A Note on the Congruence Proof for Recursion in Markovian Bisimulation Equivalence

Mario Bravetti Marco Bernardo Roberto Gorrieri

Università di Bologna, Dipartimento di Scienze dell'Informazione
Mura Anteo Zamboni 7, 40127 Bologna, Italy
E-mail: {bravetti, bernardo, gorrieri}@cs.unibo.it

Abstract

This note repairs some inaccuraces in the congruence proof for recursion previously developed for EMPA. We provide a revised proof based on standard machinery obtained by smoothly extending Milner's technique based on bisimulation up to. The machinery we introduce can be easily adapted in order to obtain accurate proofs for any other Markovian process algebra.

1 Introduction

The Markovian process algebras presented in the literature are endowed with a notion of strong Markovian bisimulation equivalence in the style of [5] accounting for both functional and performance aspects. These equivalences are shown to be congruences with respect to the operators as well as recursion. To the best of our knowledge, only in [4, 1] complete proofs of congruence for recursion have been given. The proofs follow Milner's technique of bisimulation up to [6]. A particular relation $\mathcal{B}$ is introduced such that if we are able to prove that $\mathcal{B}$ is a bisimulation up to then we can conclude that recursion satisfy the congruence property. $\mathcal{B}$ is proven to be a bisimulation up to as follows. Given two terms $(E_1, E_2) \in \mathcal{B}$, an action type a, and an equivalence class C, the proofs show by induction on the maximum depth of the derivation of the transitions of E_1 labeled with a reaching C that the aggregated rate from E_1 to C when performing a is equal to the aggregated rate from E_2 to C when performing a: $Rate(E_1, a, C) = Rate(E_2, a, C)$. After a careful reading of those proofs, we discovered that they contain the same inaccuraces both in the proofs themselves and in the definition of bisimulation up to used in the proofs. The purpose of this paper is to develop a complete proof following Milner's technique which shows that the strong Markovian bisimulation equivalence is a congruence with respect to recursion, thus providing a machinery which can be easily adapted to any Markovian process algebra.

The problem with the definition of bisimulation up to is that it should consider, following the style of [5], the classes of an equivalence relation determined from both $\sim$, the Markovian bisimulation equivalence, and $\mathcal{B}$, the relation being defined. In [4, 1] the definition of bisimulation up to considers, instead, the relation $\sim \mathcal{B} \sim$ which in general, as we will show, is not transitive even if $\mathcal{B}$ is supposed to be an equivalence relation. Similarly to [3], we solved the problem by considering the classes of a relation which is indeed an equivalence relation for any given $\mathcal{B}$: such a relation is $(\mathcal{B} \cup \mathcal{B}^{-1} \cup \sim)^+$.

The problem with the congruence proof is the following one. Since the proof proceeds by induction on the maximum depth of the derivation of the transitions of E_1 labeled with a and reaching C, several cases arise depending on the outermost operator op of E_1 and E_2 as in Milner's proof. As far as static operators are concerned the proofs in [4, 1] wrongly assume that all the terms that, when applied the static operator op, belong to C are equivalent, i.e. they form a single equivalence class. As an example, for $op =$ "$\_/L$" we have that in general $\{E \mid E/L \in C\}$ is not an equivalence class. This can be seen by considering the terms $(a.\underline{0})/\{a, b\}$ and $(b.\underline{0})/\{a, b\}$: they obviously belong to the same equivalence class C, but $a.\underline{0}$ is not equivalent to $b.\underline{0}$. Therefore, we cannot apply the induction hypothesis to conclude that $E_1 \equiv E_1'/L$ and $E_2 \equiv E_2'/L$ have the same aggregated rate to reach C when performing transitions of type a. In order to solve such a problem, we observe that the terms that belong to C when applied the operator op form in general several equivalence classes C_i, $i \in I$. As an example, for *op* = "$\_/L$" we have that $\{E \mid E/L \in C\} = \cup_{i \in I} C_i$. Therefore we should be able to apply the induction hypothesis to each class C_i. Unfortunately this can be done only for the sets C_i that are actually reachable from E'_1 via transitions of type a (the maximum depth of such transitions is certainly less than the depth of transitions from E_1 to C). For the other sets C_i we would need a converse argument related to the transitions of E'_2. The simplest solution is to split the proof into two symmetric parts and to change the induction assertion of the whole proof into $Rate(E_1, a, C) \leq Rate(E_2, a, C)$ as done in [2]. In this way, the induction hypothesis can be exploited because the aggregated rate to an unreachable class C_i is zero, hence less than or equal to any possible rate. Proving $Rate(E_1, a, C) \leq Rate(E_2, a, C)$ is enough because the reverse can be shown by a symmetric argument. In this way we follow smoothly the scheme of Milner's proof [6] which is similarly divided into two symmetric parts: in the former E_1 is assumed to have an outgoing transition and the proof proceeds by induction on the depth of the derivation of such a transition, in the latter we do the same for E_2. On the other hand a symmetric argument should also be used if we would have been able to induce on $Rate(E_1, a, C) = Rate(E_2, a, C)$ because this assertion is shown only in the case of E_1 having an outgoing transition labeled with a reaching C, so using $\leq$ leads to a very elegant solution of the problem.

The complete revised proof is presented in Sect. 3 for the stochastically timed process algebra EMPA [1] which is briefly recalled in Sect. 2, but it can be easily adapted to any Markovian process algebra.

2 Syntax, Semantics, and Equivalence for EMPA

In this section we recall from [1] the basic notions and results about the stochastically timed process algebra EMPA.

2.1 Syntax

The building blocks of EMPA are *actions*. Each action is a pair $<a, \tilde{\lambda}>$ where:

- a is the *type* of the action. According to types, actions are divided into *external* and *internal* (denoted by action type τ) depending on whether they can be seen by an external observer or not.
- $\tilde{\lambda}$ is the *rate* of the action, i.e. a concise way to represent the random variable specifying its duration. According to rates, we have the following classification:
  - *Exponentially timed actions* are actions whose rate is a positive real number. Such a number is interpreted as the parameter of the exponentially distributed random variable specifying the duration of the action.
  - *Immediate actions* are actions whose rate, denoted by $\infty_{l,w}$, is infinite. Such actions have duration zero, and each of them is given a *priority level* $l \in \mathbb{N}_+$ and a *weight* $w \in \mathbb{R}_+$, useful for expressing prioritized and probabilistic choices respectively.
  - *Passive actions* are actions whose rate, denoted by $*$, is undefined. The duration of a passive action is fixed only by synchronizing it with a nonpassive action of the same type.

We denote by

$$Act = AType \times ARate$$

the set of actions, where $AType$ is the set of types and $ARate = \mathbb{R}_+ \cup Inf \cup \{*\}$, with $Inf = \{\infty_{l,w} \mid l \in \mathbb{N}_+ \wedge w \in \mathbb{R}_+\}$, is the set of rates. Finally, we denote by $APLev = \{-1\} \cup \mathbb{N}$ the set of *action priority levels*, and we assume that $* < \lambda < \infty_{l,w}$ for all $\lambda \in \mathbb{R}_+$ and $\infty_{l,w} \in Inf$.

Let $Const$ be a set of *constants* and let $ARFun = \{\varphi : AType \longrightarrow AType \mid \varphi(\tau) = \tau \wedge \varphi(AType - \{\tau\}) \subseteq AType - \{\tau\}\}$ be a set of *action relabeling functions*.

Definition 2.1 The set $\mathcal{L}$ of *process terms* of EMPA is generated by the following syntax

$$E ::= \underline{0} \mid <a, \tilde{\lambda}>.E \mid E/L \mid E[\varphi] \mid E + E \mid E \|_S E \mid A$$

where $L, S \subseteq AType - \{\tau\}$ and $A \in Const$. We denote by $\mathcal{G}$ the set of guarded and closed terms of $\mathcal{L}$. ■

The *null term* "$\underline{0}$" represents a termination or deadlocked state. The *prefix operator* "$<a, \tilde{\lambda}>.\_$" denotes the sequential composition of an action and a term. The *functional abstraction operator* "$\_/L$" hides the actions whose type belongs to L by changing their type to τ. The *functional relabeling operator* "$\_[\varphi]$" changes the types of actions according to φ. The *alternative composition operator* "$\_ + \_$" expresses a choice between two terms: the choice is resolved according to the *race policy* whenever exponentially timed actions are involved (the fastest one succeeds), or according to the *preselection policy* whenever immediate actions are involved (only the actions having the highest priority level are executable, and each of these is given an execution probability proportional to its own weight), while the choice is purely *nondeterministic* whenever passive actions are involved. The *parallel composition operator* "$\_ \|_S \_$" expresses the concurrent execution of two terms according to the following synchronization discipline: two actions can synchronize if and only if they have the same type belonging to S and at most one of them is not passive. Finally, constants together with their corresponding defining equations of the form $A \stackrel{\Delta}{=} E$ allow for recursion.

2.2 Semantics

The integrated semantics for EMPA is represented by a labeled transition system (LTS for short) whose labels are actions. The integrated semantics is defined in the interleaving style thanks to the memoryless property of the exponential distribution. Let us call the *potential move* of a given term a pair composed of an action executable by that term when ignoring priority levels and the derivative term obtained by executing that action; let $PMove = Act \times \mathcal{G}$ be the set of all the potential moves. To cope with actions having different priority levels, the integrated interleaving semantic model is generated by a two layer semantics: first the multiset [1] of all the potential moves of a given term is inductively computed, then those moves having lower priority are discarded.

The formal definition of the integrated interleaving semantics is based on the transition relation $\longrightarrow$, which is the least subset of $\mathcal{G} \times Act \times \mathcal{G}$ satisfying the inference rule in the first part of Table 1. This rule selects the potential moves that have the highest priority level (or are passive), and then merges together those having the same action type, the same priority level, and the same derivative term. The first operation is carried out through functions $Select : \mathcal{M}u_{fin}(PMove) \longrightarrow \mathcal{M}u_{fin}(PMove)$ and $PL : Act \longrightarrow APLev$, which are defined in the third part of Table 1. The second operation is carried out through function $Melt : \mathcal{M}u_{fin}(PMove) \longrightarrow \mathcal{P}_{fin}(PMove)$ and partial function $Min : (ARate \times ARate) \longrightarrow\!\!\!\!\!\!\circ\;\; ARate$, which are defined in the fourth part of Table 1. We regard Min as an associative and commutative operation, thus we take the liberty to apply it to multisets of rates.

The multiset $PM(E) \in \mathcal{M}u_{fin}(PMove)$ of potential moves of $E \in \mathcal{G}$ is defined by structural induction in the second part of Table 1 according to the intuitive meaning of operators explained in Sect. 2.1. In order to enforce the bounded capacity assumption, which establishes that the rate at which an activity is carried out cannot be increased by synchronizing it with other activities, in the rule for the parallel composition operator a normalization is required to suitably compute the rates of potential moves resulting from the synchronization of the same nonpassive action with several independent or alternative passive actions. The normalization operates in such a way that applying Min to the rates of the synchronizations involving the nonpassive action gives as a result the rate of the nonpassive action itself, and that each synchronization is assigned the same execution probability. This normalization is carried out through partial function $Norm : (AType \times ARate \times ARate \times \mathcal{M}u_{fin}(PMove) \times \mathcal{M}u_{fin}(PMove)) \longrightarrow\!\!\!\!\!\!\circ\;\; ARate$ and function $Split : (ARate \times \mathbb{R}_{]0,1]}) \longrightarrow ARate$, which are defined in the fifth part of Table 1. Note that $Norm(a, \tilde{\lambda}_1, \tilde{\lambda}_2, PM_1, PM_2)$ is defined if and only if $\min(\tilde{\lambda}, \tilde{\mu}) = *$, which is the condition on action rates we have required in Sect. 2.1 in order for a synchronization to be permitted.

Definition 2.2 The *integrated interleaving semantics* of $E \in \mathcal{G}$ is the LTS

$$\mathcal{I}[\![E]\!] = (S_{E,\mathcal{I}}, Act, \longrightarrow_{E,\mathcal{I}}, E)$$

where:

[1] We use "$\{\!|$" and "$|\!\}$" as brackets for multisets, "$\_ \oplus \_$" to denote multiset union, $\mathcal{M}u_{fin}(S)$ ($\mathcal{P}_{fin}(S)$) to denote the collection of finite multisets (sets) over set S, $M(s)$ to denote the multiplicity of element s in multiset M, and $\pi_i(M)$ to denote the multiset obtained by projecting the tuples in multiset M on their i-th component. Thus, e.g., $(\pi_1(PM_2))(<a, *>)$ in the fifth part of Table 1 denotes the multiplicity of tuples of PM_2 whose first component is $<a, *>$.

$$\frac{(<a,\tilde{\lambda}>, E') \in Melt(Select(PM(E)))}{E \xrightarrow{a,\tilde{\lambda}} E'}$$

$$PM(\underline{0}) = \emptyset$$

$$PM(<a,\tilde{\lambda}>.E) = \{\!|\, (<a,\tilde{\lambda}>, E) \,|\!\}$$

$$\begin{aligned} PM(E/L) = {} & \{\!|\, (<a,\tilde{\lambda}>, E'/L) \mid (<a,\tilde{\lambda}>, E') \in PM(E) \wedge a \notin L \,|\!\} \oplus \\ & \{\!|\, (<\tau,\tilde{\lambda}>, E'/L) \mid (<a,\tilde{\lambda}>, E') \in PM(E) \wedge a \in L \,|\!\} \end{aligned}$$

$$PM(E[\varphi]) = \{\!|\, (<\varphi(a),\tilde{\lambda}>, E'[\varphi]) \mid (<a,\tilde{\lambda}>, E') \in PM(E) \,|\!\}$$

$$PM(E_1 + E_2) = PM(E_1) \oplus PM(E_2)$$

$$\begin{aligned} PM(E_1 \,\|_S\, E_2) = {} & \{\!|\, (<a,\tilde{\lambda}>, E'_1 \,\|_S\, E_2) \mid a \notin S \wedge (<a,\tilde{\lambda}>, E'_1) \in PM(E_1) \,|\!\} \oplus \\ & \{\!|\, (<a,\tilde{\lambda}>, E_1 \,\|_S\, E'_2) \mid a \notin S \wedge (<a,\tilde{\lambda}>, E'_2) \in PM(E_2) \,|\!\} \oplus \\ & \{\!|\, (<a,\tilde{\gamma}>, E'_1 \,\|_S\, E'_2) \mid a \in S \wedge \\ & \qquad (<a,\tilde{\lambda}_1>, E'_1) \in PM(E_1) \wedge \\ & \qquad (<a,\tilde{\lambda}_2>, E'_2) \in PM(E_2) \wedge \\ & \qquad \tilde{\gamma} = Norm(a, \tilde{\lambda}_1, \tilde{\lambda}_2, PM(E_1), PM(E_2)) \,|\!\} \end{aligned}$$

$$PM(A) = PM(E) \quad \text{if } A \stackrel{\Delta}{=} E$$

$$\begin{aligned} Select(PM) = \{\!|\, (<a,\tilde{\lambda}>, E) \in PM \mid {} & \forall (<b,\tilde{\mu}>, E') \in PM \,.\, PL(<a,\tilde{\lambda}>) \geq PL(<b,\tilde{\mu}>) \vee \\ & PL(<a,\tilde{\lambda}>) = -1 \,|\!\} \end{aligned}$$

$$PL(<a,*>) = -1 \qquad PL(<a,\lambda>) = 0 \qquad PL(<a,\infty_{l,w}>) = l$$

$$\begin{aligned} Melt(PM) = \{ (<a,\tilde{\lambda}>, E) \mid {} & \exists \tilde{\mu} \in ARate \,.\, (<a,\tilde{\mu}>, E) \in PM \;\wedge \\ & \tilde{\lambda} = Min \{\!|\, \tilde{\gamma} \mid (<a,\tilde{\gamma}>, E) \in PM \wedge PL(<a,\tilde{\gamma}>) = PL(<a,\tilde{\mu}>) \,|\!\} \} \end{aligned}$$

$$* \; Min \; * = * \qquad \lambda_1 \; Min \; \lambda_2 = \lambda_1 + \lambda_2 \qquad \infty_{l,w_1} \; Min \; \infty_{l,w_2} = \infty_{l,w_1+w_2}$$

$$Norm(a, \tilde{\lambda}_1, \tilde{\lambda}_2, PM_1, PM_2) = \begin{cases} Split(\tilde{\lambda}_1, 1/(\pi_1(PM_2))(<a,*>)) & \text{if } \tilde{\lambda}_2 = * \\ Split(\tilde{\lambda}_2, 1/(\pi_1(PM_1))(<a,*>)) & \text{if } \tilde{\lambda}_1 = * \end{cases}$$

$$Split(*, p) = * \qquad Split(\lambda, p) = \lambda \cdot p \qquad Split(\infty_{l,w}, p) = \infty_{l,w \cdot p}$$

Table 1: Inductive rules for EMPA integrated interleaving semantics

- $S_{E,\mathcal{I}}$ is the least subset of $\mathcal{G}$ such that:
  - $E \in S_{E,\mathcal{I}}$;
  - if $E_1 \in S_{E,\mathcal{I}}$ and $E_1 \xrightarrow{a,\tilde{\lambda}} E_2$, then $E_2 \in S_{E,\mathcal{I}}$.
- $\longrightarrow_{E,\mathcal{I}}$ is the restriction of $\longrightarrow$ to $S_{E,\mathcal{I}} \times Act \times S_{E,\mathcal{I}}$. ■

2.3 Equivalence

The notion of equivalence for EMPA is defined by following the notion of probabilistic bisimulation proposed in [5]. Actually, in order to get a congruence, the equivalence is defined over an extended language which comprises a priority operator "$\Theta(\_)$": priority levels are taken to be potential and they become effective only within the scope of the priority operator. We thus consider the language $\mathcal{L}_\Theta$ generated by the following syntax

$$E ::= \underline{0} \mid <a, \tilde{\lambda}>.E \mid E/L \mid E[\varphi] \mid \Theta(E) \mid E + E \mid E \,\|_S\, E \mid A$$

whose semantic rules are those in Table 1 except that the rule in the first part is replaced by

$$\frac{(<a, \tilde{\lambda}>, E') \in Melt(PM(E))}{E \xrightarrow{a,\tilde{\lambda}} E'}$$

and the following rule for the priority operator is introduced in the second part

$$PM(\Theta(E)) = Select(PM(E))$$

The priority operator is not part of EMPA in that cumbersome from the modeling point of view. It is easily seen that EMPA coincides with the set of terms $\{\Theta(E) \mid E \in \mathcal{L}\}$.

Definition 2.3 We define partial function $Rate : (\mathcal{G}_\Theta \times AType \times APLev \times \mathcal{P}(\mathcal{G}_\Theta)) \multimap ARate$ by [2]

$$Rate(E, a, l, C) = Min\{\!|\, \tilde{\lambda} \mid E \xrightarrow{a,\tilde{\lambda}} E' \wedge PL(<a, \tilde{\lambda}>) = l \wedge E' \in C \,|\!\}$$ ■

Definition 2.4 An equivalence relation $\mathcal{B} \subseteq \mathcal{G}_\Theta \times \mathcal{G}_\Theta$ is a *strong extended Markovian bisimulation (strong EMB)* if and only if, whenever $(E_1, E_2) \in \mathcal{B}$, then for all $a \in AType$, $l \in APLev$ and $C \in \mathcal{G}_\Theta/\mathcal{B}$

$$Rate(E_1, a, l, C) = Rate(E_2, a, l, C)$$ ■

Proposition 2.5 Let $\sim_{EMB}$ be the union of all the strong EMBs. Then $\sim_{EMB}$ is the largest strong EMB. ■

Definition 2.6 We call $\sim_{EMB}$ the *strong extended Markovian bisimulation equivalence (strong EMBE).* ■

Theorem 2.7 Let $E_1, E_2 \in \mathcal{G}_\Theta$. If $E_1 \sim_{EMB} E_2$ then:

(*i*) For any $<a, \tilde{\lambda}> \in Act$, $<a, \tilde{\lambda}>.E_1 \sim_{EMB} <a, \tilde{\lambda}>.E_2$.

(*ii*) For any $L \subseteq AType - \{\tau\}$, $E_1/L \sim_{EMB} E_2/L$.

(*iii*) For any $\varphi \in ARFun$, $E_1[\varphi] \sim_{EMB} E_2[\varphi]$.

(*iv*) $\Theta(E_1) \sim_{EMB} \Theta(E_2)$.

(*v*) For any $F \in \mathcal{G}_\Theta$, $E_1 + F \sim_{EMB} E_2 + F$ and $F + E_1 \sim_{EMB} F + E_2$.

(*vi*) For any $F \in \mathcal{G}_\Theta$ and $S \subseteq AType - \{\tau\}$, $E_1 \,\|_S\, F \sim_{EMB} E_2 \,\|_S\, F$ and $F \,\|_S\, E_1 \sim_{EMB} F \,\|_S\, E_2$. ■

[2] We let $Min\,\emptyset = \perp$, $\tilde{\lambda}\, Min \perp = \tilde{\lambda}$, $\perp < \tilde{\lambda}$, $Split(\perp, p) = \perp$.

3 Revised Proof of Congruence for Recursion

In [1] (as well as in [4] for a pure Markovian bisimulation equivalence) it has been shown that $\sim_{EMB}$ is a congruence also with respect to recursion. The problem is that the definition of bisimulation up to and the congruence proof for recursion are affected by the errors mentioned in Sect. 1. The aim of this section is to provide a revised, correct proof of the congruence result for recursion which is based on ideas in [3, 2] as recalled in Sect. 1. We would like to point out that the proof we are going to provide differs both from the one in [3], which introduces a correct notion of bisimulation up to but is made for an algebra without static operators, and from the one in [2], which does not resort to the notion of bisimulation up to hence deviating from Milner's technique we would like instead to follow.

3.1 Definition of bisimulation up to

As far as the notion of bisimulation up to is concerned we recall below the definition given in [1] (and similarly in [4]).

Definition 3.1 An equivalence relation $\mathcal{B} \subseteq \mathcal{G}_\Theta \times \mathcal{G}_\Theta$ is a *strong EMB up to* $\sim_{EMB}$ if and only if, whenever $(E_1, E_2) \in \mathcal{B}$, then for all $a \in AType$, $l \in APLev$ and $C \in \mathcal{G}_\Theta/(\sim_{EMB} \mathcal{B} \sim_{EMB})$

$$Rate(E_1, a, l, C) = Rate(E_2, a, l, C) \qquad \blacksquare$$

The problem of this definition is that $\sim_{EMB} \mathcal{B} \sim_{EMB}$ in general is not an equivalence relation even if we suppose $\mathcal{B}$ being an equivalence relation. For instance if $\mathcal{B}$ is defined as follows:

$$\mathcal{B} = Id \cup \{(<a,\lambda>.\underline{0}, \underline{0}), (\underline{0}, <a,\lambda>.\underline{0})\} \cup \{(<b,\mu>.\underline{0}, \underline{0} \,||_\emptyset\, \underline{0}), (\underline{0} \,||_\emptyset\, \underline{0}, <b,\mu>.\underline{0})\}$$

then $\mathcal{B}$ is an equivalence relation but $\sim_{EMB} \mathcal{B} \sim_{EMB}$ is not transitive. This can be shown as follows.

$$<a,\lambda>.\underline{0} \;\sim_{EMB}\; <a,\lambda>.\underline{0} \;\mathcal{B}\; \underline{0} \;\sim_{EMB}\; \underline{0} \,||_\emptyset\, \underline{0}$$

$$\underline{0} \,||_\emptyset\, \underline{0} \;\sim_{EMB}\; \underline{0} \,||_\emptyset\, \underline{0} \;\mathcal{B}\; <b,\mu>.\underline{0} \;\sim_{EMB}\; <b,\mu>.\underline{0}$$

but it is not the case that:

$$<a,\lambda>.\underline{0} \;\sim_{EMB} \mathcal{B} \sim_{EMB}\; <b,\mu>.\underline{0}$$

In order to obtain an equivalence relation it is sufficient to take the transitive closure of $\sim_{EMB} \mathcal{B} \sim_{EMB}$. The new relation is expressed in the simplest way by $(\mathcal{B} \cup \sim_{EMB})^+$ as in [3]. The revised definition of bisimulation up to would then become as follows.

Definition 3.2 An equivalence relation $\mathcal{B} \subseteq \mathcal{G}_\Theta \times \mathcal{G}_\Theta$ is a *strong EMB up to* $\sim_{EMB}$ if and only if, whenever $(E_1, E_2) \in \mathcal{B}$, then for all $a \in AType$, $l \in APLev$ and $C \in \mathcal{G}_\Theta/(\mathcal{B} \cup \sim_{EMB})^+$

$$Rate(E_1, a, l, C) = Rate(E_2, a, l, C) \qquad \blacksquare$$

Finally we note that it is not necessary to require that $\mathcal{B}$ is an equivalence relation. We can simply adapt the definition to any relation $\mathcal{B}$ (which does not include any redundant information) by considering the relation $(\mathcal{B} \cup \mathcal{B}^{-1} \cup \sim_{EMB})^+$. It is easy to see that this relation is always an equivalence relation, in particular $Id \subseteq (\mathcal{B} \cup \mathcal{B}^{-1} \cup \sim_{EMB})^+$ because $Id \subseteq \sim_{EMB}$. Therefore the final definition of bisimulation up to is the following one.

Definition 3.3 A relation $\mathcal{B} \subseteq \mathcal{G}_\Theta \times \mathcal{G}_\Theta$ is a *strong EMB up to* $\sim_{EMB}$ if and only if, whenever $(E_1, E_2) \in \mathcal{B}$, then for all $a \in AType$, $l \in APLev$ and $C \in \mathcal{G}_\Theta/(\mathcal{B} \cup \mathcal{B}^{-1} \cup \sim_{EMB})^+$

$$Rate(E_1, a, l, C) = Rate(E_2, a, l, C) \qquad \blacksquare$$

The following proposition shows that the new definition of bisimulation up to is correct.

Proposition 3.4 If $\mathcal{B} \subseteq \mathcal{G}_\Theta \times \mathcal{G}_\Theta$ is a strong EMB up to $\sim_{EMB}$ and $(E_1, E_2) \in \mathcal{B}$, then $E_1 \sim_{EMB} E_2$.

Proof Given $\mathcal{B} \subseteq \mathcal{G}_\Theta \times \mathcal{G}_\Theta$ strong EMB up to $\sim_{EMB}$, we first prove that $(\mathcal{B} \cup \mathcal{B}^{-1} \cup \sim_{EMB})^+$ is a strong EMB. We define $\mathcal{B}' = \mathcal{B} \cup \mathcal{B}^{-1}$. By proceeding by induction on $n \in \mathbb{N}_+$ we show that, whenever $(E_1, E_2) \in (\mathcal{B}' \cup \sim_{EMB})^n$, then for all $a \in AType$, $l \in APLev$ and $C \in \mathcal{G}_\Theta/(\mathcal{B}' \cup \sim_{EMB})^+$ we have that $Rate(E_1, a, l, C) = Rate(E_2, a, l, C)$.

- If $n = 1$, then $(E_1, E_2) \in \mathcal{B}' \cup \sim_{EMB}$. If $(E_1, E_2) \in \mathcal{B}'$ then the result trivially follows from the fact that $\mathcal{B}$ is a strong EMB up to $\sim_{EMB}$. If $(E_1, E_2) \in \sim_{EMB}$ we observe that, since $\sim_{EMB} \subseteq (\mathcal{B}' \cup \sim_{EMB})^+$, each equivalence class of $(\mathcal{B}' \cup \sim_{EMB})^+$ can be written as the union of some equivalence classes of $\sim_{EMB}$. As a consequence, for all $a \in \mathit{AType}$, $l \in \mathit{APLev}$ and $C \in \mathcal{G}_\Theta/(\mathcal{B}' \cup \sim_{EMB})^+$, it turns out $\mathit{Rate}(E_1, a, l, C) = \mathit{Rate}(E_2, a, l, C)$, because $E_1 \sim_{EMB} E_2$.
- Let $n > 1$. From $(E_1, E_2) \in (\mathcal{B}' \cup \sim_{EMB})^n$ we derive that there exists $F \in \mathcal{G}_\Theta$ such that $(E_1, F) \in (\mathcal{B}' \cup \sim_{EMB})^{n-1}$ and $(F, E_2) \in \mathcal{B}' \cup \sim_{EMB}$. Thus for all $a \in \mathit{AType}$, $l \in \mathit{APLev}$ and $C \in \mathcal{G}_\Theta/(\mathcal{B}' \cup \sim_{EMB})^+$, it turns out $\mathit{Rate}(E_1, a, l, C) = \mathit{Rate}(F, a, l, C)$ by the induction hypothesis, and $\mathit{Rate}(F, a, l, C) = \mathit{Rate}(E_2, a, l, C)$ by applying the same argument as the previous point.

To complete the proof, we observe that $\mathcal{B} \subseteq (\mathcal{B}' \cup \sim_{EMB})^+$, and $(\mathcal{B}' \cup \sim_{EMB})^+ \subseteq \sim_{EMB}$ because $(\mathcal{B}' \cup \sim_{EMB})^+$ is a strong EMB, hence $\mathcal{B} \subseteq \sim_{EMB}$ by transitivity. ■

3.2 Proof of congruence

As far as the proof of congruence for recursion is concerned, in order to explain the problems in the proofs of [4, 1] we sketch below the proof given in [1] which is similar to the one given in [4]. In particular we consider only the induction step in the case of the outermost operator being "$\_/L$". In order to present the sketch of the proof we must extend the definition of $\sim_{EMB}$ to terms that are guardedly closed up to constants devoid of defining equation. Note that such constants act as variables.

Definition 3.5 A constant $A \in \mathit{Const}$ is *free* if and only if, for no $E \in \mathcal{L}_\Theta$, $A \stackrel{\Delta}{=} E$. ■

Let us denote by st the relation subterm-of, and by $\mathit{Subst}(E)$ the set of terms obtained from E by repeatedly replacing constants by the right-hand side terms of their defining equations.

Definition 3.6 The set of constants occurring in $E \in \mathcal{L}_\Theta$ is defined by

$$\mathit{Const}(E) = \{A \in \mathit{Const} \mid \exists F \in \mathit{Subst}(E).\, A \;\mathit{st}\; F\}$$ ■

Definition 3.7 A term $E \in \mathcal{L}_\Theta$ is *partially guardedly closed (pgc)* if and only if for each constant $A \in \mathit{Const}(E)$ either A is free or

- A is equipped with exactly one defining equation $A \stackrel{\Delta}{=} E'$, and
- there exists $F \in \mathit{Subst}(E')$ such that, whenever an instance of a nonfree constant B satisfies $B \;\mathit{st}\; F$, then the same instance satisfies $B \;\mathit{st} <a, \tilde{\lambda}>.G \;\mathit{st}\; F$. ■

Definition 3.8 Let $E \in \mathcal{L}_\Theta$, $A \in \mathit{Const}$ free, and $B \in \mathcal{G}_\Theta$. The term $E\langle\!\langle A := B\rangle\!\rangle$ obtained from E by replacing each occurrence of A with B is defined by induction on the syntactical structure of E as follows:

- $\underline{0}\langle\!\langle A := B\rangle\!\rangle \equiv \underline{0}$
- $(<a, \tilde{\lambda}>.E)\langle\!\langle A := B\rangle\!\rangle \equiv <a, \tilde{\lambda}>.(E\langle\!\langle A := B\rangle\!\rangle)$
- $(E/L)\langle\!\langle A := B\rangle\!\rangle \equiv (E\langle\!\langle A := B\rangle\!\rangle)/L$
- $(E[\varphi])\langle\!\langle A := B\rangle\!\rangle \equiv (E\langle\!\langle A := B\rangle\!\rangle)[\varphi]$
- $\Theta(E)\langle\!\langle A := B\rangle\!\rangle \equiv \Theta(E\langle\!\langle A := B\rangle\!\rangle)$
- $(E_1 + E_2)\langle\!\langle A := B\rangle\!\rangle \equiv (E_1\langle\!\langle A := B\rangle\!\rangle) + (E_2\langle\!\langle A := B\rangle\!\rangle)$
- $(E_1 \,\|_S\, E_2)\langle\!\langle A := B\rangle\!\rangle \equiv (E_1\langle\!\langle A := B\rangle\!\rangle) \,\|_S (E_2\langle\!\langle A := B\rangle\!\rangle)$
- $A'\langle\!\langle A := B\rangle\!\rangle \equiv \begin{cases} B & \text{if } A' \equiv A \\ A' & \text{if } A' \not\equiv A \wedge A' \text{ free} \\ A'' & \text{if } A' \not\equiv A \wedge A' \stackrel{\Delta}{=} E \wedge A'' \stackrel{\Delta}{=} E\langle\!\langle A := B\rangle\!\rangle \end{cases}$ ■

Definition 3.9 Let $E_1, E_2 \in \mathcal{L}_\Theta$ be pgc, and suppose that $Const(E_1) \cup Const(E_2)$ contains $\{A_i \in Const \mid i \in I\}$ as free constants. We say that E_1 and E_2 are strongly EMBE if and only if, for all sets $\{B_i \in \mathcal{G}_\Theta \mid i \in I\}$ such that $E_1\langle\langle A_i := B_i\rangle\rangle_{i\in I}, E_2\langle\langle A_i := B_i\rangle\rangle_{i\in I} \in \mathcal{G}_\Theta$, it turns out that

$$E_1\langle\langle A_i := B_i\rangle\rangle_{i\in I} \sim_{EMB} E_2\langle\langle A_i := B_i\rangle\rangle_{i\in I}$$

■

Now we are in a position to present a sketch of the flawed congruence proof for recursion of [1].

Theorem 3.10 Let $E_1, E_2 \in \mathcal{L}_\Theta$ be pgc, and suppose that $Const(E_1) \cup Const(E_2)$ contains only $A \in Const$ as a free constant. Let $A_1 \triangleq E_1\langle\langle A := A_1\rangle\rangle$ and $A_2 \triangleq E_2\langle\langle A := A_2\rangle\rangle$ be in $\mathcal{G}_\Theta$. If $E_1 \sim_{EMB} E_2$, then $A_1 \sim_{EMB} A_2$.

Proof It suffices to prove that $\mathcal{B}' = \mathcal{B} \cup \mathcal{B}^{-1}$ where

$$\begin{aligned}\mathcal{B} = \{(F_1, F_2) \mid {} & F_1 \equiv F\langle\langle B := A_1\rangle\rangle \wedge F_2 \equiv F\langle\langle B := A_2\rangle\rangle \wedge \\ & F \in \mathcal{L}_\Theta \text{ pgc with at most } B \in Const_{Def_\Theta}(F) \text{ free}\}\end{aligned}$$

is a strong EMB up to $\sim_{EMB}$: the result will follow by taking $F \equiv B$. Given $(F_1, F_2) \in \mathcal{B}'$, $a \in AType$, $l \in APLev$, and $C \in \mathcal{G}_\Theta/(\sim_{EMB} \mathcal{B}' \sim_{EMB})$, we prove that $Rate(F_1, a, l, C) = Rate(F_2, a, l, C)$ by proceeding by induction on the maximum depth d of the inference of a potential move for F_1 having type a, priority level l, and derivative term in C.

- If $d = 1$, then only the rule for the prefix operator has been used to deduce the potential move. Therefore $F \equiv {<}a, \tilde{\lambda}{>}.F'$ with $PL({<}a, \tilde{\lambda}{>}) = l$, and for $j \in \{1, 2\}$ we have $F_j \equiv {<}a, \tilde{\lambda}{>}.(F'\langle\langle B := A_j\rangle\rangle)$. Since $(F'\langle\langle B := A_1\rangle\rangle, F'\langle\langle B := A_2\rangle\rangle) \in \mathcal{B}$, it turns out that $C = [F'\langle\langle B := A_1\rangle\rangle]_{\sim_{EMB}\mathcal{B}'\sim_{EMB}} = [F'\langle\langle B := A_2\rangle\rangle]_{\sim_{EMB}\mathcal{B}'\sim_{EMB}}$ hence $Rate(F_1, a, l, C) = \tilde{\lambda} = Rate(F_2, a, l, C)$.
- If $d > 1$, then several subcases arise depending on the syntactical structure of F.
  - If $F \equiv F'/L$, then for $j \in \{1, 2\}$ we have $F_j \equiv (F'\langle\langle B := A_j\rangle\rangle)/L$. Since F_1 has a potential move having type a (with $a \notin L$), priority level l, and derivative term in C, such that the depth of its inference is d, $F'\langle\langle B := A_1\rangle\rangle$ has a potential move having type b (with $b = a$ if $a \neq \tau$, $b \in L \cup \{\tau\}$ if $a = \tau$), priority level l, and derivative term $G \in C' \in \mathcal{G}_\Theta/(\sim_{EMB} \mathcal{B}' \sim_{EMB})$, such that the depth of its inference is $d - 1$ and $C = [G/L]_{\sim_{EMB}\mathcal{B}'\sim_{EMB}}$. For $j \in \{1, 2\}$ we have
  $$Rate(F_j, a, l, C) = \begin{cases} Rate(F'\langle\langle B := A_j\rangle\rangle, a, l, C') \\ Rate(F'\langle\langle B := A_j\rangle\rangle, \tau, l, C')\ Min \\ \qquad Min\{\!|\ Rate(F'\langle\langle B := A_j\rangle\rangle, b, l, C') \mid b \in L\ |\!\} \end{cases}$$
  depending on whether $a \notin L \cup \{\tau\}$ or $a = \tau$. From the induction hypothesis, it follows that $Rate(F_1, a, l, C) = Rate(F_2, a, l, C)$.
  - ...

■

This proof is flawed because in general not all the terms of $[G/L]$ can be obtained by applying the operator "$\_/L$" to the terms of $[G]$. In general the set of terms $\{E \mid E/L \in [G/L]\}$ form several equivalence classes C_i and not a single one. Therefore we should prove, by applying the induction hypothesis, that for each class C_i $Rate(F'\langle\langle B := A_1\rangle\rangle, b, l, C_i) = Rate(F'\langle\langle B := A_2\rangle\rangle, b, l, C_i)$ with $b \in L$ if $a = \tau$ and $b = a$ otherwise. In fact this can certainly be done for the sets C_i such that $F'\langle\langle B := A_1\rangle\rangle$ reaches C_i via a transition with type b and priority level l (the depth of such transitions is certainly less than the maximum depth of the transitions from F_1 to C). But a problem arises for the sets C_i that are not reachable from $F'\langle\langle B := A_1\rangle\rangle$. In this case we cannot apply the induction hypothesis, instead we would need a converse argument related to the possible moves for $F'\langle\langle B := A_2\rangle\rangle$.

The solution we adopt is to split the proof into two symmetric parts and to change the induction assertion of the whole proof into $Rate(F_1, a, l, C) \leq Rate(F_2, a, l, C)$ as in [2]. In this way we have to worry only for the sets C_i that are actually reachable from $F'\langle\langle B := A_1\rangle\rangle$ (for the others C_i it holds $Rate(F'\langle\langle B := A_1\rangle\rangle, b, l, C_i) = \bot$ so the value of $Rate(F'\langle\langle B := A_2\rangle\rangle, b, l, C_i)$ is not important.

In the following we present the revised proof. It is worth noting that in the case of the parallel composition operator the decomposition of the class C in equivalence classes C_i is not a trivial task at all.

Theorem 3.11 Let $E_1, E_2 \in \mathcal{L}_\Theta$ be pgc, and suppose that $Const(E_1) \cup Const(E_2)$ contains only $A \in Const$ as a free constant. Let $A_1 \triangleq E_1\langle\!\langle A := A_1\rangle\!\rangle$ and $A_2 \triangleq E_2\langle\!\langle A := A_2\rangle\!\rangle$ be in $\mathcal{G}_\Theta$. If $E_1 \sim_{EMB} E_2$, then $A_1 \sim_{EMB} A_2$.

Proof It suffices to prove that:

$$\begin{aligned}\mathcal{B} = \{(F_1, F_2) \mid\ & F_1 \equiv F\langle\!\langle B := A_1\rangle\!\rangle \wedge F_2 \equiv F\langle\!\langle B := A_2\rangle\!\rangle \wedge \\ & F \in \mathcal{L}_\Theta \text{ pgc with at most } B \in Const(F) \text{ free}\}\end{aligned}$$

is a strong EMB up to $\sim_{EMB}$: the result will follow by taking $F \equiv B$. We define $\mathcal{B}' = \mathcal{B} \cup \mathcal{B}^{-1}$. Given $(F_1, F_2) \in \mathcal{B}$, $a \in AType$, $l \in APLev$ and $C \in \mathcal{G}_\Theta/(\mathcal{B}' \cup \sim_{EMB})^+$, we must prove that $Rate(F_1, a, l, C) = Rate(F_2, a, l, C)$.

We start by showing that $Rate(F_1, a, l, C) \leq Rate(F_2, a, l, C)$ for each $(F_1, F_2) \in \mathcal{B}$, $a \in AType$, $l \in APLev$, $C \in \mathcal{G}_\Theta/(\mathcal{B}' \cup \sim_{EMB})^+$. If (F_1, F_2), a, l and C are such that $Rate(F_1, a, l, C) = \perp$ there is nothing to prove, otherwise we prove the result by proceeding by induction on the maximum depth d of the inferences of the potential moves for F_1 having type a, priority level l, and derivative term in C.

- If $d = 1$, then only the rule for the prefix operator has been used to deduce the existing potential move. Therefore $F \equiv {<}a, \tilde{\lambda}{>}.F'$ with $PL({<}a, \tilde{\lambda}{>}) = l$, and for $j \in \{1, 2\}$ we have $F_j \equiv {<}a, \tilde{\lambda}{>}.(F'\langle\!\langle B := A_j\rangle\!\rangle)$. Since $(F'\langle\!\langle B := A_1\rangle\!\rangle, F'\langle\!\langle B := A_2\rangle\!\rangle) \in \mathcal{B}$, it turns out that $C = [F'\langle\!\langle B := A_1\rangle\!\rangle]_{(\mathcal{B}' \cup \sim_{EMB})^+} = [F'\langle\!\langle B := A_2\rangle\!\rangle]_{(\mathcal{B}' \cup \sim_{EMB})^+}$ hence $Rate(F_1, a, l, C) = \tilde{\lambda} = Rate(F_2, a, l, C)$.
- If $d > 1$, then several subcases arise depending on the syntactical structure of F.
  - If $F \equiv F'/L$, then for $j \in \{1, 2\}$ we have $F_j \equiv (F'\langle\!\langle B := A_j\rangle\!\rangle)/L$. Since F_1 has a potential move having derivative term in C, there exists $G \in \mathcal{G}_\Theta$ such that G/L is the derivative term and $C = [G/L]_{(\mathcal{B}' \cup \sim_{EMB})^+}$. Because of the congruence property w.r.t. "$\_/L$" of $\sim_{EMB}$ and of $\mathcal{B}$ (easily provable) we have that:

    $H/L \in [G/L]_{(\mathcal{B}' \cup \sim_{EMB})^+} \Rightarrow [H]_{(\mathcal{B}' \cup \sim_{EMB})^+}/L \subseteq [G/L]_{(\mathcal{B}' \cup \sim_{EMB})^+}$ [3]

    As a consequence:

    $$[G/L]_{(\mathcal{B}' \cup \sim_{EMB})^+} = (\bigcup_i C_i/L) \cup D$$

    where C_i are distinguished equivalence classes $C_i = [G_i]_{(\mathcal{B}' \cup \sim_{EMB})^+}$ with $G_i/L \in [G/L]_{(\mathcal{B}' \cup \sim_{EMB})^+}$ and D is a set of terms not having "$\_/L$" as outermost operator, hence not reachable from F_1 or F_2. Since d is the maximum depth of the inferences of the potential moves for F_1 having type a, priority level l and derivative term in C, for each i: either (i) $F'\langle\!\langle B := A_1\rangle\!\rangle$ has no potential moves having type a, priority level l and derivative term in C_i, or (ii) $d - 1$ is the maximum depth of the inferences of the potential moves for $F'\langle\!\langle B := A_1\rangle\!\rangle$ having type a, priority level l and derivative term in C_i. For $j \in \{1, 2\}$ we have:

    $$Rate(F_j, a, l, C) = \underset{i}{Min}\ Rate(F_j, a, l, C_i/L)$$

    where for each i:

    $$Rate(F_j, a, l, C_i/L) = Rate(F'\langle\!\langle B := A_j\rangle\!\rangle, a, l, C_i)$$

    $$Rate(F_j, a, l, C_i/L) = \begin{cases} Rate(F'\langle\!\langle B := A_j\rangle\!\rangle, a, l, C_i) \\ Rate(F'\langle\!\langle B := A_j\rangle\!\rangle, \tau, l, C_i)\ Min \\ \qquad Min\{\!|\ Rate(F'\langle\!\langle B := A_j\rangle\!\rangle, b, l, C_i) \mid b \in L\ |\!\} \end{cases}$$

    depending on whether $a \notin L \cup \{\tau\}$ or $a = \tau$. By applying the induction hypothesis to each $F'\langle\!\langle B := A_1\rangle\!\rangle, b, l, C_i$ (with $b \in L$ if $a = \tau$ and $b = a$ otherwise) such that $Rate(F'\langle\!\langle B := A_j\rangle\!\rangle, b, l, C_i) \neq \perp$ we have that $Rate(F_1, a, l, C_i/L) \leq Rate(F_2, a, l, C_i/L)$ for any i. It follows that $Rate(F_1, a, l, C) \leq Rate(F_2, a, l, C)$.
  - If $F \equiv F'[\varphi]$, then the proof is similar to the one developed in the first subcase. The result follows by applying the induction hypothesis to the fact that for $j \in \{1, 2\}$ we have

    $$Rate(F_j, a, l, C_i[\varphi]) = Min\{\!|\ Rate(F'\langle\!\langle B := A_j\rangle\!\rangle, b, l, C_i) \mid \varphi(b) = a\ |\!\}$$

[3] Given a set of terms C, C/L is the set of terms $\{E/L \mid E \in C\}$.

– If $F \equiv F' + F''$, then for $j \in \{1,2\}$ we have $F_j \equiv (F'\langle\!\langle B := A_j \rangle\!\rangle) + (F''\langle\!\langle B := A_j \rangle\!\rangle)$. Since d is the maximum depth of the inferences of the potential moves for F_1 having type a, priority level l and derivative term in C, for each $G \in \{F'\langle\!\langle B := A_1 \rangle\!\rangle, F''\langle\!\langle B := A_1 \rangle\!\rangle\}$: either (i) G has no potential moves having type a, priority level l and derivative term in C, or (ii) $d-1$ is the maximum depth of the inferences of the potential moves for G having type a, priority level l and derivative term in C. For $j \in \{1,2\}$ we have:

$$Rate(F_j, a, l, C) = Rate(F'\langle\!\langle B := A_j \rangle\!\rangle, a, l, C) \; Min \; Rate(F''\langle\!\langle B := A_j \rangle\!\rangle, a, l, C)$$

By applying the induction hypothesis to $F'\langle\!\langle B := A_1 \rangle\!\rangle, a, l, C$ if $Rate(F'\langle\!\langle B := A_1 \rangle\!\rangle, a, l, C) \neq \perp$, and to $F''\langle\!\langle B := A_1 \rangle\!\rangle, a, l, C$ if $Rate(F''\langle\!\langle B := A_1 \rangle\!\rangle, a, l, C) \neq \perp$, we have that $Rate(F'\langle\!\langle B := A_1 \rangle\!\rangle, a, l, C) \leq Rate(F'\langle\!\langle B := A_2 \rangle\!\rangle, a, l, C)$ and $Rate(F''\langle\!\langle B := A_1 \rangle\!\rangle, a, l, C) \leq Rate(F''\langle\!\langle B := A_2 \rangle\!\rangle, a, l, C)$. It follows that $Rate(F_1, a, l, C) \leq Rate(F_2, a, l, C)$.

– If $F \equiv F' \,\|_S\, F''$, then for $j \in \{1,2\}$ we have $F_j \equiv (F'\langle\!\langle B := A_j \rangle\!\rangle) \,\|_S (F''\langle\!\langle B := A_j \rangle\!\rangle)$. Since F_1 has a potential move having derivative term in C, there exist $G', G'' \in \mathcal{G}_\Theta$ such that $G' \,\|_S\, G''$ is the derivative term and $C = [G' \,\|_S\, G'']_{(\mathcal{B}' \cup \sim_{EMB})^+}$.

  * If $a \notin S$ then either $G'' \equiv F''\langle\!\langle B := A_1 \rangle\!\rangle$ or $G' \equiv F'\langle\!\langle B := A_1 \rangle\!\rangle$ and we are in the case of synchronization not taking place.

    Because of the congruence property w.r.t. "$\_\,\|_S\,\_$" of $\sim_{EMB}$ and of $\mathcal{B}$ (easily provable) we have that:

    $H \,\|_S (F''\langle\!\langle B := A_1 \rangle\!\rangle) \in [G' \,\|_S\, G'']_{(\mathcal{B}' \cup \sim_{EMB})^+} \;\Rightarrow$
    $\quad [H]_{(\mathcal{B}' \cup \sim_{EMB})^+} \,\|_S (F''\langle\!\langle B := A_1 \rangle\!\rangle) \subseteq [G' \,\|_S\, G'']_{(\mathcal{B}' \cup \sim_{EMB})^+}$

    and

    $(F'\langle\!\langle B := A_1 \rangle\!\rangle) \,\|_S\, H \in [G' \,\|_S\, G'']_{(\mathcal{B}' \cup \sim_{EMB})^+} \;\Rightarrow$
    $\quad (F'\langle\!\langle B := A_1 \rangle\!\rangle) \,\|_S [H]_{(\mathcal{B}' \cup \sim_{EMB})^+} \subseteq [G' \,\|_S\, G'']_{(\mathcal{B}' \cup \sim_{EMB})^+}$

    Moreover for the congruence property w.r.t. "$\_\,\|_S\,\_$" of $\mathcal{B}$ we have that for all $\mathcal{T} \in \mathcal{P}(\mathcal{G}_\Theta)$:

    $\mathcal{T} \,\|_S (F''\langle\!\langle B := A_1 \rangle\!\rangle) \subseteq [G' \,\|_S\, G'']_{(\mathcal{B}' \cup \sim_{EMB})^+} \;\Leftrightarrow$
    $\qquad \mathcal{T} \,\|_S (F''\langle\!\langle B := A_2 \rangle\!\rangle) \subseteq [G' \,\|_S\, G'']_{(\mathcal{B}' \cup \sim_{EMB})^+}$

    and

    $(F'\langle\!\langle B := A_1 \rangle\!\rangle) \,\|_S\, \mathcal{T} \subseteq [G' \,\|_S\, G'']_{(\mathcal{B}' \cup \sim_{EMB})^+} \;\Leftrightarrow$
    $\qquad (F'\langle\!\langle B := A_2 \rangle\!\rangle) \,\|_S\, \mathcal{T} \subseteq [G' \,\|_S\, G'']_{(\mathcal{B}' \cup \sim_{EMB})^+}$

    As a consequence: $[G' \,\|_S\, G'']_{(\mathcal{B}' \cup \sim_{EMB})^+} =$

    $$(\textstyle\bigcup_i C'_i \,\|_S (F''\langle\!\langle B := A_1 \rangle\!\rangle)) \cup (\bigcup_i C'_i \,\|_S (F''\langle\!\langle B := A_2 \rangle\!\rangle)) \cup$$
    $$(\textstyle\bigcup_j (F'\langle\!\langle B := A_1 \rangle\!\rangle)) \,\|_S\, C''_j \cup (\bigcup_j (F'\langle\!\langle B := A_2 \rangle\!\rangle)) \,\|_S\, C''_j \cup D$$

    where C'_i are distinguished equivalence classes $C'_i = [H'_i]_{(\mathcal{B}' \cup \sim_{EMB})^+}$ with $H'_i \,\|_S (F''\langle\!\langle B := A_1 \rangle\!\rangle) \in [G' \,\|_S\, G'']_{(\mathcal{B}' \cup \sim_{EMB})^+}$ and C''_j are distinguished equivalence classes $C''_j = [H''_j]_{(\mathcal{B}' \cup \sim_{EMB})^+}$ with $(F'\langle\!\langle B := A_1 \rangle\!\rangle) \,\|_S\, H''_j \in [G' \,\|_S\, G'']_{(\mathcal{B}' \cup \sim_{EMB})^+}$. Besides the classes C'_i and C''_j are such that if $F_1 \equiv (F'\langle\!\langle B := A_1 \rangle\!\rangle) \,\|_S (F''\langle\!\langle B := A_1 \rangle\!\rangle) \in [G' \,\|_S\, G'']_{(\mathcal{B}' \cup \sim_{EMB})^+}$ then there exists i such that $F'\langle\!\langle B := A_1 \rangle\!\rangle \in C'_i$ and j such that $F''\langle\!\langle B := A_1 \rangle\!\rangle \in C''_j$. Moreover D is a set of terms not of the form $H \,\|_S (F''\langle\!\langle B := A_j \rangle\!\rangle)$ or $(F'\langle\!\langle B := A_j \rangle\!\rangle) \,\|_S\, H$ for any term H, hence not reachable from F_1 or F_2. Since d is the maximum depth of the inferences of the potential moves for F_1 having type a, priority level l and derivative term in C, considered term $F'\langle\!\langle B := A_1 \rangle\!\rangle$ ($F''\langle\!\langle B := A_1 \rangle\!\rangle$) we have that for each i (for each j): either (i) $F'\langle\!\langle B := A_1 \rangle\!\rangle$ ($F''\langle\!\langle B := A_1 \rangle\!\rangle$) has no potential moves having type a, priority level l and derivative term in C'_i (C''_j), or (ii) $d-1$ is the maximum depth of the inferences of the potential moves for $F'\langle\!\langle B := A_1 \rangle\!\rangle$ ($F''\langle\!\langle B := A_1 \rangle\!\rangle$) having type a, priority level l and derivative term in C'_i (C''_j). For $j \in \{1,2\}$ we have:

    $$Rate(F_j, a, l, C) = \underset{i}{Min}\; Rate(F_j, a, l, C'_i \,\|_S (F''\langle\!\langle B := A_j \rangle\!\rangle)) \; Min$$
    $$\underset{j}{Min}\; Rate(F_j, a, l, (F'\langle\!\langle B := A_j \rangle\!\rangle) \,\|_S\, C''_j)$$

    where for each i:

$$Rate(F_j, a, l, C'_i \,\|_S (F''\langle\!\langle B := A_j\rangle\!\rangle)) = Rate(F'\langle\!\langle B := A_j\rangle\!\rangle, a, l, C'_i)$$

and for each j:

$$Rate(F_j, a, l, (F'\langle\!\langle B := A_j\rangle\!\rangle) \,\|_S\, C''_j) = Rate(F''\langle\!\langle B := A_j\rangle\!\rangle, a, l, C''_j)$$

By applying the induction hypothesis to each $F'\langle\!\langle B := A_1\rangle\!\rangle, a, l, C'_i$ such that $Rate(F'\langle\!\langle B := A_1\rangle\!\rangle, a, l, C'_i) \neq \bot$ and to each $F''\langle\!\langle B := A_1\rangle\!\rangle, a, l, C''_j$ such that $Rate(F''\langle\!\langle B := A_1\rangle\!\rangle, a, l, C''_j) \neq \bot$ we have that $Rate(F_1, a, l, C'_i \,\|_S (F''\langle\!\langle B := A_1\rangle\!\rangle)) \leq Rate(F_2, a, l, C'_i \,\|_S (F''\langle\!\langle B := A_2\rangle\!\rangle))$ for any i and that $Rate(F_1, a, l, (F'\langle\!\langle B := A_1\rangle\!\rangle) \,\|_S\, C''_j) \leq Rate(F_2, a, l, (F'\langle\!\langle B := A_2\rangle\!\rangle) \,\|_S\, C''_j)$ for any j. It follows that $Rate(F_1, a, l, C) \leq Rate(F_2, a, l, C)$.

* If $a \in S$ we are in the case of synchronization.
  Because of the congruence property w.r.t. "$\_ \|_S \_$" of $\sim_{EMB}$ and of $\mathcal{B}$ we have that:

  $H' \,\|_S\, H'' \in [G' \,\|_S\, G'']_{(\mathcal{B}' \cup \sim_{EMB})^+} \Rightarrow$

  $\quad [H']_{(\mathcal{B}' \cup \sim_{EMB})^+} \,\|_S [H'']_{(\mathcal{B}' \cup \sim_{EMB})^+} \subseteq [G' \,\|_S\, G'']_{(\mathcal{B}' \cup \sim_{EMB})^+}$ [4]

  As a consequence:

  $$[G' \,\|_S\, G'']_{(\mathcal{B}' \cup \sim_{EMB})^+} = (\bigcup_i C'_i \,\|_S\, C''_i) \cup D$$

  where C'_i, C''_i are distinguished pairs of equivalence classes $C'_i = [G'_i]_{(\mathcal{B}' \cup \sim_{EMB})^+}$, $C''_i = [G''_i]_{(\mathcal{B}' \cup \sim_{EMB})^+}$ with $G'_i \,\|_S\, G''_i \in [G' \,\|_S\, G'']_{(\mathcal{B}' \cup \sim_{EMB})^+}$ and D is a set of terms not having "$\_ \|_S \_$" as outermost operator, hence not reachable from F_1 or F_2. Since d is the maximum depth of the inferences of the potential moves for F_1 having type a, priority level l and derivative term in C, for each i: if $Rate(F''\langle\!\langle B := A_1\rangle\!\rangle, a, -1, C''_i) \neq \bot$ ($Rate(F'\langle\!\langle B := A_1\rangle\!\rangle, a, -1, C'_i) \neq \bot$) then either (i) $F'\langle\!\langle B := A_1\rangle\!\rangle$ ($F''\langle\!\langle B := A_1\rangle\!\rangle$) has no potential moves having type a, priority level l and derivative term in C'_i (C''_i), or (ii) $d-1$ is the maximum depth of the inferences of the potential moves for $F'\langle\!\langle B := A_1\rangle\!\rangle$ ($F''\langle\!\langle B := A_1\rangle\!\rangle$) having type a, priority level l and derivative term in C'_i (C''_i). For $j \in \{1, 2\}$ we have:

  $$Rate(F_j, a, l, C) = \underset{i}{Min}\; Rate(F_j, a, l, C'_i \,\|_S\, C''_i)$$

  where for each i:

  $$Rate(F_j, a, l, C'_i \,\|_S\, C''_i) = \begin{cases} Rate(F'\langle\!\langle B := A_j\rangle\!\rangle, a, l, C'_i)\; Min\; Rate(F''\langle\!\langle B := A_j\rangle\!\rangle, a, l, C''_i) \\ Rate(F'\langle\!\langle B := A_j\rangle\!\rangle, a, l, C'_i) \\ Rate(F''\langle\!\langle B := A_j\rangle\!\rangle, a, l, C''_i) \\ \bot \end{cases}$$

  depending on whether, defined $R'_j = Rate(F'\langle\!\langle B := A_j\rangle\!\rangle, a, -1, C'_i)$ and $R''_j = Rate(F''\langle\!\langle B := A_j\rangle\!\rangle, a, -1, C''_i)$, $R'_j \neq \bot$ and $R''_j \neq \bot$, $R'_j = \bot$ and $R''_j \neq \bot$, $R'_j \neq \bot$ and $R''_j = \bot$ or $R'_j = \bot$ and $R''_j = \bot$. By applying the induction hypothesis to each $F'\langle\!\langle B := A_1\rangle\!\rangle, a, l, C'_i$ such that $Rate(F'\langle\!\langle B := A_1\rangle\!\rangle, a, l, C'_i) \neq \bot$ and to each $F''\langle\!\langle B := A_1\rangle\!\rangle, a, l, C''_i$ such that $Rate(F''\langle\!\langle B := A_1\rangle\!\rangle, a, l'', C''_i) \neq \bot$, we have that $Rate(F_1, a, l, C'_i \,\|_S\, C''_i) \leq Rate(F_2, a, l, C'_i \,\|_S\, C''_i)$ for any i. It follows that $Rate(F_1, a, l, C) \leq Rate(F_2, a, l, C)$.

– If $F \equiv B'$, then for $j \in \{1, 2\}$ we have $F_j \equiv B'\langle\!\langle B := A_j\rangle\!\rangle$.

  * If $B' \equiv B$, then for $j \in \{1, 2\}$ we have $F_j \equiv A_j$. Since d is the maximum depth of the inferences of the potential moves for F_1 having type a, priority level l and derivative term in C, then $d-1$ is the maximum depth of the inferences of the potential moves for $E_1\langle\!\langle A := A_1\rangle\!\rangle$ having type a, priority level l and derivative term in C. For $j \in \{1, 2\}$ we have:

    $$Rate(F_j, a, l, C) = Rate(E_j\langle\!\langle A := A_j\rangle\!\rangle, a, l, C)$$

    By applying the induction hypothesis to $E_1\langle\!\langle A := A_1\rangle\!\rangle, a, l, C$ we have that $Rate(E_1\langle\!\langle A := A_1\rangle\!\rangle, a, l, C) \leq Rate(E_1\langle\!\langle A := A_2\rangle\!\rangle, a, l, C)$. From the fact that $E_1 \sim_{EMB} E_2$ we derive $Rate(E_1\langle\!\langle A := A_2\rangle\!\rangle, a, l, C) = Rate(E_2\langle\!\langle A := A_2\rangle\!\rangle, a, l, C)$. It follows that $Rate(F_1, a, l, C) \leq Rate(F_2, a, l, C)$.

[4] Given a set of terms $\mathcal{T}_1$ and a set of terms $\mathcal{T}_2$, $\mathcal{T}_1 \,\|_S\, \mathcal{T}_2$ is the set of terms $\{E' \,\|_S\, E'' \mid E' \in \mathcal{T}_1 \wedge E'' \in \mathcal{T}_2\}$.

* If $B' \not\equiv B$, then let $B' \stackrel{\Delta}{=} F'$ be the defining equation of B'. Since d is the maximum depth of the inferences of the potential moves for F_1 having type a, priority level l and derivative term in C, then $d-1$ is the maximum depth of the inferences of the potential moves for $F' \langle\!\langle B := A_1 \rangle\!\rangle$ having type a, priority level l and derivative term in C. For $j \in \{1,2\}$ we have:
$$Rate(F_j, a, l, C) = Rate(F' \langle\!\langle B := A_j \rangle\!\rangle, a, l, C)$$
By applying the induction hypothesis to $F' \langle\!\langle B := A_1 \rangle\!\rangle, a, l, C$ we have that $Rate(F' \langle\!\langle B := A_1 \rangle\!\rangle, a, l, C) \leq Rate(F' \langle\!\langle B := A_2 \rangle\!\rangle, a, l, C)$. It follows that $Rate(F_1, a, l, C) \leq Rate(F_2, a, l, C)$.

By applying a symmetric argument we have also that $Rate(F_2, a, l, C) \leq Rate(F_1, a, l, C)$ for each $(F_1, F_2) \in \mathcal{B}$, $a \in AType$, $l \in APLev$ and $C \in \mathcal{G}_\Theta / (\mathcal{B}' \cup \sim_{EMB})^+$, hence we conclude that $Rate(F_1, a, l, C) = Rate(F_2, a, l, C)$. ■

Acknowledgements

This research has been partially funded by MURST and Progetto Strategico CNR "Modelli e Metodi per la Matematica e l'Ingegneria".

References

[1] M. Bernardo, R. Gorrieri, *"A Tutorial on EMPA: A Theory of Concurrent Processes with Nondeterminism, Priorities, Probabilities and Time"*, to appear in Theoretical Computer Science, 1998

[2] R. van Glabbeek, S.A. Smolka, B. Steffen, *"Reactive, Generative and Stratified Models of Probabilistic Processes"*, in Information and Computation 121:59-80, 1995

[3] H. Hermanns, M. Lohrey, *"Observation Congruence in a Stochastic Timed Calculus with Maximal Progress"*, Tech. Rep. IMMD VII-7/97, University of Erlangen (Germany), 1997

[4] J. Hillston, *"A Compositional Approach to Performance Modelling"*, Cambridge University Press, 1996

[5] K.G. Larsen, A. Skou, *"Bisimulation through Probabilistic Testing"*, in Information and Computation 94:1-28, 1991

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