{\alpha.G_{\eta,\eta'}\}$; if $\alpha = X$ for some X then we update A_{ij} to be $A_{ij} \cup \{X\}$. Similarly for each η' with $Y_j \xrightarrow{\alpha} \eta'$, arbitrarily choose one η (if it exists) satisfying $\eta \equiv_{\mathcal{R}} \eta'$ and $X_i \stackrel{\alpha}{\Longrightarrow}_c \eta$. If $\alpha \in Act$ then we construct the expression $G_{\eta,\eta'}$ and update A_{ij} to be $A_{ij} \cup \{\alpha.G_{\eta,\eta'}\}$; if $\alpha = X$ for some X then we update A_{ij} to be $A_{ij} \cup \{X\}$.
3. For each η with $X_i \xrightarrow{\tau} \eta$, arbitrarily choose one η' (if it exists) satisfying $\eta \equiv_{\mathcal{R}} \eta'$, $Y_j \Longrightarrow_c \eta'$ but not $Y_j \stackrel{\tau}{\Longrightarrow}_c \eta'$, construct the expression $G_{\eta,\eta'}$ and update B_{ij} to be $B_{ij} \cup \{\tau.G_{\eta,\eta'}\}$.
4. For each η' with $Y_j \xrightarrow{\tau} \eta'$, arbitrarily choose one η (if it exists) satisfying $\eta \equiv_{\mathcal{R}} \eta'$, $X_i \Longrightarrow_c \eta$ but not $X_i \stackrel{\tau}{\Longrightarrow}_c \eta$, construct $G_{\eta,\eta'}$ and update C_{ij} to be $C_{ij} \cup \{\tau.G_{\eta,\eta'}\}$.

Clearly the three sets constructed in this way are finite. Now we build a new equation set

$$U : \widetilde{Z} = \widetilde{L}$$

where U_{11} is the distinguished variable and

$$L_{ij} = \begin{cases} \sum_{G \in A_{ij}} G & \text{if } B_{ij} \cup C_{ij} = \emptyset \\ \tau.(\sum_{G \in A_{ij} \cup B_{ij} \cup C_{ij}} G) & \text{otherwise.} \end{cases}$$

We assert that E provably satisfies the equation set U. To see this, we choose expressions

$$G_{ij} = \begin{cases} E_i & \text{if } B_{ij} \cup C_{ij} = \emptyset \\ \tau.E_i & \text{otherwise} \end{cases}$$

and verify that $\mathcal{A}_o \vdash G_{ij} = L_{ij}\{\widetilde{G}/\widetilde{Z}\}$.

In the case that $B_{ij} \cup C_{ij} = \emptyset$, all those summands of $L_{ij}\{\widetilde{G}/\widetilde{Z}\}$ which are not variables are of the form:

$$u.\bigoplus_{(i,j)\in K_{\eta,\eta'}} \frac{p_i q_j}{\nu_i} E'_i$$

where $E'_i = E_i$ or $E'_i = \tau.E_i$ for each i. By **T4** we can prove that

$$u.\bigoplus_{(i,j)\in K_{\eta,\eta'}} \frac{p_i q_j}{\nu_i} E'_i = u.\bigoplus_{(i,j)\in K_{\eta,\eta'}} \frac{p_i q_j}{\nu_i} E_i.$$

Then by some arguments similar to those in Theorem 4, together with Lemma 3, we can show that

$$\mathcal{A}_o \vdash L_{ij}\{\widetilde{G}/\widetilde{Z}\} = H_i\{\widetilde{E}/\widetilde{X}\} = E_i.$$

On the other hand, if $B_{ij} \cup C_{ij} \neq \emptyset$, we let $C_{ij} = \{D_1, ..., D_o\}$ ($C_{ij} = \emptyset$ is a special case of the following argument) and $D = \sum_{l\in 1..o} D_l\{\widetilde{G}/\widetilde{Z}\}$. As in last case we can show that

$$\mathcal{A}_o \vdash L_{ij}\{\widetilde{G}/\widetilde{Z}\} = \tau.(H_i\{\widetilde{E}/\widetilde{X}\} + D).$$

For any l with $1 \leq l \leq o$, let $D_l\{\widetilde{G}/\widetilde{Z}\} = \tau.\bigoplus_k p_k E_k$. It is easy to see that $E_i \Longrightarrow_c \eta$ with $\eta = \{E_k : p_k\}_k$. So by Lemma 5 it holds that

$$\mathcal{A}_o \vdash \tau.E_i = \tau.E_i + D_l\{\widetilde{G}/\widetilde{Z}\}.$$

As a result we can infer

$$\mathcal{A}_o \vdash \tau.E_i = \tau.E_i + D = \tau.E_i + (E_i + D).$$

by Lemma 3. Similarly,

$$\mathcal{A}_o \vdash \tau.(E_i + D) = \tau.(E_i + D) + E_i.$$

Consequently it follows from **T5** that

$$\mathcal{A}_o \vdash \tau.E_i = \tau.(E_i + D) = \tau.(H_i\{\widetilde{E}/\widetilde{X}\} + D) = L_{ij}\{\widetilde{G}/\widetilde{Z}\}.$$

In the same way we can show that F provably satisfies U. At last U is guarded because S and T are guarded. □

Theorem 9 (Completeness of $\mathcal{A}_o$). *If E and F are guarded expressions and $E \simeq F$, then $\mathcal{A}_o \vdash E = F$.*

Proof. A direct consequence by combining Theorems 6, 8 and 7. □

In the axiom system $\mathcal{A}_o$ the rule **T5** deserves more explanations. For the two expressions F_1, F_2 given in Example 1 (cf. Section 4.2), we can derive the equality $\tau.F_1 = \tau.F_2$ by using **T5**. Alternatively, we could use the following axiom

$$\tau.E = \tau.(E + \tau.((1-p)E \oplus \textstyle\bigoplus_i pp_iE_i)) \qquad \text{where } E = \tau.(\tau.\textstyle\bigoplus_i p_iE_i + F)$$

which is sound and indeed derivable from **T5**. In fact, we could have introduced the cumbersome axiom in place of **T5** in the axiomatization for $\simeq$ — we would still be able to prove Theorem 8 and the completeness of the alternative axiomatization. In this paper we have chosen **T5** instead merely because it looks more elegant than the above axiom.

7 Conclusion and related work

We have proposed a probabilistic process calculus which combines both nondeterministic and probabilistic behavior in the style of Segala and Lynch's simple probabilistic automata. The calculus also admits a restricted form of parallel composition to allow for compositional reasoning of finite-state behaviors. We have presented sound and complete axiomatizations for two behavioral equivalences: strong bisimilarity and observational equivalence.

In CCS there are other static operators such as restriction and relabeling that are not studied in this paper. As parallel composition, these operators should be dealt with carefully. For example, the expression $\mu_X((a.X \mid \bar{a})\backslash a)$ appears to be guarded (cf. Definition 1), but actually it is strongly bisimilar to $\mu_X(\tau.X)$ thus should be deemed unguarded. When considering axiomtizations one tends to disallow this kind of expressions by imposing the constraint that free variables do not occur in the scope of static operators [11, 5].

As we said before, in this paper many concepts and proof techniques are inherited from [16, 15]. The main differences are as follows: (i) in this paper we have added a parallel composition operator to our probabilistic process calculus; (ii) to define the operational semantics of this operator we restrict ourself to simple probabilistic automata, while the results of [16, 15] are valid for all probabilistic automata; (iii) besides strong bisimilarity and observational equivalence, in [16, 15] we also axiomatized two other equivalences: a strong probabilistic bisimilarity and a divergency-sensitive equivalence. We think that it should be possible to adapt those results to the framework of this paper.

In [25] and [27] Milner gave complete axiomatizations for strong bisimilarity and observational equivalence, respectively, for a core CCS [26]. Our results in Section 5 and Section 6 extend [25] and [27] (for guarded expressions) respectively, to a strictly larger language with a probabilistic choice and a parallel composition operator.

Bandini and Segala [7] axiomatized two strong and two weak equivalences for a language similar to the fragment of our calculus without recursion and parallelism. They considered two types of semantics. In both cases, their completeness proofs are done by structural induction on processes, which is, of course, impossible in our setting because of recursion.

Giacalone, Jou and Smolka [18] axiomatized strong bisimulation for a fully probabilistic (i.e. without nondeterminism) extension of Milner's SCCS [24], where parallel composition is synchronous. In contrast, we consider an asynchronous parallel composition and we admit nondeterminism.

Baeten, Bergstra and Smolka [4] proposed a probabilistic ACP by introducing a parameterized composition. They considered generative models, which are fully probabilistic, and axiomatized strong probabilistic bisimilarity for finite processes (without recursion).

Andova [3] studied a different version of probabilistic ACP by allowing nondeterminism and a parallel composition which is not parameterized. She provided a sound and complete axiomatization for strong probabilistic bisimilarity in the case of finite processes. She also gave some sound verification rules for probabilistic branching bisimilarity in a fully probabilistic model without parallelism.

Strong probabilistic bisimilarity was also axiomatized by Stark and Smolka in [31]. They gave a probabilistic version of the results of [25]. However, neither nondeterminism nor parallelism is considered. Later the same calculus was studied in [1], which uses some axioms from iteration algebra to characterize recursion.

In the nonprobabilistic setting, Bergstra and Klop [10] established a sound and complete axiomatization for regular processes with τ-steps and free merge (which allows arbitrary interleaving but no communication). They required that free merge should not appear in the body of any recursive expression. To give a linearization algorithm for pCRL, Groote, Ponse and Usenko adopted a similar restriction for parallel composition [19]. Usenko extended this result to μCRL in his thesis [33]. In this paper our parallel composition operator allows communication and it can appear in the body of a recursive expression, though only in a restricted way. For example, the expression

$$\mu_X(a.X + a.\mu_Y(b.Y) \mid \bar{a}.\mu_Z(c.Z))$$

is a legal expression in our calculus and we are able to manipulate it in our axiom systems.

Baeten and Bravetti [5] axiomatized observational equivalence in a generic process algebra. Their restriction enforced to parallel composition is the same as ours in spirit. Interestingly, they reduced two of Milner's axioms for unguarded recursion [27] to just a single axiom. It remains open whether their results can be adapted to a probabilistic setting. Similarly, it might be interesting to extend van Glabbeek's axiomatization for branching congruence [34] to a probabilistic setting. We believe that the general proof schema laid out in this paper could be reused for branching congruence, but the soundness proof of some axioms such as $\mathbf{R2}'$ would be very complicated because, besides the probabilistic and nondeterministic features, we need to consider the branching structure of processes, which is ignored in observational congruence.

Christensen, Hirshfeld and Moller studied a class of standard form CCS [13] where open expressions are allowed to be put in parallel composition. In that language, strong bisimulation is decidable and they obtained a sound and complete sequent based equational theory, but observational equivalence is semi-decidable [12]. In this paper we follow [25, 27] and characterize recursion by laws concerning the explicit fixed point operator μ, while we capture by τ-laws the difference between observational equivalence and strong bisimulation.

Several works in the literature address the problem of how to define appropriate parallel composition operators on various probabilistic models, see [14] for more discussions and [30] for a good survey. In this paper, we work at simple probabilistic automata where parallel composition is easy to define (cf. Table 1).

References

1. L. Aceto, Z. Ésik, and A. Ingólfsdóttir. Equational axioms for probabilistic bisimilarity (preliminary report). Technical Report RS-02-6, BRICS, 2002.
2. L. Aceto and W. J. Fokkink. The quest for equational axiomatizations of parallel composition: Status and open problems. In *Proceedings of the Workshop on Algebraic Process Calculi: The First Twenty Five Years and Beyond*, BRICS Notes Series, 2005. To appear.
3. S. Andova. *Probabilistic Process Algebra*. PhD thesis, Eindhoven University of Technology, 2002.
4. J. C. M. Baeten, J. A. Bergstra, and S. A. Smolka. Axiomatizing probabilistic processes: ACP with generative probabilities. *Information and Computation*, 121(2):234–255, 1995.
5. J. C. M. Baeten and M. Bravetti. A ground-complete axiomatization of finite state processes in process algebra. In *Proceedings of the 16th International Conference on Concurrency Theory*, Lecture Notes in Computer Science. Springer, 2005. To appear.
6. J. C. M. Baeten and W. P. Weijland. *Process Algebra*, volume 18 of *Cambridge Tracts in Theoretical Computer Science*. Cambridge University Press, 1990.
7. E. Bandini and R. Segala. Axiomatizations for probabilistic bisimulation. In *Proceedings of the 28th International Colloquium on Automata, Languages and Programming*, volume 2076 of *Lecture Notes in Computer Science*, pages 370–381. Springer, 2001.
8. J. A. Bergstra and J. W. Klop. Process algebra for synchronous communications. *Information and Control*, 60:109–137, 1984.
9. J. A. Bergstra and J. W. Klop. Verification of an alternating bit protocol by means of process algebra. In *Proceedings of the International Spring School on Mathematical Methods of Specification and Synthesis of Software Systems*, volume 215 of *Lecture Notes in Computer Science*, pages 9–23. Springer, 1986.
10. J. A. Bergstra and J. W. Klop. A complete inference system for regular processes with silent moves. In *Proceedings of Logic Colloquium 1986*, pages 21–81. North Holland, Amsterdam, 1988.
11. M. Bravetti and R. Gorrieri. Deciding and axiomatizing weak ST bisimulation for a process algebra with recursion and action refinement. *ACM Transactions on Computational Logic*, 3(4):465–520, 2002.
12. S. Christensen. *Decidability and Decomposition in Process Algebras*. PhD thesis, University of Edinburgh, 1993.
13. S. Christensen, Y. Hirshfeld, and F. Moller. Decidable subsets of ccs. *Computer Journal*, 37(4):233–242, 1994.
14. P. R. D'Argenio, H. Hermanns, and J.-P. Katoen. On generative parallel composition. *Electronic Notes in Theoretical Computer Science*, 22, 1999.
15. Y. Deng. *Axiomatisations and types for probabilistic and mobile processes*. PhD thesis, Ecole des Mines de Paris, 2005.
16. Y. Deng and C. Palamidessi. Axiomatizations for probabilistic finite-state behaviors. In *Proceedings of the 8th International Conference on Foundations of Software Science and Computation Structures*, volume 3441 of *Lecture Notes in Computer Science*, pages 110–124. Springer, 2005.
17. W. J. Fokkink, J. F. Groote, J. Pang, B. Badban, and J. C. van de Pol. Verifying a sliding window protocol in μCRL. In *10th Conference on Algebraic Methodology and Software Technology, Proceedings*, volume 3116 of *Lecture Notes in Computer Science*, pages 148–163. Springer, 2004.

18. A. Giacalone, C.-C. Jou, and S. A. Smolka. Algebraic reasoning for probabilistic concurrent systems. In *Proceedings of IFIP WG 2.2/2.3 Working Conference on Programming Concepts and Methods*, pages 453–459, 1990.
19. J. F. Groote, A. Ponse, and Y. S. Usenko. Linearization in parallel pCRL. *Journal of Logic and Algebraic Programming*, 48(1-2):39–72, 2001.
20. M. Hennessy and R. Milner. Algebraic laws for nondeterminism and concurrency. *Journal of ACM*, 32:137–161, 1985.
21. C. A. R. Hoare. *Communicating Sequential Processes*. Prentice Hall, 1985.
22. K. G. Larsen and A. Skou. Bisimulation through probabilistic testing. *Information and Computation*, 94(1):1–28, 1991.
23. N. A. Lynch, I. Saias, and R. Segala. Proving time bounds for randomized distributed algorithms. In *Proceedings of the 13th Annual ACM Symposium on the Principles of Distributed Computing*, pages 314–323, 1994.
24. R. Milner. Calculi for synchrony and asynchrony. *Theoretical Computer Science*, 25:267–310, 1983.
25. R. Milner. A complete inference system for a class of regular behaviours. *Journal of Computer and System Science*, 28:439–466, 1984.
26. R. Milner. *Communication and Concurrency*. Prentice-Hall, 1989.
27. R. Milner. A complete axiomatisation for observational congruence of finite-state behaviours. *Information and Computation*, 81:227–247, 1989.
28. A. Pogosyants, R. Segala, and N. A. Lynch. Verification of the randomized consensus algorithm of Aspnes and Herlihy: a case study. *Distributed Computing*, 13(3):155–186, 2000.
29. R. Segala and N. A. Lynch. Probabilistic simulations for probabilistic processes. In *Proceedings of the 5th International Conference on Concurrency Theory*, volume 836 of *Lecture Notes in Computer Science*, pages 481–496. Springer, 1994.
30. A. Sokolova and E. P. de Vink. Probabilistic automata: system types, parallel composition and comparison. In *Validation of Stochastic Systems: A Guide to Current Research*, volume 2925 of *Lecture Notes in Computer Science*, pages 1–43. Springer, 2004.
31. E. W. Stark and S. A. Smolka. A complete axiom system for finite-state probabilistic processes. In *Proof, language, and interaction: essays in honour of Robin Milner*, pages 571–595. MIT Press, 2000.
32. M. Stoelinga and F. Vaandrager. Root contention in IEEE 1394. In *Proceedings of the 5th International AMAST Workshop on Formal Methods for Real-Time and Probabilistic Systems*, volume 1601 of *Lecture Notes in Computer Science*, pages 53–74. Springer, 1999.
33. Y. S. Usenko. *Linearization in μCRL.* PhD thesis, Edindhoven University of Technology, 2002.
34. R. J. van Glabbeek. A complete axiomatization for branching bisimulation congruence of finite-state behaviours. In *Proceedings of the 18th International Symposium on Mathematical Foundations of Computer Science*, volume 711 of *Lecture Notes in Computer Science*, pages 473–484. Springer, 1993.

Appendix

A Transitivity of Weak Bisimulation

It seems natural to define weak bisimulation in the following way.

Definition (Tentative). *An equivalence relation $\mathcal{R} \subseteq \mathcal{E} \times \mathcal{E}$ is a* weak bisimulation *if $E\ \mathcal{R}\ F$ implies:*

- *whenever $E \xrightarrow{\alpha} \eta_1$, there exists η_2 such that $F \stackrel{\hat{\alpha}}{\Longrightarrow} \eta_2$ and $\eta_1 \equiv_{\mathcal{R}} \eta_2$.*

E and F are weak bisimilar*, written $E \asymp F$, whenever there exists a weak bisimulation $\mathcal{R}$ s.t. $E\ \mathcal{R}\ F$.*

Unfortunately the above definition is incorrect because it defines a relation which is not transitive. To see this, consider the following expressions:

$$\begin{aligned}
R &\stackrel{\text{def}}{=} \tau.(\tfrac{1}{2}a \oplus \tfrac{1}{2}b)\\
E &\stackrel{\text{def}}{=} \tau.(\tfrac{1}{2}R \oplus \tfrac{1}{2}R) + \tau.(\tfrac{1}{2}R \oplus \tfrac{1}{4}a \oplus \tfrac{1}{4}b)\\
F &\stackrel{\text{def}}{=} \tau.(\tfrac{1}{2}R \oplus \tfrac{1}{2}R)\\
G &\stackrel{\text{def}}{=} \tau.R
\end{aligned}$$

It can be checked that $E \asymp F$ and $F \asymp G$ but $E \not\asymp G$. The transition $E \xrightarrow{\tau} \eta$ cannot be matched by any of the three possible weak transitions from $G : G \Longrightarrow \eta_i$ $(i = 1, 2, 3)$, where $\eta_1 = \{G : 1\}$, $\eta_2 = \{R : 1\}$ and $\eta_3 = \{a : \frac{1}{2}, b : \frac{1}{2}\}$, since neither η_1 nor η_2 nor η_3 is equivalent to η.

To obtain a transitive weak bisimilarity, we have used combined weak transitions in Definition 4.

B Proof of Proposition 4

Lemma 6. *If $fv(E) \subseteq \{\widetilde{X}, Z\}$ and $Z \notin fv(\widetilde{F})$, then*

$$E\{E'/Z\}\{\widetilde{F}/\widetilde{X}\} \equiv E\{\widetilde{F}/\widetilde{X}\}\{E'\{\widetilde{F}/\widetilde{X}\}/Z\}.$$

Proof. By induction on the structure of E. □

Lemma 7. *Let $\eta = r_1\eta_1 + ... + r_n\eta_n$ and $\eta' = r_1\eta'_1 + ... + r_n\eta'_n$ with $\sum_{i\in 1..n} r_i = 1$. If $\eta_i \equiv_{\mathcal{R}} \eta'_i$ for each $i \leq n$, then $\eta \equiv_{\mathcal{R}} \eta'$.*

Proof. For any $V \in \mathcal{E}/\mathcal{R}$, we have

$$\eta(V) = \sum_{i\in 1..n} r_i\eta_i(V) = \sum_{i\in 1..n} r_i\eta'_i(V) = \eta'(V).$$

Therefore $\eta \equiv_{\mathcal{R}} \eta'$ by definition. □

Proposition 6. *If $E \sim F$ then $E \mid G \sim F \mid G$.*

Proof. We show that the relation $\sim^{|}$ is a strong bisimulation. There are four cases, among which we consider two of them, the others are similar.

Case 1: Suppose $\eta_1 = \{E_i \mid G : p_i\}_i$ and $E \mid G \xrightarrow{\alpha} \eta_1$ is derived from the transition $E \xrightarrow{\alpha} \theta_1 = \{E_i : p_i\}_i$. Since $E \sim F$, there exists θ_2 such that $F \xrightarrow{\alpha} \theta_2$ and $\theta_1 \equiv_\sim \theta_2$. Let $\theta_2 = \{F_j : q_j\}_j$, by rule par we have the transition $F \mid G \xrightarrow{\alpha} \{F_j \mid G : q_j\}_j = \eta_2$. Let $\theta = \{G : 1\}$, then we have $\eta_1 = \theta_1 \mid \theta$ and $\eta_2 = \theta_2 \mid \theta$. By Lemma 2 it follows that $\eta_1 \equiv_{\sim^|} \eta_2$.

Case 2: Suppose $E \xrightarrow{a} \theta_1$, $G \xrightarrow{\bar{a}} \theta$, and $E \mid G \xrightarrow{\tau} \eta_1$ with $\eta_1 = \theta_1 \mid \theta$. Since $E \sim F$, there exists θ_2 such that $F \xrightarrow{a} \theta_2$ and $\theta_1 \equiv_\sim \theta_2$. By rule com we have the transition $F \mid G \xrightarrow{\tau} \eta_2$ with $\eta_2 = \theta_2 \mid \theta$. By Lemma 2 it follows that $\eta_1 \equiv_{\sim^|} \eta_2$. $\square$

Proposition 7. *If $E \sim F$ then $E\{G/X\} \sim F\{G/X\}$ for any $G \in \mathcal{E}$.*

Proof. Similar to the proof of Proposition 13, which is detailed in next section. $\square$

Proposition 8. *If $E \sim F$ then $\mu_X E \sim \mu_X F$.*

Proof. Let $\rho \stackrel{\text{def}}{=} \{\mu_X E/X\}$ and $\sigma \stackrel{\text{def}}{=} \{\mu_X F/X\}$. We show that the relation

$$\mathcal{R} = \{(G\rho, G\sigma) \;\big|\; fv(G) \subseteq \{X\}\}$$

is a strong bisimulation up to $\sim$. Because of symmetry we only show the assertion:

"if $G\rho \xrightarrow{\alpha} \eta_1$ then there exists η_2 s.t. $G\sigma \xrightarrow{\alpha} \eta_2$ and $\eta_1 \equiv_{\mathcal{R}_\sim} \eta_2$"

by induction on the depth of the inference $G\sigma \to \eta_1$. There are several cases, depending on the structure of G.

1. $G \equiv X$: Then $G\rho \equiv \mu_X E \xrightarrow{\alpha} \eta_1$ and there is a shorter inference $E\rho \xrightarrow{\alpha} \eta_1$. By induction hypothesis there is some θ s.t. $E\sigma \xrightarrow{\alpha} \theta$ and $\eta_1 \equiv_{\mathcal{R}_\sim} \theta$. Since $E \sim F$ we know that $E\sigma \sim F\sigma$ by Proposition 7. Hence there exists some η_2 s.t. $F\sigma \xrightarrow{\alpha} \eta_2$ and $\theta \equiv_\sim \eta_2$. By Lemma 1 and the transitivity of $\equiv_{\mathcal{R}_\sim}$ it follows that $\eta_1 \equiv_{\mathcal{R}_\sim} \eta_2$.
2. $G \equiv u.\bigoplus_i p_i G_i$: Then we have $G\rho \xrightarrow{u} \eta_1 \equiv \{G_i\rho : p_i\}_i$ and $G\sigma \xrightarrow{u} \eta_2 \equiv \{G_i\sigma : p_i\}_i$. Since $G_i\rho \;\mathcal{R}\; G_i\sigma$, it is easy to see that $\eta_1 \equiv_{\mathcal{R}_\sim} \eta_2$.
3. $G \equiv \sum_{i \in 1..m} G_i$: If $G\rho \xrightarrow{\alpha} \eta_1$, then $G_j\rho \xrightarrow{\alpha} \eta_1$ for some $j \in 1..m$, by a shorter inference. By induction hypothesis we have that $G_j\sigma \xrightarrow{\alpha} \eta_2$ such that $\eta_1 \equiv_{\mathcal{R}_\sim} \eta_2$.
4. $G \equiv \mu_Y G'$: If $G\rho \xrightarrow{\alpha} \eta_1$ then $G'\rho\{G\rho/Y\}$ by a shorter inference. Since $G'\rho\{G\rho/Y\} \equiv (G'\{G/Y\})\rho$ we have that $(G'\{G/Y\})\rho \xrightarrow{\alpha} \eta_1$. By induction hypothesis it follows that $(G'\{G/Y\})\sigma \xrightarrow{\alpha} \eta_2$ with $\eta_1 \equiv_{\mathcal{R}_\sim} \eta_2$. Thus $G'\sigma\{G\sigma/Y\} \xrightarrow{\alpha} \eta_2$, which implies $G\sigma \xrightarrow{\alpha} \eta_2$ by the rule rec.

5. $G \equiv G_1 \mid G_2$: Suppose $G\rho \xrightarrow{\alpha} \eta_1$. Depending on the last rule used for deriving the transition, there are four cases. We consider one typical case where the last rule used is com. So we have the transitions $G_1\rho \xrightarrow{a} \theta_1$, $G_2\rho \xrightarrow{\bar{a}} \theta_1'$ and $G\rho \xrightarrow{\tau} \eta_1$ with $\eta_1 = \theta_1 \mid \theta_1'$. By induction hypothesis we have the simulating transitions $G_1\sigma \xrightarrow{a} \theta_2$ and $G_2\sigma \xrightarrow{\bar{a}} \theta_2'$ such that $\theta_1 \equiv_{\mathcal{R}_\sim} \theta_2$ and $\theta_1' \equiv_{\mathcal{R}_\sim} \theta_2'$. By rule com we infer that $G\sigma \xrightarrow{\tau} \eta_2$ with $\eta_2 = \theta_2 \mid \theta_2'$. It is easy to see that $\mathcal{R}$ is closed under parallel composition (here we need the condition of composing closed expressions). By Proposition 6 we know that $\sim$ is also closed under parallel composition. It follows that $\mathcal{R}_\sim$ is closed under parallel composition as well. Therefore by Corollary 1 we can derive that $\eta_1 \equiv_{\mathcal{R}_\sim} \eta_2$.

$\square$

Proposition 9 (Congruence). *If* $\widetilde{E} \sim \widetilde{F}$ *then*

1. $u.\bigoplus_i p_i E_i \sim u.\bigoplus_i p_i F_i$;
2. $\sum_i E_i \sim \sum_i F_i$;
3. $E_1 \mid E_2 \sim F_1 \mid F_2$;
4. $\mu_X E_1 \sim \mu_X F_1$.

Proof. The first two clauses are easy to prove; the last two follow from Proposition 6 and Proposition 8 respectively. $\square$

Proposition 10. $\mu_X E \sim E\{\mu_X E/X\}$.

Proof. Observe that $\mu_X E \xrightarrow{\alpha} \eta$ iff $E\{\mu_X E/X\} \xrightarrow{\alpha} \eta$. $\square$

Proposition 11. $\mu_X(E+X) \sim \mu_X E$

Proof. Let $\rho \stackrel{\text{def}}{=} \{\mu_X(E+X)/X\}$ and $\sigma \stackrel{\text{def}}{=} \{\mu_X E/X\}$. We show that the relation

$$\mathcal{R} = \{(G\rho, G\sigma \;\big|\; fv(G \subseteq \{X\}))\}$$

is a strong bisimulation up to $\sim$. We prove the following two assertions:

1. If $G\rho \xrightarrow{\alpha} \eta_1$ then $G\sigma \xrightarrow{\alpha} \eta_2$ and $\eta_1 \equiv_{\mathcal{R}_\sim} \eta_2$;
2. If $G\sigma \xrightarrow{\alpha} \eta_2$ then $G\rho \xrightarrow{\alpha} \eta_1$ and $\eta_1 \equiv_{\mathcal{R}_\sim} \eta_2$.

The proof is carried out by induction on transitions, similar to the proof of Proposition 8. Here we only consider the case that $G \equiv X$.

1. If $G\rho \equiv X\rho \xrightarrow{\alpha} \eta_1$ then $(E+X)\rho \xrightarrow{\alpha} \eta_1$ by a shorter inference. By induction hypothesis it follows that $(E+X)\sigma \xrightarrow{\alpha} \eta_2$ and $\eta_1 \equiv_{\mathcal{R}_\sim} \eta_2$. Then either $E\sigma \xrightarrow{\alpha} \eta_2$ or $X\sigma \xrightarrow{\alpha} \eta_2$. From the first case we can also obtain $X\sigma \xrightarrow{\alpha} \eta_2$ by rule rec. Therefore in both cases we have $G\sigma \xrightarrow{\alpha} \eta_2$.
2. If $G\sigma \equiv X\sigma \xrightarrow{\alpha} \eta_2$ then $E\sigma \xrightarrow{\alpha} \eta_2$ by a shorter inference. By induction hypothesis it follows that $E\rho \xrightarrow{\alpha} \eta_1$ with $\eta_1 \equiv_{\mathcal{R}_\sim} \eta_2$. By the rule nsum we derive $(E+X)\rho \xrightarrow{\alpha} \eta_1$. By rec we get the required result that $G\rho \equiv X\rho \xrightarrow{\alpha} \eta_1$.

□

Lemma 8. *Suppose $fv(G) \subseteq \{X\}$ and all free occurrences of X in G are weakly guarded. If $G\{E/X\} \xrightarrow{\alpha} \eta_1$ with $\eta_1 \equiv \{G_i : p_i\}_i$ then G_i takes the form $G'_i\{E/X\}$; Moreover, for any F, $G\{F/X\} \xrightarrow{\alpha} \eta_2$ with $\eta_2 \equiv \{G'_i\{F/X\} : p_i\}_i$ and $\eta_1 \equiv_{\mathcal{R}_\sim} \eta_2$ where*

$$\mathcal{R} = \{(G\{E/X\}, G\{F/X\}) \mid G \in \mathcal{E} \textit{ and } fv(G) \subseteq \{X\}\}.$$

Proof. By transition induction. □

Proposition 12. *If $E \sim F\{E/X\}$, where all occurrences of X in F are weakly guarded, then $E \sim \mu_X F$.*

Proof. Similar to the proof of Proposition 8. Now we take $\mathcal{R}$ as:

$$\mathcal{R} = \{(G\{E/X\}, G\{\mu_X F/X\}) \mid G \in \mathcal{E} \text{ and } fv(G) \subseteq \{X\}\}$$

Let us consider the case that $G \equiv X$. Suppose $E \xrightarrow{\alpha} \eta_1$. Since $E \sim F\{E/X\}$, there exists θ s.t. $F\{E/X\} \xrightarrow{\alpha} \theta$ and $\eta_1 \equiv_\sim \theta$. By Lemma 8 there exists η_2 s.t. $F\{\mu_X F/X\} \xrightarrow{\alpha} \eta_2$ and $\theta \equiv_{\mathcal{R}_\sim} \eta_2$. By rule rec we have $\mu_X F \xrightarrow{\alpha} \eta_2$. By Lemma 1 and the transitivity of $\equiv_{\mathcal{R}_\sim}$, we have $\eta_1 \equiv_{\mathcal{R}_\sim} \eta_2$. With similar reasoning, one can show that if $\mu_X F \xrightarrow{\alpha} \eta_2$ there exists η_1 s.t. $E \xrightarrow{\alpha} \eta_1$ and $\eta_1 \equiv_{\mathcal{R}_\sim} \eta_2$. □

At last Proposition 4 is proved by collecting all the results in Propositions 9-12.

C Proof of Proposition 5

Lemma 9. *1. If $E \xrightarrow{u} \{E_i : p_i\}_i$ then $E\{G/X\} \xrightarrow{u} \{E_i\{G/X\} : p_i\}_i$;*
2. If $E \xRightarrow{u} \{E_i : p_i\}_i$ then $E\{G/X\} \xRightarrow{u} \{E_i\{G/X\} : p_i\}_i$;
3. If $E \xRightarrow{u}_c \{E_i : p_i\}_i$ then $E\{G/X\} \xRightarrow{u}_c \{E_i\{G/X\} : p_i\}_i$;
4. If $E \xRightarrow{\hat{u}}_c \{E_i : p_i\}_i$ then $E\{G/X\} \xRightarrow{\hat{u}}_c \{E_i\{G/X\} : p_i\}_i$.

Proof. Straightforward by induction on inference. □

Lemma 10. *1. If $E \xrightarrow{X} \{\mathbf{0} : 1\}$ and $G \xrightarrow{\alpha} \eta$ then $E\{G/X\} \xrightarrow{\alpha} \eta$.*
2. If $E \xRightarrow{X} \{\mathbf{0} : 1\}$ and $G \xrightarrow{\alpha} \eta$ then $E\{G/X\} \xRightarrow{\alpha} \eta$.

Proof. Straightforward by examining the structure of E. □

Lemma 11. *If $E\{G/X\} \xrightarrow{\alpha} \eta$ then one of the following two cases holds.*

1. *$E \xrightarrow{X} \{\mathbf{0} : 1\}$ and $G \xrightarrow{\alpha} \eta$;*
2. *$\eta = \{E_i\{G/X\} : p_i\}_i$ and $E \xrightarrow{\alpha} \{E_i : p_i\}_i$.*

Proof. By induction on the depth of the inference of $E\{G/X\} \xrightarrow{\alpha} \eta$. □

Proposition 13. *If $E \approx F$ then $E\{G/X\} \approx F\{G/X\}$ for any $G \in \mathcal{E}$.*

Proof. Consider the relation $\mathcal{R} = \{(E\{G/X\}, F\{G/X\}) \mid E, F \in \mathcal{E}$ and $E \approx F\}$. Since $\approx$ is an equivalence relation, it follows that $\mathcal{R}$ is also an equivalence relation. So if we can show the assertion:
"If $E\{G/X\} \xrightarrow{\alpha} \eta_1$ then there exists η_2 s.t. $F\{G/X\} \stackrel{\hat{\alpha}}{\Longrightarrow}_c \eta_2$ and $\eta_1 \equiv_{\mathcal{R}} \eta_2$"
then it follows from Definition 4 that $\mathcal{R}$ is a weak probabilistic bisimulation.

We now prove the above assertion. From Lemma 11 we know that there are two possibilities:

1. $E \xrightarrow{X} \{\mathbf{0} : 1\}$ and $G \xrightarrow{\alpha} \eta_1$. Thus $F \stackrel{X}{\Longrightarrow}_c \{\mathbf{0} : 1\}$ because $E \approx F$. From Lemma 4 we know that $F \stackrel{X}{\Longrightarrow} \{\mathbf{0} : 1\}$. By Lemma 10 it follows that $F\{G/X\} \stackrel{\alpha}{\Longrightarrow} \eta_1$. We can simply take η_1 as η_2 and finish this case.
2. $\eta_1 = \{E_i\{G/X\} : p_i\}$ and $E \xrightarrow{\alpha} \theta_1 = \{E_i : p_i\}_i$. Since $E \approx F$ there exists $\theta_2 = \{F_j : q_j\}_j$ s.t. $F \stackrel{\hat{\alpha}}{\Longrightarrow}_c \theta_2$ and $\theta_1 \equiv_{\approx} \theta_2$. By Lemma 9 we can derive $F\{G/X\} \stackrel{\hat{\alpha}}{\Longrightarrow}_c \eta_2 = \{F_j\{G/X\} : q_j\}_j$. Observe that for any $E', F' \in \{E_i\}_i \cup \{F_j\}_j$ it holds that $E' \approx F'$ iff $E'\{G/X\} \; \mathcal{R} \; F'\{G/X\}$. Hence it follows from $\theta_1 \equiv_{\approx} \theta_2$ that $\eta_1 \equiv_{\mathcal{R}} \eta_2$ and we complete the proof of this case.

□

Proposition 14. *If $E \simeq F$ then $E\{G/X\} \simeq F\{G/X\}$ for any $G \in \mathcal{E}$.*

Proof. Due to symmetry, it suffices to verify that if $E\{G/X\} \xrightarrow{\alpha} \eta_1$ then there exists η_2 s.t. $F\{G/X\} \stackrel{\alpha}{\Longrightarrow}_c \eta_2$ and $\eta_1 \equiv_{\approx} \eta_2$. From Lemma 11 we know that there are two possibilities:

1. $E \xrightarrow{X} \{\mathbf{0} : 1\}$ and $G \xrightarrow{\alpha} \eta_1$. Thus $F \stackrel{X}{\Longrightarrow}_c \{\mathbf{0} : 1\}$ because $E \simeq F$. From Lemma 4 we know that $F \stackrel{X}{\Longrightarrow} \{\mathbf{0} : 1\}$. By Lemma 10 it follows that $F\{G/X\} \stackrel{\alpha}{\Longrightarrow} \eta_1$. We we can simply take η_1 as η_2 and finish this case.
2. $\eta_1 = \{E_i\{G/X\} : p_i\}$ and $E \xrightarrow{\alpha} \theta_1 = \{E_i : p_i\}_i$. Since $E \simeq F$ there exists $\theta_2 = \{F_j : q_j\}_j$ s.t. $F \stackrel{\alpha}{\Longrightarrow}_c \theta_2$ and $\theta_1 \equiv_{\approx} \theta_2$. By Lemma 9 we can derive $F\{G/X\} \stackrel{\alpha}{\Longrightarrow}_c \eta_2 = \{F_j\{G/X\} : q_j\}_j$. By Proposition 13 it holds that for any $E', F' \in \{E_i\}_i \cup \{F_j\}_j$ if $E' \approx F'$ then $E'\{G/X\} \approx F'\{G/X\}$. Hence it follows from $\theta_1 \equiv_{\approx} \theta_2$ that $\eta_1 \equiv_{\approx} \eta_2$ and we complete the proof of this case.

□

Lemma 12. *1. The following rules are derivable:*

$$\mathsf{D1}\ \frac{E_j \stackrel{\alpha}{\Longrightarrow}_c \eta}{\sum_{i \in 1..n} E_i \stackrel{\alpha}{\Longrightarrow}_c \eta} \quad \textit{for some } j \in 1..n \qquad \mathsf{D2}\ \frac{E\{\mu_X E/X\} \stackrel{\alpha}{\Longrightarrow}_c \eta}{\mu_X E \stackrel{\alpha}{\Longrightarrow}_c \eta}$$

$$\mathsf{D3}\ \frac{E \stackrel{\hat{\alpha}}{\Longrightarrow}_c \{E_i : p_i\}_i}{E \mid F \stackrel{\hat{\alpha}}{\Longrightarrow}_c \{E_i \mid F : p_i\}_i}$$

$$\mathsf{D4}\ \frac{E \stackrel{a}{\Longrightarrow}_c \{E_i : p_i\}_{i \in I} \qquad F \xrightarrow{\bar{a}} \{F_j : q_j)\}_{j \in J}}{E \mid F \stackrel{\tau}{\Longrightarrow}_c \{E_i \mid F_j : p_i q_j)\}_{i \in I, j \in J}}$$

2. *If* $\sum_{i\in 1..n} E_i \stackrel{\alpha}{\Longrightarrow} \eta$ *then* $E_j \stackrel{\alpha}{\Longrightarrow} \eta$ *for some* $j \in 1..n$, *with a shorter inference.*
3. *If* $\mu_X E \stackrel{\alpha}{\Longrightarrow} \eta$ *then* $E\{\mu_X E/X\} \stackrel{\alpha}{\Longrightarrow} \eta$, *with a shorter inference.*

Proof. Straightforward by induction on inference. □

Lemma 13. *1. Let* $\mathcal{R}$ *be a weak probabilistic bisimulation. If* $E\ \mathcal{R}\ F$ *then whenever* $E \stackrel{\hat{\alpha}}{\Longrightarrow}_c \eta$, *there exists* η' *such that* $F \stackrel{\hat{\alpha}}{\Longrightarrow}_c \eta'$ *and* $\eta \equiv_{\mathcal{R}} \eta'$.
2. *Suppose* $E \simeq F$. *If* $E \stackrel{\alpha}{\Longrightarrow}_c \eta$ *then there exists* η' *s.t.* $F \stackrel{\alpha}{\Longrightarrow}_c \eta'$ *and* $\eta \equiv_{\approx} \eta'$.

Proof. By transition induction. □

Lemma 14. *If* $E \approx F$ *then* $E \mid G \approx F \mid G$.

Proof. We show that the relation $\approx^{|}$ is a weak probabilistic bisimulation. There are four cases, among which we consider two of them, the others are similar.

Case 1: Suppose $\eta_1 = \{E_i \mid G : p_i\}_i$ and $E \mid G \stackrel{\alpha}{\longrightarrow} \eta_1$ is derived from the transition $E \stackrel{\alpha}{\longrightarrow} \theta_1 = \{E_i : p_i\}_i$. Since $E \approx F$, there exists θ_2 such that $F \stackrel{\hat{\alpha}}{\Longrightarrow}_c \theta_2$ and $\theta_1 \equiv_{\approx} \theta_2$. Let $\theta_2 = \{F_j : q_j\}_j$, by rule D3 we have the transition $F \mid G \stackrel{\hat{\alpha}}{\Longrightarrow}_c \{F_j \mid G : q_j\}_j = \eta_2$. Let $\theta = \{G : 1\}$, then we have $\eta_1 = \theta_1 \mid \theta$ and $\eta_2 = \theta_2 \mid \theta$. By Lemma 2 it follows that $\eta_1 \equiv_{\approx^{|}} \eta_2$.

Case 2: Suppose $E \stackrel{a}{\longrightarrow} \theta_1$, $G \stackrel{\bar{a}}{\longrightarrow} \theta$, and $E \mid G \stackrel{\tau}{\longrightarrow} \eta_1$ with $\eta_1 = \theta_1 \mid \theta$. Since $E \approx F$, there exists θ_2 such that $F \stackrel{a}{\Longrightarrow}_c \theta_2$ and $\theta_1 \equiv_{\approx} \theta_2$. By rule D4 we have the transition $F \mid G \stackrel{\tau}{\Longrightarrow}_c \eta_2$ with $\eta_2 = \theta_2 \mid \theta$. By Lemma 2 it follows that $\eta_1 \equiv_{\approx^{|}} \eta_2$. □

Proposition 15. *If* $E \simeq F$ *then* $E \mid G \simeq F \mid G$.

Proof. Similar to the proof of Lemma 14. We need to use the above proved result that $\approx^{|} \subseteq \approx$. □

Proposition 16. *If* $E \simeq F$ *then* $\mu_X E \simeq \mu_X F$.

Proof. Let $\rho = \{\mu_X E/X\}$ and $\sigma = \{\mu_X F/X\}$. We show that the relation

$$\mathcal{R} = \{(G\rho, G\sigma) \mid E, F, G \in \mathcal{E} \text{ and } E \simeq F\}$$

is an observational equivalence up to $\simeq$. Because of symmetry we only need to show that if $G\rho \stackrel{\alpha}{\Longrightarrow} \eta$ there exists η' s.t. $G\sigma \stackrel{\alpha}{\Longrightarrow}_c \eta'$ and $\eta \equiv_{\mathcal{R}_{\approx}} \eta'$. The proof is carried out by induction on the depth of the inference of $G\rho \stackrel{\alpha}{\Longrightarrow} \eta$. There are several cases depending on the structure of G. We consider three typical ones.

– $G \equiv X$: Then $G\rho \equiv \mu_X E \stackrel{\alpha}{\Longrightarrow} \eta$. By Lemma 12 we have a shorter inference with the conclusion $E\rho \stackrel{\alpha}{\Longrightarrow} \eta$. By induction hypothesis there exists θ s.t. $E\sigma \stackrel{\alpha}{\Longrightarrow}_c \theta$ and $\eta \equiv_{\mathcal{R}_{\approx}} \theta$. Since $E \simeq F$ we have $E\sigma \simeq F\sigma$ by Proposition 14. By Lemma 13 (2) there exists η' s.t. $F\sigma \stackrel{\alpha}{\Longrightarrow}_c \eta'$ and $\theta \equiv_{\approx} \eta'$. By rule D2 it holds that $\mu_X F \stackrel{\alpha}{\Longrightarrow}_c \eta'$. At last it follows from Lemma 1 and the transitivity of $\equiv_{\mathcal{R}_{\approx}}$ that $\eta \equiv_{\mathcal{R}_{\approx}} \eta'$.

– $G \equiv \sum_{i\in 1..n} G_i$: If $G\rho \stackrel{\alpha}{\Longrightarrow} \eta$ then by Lemma 12, $G_j\rho \stackrel{\alpha}{\Longrightarrow} \eta$ for some $j \in 1..n$ with a shorter inference. By induction hypothesis there exists η' s.t. $G_j\sigma \stackrel{\alpha}{\Longrightarrow}_c \eta'$ and $\eta \equiv_{\mathcal{R}_\approx} \eta'$. By rule $\mathsf{D1}$ it holds that $G\sigma \stackrel{\alpha}{\Longrightarrow}_c \eta'$.
– $G \equiv G_1 \mid G_2$: Then $fv(G) = \emptyset$ and $G = G\rho = G\sigma$. Clearly if $G\rho \stackrel{\alpha}{\Longrightarrow} \eta$ then $G\sigma \stackrel{\alpha}{\Longrightarrow} \eta$.

□

Proposition 17. $\simeq$ *is a congruence relation.*

Proof. Given $\widetilde{E} \simeq \widetilde{F}$, we need to show the following three clauses:

1. $u.\bigoplus_i p_i E_i \simeq u.\bigoplus_i p_i F_i$;
2. $\sum_{i\in 1..n} E_i \simeq \sum_{i\in 1..n} F_i$;
3. $E_1 \mid E_2 \simeq F_1 \mid F_2$;
4. $\mu_X E_1 \simeq \mu_X F_1$.

Among them, the first two clauses are easy to prove; the last two are shown in Proposition 15 and Proposition 16 respectively. □

Proposition 18. *1. $E \approx F$ iff $\tau.E \simeq \tau.F$;*
2. If $\tau.E \simeq \tau.E + F$ and $\tau.F \simeq \tau.F + E$ then $\tau.E \simeq \tau.F$.

Proof. The first clause is straightforward. For the second one, it suffices to prove that $E \approx F$. Consider the relation

$$\mathcal{R} = \{(E, F) \mid E, F \in \mathcal{E}, \tau.E \simeq \tau.E + F \text{ and } \tau.F \simeq \tau.F + E\}.$$

We show that $\mathcal{R}$ is a weak probabilistic bisimulation up to $\approx$. Suppose that $E \stackrel{\alpha}{\Longrightarrow} \eta$. By the condition $E + \tau.F \simeq \tau.F$ and Lemma 13 (2), there exists η' s.t. $\tau.F \stackrel{\alpha}{\Longrightarrow}_c \eta'$ and $\eta \equiv_\approx \eta'$. Since $\tau.F \approx F$, by Lemma 13 (1) there exists η'' s.t. $F \stackrel{\hat{\alpha}}{\Longrightarrow}_c \eta''$ and $\eta' \equiv_\approx \eta''$. Then it is easy to see that $\eta \equiv_{\mathcal{R}_\approx} \eta''$. Similar result holds when E and F exchange their roles. □

We use a measure $d_X(E)$ to count the depth of guardedness of the free variable X in expression E.

$$\begin{aligned}
d_X(X) &= 0 \\
d_X(Y) &= 0 \\
d_X(E \mid F) &= 0 \\
d_X(a.E) &= d_X(E) + 1 \\
d_X(\tau.E) &= d_X(E) \\
d_X(\textstyle\bigoplus_i p_i E_i) &= min\{d_X(E_i)\}_i \\
d_X(\textstyle\sum_i E_i) &= min\{d_X(E_i)\}_i \\
d_X(\mu_Y E) &= d_X(E)
\end{aligned}$$

Note that $d_X(E \mid F) = 0$ because $fv(E \mid F) = \emptyset$. If $d_X(E) > 0$ then X is guarded in E.

Lemma 15. *Let $d_X(G) = n$ and $\eta = \{G_i : p_i\}_{i \in I}$. Suppose $G\{E/X\} \stackrel{\alpha}{\Longrightarrow} \eta$. For all $i \in I$, it holds that*

1. *If $n > 0$ and $\alpha = \tau$ then $G_i = G'_i\{E/X\}$ and $d_X(G'_i) \geq n$;*
2. *If $n > 1$ and $\alpha \neq \tau$ then $G_i = G'_i\{E/X\}$ and $d_X(G'_i) \geq n - 1$.*

Proof. By induction on the depth of the inference of $G\{E/X\} \stackrel{\alpha}{\Longrightarrow} \eta$. □

Lemma 16. *Suppose $d_X(G) > 1$, $\eta = \{G_i : p_i\}_{i \in I}$ and $G\{E/X\} \stackrel{\alpha}{\Longrightarrow} \eta$. Then $G_i = G'_i\{E/X\}$ for each $i \in I$. Moreover, $G\{F/X\} \stackrel{\alpha}{\Longrightarrow} \eta'$ and $\eta \equiv_{\mathcal{R}^*} \eta'$, where $\eta' = \{G'_i\{F/X\} : p_i\}_{i \in I}$ and $\mathcal{R} = \{(G\{E/X\}, G\{F/X\}) \mid$ for any $G \in \mathcal{E}\}$.*

Proof. A direct consequence of Lemma 15. □

The following Lemma is a counterpart of Lemma 8.

Lemma 17. *Let $d_X(G) > 1$. If $G\{E/X\} \stackrel{\alpha}{\Longrightarrow}_c \eta$ then $G\{F/X\} \stackrel{\alpha}{\Longrightarrow}_c \eta'$ such that $\eta \equiv_{\mathcal{R}^*} \eta'$ where $\mathcal{R} = \{(G\{E/X\}, G\{F/X\}) \mid$ for any $G \in \mathcal{E}\}$.*

Proof. Let $\eta = r_1\eta_1 + ... + r_n\eta_n$ and $G\{E/X\} \stackrel{\alpha}{\Longrightarrow} \eta_i$ for each $i \leq n$. By Lemma 16, for each $i \leq n$, there exists η'_i s.t. $G\{F/X\} \stackrel{\alpha}{\Longrightarrow} \eta'_i$ and $\eta_i \equiv_{\mathcal{R}^*} \eta'_i$. Now let $\eta' = r_1\eta'_1 + ... + r_n\eta'_n$, thus $G\{F/X\} \stackrel{\alpha}{\Longrightarrow}_c \eta'$. By lemma 7 it follows that $\eta \equiv_{\mathcal{R}^*} \eta'$. □

Proposition 19. *If $E \simeq F\{E/X\}$ and X is guarded in F then $E \simeq \mu_X F$.*

Proof. We show that the relation $\mathcal{R} = \{(G\{E/X\}, G\{\mu_X F/X\}) \mid$ for any $G \in \mathcal{E}\}$ is an observational equivalence up to $\simeq$. That is, we need to show the following assertions:

1. if $G\{E/X\} \stackrel{\alpha}{\Longrightarrow} \eta$ then there exists η' s.t. $G\{\mu_X F/X\} \stackrel{\alpha}{\Longrightarrow}_c \eta'$ and $\eta \equiv_{\mathcal{R}_\approx} \eta'$;
2. if $G\{\mu_X F/X\} \stackrel{\alpha}{\Longrightarrow} \eta'$ then there exists η s.t. $G\{E/X\} \stackrel{\alpha}{\Longrightarrow}_c \eta$ and $\eta \equiv_{\mathcal{R}_\approx} \eta'$;

We concentrate on the first clause since the second one is similar. The proof follows closely the arguments in proving Proposition 16, thus we only consider the case that $G \equiv X$.

We write $G(E)$ for $G\{E/X\}$ and $G^2(E)$ for $G(G(E))$. Since $E \simeq F(E)$, we have $E \simeq F^2(E)$ since $\simeq$ is an congruence relation by Proposition 17. If $E \stackrel{\alpha}{\Longrightarrow} \eta$ then by Lemma 13 (2) there exists θ_1 s.t. $F^2(E) \stackrel{\alpha}{\Longrightarrow}_c \theta_1$ and $\eta \equiv_\approx \theta_1$. Since X is guarded in F, i.e., $d_X(F) > 0$, then it follows that $d_X(F^2(X)) > 1$. By Lemma 17, there exists θ_2 s.t. $F^2(\mu_X F) \stackrel{\alpha}{\Longrightarrow}_c \theta_2$ and $\theta_1 \equiv_{\mathcal{R}^*} \theta_2$. From Proposition 10 we have $\mu_X F \sim F^2(\mu_X F)$, thus $\mu_X F \simeq F^2(\mu_X F)$. By Lemma 13 (2) there exists η' s.t. $\mu_X F \stackrel{\alpha}{\Longrightarrow}_c \eta'$ and $\theta_2 \equiv_\approx \eta'$. From Lemma 1 and the transitivity of $\equiv_{\mathcal{R}_\approx}$ it follows that $\eta \equiv_{\mathcal{R}_\approx} \eta'$. □

Finally Proposition 5 is proved by collecting all the results in Propositions 17-19.