Stochastic Pi-Calculus Revisited

Luca Cardelli[1], Radu Mardare[2⋆]

[1] Microsoft Research, Cambridge, UK
[2] University of Aalborg, Denmark

Abstract. We develop a version of stochastic Pi-calculus with a semantics based on measure theory. We define the behaviour of a process in a rate environment using measures over the measurable space of processes induced by structural congruence. We extend the stochastic bisimulation to include the concept of rate environment and prove that this equivalence is a congruence which extends the structural congruence.

1 Introduction

The problem of specifying and analysing nondeterministic concurrent systems has found a successful solution in the class of *Process Algebras* (PAs) [2]. The compositionality of the processes is reflected by the construction principles of PAs, while their behaviours are transition systems. As a result, one obtains a class of processes with an elegant algebraic-coalgebraic structure, supported by appealing theories and easy to adapt to various modelling requirements.

The same approach has been taken for probabilistic and stochastic concurrent systems. *Probabilistic process algebras* [2], *interactive Markov chain algebra* [14, 4] and *stochastic process algebras* (SPA) such as TIPP [11], PEPA [12, 13], EMPA [3] and *stochastic Pi-calculus* [20] are extensions of classic PAs. The nondeterminism is replaced by a race policy and this requires important modifications in the semantic format. Stressed to mimic the pointwise structural operational semantics (SOS) of nondeterministic PAs, SPAs find *ad hoc* solutions to the problems introduced by stochasticity, such as the *multi-transition system* approach of PEPA or the *proved SOS* approach of stochastic Pi-calculus. These result in complex constructs that are difficult to extend to a general format for well-behaved stochastic specifications and problematic when recursion or fresh name quantification are considered. As underlined in [15], for stochastic pi-calculus of [20] the parallel composition fails to be associative up to bisimulation, while for PEPA, if arbitrary relations between the rates of processes and subprocesses are allowed, stochastic bisimulation ceases to be a congruence. An explanation for these situations is given in [15]: the information carried by the aforementioned SOS frameworks is excessive, while a well-behaved framework should only carry the exact amount of data required for the derivation of the intended semantics.

⋆ Research partially supported by Sapere Aude: DFF-Young Researchers Grant 10-085054 of the Danish Council for Independent Research.

These problems motivate our research, initiated with [6], that aims to reconsider the semantics of SPAs from a perspective faithful to the algebraic-coalgebraic structure of stochastic processes. The key observation is that *structural congruence* induces a σ-algebra on processes and organizes a measurable space of stochastic processes. We propose a semantics that assign to each process a set of measures indexed by observable actions. Thus, difficult instance-counting problems that otherwise require complicated versions of SOS can be solved by exploiting the properties of measures (e.g. additivity). Our previous work showed that along this line one obtains an elegant semantics that resembles the one of nondeterministic PAs and provides a well-behaved notion of bisimulation. In [6] we proved this concept for a fragment of stochastic CCS. In this paper we approach stochastic Pi-calculus that includes channel-based communication, mobility, fresh name quantification and replication. This calculus is designed to satisfy the specific requirements of Systems Biology.

There are several novel ideas in our approach. The processes are interpreted in *stochastic environments* that associate *basic rates* to channels. In a rate environment E, a process P has associated a class of measures μ, written $E \vdash P \to \mu$. For each action α, $\mu(\alpha)$ is a measure over the space of processes; $\mu(\alpha)(S) \in \mathbb{R}^+$ is the rate of an exponentially distributed random variable that characterizes the α-transitions from P to (elements of) a measurable set S. Only the structural congruence-closed sets are measurable. This is essential for modelling in systems biology, where such sets represent chemical soups[1]. This choice induces an elegant semantics that supports a smooth development of the basic theory. It provides simple solutions to the problems of replications and bound outputs which otherwise, as with Milner's Abstraction-Concretion method [18], require complicated high-order reasoning. Also novel is our concept of *stochastic bisimulation* that extends other similar ones [17, 15, 6, 19] by making explicit the role of the rate environments. We show that bisimulation is a congruence that extends the structural congruence.

Related works. The idea of transitions from states to measures has been advocated in the context of probabilistic automata [16, 22] and Markov processes [19]. The *transition-systems-as-coalgebras* paradigm [8, 21] exploits it providing a uniform characterisation of transition systems that covers the sequence nondeterministic, probabilistic and stochastic systems. Similar approaches have been tested with SPAs in [7] and a general SOS format for SPAs without new name operators or recursion is proposed in [15]; these approaches consider the space of processes organized by powerset. Instead, we take a different measurable space that answers to practical modelling requirements, simplifies the semantics and gives us smooth solutions for the fresh name quantification and replication without requiring additional constructs. The use of name environments has been consider in [9, 10] where it involves the machinery of nominal sets. We have tried to avoid this together with any coalgebraic description of the lifting from processes to measures, as our intention is to make these ideas accessible for the readers less familiar with the jargon of Category Theory.

[1] Structural congruence has been introduced in [1] as a chemical analogy.

2 Preliminaries

In this section we introduce the terminology and the notations used in the paper.

For the sets A and B, 2^A denotes the powerset of A, $[A \to B]$ and B^A the class of functions from A to B. For an equivalence relation $\sim$ on A, $A^\sim$ is the set of equivalence classes and $a^\sim$ the equivalence class of $a \in A$.

Given a set M, $\Sigma \subseteq 2^M$ that contains M and is closed under complement and countable union is a *σ-algebra* over M; (M, Σ) is a *measurable space* and the elements of Σ are *measurable sets*. $\Omega \subseteq 2^M$ with disjoint elements is a *base for* Σ if Σ is the closure of Ω under complement and countable union.

A *measure* on (M, Σ) is a function $\mu : \Sigma \to \mathbb{R}^+$ such that $\mu(\emptyset) = 0$ and for any $\{N_i | i \in I \subseteq \mathbb{N}\} \subseteq \Sigma$ with pairwise disjoint elements, $\mu(\bigcup_{i\in I} N_i) = \sum_{i\in I} \mu(N_i)$. The *null measure* ω is such that $\omega(M) = 0$. For a base $\Omega \ni N$, then the *N-Dirac measure* D_N is defined by $D_N(N) = r$, $D_N(N') = 0$ for $N \neq N'$ and $D_N(\cup_{i\in I} N_i) = \sum_{i\in I} D_N(N_i)$. $\Delta(M, \Sigma)$ denotes the set of measures on (M, Σ).

If $\mathfrak{R} \subseteq M \times M$, $N \subseteq M$ is $\mathfrak{R}$-closed iff $\{m \in M \mid \exists n \in N, (n, m) \in \mathfrak{R}\} \subseteq N$. If (M, Σ) is a measurable space, $\Sigma(\mathfrak{R})$ is the set of measurable $\mathfrak{R}$-closed sets.

3 Stochastic Pi-Calculus

In this section we introduce a version of stochastic Pi-calculus equipped with an *early semantics* [2] expressed in terms of measure theory. Being developed mainly for applications in Systems Biology, this calculus is designed to respect the *chemical kinetics* (the *Chemical Master Equation*) [5] which provides the mathematical principles for calculating the rates of the channel-based communications. The class $\mathbb{P}$ of processes is endowed with structural congruence which generates a σ-algebra Π on $\mathbb{P}$. In addition, rate environments assess base rates to channel names. The behaviour of a process P in a rate environment E is defined by an indexed set of measures $\mu : \mathbb{A}^+ \to \Delta(\mathbb{P}, \Pi)$, where $\mathbb{A}^+$ is the set of observable actions.

3.1 Syntax

Definition 1 (Processes). *Let $\mathcal{N}$ be a countable set. The* stochastic processes *are defined, on top of* 0*, for arbitrary $r \in \mathbb{Q}^+$ and $a, b, c \in \mathcal{N}$, as follows.*

$$P := 0 \vdots x.P \vdots (a@r)P \vdots P|P \vdots P + P \vdots !P, \qquad x := a(b) \vdots a[b].$$

Let $\mathbb{P}$ be the set of stochastic processes. 0 stays for the inactive process. An *input* "$a(b)$" is the capability of the process $a(b).P$ to receive a name on channel a that replaces b in all its occurrences inside P. An *output* prefix "$a[b]$" represents the action of sending a name b on channel a. "$(a@r)$" is the *fresh name operator* that, unlike in nondeterministic PAs, also specifies the rate r of the fresh name. As usual in Pi-calculus, we have the *parallel composition* "|", the *choice operator* "+" and the *replication operator* "!". Let $\mathcal{N}^* = \{a(b), a[b] \mid a, b \in \mathcal{N}\}$; in what follows a, b, c, a', a_i range over $\mathcal{N}$ and x, x', x_i range over $\mathcal{N}^*$.

For arbitrary $P \in \mathbb{P}$, we define the set $fn(P)$ of the *free names* of P inductively by $fn(0) = \emptyset$, $fn(a(b).P) = (fn(P) \setminus \{b\}) \cup \{a\}$, $fn(a[b].P) = fn(P) \cup \{a, b\}$, $fn(P|Q) = fn(P + Q) = fn(P) \cup fn(Q)$, $(a@r)P = fn(P) \setminus \{a\}$ and $fn(!P) = fn(P)$. As usual in process algebras, for arbitrary $a, b \in \mathcal{N}$, we write $P_{\{a/b\}}$ for the process term obtained from P by substituting all the free occurrences of b with a, renaming as necessary to avoid capture.

Definition 2 (Structural congruence). *Structural congruence is the smallest equivalence relation $\equiv \subseteq \mathbb{P} \times \mathbb{P}$ satisfying the following conditions.*
I. *$(\mathbb{P}, |, 0)$ is a commutative monoid for $\equiv$, i.e.,*
1. $P|Q \equiv Q|P$; 2. $(P|Q)|R \equiv P|(Q|R)$; 3. $P|0 \equiv P$.

II. *$(\mathbb{P}, +, 0)$ is a commutative monoid for $\equiv$, i.e.,*
1. $P + Q \equiv Q + P$; 2. $(P + Q) + R \equiv P + (Q + R)$; 3. $P + 0 \equiv P$.

III. *$\equiv$ is a congruence for the algebraic structure of $\mathbb{P}$, i.e., if $P \equiv Q$, then*
1. $P|R \equiv Q|R$; 2. $P + R \equiv Q + R$; 3. $x.P \equiv x.Q$;
4. $(a@r)P \equiv (a@r)Q$; 5. $!P \equiv !Q$.

IV. *the fresh name quantifiers satisfy the following conditions*
1. *if $a \neq b$, then* $(a@r)(b@s)P \equiv (b@s)(a@r)P$; 2. $(a@r)0 \equiv 0$;
3. *if $a \notin fn(P)$, then* $(a@r)(P|Q) \equiv P|(a@r)Q$ *and* $(a@r)(P+Q) \equiv P+(a@r)Q$.

V. *the replication satisfies the following conditions*
1. $!0 \equiv 0$; 2. $!(P|Q) \equiv !P|!Q$.

VI. *$\equiv$ satisfies the alpha-conversion rules*
1. $(a@r)P \equiv (b@r)P_{\{b/a\}}$; 2. $a(b)P \equiv a(c)P_{\{c/b\}}$.

If Q is obtained from P by alpha-conversion (VI) 1-2, we write $P \equiv^* Q$. Let Π be the set of the $\equiv$-closed subsets of $\mathbb{P}$. Note that $\mathbb{P}^{\equiv}$ is a countable partition of $\mathbb{P}$ and Π is the σ-algebra generated by $\mathbb{P}^{\equiv}$.

Notice that, unlike in the nondeterministic case, we do not have $!!P \equiv !P$ nor $!P \equiv P|!P$. These are not sound due to the rate competition which else will generate processes with infinite rates.

Theorem 1. *$(\mathbb{P}, \Pi)$ is a measurable space.*

The measurable sets of the space $(\mathbb{P}, \Pi)$ are the (finite or denumerable) reunions of $\equiv$-equivalence classes on $\mathbb{P}$. In what follows $\mathcal{P}, \mathcal{P}_i, \mathcal{R}, \mathcal{Q}$ range over Π. For the economy of the paper it is useful to lift some functions and algebraic operations from processes to measurable sets.

For arbitrary $\mathcal{P}, \mathcal{Q} \in \Pi$, $a, b \in \mathcal{N}$ and $r \in \mathbb{Q}^+$, consider

$$fn(\mathcal{P}) = \bigcup_{P \in \mathcal{P}} fn(P), \qquad \mathcal{P}_{\{a/b\}} = \bigcup_{P \in \mathcal{P}} P_{\{a/b\}}, \qquad \mathcal{P}|\mathcal{Q} = \bigcup_{P \in \mathcal{P}}^{Q \in \mathcal{Q}} (P|Q)^{\equiv}$$

$$, \qquad \mathcal{P}_{\mathcal{Q}} = \bigcup_{R|Q \in \mathcal{P}}^{Q \in \mathcal{Q}} R^{\equiv}, \qquad (a@r)\mathcal{P} = \bigcup_{P \in \mathcal{P}} (a@r)P^{\equiv}.$$

The next lemma states that the operations introduced before are internal operations of Π.

Lemma 1. *If $\mathcal{P}, \mathcal{Q} \in \Pi$, $a, b \in \mathcal{N}$, $r \in \mathbb{Q}^+$, then $\mathcal{P}_{\{a/b\}}, \mathcal{P}|\mathcal{Q}, \mathcal{P}_{\mathcal{Q}}, (a@r)\mathcal{P} \in \Pi$.*

3.2 Rate environments

Now we introduce rate environments used to interpret stochastic processes.

Definition 3 (Rate Environment). *The* rate environments *associated to* $\mathcal{N}$ *are defined, on top of a constant* ε*, for arbitrary* $a \in \mathcal{N}$ *and* $r \in \mathbb{Q}^+$*, by*

$$E := \varepsilon \vdots E, a@r.$$

Let $\mathbb{E}$ be the set of rate environments. A suffix $a@r$ is called *rate declaration*. If $a@r$ appears in E, we write $a@r \in E$. ε is the *empty environment*. We treat "," as concatenation symbol for rate environments and use "E, E'" to denote the concatenation of E and E'. ε is the empty symbol for concatenation.

For $E = E_1, ..., E_n \in \mathbb{E}$ and $\{1, .., n\} = \{i_1, .., i_k\} \cup \{j_1, .., j_{n-k}\}$ with $i_1 < .. < i_k$, $j_1 < ... < j_{n-k}$, if $E' = E_{i_1}, .., E_{i_k}$ and $E'' = E_{j_1}, .., E_{j_{n-k}}$, we write $E' \subset E$ and $E'' = E \setminus E'$. Notice that $\varepsilon \subset E$, $E \subset E$, $E = E \setminus \varepsilon$ and $\varepsilon = E \setminus E$. The *domain of a rate environment* is the partial function on $\mathbb{E}$ defined as follows.

1. $dom(\varepsilon) = \emptyset$;
2. if $dom(E)$ is defined and $a \notin dom(E)$, then $dom(E, a@r) = dom(E) \cup \{a\}$;
3. undefined else.

In what follows, whenever we use $dom(E)$ we implicitly assume that dom is defined in E. Observe that, if $a \in dom(E)$, then there exists a rate declaration $a@r \in E$ and for no $s \neq r$, $a@s \in E$; for this reason we also write $r = E(a)$. This suggests that an alternative approach would be to simply consider E as a partial function. When $dom(E)$ is defined, let $dom(E)^* = \{a \in dom(E) \text{ s.t. } E(a) \neq 0\}$.

The rate environments could be alternatively introduced as partial functions on $\mathcal{N}$. Such a solution simplifies some semantic rules, but we find it not "in the spirit" of process algebras. A more appropriate alternative is to define a type systems for environment correctness, but this would complicate the semantics. We find our solution a good trade-off between these possibilities.

3.3 The class of indexed measures

The semantics will involve terms of type $E \vdash P \to \mu$, where E is a rate environment, P is a process and $\mu : \mathbb{A}^+ \to \Delta(\mathbb{P}, \Pi)$ is a mapping that defines a set of labeled measures. The labels are the observable actions collected in the set $\mathbb{A}^+$ defined below.

$$\mathbb{A} = \{a[b], a[@r], ab, \quad \text{for} \quad a, b \in \mathcal{N}, r \in \mathbb{Q}^+\} \text{ and } \mathbb{A}^+ = \mathbb{A} \cup \{\tau\}.$$

The observable actions consist of four classes: (i) *free outputs* of type $a[b]$ denoting the action of sending a free name b over the channel a, (ii) *bound outputs* of type $a[@r]$ denoting the action of sending a fresh unspecified name, with base-rate r, on channel a, (iii) *input actions* of type ab representing the fact that channel a has received a name b (as the result of an output action on a), (iv) *internal action* τ – communications. In what follows we use $\alpha, \alpha', \alpha_i$ to represent arbitrary elements of $\mathbb{A}^+$.

Notice the relation between the syntactic prefixes of the calculus and the observable actions. The output prefixes, as in pi-calculus, represent observable

output actions. The input prefix of the calculus, such as $a(b)$ in the process $a(b).P$, does not represent an authentic action, but the capability of P to receive a name on channel a; consequently we adopt an *early semantics* [2]: if a name c is sent on a, the input action is ac and it labels the transitions to $P_{\{c/b\}}$. In this way, to a single prefix $a(b)$ correspond as many input actions ac as names c can be sent on a in the given rate-environment. Unlike the nondeterministic case, for stochastic Pi-calculus we cannot define a *late semantics* [2] because only the input actions of type ac correspond to a measure on the space of processes, while $a(b)$ represents a set of measures, one for each name received. Because our semantics aims to associate a measure to each process and action label, we need to refuse the inputs of type $a(b)$ in the set of labels and chose an early semantics.

The bound output $a[@r]$ in the form that ignores the argument of communication is novel. It labels a bound output of type $(b@r)a[b].P$. The example bellow explains its action; anticipating the semantics, $E \vdash P \xrightarrow{\alpha,r} Q^{\equiv}$ means that in the environment E, P can do an α-transition with rate r to the elements of $Q^{\equiv}$.

Example 1. The processes $Q = (b@r)a[b].P$ and $R = (c@r)a[c].P_{\{c/b\}}$ are structural congruent and we want them bisimilar in our semantics. If we consider that the (only) observable transition in which Q can be involved is $a[b@r]$, as it is done in other PAs, then the transition is $E \vdash (b@r)a[b].P \xrightarrow{a[b@r],E(a)} (b@r)P^{\equiv}$, while for R the transition is $E \vdash (c@r)a[c].P_{\{c/b\}} \xrightarrow{a[c@r],E(a)} (c@r)P^{\equiv}_{\{c/b\}}$. Obviously, $(b@r)P^{\equiv} = (c@r)P^{\equiv}_{\{c/b\}}$, but if $b \neq c$, then $a[b@r] \neq a[c@r]$ and in effect, Q and R are not bisimilar in this interpretation.

For obtaining the expected bisimulations, one needs to accept that for any $b, c \in \mathcal{N}$, $a[b@r] = a[c@r]$; and this is equivalent with accepting that an external observer can only see that a private name at rate r has been sent on channel a without seeing the name. Hence, the real observable action has to be $a[@r]$.

Our solution is similar to the *Abstraction-Concretion method* proposed in [18] for nondeterministic pi-calculus. $a[@r]$ does the job of Abstraction, as our measurable sets of processes are Milner's *abstracted processes*. Only that in our case, because the transitions are not between processes but from processes to structural-congruence classes, we need no Concretions. So, the main advantage of our approach is that it solves the problem of bound outputs without using higher order syntax as in the classic pi-calculus[2].

To introduce the semantic rules in the next section, we need some operations on $\Delta(\mathbb{P}, \Pi)^{\mathbb{A}^+}$. Let $\mathbb{A}_{@} = \{a[@r], \text{ for } a \in \mathcal{N}, r \in \mathbb{Q}^+\}$ and for $a \in \mathcal{N}$, let $\mathbb{A}_a = \{a[b], ab, a[@r], \text{ for } b \in \mathcal{N}, r \in \mathbb{Q}^+\}$. $\mu \in \Delta(\mathbb{P}, \Pi)^{\mathbb{A}^+}$ has *finite support* if the set of $\alpha \in \mathbb{A}^+$ such that α is not an input action and $\mu(\alpha) \neq \omega$ is finite or empty. Recall that ω is the null measure and $D_{P^{\equiv}}$ the $P^{\equiv}$-Dirac measure.

Definition 4. *Consider the following operations on* $\Delta(\mathbb{P}, \Pi)^{\mathbb{A}^+}$.

[2] By translating nondeterministic Pi-calculus into stochastic Pi-calculus where all rates are 1.0, one can get a similar solution for the classic Pi-calculus with a semantics based on the transitions from processes to structural-congruence classes.

1. Operations of arity 0.
(i) Let $\overline{\omega} : \mathbb{A}^+ \to \Delta(\mathbb{P}, \Pi)$ *defined by* $\overline{\omega}(\alpha) = \omega$ *for arbitrary* $\alpha \in \mathbb{A}^+$*;*
(ii) For $x \in \mathcal{N}^*$, $E \in \mathbb{E}$, $\mathcal{P} \in \Pi$ *with* $fn(\mathcal{P}) \subseteq dom(E)$, *let* $E^x_{\mathcal{P}} : \mathbb{A}^+ \to \Delta(\mathbb{P}, \Pi)$,
$E^{a[b]}_{\mathcal{P}}(a[b]) = E(a) \sum_{P^{\equiv} \subseteq \mathcal{P}} D_{P^{\equiv}}$ *and for* $\alpha \neq a[b], E^{a[b]}_{\mathcal{P}}(\alpha) = \omega$;
$E^{a(b)}_{\mathcal{P}}(ac) = E(a) \sum_{P^{\equiv}_{\{c/b\}} \subseteq \mathcal{P}} D_{P^{\equiv}_{\{c/b\}}}$ *and for* $\alpha \neq a(b), E^{a(b)}_{\mathcal{P}}(\alpha) = \omega$.
2. Operations of arity 1.
(i) For $\mu \in \Delta(\mathbb{P}, \Pi)^{\mathbb{A}^+}$, $\mathcal{P} \in \Pi$, *let* $\mu_{\mathcal{P}} : \mathbb{A}^+ \to \Delta(\mathbb{P}, \Pi)$, $\mu_{\mathcal{P}}(\alpha)(\mathcal{R}) = \mu(\alpha)(\mathcal{R}_{\mathcal{P}})$.
(ii) For $\mu \in \Delta(\mathbb{P}, \Pi)^{\mathbb{A}^+}$, $a \in \mathcal{N}$ *and* $r \in \mathbb{Q}^+$, *let* $(a@r)\mu : \mathbb{A}^+ \to \Delta(\mathbb{P}, \Pi)$,

$$(a@r)\mu(\alpha)(\mathcal{R}) = \begin{cases} \mu(\alpha)(\mathcal{P}), & \text{if } \alpha \notin \mathbb{A}_a \cup \mathbb{A}_@, \mathcal{R} = (a@r)\mathcal{P} \\ \mu(b[a])(\mathcal{P}) + \mu(b[@r])(\mathcal{P}), & \text{if } \alpha = b[@r], \mathcal{R} = (a@r)\mathcal{P} \\ 0, & \text{else} \end{cases}$$

3. Operations of arity 2.
(i) For $\mu, \eta \in \Delta(\mathbb{P}, \Pi)^{\mathbb{A}^+}$, *let* $\mu \oplus \eta : \mathbb{A}^+ \to \Delta(\mathbb{P}, \Pi)$, $(\mu \oplus \eta)(\alpha) = \mu(\alpha) + \eta(\alpha)$.
(ii) For $\mu, \eta \in \Delta(\mathbb{P}, \Pi)^{\mathbb{A}^+}$ *with finite support,* $\mathcal{P}, \mathcal{Q} \in \Pi$ *and* $E \in \mathbb{E}$ *for which* $dom(E)$ *is defined, let* $\mu \ {}_{\mathcal{P}}\!\otimes^E_{\mathcal{Q}} \eta : \mathbb{A}^+ \to \Delta(\mathbb{P}, \Pi)$,
– *for* $\alpha \in \mathbb{A}$, $\quad (\mu \ {}_{\mathcal{P}}\!\otimes^E_{\mathcal{Q}} \eta)(\alpha)(\mathcal{R}) = \mu_{\mathcal{Q}}(\alpha)(\mathcal{R}) + \eta_{\mathcal{P}}(\alpha)(\mathcal{R})$;

– *for* τ, $\quad (\mu \ {}_{\mathcal{P}}\!\otimes^E_{\mathcal{Q}} \eta)(\tau)(\mathcal{R}) = \mu_{\mathcal{Q}}(\tau)(\mathcal{R}) + \eta_{\mathcal{P}}(\tau)(\mathcal{R}) +$

$$\sum_{\substack{a \in dom(E)^* \\ b \in \mathcal{N}}} \sum_{\mathcal{P}_1 | \mathcal{P}_2 \subseteq \mathcal{R}} \frac{\mu(a[b])(\mathcal{P}_1) \cdot \eta(ab)(\mathcal{P}_2) + \eta(a[b])(\mathcal{P}_1) \cdot \mu(ab)(\mathcal{P}_2)}{E(a)} +$$

$$\sum_{\substack{((x@r)y[x].P'|P'') + P'''^{\equiv} \subseteq \mathcal{P} \\ (y(z).Q'|Q'') + Q'''^{\equiv} \subseteq \mathcal{Q}}} \sum_{(x@r)(P'|Q'_{\{x/z\}})|P''|Q''^{\equiv} \subseteq \mathcal{R}} \frac{\mu(y[@r])((x@r)P'|P''^{\equiv}) \cdot \eta(yx)(Q'_{\{x/z\}}|Q''^{\equiv})}{E(a)} +$$

$$\sum_{\substack{(y(z).P'|P'') + P'''^{\equiv} \subseteq \mathcal{P} \\ ((x@r)y[x].Q'|Q'') + Q'''^{\equiv} \subseteq \mathcal{Q}}} \sum_{(x@r)(P'_{\{x/z\}}|Q')|P''|Q''^{\equiv} \subseteq \mathcal{R}} \frac{\mu(yx)(P'_{\{x/z\}}|P''^{\equiv}) \cdot \eta(y[@r])((x@r)Q'|Q''^{\equiv})}{E(a)}$$

Observe that because we work with functions with finite support and because $dom(E)$ is defined and finite, the sums involved in the definition of $\mu \ {}_{\mathcal{P}}\!\otimes^E_{\mathcal{Q}} \eta$ have finite numbers of non-zero summands. The meanings of these operations are clarified in the next section where they play an active role in the semantic rules.

Lemma 2. *1. For* $\mu, \mu', \mu'' \in \Delta(\mathbb{P}, \Pi)^{\mathbb{A}^+}$, $\mu \oplus \mu' \in \Delta(\mathbb{P}, \Pi)^{\mathbb{A}^+}$ *and*
(a). $\mu \oplus \mu' = \mu' \oplus \mu$, $\quad$ *(b).* $(\mu \oplus \mu') \oplus \mu'' = \mu \oplus (\mu' \oplus \mu'')$, $\quad$ *(c).* $\mu = \mu \oplus \overline{\omega}$.
2. For $\mu, \eta, \rho \in \Delta(\mathbb{P}, \Pi)^{\mathbb{A}^+}$ *with finite support,* $\mu \ {}_{\mathcal{P}}\!\otimes^E_{\mathcal{Q}} \eta \in \Delta(\mathbb{P}, \Pi)^{\mathbb{A}^+}$ *and*
(a). $\mu \ {}_{\mathcal{P}}\!\otimes^E_{\mathcal{Q}} \eta = \eta \ {}_{\mathcal{Q}}\!\otimes^E_{\mathcal{P}} \mu$, $\quad$ *(b).* $(\mu \ {}_{\mathcal{P}}\!\otimes^E_{\mathcal{Q}} \eta) \ {}_{\mathcal{P}|\mathcal{Q}}\!\otimes^E_{\mathcal{R}} \rho = \mu \ {}_{\mathcal{P}}\!\otimes^E_{\mathcal{Q}|\mathcal{R}} (\eta \ {}_{\mathcal{Q}}\!\otimes^E_{\mathcal{R}} \rho)$,
(c). $\mu \ {}_{\mathcal{P}}\!\otimes^E_{0^{\equiv}} \overline{\omega} = \mu$.

3.4 Semantics

The *stochastic transition relation* is the smallest relation $\mathfrak{T} \subseteq \mathbb{E} \times \mathbb{P} \times \Delta(\mathbb{P}, \Pi)^{\mathbb{A}^+}$ satisfying the semantics rules listed bellow, where $E \vdash P \to \mu$ denotes $(E, P, \mu) \in \mathfrak{T}$; it states that the behaviour of P in the environment E is defined by the mapping $\mu \in \Delta(\mathbb{P}, \Pi)^{\mathbb{A}^+}$. For each $\equiv$-closed set of processes $\mathcal{P} \in \Pi$ and each $\alpha \in \mathbb{A}^+$, $\mu(\alpha)(\mathcal{P}) \in \mathbb{R}^+$ represents the total rate of the α-reductions of P to the elements of $\mathcal{P}$. The rules involve also predicates of type $E \vdash ok$ that encode the correctness of E, i.e. that the environment associates base rates to a finite number of channels only, and that no channel appears in more than one rate declaration in that environment. Recall that $\equiv^*$ denotes alpha-conversion.

$$(Env\varepsilon). \quad \frac{}{\varepsilon \vdash ok} \qquad (Env@). \quad \frac{E \vdash ok \qquad a \notin dom(E)}{E, a@r \vdash ok}$$

$$(Null). \quad \frac{E \vdash ok}{E \vdash 0 \to \overline{\omega}} \qquad (Guard). \quad \frac{E \vdash ok \qquad fn(x.P) \subseteq dom(E)}{E \vdash x.P \to E^x_{P^{\equiv}}}$$

$$(Sum). \quad \frac{E \vdash P \to \mu \qquad E \vdash Q \to \eta}{E \vdash P + Q \to \mu \oplus \eta} \qquad (Par). \quad \frac{E \vdash P \to \mu \qquad E \vdash Q \to \eta}{E \vdash P|Q \to \mu \ {}_{P^{\equiv}}\otimes^E_{Q^{\equiv}} \eta}$$

$$(New). \quad \frac{E, a@r \vdash P \to \mu}{E \vdash (a@r)P \to (a@r)\mu} \qquad (Rep). \quad \frac{E \vdash P \to \mu}{E \vdash !P \to \mu_{!P^{\equiv}}}$$

$$(Alpha). \quad \frac{E \vdash P \to \mu \qquad P \equiv^* Q}{E \vdash Q \to \mu}$$

$(Null)$ guarantees that in any correct environment the behaviour of process 0 is described by $\overline{\omega}$, which associates the rate 0 to any transition.

$(Guard)$ associates to any prefixed process $x.P$ the mapping $E^x_{P^{\equiv}}$ which, as described in Definition 4, associates the base-rate of the channel of x to the x-transitions from $x.P$ to $P^{\equiv}$ and rate 0 to the other transitions.

(Sum) computes the rate of the α-transitions from $P + Q$ to $\mathcal{R} \in \Pi$, as the sum of the rates of the α-transitions from P and Q to $\mathcal{R}$ respectively.

(Par) takes into account the possible interactions between the processes. If $\rho = \mu \ {}_{P^{\equiv}}\otimes^E_{Q^{\equiv}} \eta$, the rate $\rho(\alpha)(\mathcal{R})$ of the α-transitions from $P|Q$ to $\mathcal{R}$ for $\alpha \neq \tau$, is the sum of the rates $\mu(\alpha)(\mathcal{R}_{Q^{\equiv}})$ and $\eta(\alpha)(\mathcal{R}_{P^{\equiv}})$ of the α-transitions from P to $\mathcal{R}_Q$ and from Q to $\mathcal{R}_P$ respectively; the rate of the τ-transitions from $P|Q$ to $\mathcal{R}$ is the sum of the rates of the τ-transitions that P or Q can do independently plus the rate of all communications between P and Q (bound represented by the first sum in Definition 4 3.(ii) and unbound represented by the last two sums). Because we use the base rate of the channel a when we calculate the rates of both inputs and outputs on a, the sums in Definition 4 3.(ii) are normalised by $E(a)$.

(New) establishes that the rate of the transitions from $(a@r)P$ to $(a@r)\mathcal{R} \in \Pi$ in the environment E is the rate of the corresponding transitions from P to

$\mathcal{R}$ in the environment $E, a@r$. The only thing one needs to take care of (see Definition 4) is when an output becomes bound while (New) is used. Consider, for instance, the process[3] $Q = b[a].P + (c@r)b[c].P_{\{c/a\}}$.

$E, a@r \vdash Q \xrightarrow{b[a],E(b)} P^{\equiv}$ and $E, a@r \vdash Q \xrightarrow{b[@r],r} (c@r)P^{\equiv}_{\{c/a\}}$.

Now, if we consider $(a@r)Q \equiv (a@r)b[a].P + (c@r)b[c].P_{\{c/a\}}$, because $(a@r)P \equiv (c@r)P_{\{c/a\}}$, the rates of the transitions in the environment E should be

$E \vdash (a@r)Q \xrightarrow{b[a],0} (a@r)P^{\equiv}$ and $E \vdash (a@r)Q \xrightarrow{b[@r],2r} (a@r)P^{\equiv}$.

Notice that the rate of $b[a]$-transition of Q contributes to the rate of $b[@r]$-transition of $(a@r)Q$ and this is how Definition 4 introduces $(a@r)\mu$.

(Rep) encodes the intuition that in the case of stochastic systems, if $E \vdash P \xrightarrow{\alpha,r} Q^{\equiv}$, then $E \vdash !P \xrightarrow{\alpha,r} !P|Q^{\equiv}$.

($Alpha$) proves properties by alpha-conversion: it guarantees that the behaviour of a process does not change if the bound variables are renamed. The standard presentations of PAs with unlabeled reduction mix structural congruence with reductions by rules of type (Struct). Because our reductions are labeled (the labels are hiden into the mappings), alpha conversion needs to be separately incorporated both in the algebra and coalgebra.

Notice that we do not have, for a fixed environment E, a binary operator on $\Delta(\mathbb{P}, \Pi)^{\mathbb{A}^+}$ to reflect the parallel composition of processes. Such a definition is, in fact, impossible. Assume, otherwise, that there exists an operator $\otimes^E$ such that if $E \vdash P \to \mu$ and $E \vdash Q \to \eta$, then $E \vdash P|Q \to \mu \otimes^E \eta$. The processes $P = a[b].0|c[d].0$ and $Q = a[b].c[d].0 + c[d].a[b].0$ have associated, in any correct environment E, the same mapping $\mu \in \Delta(\mathbb{P}, \Pi)^{\mathbb{A}^+}$. Suppose that $E \vdash R \to \eta$, where $R = e[f].0$. If, indeed, the operator $\otimes^E$ is well defined, then $E \vdash P|R \to \mu \otimes^E \eta$ and $E \vdash Q|R \to \mu \otimes^E \eta$, i.e. $P|R$ and $Q|R$ have associated the same mapping. But this is not the case, because $P^{\equiv} \neq Q^{\equiv}$ and

$E \vdash P|R \xrightarrow{e[f],E(e)} P^{\equiv}$ and $E \vdash P|R \xrightarrow{e[f],0} Q^{\equiv}$, while

$E \vdash Q|R \xrightarrow{e[f],0} P^{\equiv}$ and $E \vdash Q|R \xrightarrow{e[f],E(e)} Q^{\equiv}$.

This explains why we need to index $\otimes^E$ with $P^{\equiv}$ and $Q^{\equiv}$ and why the algebraic signature is changed when the structure of processes is lifted to indexed measures.

The next example illustrates some transitions in our framework.

Example 2. $E \vdash (b@r)(a[b].P)|a(c).Q \xrightarrow{\tau,E(a)} (b@r)(P|Q_{\{b/c\}})^{\equiv}$.

From (Guard) we derive $E, b@r \vdash a[b].P \xrightarrow{a[b],E(a)} P^{\equiv}$. (New) gives us further that $E \vdash (b@r)a[b].P \xrightarrow{a[@r],E(a)} (b@r)P^{\equiv}$ and this is the only transition with non-zero rate. Observe that the definition of $E^{a(c)}_{Q^{\equiv}}$ implies $E \vdash a(c).Q \xrightarrow{ab,E(a)} Q^{\equiv}_{\{b/c\}}$.

Applying the definition of $\otimes^E_{a(c).Q^{\equiv}}$, we obtain $E \vdash (b@r)(a[b].P)|a(c).Q \xrightarrow{\tau,s} (b@r)(P|Q_{\{b/c\}})^{\equiv}$ for $s = E(a)$ if $E(a) \neq 0$ and $s = 0$ if $E(a) = 0$.

[3] For simplicity, we continue using the notation of Example 1: $E \vdash P \xrightarrow{\alpha,r} \mathcal{R}$ denotes that $E \vdash P \to \mu$, and $\mu(\alpha)(\mathcal{R}) = r$.

A consequence of this result is the well known case of communication of a private name used for a private communication
$E \vdash (b@r)(a[b].b(e).P)|a(c).c[d].0 \stackrel{\tau,E(a)}{\longrightarrow} (b@r)(b(e).P|b[d].0) \stackrel{\equiv}{\stackrel{\tau,r}{\longrightarrow}} (b@r)P\{d/e\}$.
The first transition is a particular case of the example. For the second transition we apply the case 3 (ii) of Definition 4.

The next theorem states that $\mathfrak{T}$ is well defined and characterizes the correctness of an environment.

Theorem 2. *(i) If $E \vdash ok$ and $fn(P) \subseteq dom(E)$, then there exists a unique $\mu \in \Delta(\mathbb{P}, \Pi)^{\mathbb{A}^+}$ such that $E \vdash P \to \mu$.*
(ii) If $E \vdash P \to \mu$, then $E \vdash ok$. Moreover, $E \vdash ok$ iff $E \vdash 0 \to \overline{\omega}$.

The next theorem states a property of type (Struct).

Theorem 3. *If $E \vdash P' \to \mu$ and $P' \equiv P''$, then $E \vdash P'' \to \mu$.*

The next lemma describes how the environments can vary without influencing the mapping associated to a process.

Lemma 3. *1. If for any $a \in \mathcal{N}$ and $r \in \mathbb{Q}$, $[a@r \in E$ iff $a@r \in E']$, then $E \vdash P \to \mu$ iff $E' \vdash P \to \mu$.*
2. If $E' \vdash ok$, $E \subset E'$ and $E \vdash P \to \mu$, then $E' \vdash P \to \mu$.
3. If $E \subset E'$, $E \vdash P \to \mu$ and $dom(E' \setminus E) \cap fn(P) = \emptyset$, then $E' \vdash P \to \mu$.

4 Stochastic bisimulation

In this section we focus on stochastic bisimulation that reproduces, at the stochastic level, Larsen-Skou probabilistic bisimulation [17]. We have introduced a similar concept in [6] for the case of stochastic CCS. The novelty with the present definition consists in the role of the rate environments: two processes are stochastic bisimilar if they have similar stochastic behaviours in any rate environment.

Definition 5 (Stochastic Bisimulation). *A* rate-bisimulation *on $\mathbb{P}$ is an equivalence relation $\mathfrak{R} \subseteq \mathbb{P} \times \mathbb{P}$ such that $(P, Q) \in \mathfrak{R}$ iff for any $E \in \mathbb{E}$,*
– if $E \vdash P \to \mu$, then there exists $\eta \in \Delta(\mathbb{P}, \Pi)^{\mathbb{A}^+}$ such that $E \vdash Q \to \eta$ and for any $C \in \Pi(\mathfrak{R})$ and $\alpha \in \mathbb{A}^+$, $\mu(\alpha)(C) = \eta(\alpha)(C)$.
– if $E \vdash Q \to \eta$, then there exists $\mu \in \Delta(\mathbb{P}, \Pi)^{\mathbb{A}^+}$ such that $E \vdash P \to \mu$ and for any $C \in \Pi(\mathfrak{R})$ and $\alpha \in \mathbb{A}^+$, $\eta(\alpha)(C) = \mu(\alpha)(C)$.
Two processes $P, Q \in \mathbb{P}$ are stochastic bisimilar, denoted $P \sim Q$, if there exists a rate-bisimulation connecting them.

Observe that stochastic bisimulation is the largest rate-bisimulation on $\mathbb{P}$.

Example 3. If $a, b, x, y \in \mathcal{N}$, $a \neq b$ and $x \notin fn(b[y].Q)$, then
$a(x).P|b[y].Q \sim a(x).(P|b[y].Q) + b[y].(a(x).P|Q)$.
Indeed, for any compatible rate environment E,

$E \vdash a(x).P|b[y].Q \to E_P^{a(x)}{}_{a(x).P} \otimes_{b[y].Q} E_Q^{b[y]}$,

$E \vdash a(x).(P|b[y].Q) + b[y].(a(x).P|Q) \to E^{a(x)}_{P|b[y].Q} \oplus E^{b[y]}_{a(x).P|Q}$

and for arbitrary $C \in \Pi(\sim)$,

$E_P^{a(x)}{}_{a(x).P} \otimes_{b[y].Q} E_Q^{b[y]}(\alpha)(C) = E^{a(x)}_{P|b.Q} \oplus E^{b[y]}_{a(x).P|Q}(\alpha)(C) =$

$$\begin{cases} E(a) & \text{if } \alpha = ac,\ P_{\{c/x\}}|b[y].Q \in C, \\ 0 & \text{if } \alpha = ac,\ P_{\{c/x\}}|b[y].Q \notin C, \\ E(b) & \text{if } x = b[y],\ a(x).P|Q \in C, \\ 0 & \text{if } x = b[y],\ a(x).P|Q \notin C, \\ 0 & \text{else .} \end{cases}$$

The previous example shows bisimilar processes which are not structurally congruent. The reverse affirmation is not true.

Theorem 4. *If $P \equiv Q$, then $P \sim Q$.*

The next theorem, stating that stochastic bisimulation is a congruence, proves that we have identified a well-behaved semantics.

Theorem 5 (Congruence). *If $P \sim Q$, then*
1. for any $x \in \mathcal{N}^*$, $x.P \sim x.Q$;
2. for any $R \in \mathbb{P}$, $P + R \sim Q + R$,
3. for any $a \in \mathcal{N}$ and $r \in \mathbb{Q}^+$, $(a@r)P \sim (a@r)Q$;
4. for any $R \in \mathbb{P}$, $P|R \sim Q|R$.
5. $!P \sim !Q$.

5 Conclusions and future work

In this paper we propose a way of introducing stochastic process algebras that is faithful to the algebraic-coalgebraic structures of the concurrent Markovian processes. The semantics is given in terms of measure theory and describes the lifting of the algebraic structure of processes to the level of measures on the measurable space of processes. The paper treats the case of the complete stochastic Pi-calculus. Instead of the discrete measurable space of processes, we consider the measurable space induced by structural congruence and this idea has important advantages. Firstly, it matches practical modelling requirements: the identity of a system is not given by the stochastic process used to model it, but by its structural-congruence class (for systems biology this represents a chemical soup). Secondly, by working with measures on this space, we get important advantages on the level of the underlying theory such as a simple and elegant semantics, simple solutions for the problems related to bound output and replication (that otherwise require complicate transition labeling and higher order reasoning) and a well-behaved notion of stochastic bisimulation including associativity. Other advantages derive from the use of the rate environments that guarantees a certain robustness in modelling: a model cab be easily refined by modifying its rate environmet.

Our approach opens some future research directions. One is the study of the GSOS format where the main challenge is to understand the underlying category. Another is the definition of a pseudometric, similar with the one we introduce in [6], to measure the distance between processes in terms of similar behaviours. Our semantics is particularly appropriate for introducing such metrics via the metrics on measures such as the Kantorovich metrics on distributions used, for instance, in [19].

References

1. G. Berry, G. Boudol, *The Chemical Abstract Machine*, In Proc. POPL 1990:81-94.
2. J.A. Bergstra, et.al (Eds.), *Handbook of Process Algebra.* Elsevier, 2001.
3. M. Bernardo, R. Gorrieri. *A tutorial on EMPA: A theory of concurrent processes with nondeterminism, priorities, probabilities and time.* TCS 202(1-2), 1998.
4. M. Bravetti, H. Hermanns, J-P. Katoen, *YMCA: Why Markov Chain Algebra?*, ENTCS 162, 2006.
5. L. Cardelli, *A Process Algebra Master Equation.* In Proc. QEST'07, 2007.
6. L. Cardelli, R. Mardare. *The Measurable Space of Stochastic Processes.* QEST 2010, IEEE Press, 2010.
7. R. De Nicola, D. Latella, M. Loreti, M. Massink, *Rate-Based Transition Systems for Stochastic Process Calculi.* ICALP'09, LNCS 5556, 2009
8. E.P. de Vink, J. Rutten, *Bisimulation for probabilistic transition systems: A coalgebaic approach*, TCS 221(1-2), 1999.
9. M.P.Fiore, D.Turi. *Semantics of name and value passing.* LICS'01, IEEE Press, 2001.
10. M.P.Fiore, S.Staton. *A congruence rule format for name-passing process calculi.* Inf. and Comp., 207(2), 2009.
11. N. Gotz, U. Herzog, M. Rettelbach, *TIPP - A language for timed processes and performance evaluation.* Tech.Rep. 4/92 IMMD VII, University of Erlangen-Nurnberg.
12. J. Hillston, *A compositional approach to performance modelling.* Distinguished dissertation in Computer Science. Cambridge University Press, 1996.
13. J. Hillston, *Process algebras for quantitative analysis.* LICS'05, IEEE Press, 2005.
14. H. Hermanns, *Interactive Markov Chains.* LNCS 2428, 2008.
15. B. Klin, V. Sassone, *Structural Operational Semantics for Stochastic Process Calculi*, FOSSACS'08, LNCS 4968, 2008.
16. M. Kwiatkowska, et.al, *Automatic Verification of Real-Time Systems With Discrete Probability Distributions.*, LNCS 1601, 1999.
17. K.G. Larsen and A. Skou, *Bisimulation through probabilistic testing.* Inf. and Comp., 94, 1991.
18. R. Milner, *Communicating and Mobile Systems: the Pi-Calculus*, Cambridge Univ. Press, 1999.
19. P. Panangaden, *Labelled Markov Processes.* Imperial College Press, 2009.
20. C. Priami, *Stochastic π-Calculus.* Computer Journal, 38(7), 1995.
21. J. Rutten, *Universal coalgebra: a theory of systems*, TCS, 249, 2000.
22. R. Segala, N. Lynch, *Probabilistic Simulations for Probabilistic Processes*, Nordic J. of Comp., 2(2), 1995.
23. D. Turi, G.D. Plotkin, *Towards a mathematical operational semantics*, Lics'97, IEEE Press, 1997.

Appendix

In this appendix we have collected some of the proofs of the main results presented in the paper.

Proof (Theorem 2). (i) The existential part is proved by induction on the structure of P and the uniqueness by induction on derivations.

First we prove the existential part.

For $P = 0$ and $P = x.Q$, (Null) and (Guard) respectively guarantee the existence of μ.

For $P = Q + R$: because $fn(P) = fn(Q) \cup fn(R)$, $fn(Q) \subseteq dom(E)$ and $fn(R) \subseteq dom(E)$. We use the inductive hypothesis and obtain that exist two functions η, ρ such that $E \vdash Q \to \eta$ and $E \vdash R \to \rho$. From (Sum) we obtain that exists $\mu = \eta \oplus \rho$ such that $E \vdash P \to \mu$.

For $P = Q|R$: because $fn(P) = fn(Q) \cup fn(R)$, $fn(Q) \subseteq dom(E)$ and $fn(R) \subseteq dom(E)$. We use the inductive hypothesis and obtain that exist two functions η, ρ such that $E \vdash Q \to \eta$ and $E \vdash R \to \rho$. From (Par) we obtain that exists $\mu = \eta\langle_{Q^{\equiv}} E_{R^{\equiv}}\rangle\rho$ such that $E \vdash P \to \mu$.

For $P = (a@r)Q$: if $a \notin dom(E)$, then $E, a@r \vdash ok$ and the inductive hypothesis guarantees the existence of η such that $E, a@r \vdash Q \to \eta$. Further, applying (New), we get $E \vdash P \to (a@r)\eta$. If $a \in dom(E)$, let $b \in \mathcal{N} \setminus dom(E)$. Then $E, b@r \vdash ok$ and the inductive hypothesis guarantees the existence of η such that $E, b@r \vdash Q_{\{b/a\}} \to \eta$. Further, applying (New), we get $E \vdash (b@r)Q_{\{b/a\}} \to (b@r)\eta$ and (Alpha) gives $E \vdash (a@r)Q \to (b@r)\eta$. Consequently, in all the cases there exists μ such that $E \vdash (a@r)Q \to \mu$.

For $P = !Q$: because $fn(Q) = fn(P)$, the inductive hypothesis guarantees the existence of a unique η such that $E \vdash Q \to \eta$. Further, applying (Rep), we get $E \vdash P \to \eta_{!Q}$.

The uniqueness part is done by induction on derivations.

The rules (Envε) and (Env@) are only proving the correctness of environments and consequently will not interfere with our proof.

Observe that all the derivations involving only the rules (Sum), (Par), (New) and (Rep), called in what follows *basic proofs*, demonstrate properties about processes with a more complex syntax than the processes involved in the hypotheses. Consequently, taking (Null) and (Guard) as basic cases, an induction on the structures of the processes involved in the derivations shows the uniqueness of μ for the situation of the basic proofs. Notice, however, that due to (New) a basic proof proves properties of type $E \vdash P \to \mu$ only for cases when $new(P) \cap dom(E) = \emptyset$, where $new(P)$ is the set of names of P bound by fresh name quantifiers. To conclude the proof we need to show that if $Q = P_{\{a/b\}}$ with $a, b \notin fn(P)$ and if $E \vdash P \to \mu$ and $E \vdash Q \to \eta$ can be proved with basic proofs, then $\mu = \eta$.We do this by induction on P.
If $P = 0$, then $Q = 0$ and $\eta = \mu = \overline{\omega}$.
If $P = c[d].R$, then $Q = c[d].R_{\{a/b\}}$ and $a, b \notin fn(R)$. Moreover, $\mu = E^{c[d]}_{R^{\equiv}}$ and $\eta = E^{c[d]}_{R^{\equiv}_{\{a/b\}}}$. But because $a, b \notin fn(R)$, $R \equiv R_{\{a/b\}}$ implying further $\mu = \eta$.

If $P = c(d).R$, then if $d \neq b$ the proof goes as in the previous case. If $P = c(b).R$, then $Q = c(a).R_{\{a/b\}}$, $\mu = E_R^{c(b)}$ and $\eta = E_{R_{\{a/b\}}}^{c(a)}$. It is trivial to verify that $\mu = \eta$.
If $P = S+T$, then $Q = S_{\{a/b\}}+T_{\{a/b\}}$. Suppose that $E \vdash S \to \rho$ and $E \vdash T \to \nu$, then from the inductive hypothesis, $E \vdash S_{\{a/b\}} \to \rho$ and $E \vdash T_{\{a/b\}} \to \nu$. Hence, $\mu = \eta = \rho \oplus \nu$.
If $P = S|T$ the proof goes as in the previous case.
If $P =!R$, $Q =!R_{\{a/b\}}$. Suppose that $E \vdash R \to \rho$. From the inductive hypothesis we also obtain that $E \vdash R_{\{a/b\}} \to \rho$. The conclusion derives further from the fact that $!R \equiv !R_{\{a/b\}}$ because $a, b \notin fn(R)$.
If $P = (c@r)R$ with $c \neq b$, then $Q = (c@r)R_{\{a/b\}}$. Because we are in the case of a basic proof, $c \notin dom(E)$. Suppose that $E, c@r \vdash R \to \rho$. This is the unique hypothesis that proves $E \vdash P \to \mu$. Then, $\mu = (c@r)\rho$ and the inductive hypothesis implies that $E, c@r \vdash R_{\{a/b\}} \to \rho$ is the unique hypothesis that proves $E \vdash Q \to \eta$. Further we get $E \vdash (c@r)R_{\{a/b\}} \to (c@r)\rho$. Hence, in this case, $\mu = \eta$.
If $P = (b@r)R$, then $Q = (a@r)R_{\{a/b\}}$. Because we work with basic proofs, we have $a, b \notin dom(E)$. A simple induction proves that if $E, b@r \vdash R \to \rho$, then $E, a@r \vdash R_{\{a/b\}} \to \rho'$, where for any $\alpha \in \mathbb{A}^+$ and any $\mathcal{R} \in \Pi$, $\rho(\alpha)(\mathcal{R}) = \rho'(\alpha_{\{a/b\}})(\mathcal{R}_{\{a/b\}})$. From here we get $(b@r)\rho = (a@r)\rho'$. Observe that $E, b@r \vdash R \to \rho$ is the unique hypothesis that can be used in a basic proof to derive $E \vdash (b@r)R \to \mu$ and $\mu = (b@r)\rho$. Similarly, $E, a@r \vdash R_{\{a/b\}} \to \rho'$ is the unique hypothesis to prove $E \vdash (a@r)R_{\{a/b\}} \to \eta$ and $\eta = (a@r)\rho'$. Hence, also in this case, $\mu = \eta$.

In this way we have proved that any couple of alpha-converted processes have associated the same mapping by basic proofs. In addition, (Alpha) guarantees that any kind of proofs will associate to alpha-converted processes the same mapping and this concludes our proof.

(ii) We prove the first part by induction on derivations. The second part is a consequence of the first part and (Null).
If $E \vdash P \to \mu$ is proved by (Null) or (Guard), $E \vdash ok$ is required as hypothesis.
If $E \vdash P \to \mu$ is proved by (Sum), $P = Q + R$, $\mu = \eta \oplus \rho$ and $E \vdash Q \to \eta$ and $E \vdash R \to \rho$ are the hypothesis and we can use the inductive hypothesis.
If $E \vdash P \to \mu$ is proved by (Par), the argument goes as in the previous case.
If $E \vdash P \to \mu$ is proved by (New), then $P = (a@r)Q$ and the hypothesis is of type $E, a@r \vdash Q \to \eta$. The inductive hypothesis gives $E, a@r \vdash ok$ and this can only be proved by (Env@) from $E \vdash ok$.
If $E \vdash P \to \mu$ is proved by (Rep), then $P =!Q$ and $E \vdash Q$ is the hypothesis and we can apply the inductive step.
If $E \vdash P \to \mu$ is proved by (Alpha), we can use the inductive hypothesis again.

Proof (Lemma 3). **1.** A simple induction on derivations that involve only (Envε) and (Env@) proves that $E \vdash ok$ iff $E' \vdash ok$. For proving our lemma we will proceed with an induction on the derivation of $E \vdash P \to \mu$.

If $E \vdash P \to \mu$ is proved by (Null), we have that $P = 0$ and due to Theorem 2, $\mu = \overline{\omega}$. Applying (Null) we obtain $E' \vdash P \to \mu$.

If $E \vdash P \to \mu$ is proved by (Guard), we have that $P = x.Q$ and due to Theorem 2, $\mu = E^x_Q$. Because $E^x_Q = E'^x_Q$ and $dom(E) = dom(E')$, we obtain $E' \vdash P \to \mu$.

If $E \vdash P \to \mu$ is proved by (Sum), we have that $P = Q + R$, $\mu = \eta \oplus \rho$ and the hypothesis are $E \vdash Q \to \eta$ and $E \vdash R \to \rho$. From the inductive hypothesis we obtain $E' \vdash Q \to \eta$ and $E' \vdash R \to \rho$. Further, applying (Sum) we get $E' \vdash P \to \mu$.

If $E \vdash P \to \mu$ is proved by (Par) we have that $P = Q|R$, $\mu = \eta \ {}_Q\otimes^E_R \rho$ and the hypothesis are $E \vdash Q \to \eta$ and $E \vdash R \to \rho$. From the inductive hypothesis we obtain $E' \vdash Q \to \eta$ and $E' \vdash R \to \rho$. Further, applying (Par) we get $E' \vdash P \to \eta \ {}_Q\otimes^{E'}_R \rho$. But $\eta \ {}_Q\otimes^E_R \rho = \eta \ {}_Q\otimes^{E'}_R \rho$.

If $E \vdash P \to \mu$ is proved by (Rep), we have that $P = !Q$, $\mu = \eta_{!Q}$ and the hypothesis is $E \vdash Q \to \eta$. Applying the inductive step we get $E' \vdash Q \to \eta$ and (Rep) guarantees that $E' \vdash P \to \mu$.

If $E \vdash P \to \mu$ is proved by (New), we have that $P = (a@r)Q$, $\mu = (a@r)\eta$ and the hypothesis is $E, a@r \vdash Q \to \eta$. Hence, $a \notin dom(E) = dom(E')$ and we can apply the inductive hypothesis because $b@s \in E, a@r$ iff $b@s \in E', a@r$ and obtain $E', a@r \vdash Q \to \eta$ where from we get $E' \vdash P \to \mu$.

If $E \vdash P \to \mu$ is proved by (Alpha), we have that $P = Q_{\{a/b\}}$ with $a, b \notin fn(P) = fn(Q)$ and the hypothesis is $E \vdash Q \to \mu$. As before, the inductive hypothesis guarantees that $E' \vdash Q \to \mu$ and because $a, b \notin fn(Q)$, (Alpha) proves $E' \vdash P \to \mu$.

2. Induction on the derivation of $E \vdash P \to \mu$.

If $E \vdash P \to \mu$ is proved by (Null), we have that $P = 0$ and due to Theorem 2, $\mu = \overline{\omega}$. Applying (Null) we obtain $E' \vdash P \to \mu$.

If $E \vdash P \to \mu$ is proved by (Guard), we have that $P = x.Q$ and due to Theorem 2, $\mu = E^x_Q$. Because $fn(P) \subseteq dom(E) \subseteq dom(E')$ and $E^x_Q = E'^x_Q$, we obtain $E' \vdash P \to \mu$.

If $E \vdash P \to \mu$ is proved by (Sum), we have that $P = Q + R$, $\mu = \eta \oplus \rho$ and the hypothesis are $E \vdash Q \to \eta$ and $E \vdash R \to \rho$. From the inductive hypothesis we obtain $E' \vdash Q \to \eta$ and $E' \vdash R \to \rho$. Further, applying (Sum) we get $E' \vdash P \to \mu$.

If $E \vdash P \to \mu$ is proved by (Par) we have that $P = Q|R$, $\mu = \eta \ {}_Q\otimes^E_R \rho$ and the hypothesis are $E \vdash Q \to \eta$ and $E \vdash R \to \rho$. From the inductive hypothesis we obtain $E' \vdash Q \to \eta$ and $E' \vdash R \to \rho$. Further, applying (Par) we get $E' \vdash P \to \eta \ {}_Q\otimes^{E'}_R \rho$. But $\eta \ {}_Q\otimes^E_R \rho = \eta \ {}_Q\otimes^{E'}_R \rho$.

If $E \vdash P \to \mu$ is proved by (Rep), we have that $P = !Q$, $\mu = \eta_{!Q}$ and the hypothesis is $E \vdash Q \to \eta$. Applying the inductive step we get $E' \vdash Q \to \eta$ and (Rep) guarantees that $E' \vdash P \to \mu$.

If $E \vdash P \to \mu$ is proved by (Alpha), we have that $P = Q_{\{a/b\}}$ with $a, b \notin fn(P) = fn(Q)$ and the hypothesis is $E \vdash Q \to \mu$. As before, the inductive hypothesis guarantees that $E' \vdash Q \to \mu$ and because $a, b \notin fn(Q)$, (Alpha) proves that $E' \vdash P \to \mu$.

If $E \vdash P \to \mu$ is proved by (New), we have that $P = (a@r)Q$, $\mu = (a@r)\eta$ and the hypothesis is $E, a@r \vdash Q \to \eta$. Hence, $a \notin dom(E)$. If $a \notin dom(E')$, the inductive hypothesis guarantees that $E', a@r \vdash Q \to \eta$ where from we get $E' \vdash P \to \mu$. If $a \in dom(E')$, let $b \notin dom(E') \cup fn(P)$. Because $E, a@r \vdash Q \to \eta$ is provable, also $E, b@r \vdash Q_{\{b/a\}} \to \eta_{\{b/a\}}$ is provable, where $\eta_{\{b/a\}}$ is the mapping obtained from η replacing all the occurrences of a in the definition of η (in processes and labels) with b. Moreover, to each proof of $E, a@r \vdash Q \to \eta$ corresponds a proof of $E, b@r \vdash Q_{\{b/a\}} \to \eta_{\{b/a\}}$ that is, from the point of view of our induction, at the same level with the proof of $E, a@r \vdash Q \to \eta$. Consequently, we can apply the inductive hypothesis to $E, b@r \vdash Q_{\{b/a\}} \to \eta_{\{b/a\}}$ and obtain $E', b@r \vdash Q_{\{b/a\}} \to \eta_{\{b/a\}}$. (New) implies $E' \vdash (b@r)Q_{\{b/a\}} \to (b@r)\eta_{\{b/a\}}$ and (Alpha) $E' \vdash (a@r)Q \to (b@r)\eta_{\{b/a\}}$. To conclude, it is sufficient to verify that $(a@r)\eta = (b@r)\eta_{\{b/a\}}$.

3. The proof goes similarly with the proof of the previous case. We use an induction on the derivation of $E \vdash P \to \mu$.

If $E \vdash P \to \mu$ is proved by (Null), we have that $P = 0$ and $\mu = \overline{\omega}$. Applying (Null) we obtain $E' \vdash P \to \mu$.

If $E \vdash P \to \mu$ is proved by (Guard), we have that $P = x.Q$ and $\mu = G'^x_Q$. Because $fn(P) \subseteq dom(E)$, $fn(P) \cap dom(E \setminus E') = \emptyset$ and $E^x_Q = E'^x_Q$, we obtain $E' \vdash P \to \mu$.

If $E \vdash P \to \mu$ is proved by (Sum), we have that $P = Q + R$, $\mu = \eta \oplus \rho$ and the hypothesis are $E \vdash Q \to \eta$ and $E \vdash R \to \rho$. From the inductive hypothesis we obtain $E' \vdash Q \to \eta$ and $E' \vdash R \to \rho$. Further, applying (Sum) we get $E' \vdash P \to \mu$.

If $E \vdash P \to \mu$ is proved by (Par) we have that $P = Q|R$, $\mu = \eta\ {}_Q\otimes^E_R\ \rho$ and the hypothesis are $E \vdash Q \to \eta$ and $E \vdash R \to \rho$. From the inductive hypothesis we obtain $E' \vdash Q \to \eta$ and $E' \vdash R \to \rho$. Further, applying (Par) we get $E' \vdash P \to \eta\ {}_Q\otimes^{E'}_R\ \rho$. But $\eta\ {}_Q\otimes^E_R\ \rho = \eta\ {}_Q\otimes^{E'}_R\ \rho$.

If $E \vdash P \to \mu$ is proved by (Rep), we have that $P = !Q$, $\mu = \eta_{!Q}$ and the hypothesis is $E \vdash Q \to \eta$. Applying the inductive step we get $E' \vdash Q \to \eta$ and (Rep) guarantees that $E' \vdash P \to \mu$.

If $E \vdash P \to \mu$ is proved by (Alpha), we have that $P = Q_{\{a/b\}}$ with $a, b \notin fn(P) = fn(Q)$ and the hypothesis is $E \vdash Q \to \mu$. As before, the inductive hypothesis guarantees that $E' \vdash Q \to \mu$ and because $a, b \notin fn(Q)$, (Alpha) proves that $E' \vdash P \to \mu$.

If $E \vdash P \to \mu$ is proved by (New), we have that $P = (a@r)Q$, $\mu = (a@r)\eta$ and the hypothesis is $E, a@r \vdash Q \to \eta$. Hence, $a \notin dom(E)$ and because $dom(E') \subseteq dom(E)$, we obtain that $a \notin dom(E')$. Because $E, a@r \subset E', a@r$ and $dom((E', a@r) \setminus (E, a@r)) = dom(E' \setminus E)$, we can apply the inductive hypothesis and from $E, a@r \vdash Q \to \eta$ we obtain $E', a@r \vdash Q \to \eta$ where from we get $E' \vdash P \to \mu$.

Proof (Theorem 5). From $P' \equiv P''$ we obtain that $fn(P') = fn(P'')$ and Theorem 2 ensures that $E \vdash P' \to \mu$ implies that there exists a unique μ' such that $E \vdash P'' \to \mu'$.

We prove now that $E \vdash P' \to \mu$ implies $E \vdash P'' \to \mu$. The proof is an induction following the rules of structural congruence presented in Definition 2.
Rule I.1: if $P' = P|Q$ and $P'' = Q|P$. Suppose that $E \vdash P \to \eta$ and $E \vdash Q \to \rho$. Then $\mu = \eta \ {}_P\otimes^E_Q \rho$ and Lemma 2 guarantees that $E \vdash P'' \to \mu$.

Similarly we can treat all the rules of group I.
Rules of group II: As previously, the results derive from the properties of $\oplus$ stated in Lemma 2.
Rules of group III: If ($P' = P|R$ and $P'' = Q|R$), or ($P' = P + R$ and $P'' = Q + R$), or ($P' = x.P$ and $P'' = x.Q$), or ($P' =!P$ and $P'' =!Q$) for $P \equiv Q$, we can apply the inductive hypothesis that guarantees that $E \vdash P \to \eta$ iff $E \vdash Q \to \eta$. Further, if $E \vdash R \to \rho$, we obtain the desired results because $\eta \ {}_P\otimes^E_R \rho = \eta \ {}_Q\otimes^E_R \rho$, $\eta \oplus \rho = \eta \oplus \rho$, $E^x_P = E^x_Q$ and $\mu_{!P} = \mu_{!Q}$.
If $P' = (a@r)P$ and $P'' = (a@r)Q$, we have two subcases.

Subcase 1: $a \notin dom(E)$. Suppose that $E, a@r \vdash P \to \eta$. From the inductive hypothesis we obtain that $E, a@r \vdash Q \to \eta$. Further, rule (New) proves that $\mu = (a@r)\eta$ and $E \vdash (a@r)Q \to \mu$.

Subcase 2: $a \in dom(E)$. Let $b \in \mathcal{N} \setminus dom(E)$. Suppose that $E, b@r \vdash P_{\{b/a\}} \to \eta$. Then, (New) implies $E \vdash (b@r)P_{\{b/a\}} \to (b@r)\eta$ and (Alpha) proves $E \vdash (a@r)P \to (b@r)\eta$. Hence, $\mu = (b@r)\eta$. On the other hand, the inductive hypothesis implies $E, b@r \vdash Q_{\{b/a\}} \to \eta$, (New) proves $E \vdash (b@r)Q_{\{b/a\}} \to (b@r)\eta$ and (Alpha) implies $E \vdash (a@r)Q \to (b@r)\eta$.
Rule IV.1: If $P' = (a@r)(b@s)P$ and $P'' = (b@s)(a@r)P$. Let $c, d \in \mathcal{N} \setminus dom(E)$. Suppose that $E; c@r; d@s \vdash P_{\{c/a,d/b\}} \to \eta$. Applying twice (New) we obtain $E \vdash (c@r)(d@s)P_{\{c/a,d/b\}} \to (c@r)(d@s)\eta$ and applying twice (Alpha) we get $E \vdash (a@r)(b@s)P \to (c@r)(d@s)\eta$. Hence, $\mu = (c@r)(d@s)\eta$. On the other hand, Lemma 3.1 guarantees that $E; c@r; d@s \vdash P_{\{c/a,d/b\}} \to \eta$ implies $E; d@s; c@r \vdash P_{\{c/a,d/b\}} \to \eta$ and, as before, we eventually obtain $E \vdash (b@s)(a@r)P \to (d@s)(c@r)\eta$. Now it is suficient to verify that $(d@s)(c@r)\eta = (c@r)(d@s)\eta$.
Rule IV.2: If $P' = (a@r)0$ and $P'' = 0$. In this case it is sufficient to notice that $(a@r)\overline{\omega} = \overline{\omega}$.
Rule IV.3: If $P' = (a@r)(P|Q)$ and $P'' = P|(a@r)Q$, where $a \notin fn(P)$. Let $b \in \mathcal{N} \setminus (dom(E) \cup fn(P))$. Suppose that $E, b@r \vdash P \to \eta$ and $E, b@r \vdash Q_{\{b/a\}} \to \rho$. Observe that because $a \notin fn(P)$, we also have $E, b@r \vdash P_{\{b/a\}} \to \eta$. Further we obtain

$$E, b@r \vdash (P|Q)_{\{b/a\}} \to \eta \ {}_{P_{\{b/a\}}}\otimes^{E,b@r}_{Q_{\{b/a\}}} \rho \text{ and}$$

$$E \vdash (b@r)((P|Q)_{\{b/a\}}) \to (b@r)(\eta \ {}_{P_{\{b/a\}}}\otimes^{E,b@r}_{Q_{\{b/a\}}} \rho).$$

Now we apply (Alpha) and obtain

$$E \vdash (a@r)(P|Q) \to (b@r)(\eta \ {}_P\otimes^{E,b@r}_{Q_{\{b/a\}}} \rho).$$

On the other hand, because $b \notin fn(P)$, from $E, b@r \vdash P \to \eta$ Lemma 3.2 proves $E \vdash P \to \eta$ and from $E, b@r \vdash Q_{\{b/a\}} \to \rho$ we obtain, applying (New), $E \vdash (b@r)Q_{\{b/a\}} \to (b@r)\rho$. And further,

$$E \vdash P|(b@r)Q_{\{b/a\}} \to \eta \ {}_P\otimes^E_{(b@r)Q_{\{b/a\}}} (b@r)\rho.$$

Applying (alpha) we obtain

$$E \vdash P|(a@r)Q \rightarrow \eta\ {}_P\otimes^E_{(b@r)Q_{\{b/a\}}}\ (b@r)\rho.$$

A simple verification based on the observation that (if for all $R \in \mathcal{R}$, $b \notin fn(R)$, then $(b@r)\mathcal{R} = \mathcal{R}$) proves that

$$(b@r)(\eta\ {}_P\otimes^{E,b@r}_{Q_{\{b/a\}}}\ \rho) = \eta\ {}_P\otimes^E_{(b@r)Q_{\{b/a\}}}\ (b@r)\rho.$$

Similarly can be proved that case $P' = (a@r)(P+Q)$ and $P'' = P+(a@r)Q$, where $a \notin fn(P)$.

Rules of group V: By a simple verification one can prove that $\overline{\omega}_{!0} = \overline{\omega}$. For the second rule, observe that if $E \vdash P \rightarrow \eta$ and $E \vdash Q \rightarrow \rho$, then $E \vdash !(P|Q) \rightarrow (\eta\ {}_P\otimes^E_Q\ \rho)_{!(P|Q)}$ and $E \vdash !P|!Q \rightarrow \eta\ {}_{!Q|P}\otimes^E_{!P|Q}\ \rho$. And a simple verification proves that

$$(\eta\ {}_P\otimes^E_Q\ \rho)_{!(P|Q)} = \eta\ {}_{!Q|P}\otimes^E_{!P|Q}\ \rho.$$

Rules of group VI: These rules are a direct consequence of (Alpha).

Proof (Theorem 5). **1. Prefix:** For any $C \in \Pi(\sim)$, $P \in C$ iff $Q \in C$. This entails that for any $E \in \mathbb{E}$ with $fn(x.P) \cup fn(x.Q) \subseteq dom(E)$ and any $\alpha \in \mathbb{A}^+$, $E^x_P(\alpha)(C) = E^x_Q(\alpha)(C)$.

2. Choice: We can suppose, without loosing generality, that $E \vdash P \rightarrow \mu$, $E \vdash Q \rightarrow \eta$ and $E \vdash R \rightarrow \rho$ (the other cases are trivially true). Then, $E \vdash P + R \rightarrow \mu \oplus \rho$ and $E \vdash Q + R \rightarrow \eta \oplus \rho$. Let $C \in \Pi(\sim)$ and $\alpha \in \mathbb{A}^+$. Because $P \sim Q$, $\mu(\alpha)(C) = \eta(\alpha)(C)$ implying $\mu(\alpha)(C) + \rho(\alpha)(C) = \eta(\alpha)(C) + \rho(\alpha)(C)$. This means that $(\mu \oplus \rho)(\alpha)(C) = (\eta \oplus \rho)(\alpha)(C)$.

3. Fresh name quantification: Let $E \in \mathbb{E}$ and $b \notin dom(E) \cup fn(P) \cup fn(Q)$. Observe that from $P \sim Q$, following an observation that we used also in the proof of Lemma 3 concerning the relation between a mapping η its correspondent $\eta_{\{b/a\}}$, we derive $P_{\{b/a\}} \sim Q_{\{b/a\}}$. Suppose that $E, b@r \vdash P_{\{b/a\}} \rightarrow \mu$ and $E, b@r \vdash Q_{\{b/a\}} \rightarrow \eta$. Applying (New) we obtain $E \vdash (b@r)P_{\{b/a\}} \rightarrow (b@r)\mu$ and $E \vdash (b@r)Q_{\{b/a\}} \rightarrow (b@r)\eta$. (Alpha) implies $E \vdash (a@r)P \rightarrow (b@r)\mu$ and $E \vdash (a@r)Q \rightarrow (b@r)\eta$. From $P_{\{b/a\}} \sim Q_{\{b/a\}}$ we obtain that for any $\alpha \in \mathbb{A}^+$ and any $C \in \Pi(\sim)$, $\mu(\alpha)(C) = \eta(\alpha)(C)$. to conclude the proof it is sufficient to verify that $(b@r)\mu(\alpha)(C) = (b@r)\eta(\alpha)(C)$.

4. Parallel composition: For the beginning we consider the processes that, to all syntactic levels, contain no subprocess form the class $0^{\equiv}$ in a parallel composition. Let's call them *processes with non-trivial forms*. We will first prove the lemma for processes with non-trivial forms.

For arbitrary $n \in \mathbb{N}$, let $\mathbb{P}^n$ be the set of process terms with non-trivial forms and no more than n occurrences of the operator "|". Let $\sim^n \subseteq \mathbb{P}^n \times \mathbb{P}^n$ be the largest rate-bisimulation defined on $\mathbb{P}^n$. We define $\approx^n \in \mathbb{P}^n \times \mathbb{P}^n$ by

$$\approx^n = \sim^{n-1} \cup$$

$$\{(P_1|...|P_k, Q_1|...|Q_k), (P_1 + ...P_k, Q_1 + ...Q_k) \text{ for } P_i \sim^{n-1} Q_i, i = 1..k, k \leq n\}.$$

We show, by induction on n, that $\approx^n$ is a rate-bisimulation, i.e. that $\approx^n \subseteq \sim^n$.

Suppose that $P \approx^n Q$. We need to prove that if $E \vdash P \to \mu$ and $E \vdash Q \to \eta$, then for any $\alpha \in \mathbb{A}^+$ and any $C \in \Pi(\approx^n)$, $\mu(\alpha)(C) = \eta(\alpha)(C)$.

Observe that, from the way we construct $\approx^n$, there are three possibilities: either $P \sim^{n-1} Q$, or $P = P_1 + ...P_k$ and $Q = Q_1 + ...Q_k$, or $P = P_1|...|P_k$ and $Q = Q_1|...|Q_k$, for $k \leq n$, with $P_i \sim^{n-1} Q_i$ for each $i = 1..k$. In the first two cases, using also the case of choice operator that we have already proved, it is trivial to verify that $\mu(\alpha)(C) = \eta(\alpha)(C)$.

To prove the last case observe for the beginning that because $\sim^{n-1} \subseteq \sim^n$, the inductive hypothesis guarantees that for each $i = 1..k$,
$P_1|...|P_{i-1}|P_{i+1}|...|P_k \approx^{n-1} Q_1|...|Q_{i-1}|Q_{i+1}|...|Q_k$ and consequently that
$P_1|...|P_{i-1}|P_{i+1}|...|P_k \sim^{n-1} Q_1|...|Q_{i-1}|Q_{i+1}|...|Q_k$.

Suppose that $E \vdash P_i \to \mu_i$ and $E \vdash Q_i \to \eta_i$ for all $i = 1..k$. Then,

$$\mu = \mu_1 \ {}_{P_1}\otimes^E_{P_2|...|P_k} (\mu_2 \ {}_{P_2}\otimes^E_{P_3|...|P_k} (...(\mu_{k-1} \ {}_{P_{k-1}}\otimes^E_{P_k} \mu_k)...),$$

$$\eta = \eta_1 \ {}_{Q_1}\otimes^E_{Q_2|...|Q_k} (\eta_2 \ {}_{Q_2}\otimes^E_{Q_3|...|Q_k} (...(\eta_{k-1} \ {}_{Q_{k-1}}\otimes^E_{Q_k} \eta_k)...),$$

Consider an arbitrary $\alpha \in \mathbb{A}$. Then,

$$\mu(\alpha)(C) = \sum_{i=1..k} \mu_i(\alpha)(C_{P_1|...|P_{i-1}|P_{i+1}|...|P_k}),$$

$$\eta(\alpha)(C) = \sum_{i=1..k} \eta_i(\alpha)(C_{Q_1|...|Q_{i-1}|Q_{i+1}|...|Q_k}).$$

Because $C \in \Pi(\approx^n)$, $C_{P_1|...|P_{i-1}|P_{i+1}|...|P_k}$ and $C_{Q_1|...|Q_{i-1}|Q_{i+1}|...|Q_k}$ contain only processes with at most $n-1$ occurrences of $|$, for any i. And because $P_1|...|P_{i-1}|P_{i+1}|...|P_k \sim^{n-1} Q_1|...|Q_{i-1}|Q_{i+1}|...|Q_k$, we obtain

$$C_{P_1|...|P_{i-1}|P_{i+1}|...|P_k} = C_{Q_1|...|Q_{i-1}|Q_{i+1}|...|Q_k} \in \Pi(\sim^{n-1}).$$

Further, using the fact that $\sim^{n-1}$ is a rate bisimulation, we obtain

$$\mu(\alpha)(C_{P_1|...|P_{i-1}|P_{i+1}|...|P_k}) = \eta(\alpha)(C_{Q_1|...|Q_{i-1}|Q_{i+1}|...|Q_k})$$

that implies $\mu(\alpha)(C) = \eta(\alpha)(C)$.

A similar argument proves the case $\alpha = \tau$. Consequently, $\approx^n$ is a rate-bisimulation.

Returning to our lemma, suppose that P and Q are two processes with non-trivial forms such that $P \sim Q$. Then, there exists $n \in \mathbb{N}$ such that $P \sim^n Q$. Suppose that $R \in \mathbb{P}^m$ for some $m \in \mathbb{N}$. Then $P \sim^{m+n-1} Q$ and $R \sim^{m+n-1} R$ implying $P|R \approx^{m+n} Q|R$. Because $\approx^{m+n}$ is a rate-bisimulation, we obtain that $P|R \sim Q|R$.

If P, Q or R (or some of them) have "trivial forms", then there exist $P' \equiv P$, $Q' \equiv Q$ and $R' \equiv R$ with non-trivial forms. And because the bisimulation is an

equivalence that extends the structural congruence, we obtain the desired result also for the general case.

5. Replication: We use the same proof strategy as for the parallel composition. We say that a process is in canonic form if it contains no parallel composition of replicated subprocesses and no replicated process from the class $0^{\equiv}$. In other words, $!(P|Q)$ is in canonic form while $!P|!Q$ and $!(P|Q)|!!0$ are not; using the structural congruence rules, we can associate to each process P a structural congruent process with a canonic form called a canonic representative for P. Notice also that all the canonic representatives of a given process have the same number of occurrences of the operator "!". Let $\mathbb{P}_*$ be the set of process terms with canonic form. Observe that because structural congruence is a subset of bisimulation, it is sufficient to prove our lemma only for processes in $\mathbb{P}_*$.

As before, let $\mathbb{P}_*^n$ be the set of processes (in canonic form) with no more than n occurrences of the operator "!". Let $\sim^n$ be the stochastic bisimulation on $\mathbb{P}_*^n$ and $\approx^n \subseteq \mathbb{P}_*^n \times \mathbb{P}_*^n$ defined by

$$\approx^n = \sim^{n-1} \cup \{(!P, !Q) \mid P \sim^{n-1} Q\}.$$

We firstly show, inductively on n, that $\approx^n$ is a rate-bisimulation. Consider two arbitrary processes P and Q such that $P \approx^n Q$. We prove that if $E \vdash P \to \mu$ and $E \vdash Q \to \eta$, then for arbitrary $\alpha \in \mathbb{A}^+$ and $C \in \Pi(\approx^n)$, $\mu(\alpha)(C) = \eta(\alpha)(C)$.

Observe that if $P \approx^n Q$, then either $P \sim^{n-1} Q$, or $P \equiv !R$ and $Q \equiv !S$ with $R \sim^{n-1} S$. In the first case the equality is trivially true. In the other case, suppose that $E \vdash R \to \mu'$ and $E \vdash S \to \eta'$. Then, $\mu = \mu'_{!R}$ and $\eta = \eta'_{!S}$. We have

$$\mu(\alpha)(C) = \mu'(\alpha)(C_{!R}), \qquad \eta(\alpha)(C) = \eta'(\alpha)(C_{!S}).$$

We prove that $C_{!R} = C_{!S}$. Let $U \in C_{!R}$. Then, $U|!R \in C$ and from the construction of $C \in \Pi(\approx^n)$, we obtain that there exists $T \in \mathbb{P}_*^{n-1}$ such that $U = !T$. Because $!R|!T \in C$, $!(R|T) \in C$. Now, from $R \sim^{n-1} S$ we obtain $R \sim S$ and because $T \sim T$, the case of parallel operator that we have proved guarantees that $R|T \sim S|T$. But the canonic representatives V, W of $R|T$ and $S|T$ respectively are in $\mathbb{P}_*^{n-1}$ meaning that $V \sim^{n-1} W$. The construction of $\approx^n$ guarantees further that $!V \approx^n !W$ and because $W \equiv S|T$ we obtain $!(S|T) \in C$ and $U \equiv !T \in C_{!S}$.

Because $C_{!R} = C_{!S}$ and $\mu'(\alpha)(C_{!R}) = \eta'(\alpha)(C_{!S})$ (this is implied by $R \sim^{n-1} S$), then $\mu(\alpha)(C) = \eta(\alpha)(C)$.