ELSEVIER

Theoretical Computer Science 254 (2001) 691–694

Theoretical Computer Science

www.elsevier.com/locate/tcs

Erratum

Corrigendum to "A tutorial on EMPA: a theory of concurrent processes with nondeterminism, priorities, probabilities and time" [Theoret. Comput. Sci. 202 (1998) 1–54] ☆

Marco Bernardo[a], Roberto Gorrieri[b, *]

[a] *Dipartimento di Informatica, Università di Torino, Corso Svizzera 185, 10149 Torino, Italy*
[b] *Dipartimento di Scienze dell'Informazione, Università di Bologna, Mura Anteo Zamboni 7, I-40127 Bologna, Italy*

Received 3 April 2000; accepted 26 April 2000

In [2] we presented a tutorial on the stochastically timed process algebra EMPA together with the related theory: semantics, equivalence, and axiomatization. The purpose of this note is to remedy to two errors contained in that paper which are related to the strong extended Markovian bisimulation equivalence $\sim_{\mathrm{EMB}}$ defined for EMPA. The first error is contained in the proof of the congruence property of $\sim_{\mathrm{EMB}}$ w.r.t. recursive definitions but does not affect the validity of the result. The second error is contained in the proof of the congruence property of $\sim_{\mathrm{EMB}}$ w.r.t. the parallel composition operator and affects the validity of the result, as it holds only for a class of terms allowing for a restricted form of nondeterminism.

The first error, discovered by Mario Bravetti, is concerned with the proof of the congruence property w.r.t. recursive definitions of Theorem 5.19. The technique used in [2] consists of proving by induction that a certain relation over EMPA terms is a strong extended Markovian bisimulation up to $\sim_{\mathrm{EMB}}$. As recognized in [4], the proof of Theorem 5.19 contains two inaccuracies related to the employed notion of strong extended Markovian bisimulation up to $\sim_{\mathrm{EMB}}$ and the structure of the inductive proof itself.

The problem with the definition of strong extended Markovian bisimulation up to $\sim_{\mathrm{EMB}}$ of Definition 5.12 is that, following the style of [7], it should be given w.r.t. the classes of an equivalence relation determined by $\sim_{\mathrm{EMB}}$ and $\mathscr{B}$, the relation over EMPA terms being defined. In Definition 5.12, instead, the classes of the relation $\sim_{\mathrm{EMB}} \mathscr{B} \sim_{\mathrm{EMB}}$ are considered which, in general, is not transitive even if $\mathscr{B}$ is supposed to

☆ PII: S0304-3975(97)00127-8.

* Corresponding author.
E-mail addresses: bernardo@di.unito.it (M. Bernardo), gorrieri@cs.unibo.it (R. Gorrieri).

PII: S0304-3975(00)00256-5

be an equivalence relation. Similar to [6], in [4] it is proposed to solve this problem by considering the classes of $(\mathscr{B} \cup \mathscr{B}^{-1} \cup \sim_{\mathrm{EMB}})^{+}$.

The problem with the structure of the proof is the following. Given two terms E_1 and E_2, since the proof proceeds by induction on the maximum depth of the derivation of the transitions of E_1 labeled with type a, having priority level l, and reaching an arbitrary equivalence class C w.r.t. $\mathscr{B}$ (the relation over EMPA terms that has to be proved to be a strong extended Markovian bisimulation up to $\sim_{\mathrm{EMB}}$), several cases arise depending on the outermost operator, as in the proof of the corresponding result in [8]. As far as static operators are concerned, the proof of Theorem 5.19 wrongly assumes that all the terms that, when applying the same static operator, belong to the same equivalence class C are equivalent, i.e., they form a single equivalence class. Instead, such terms form in general several equivalence classes, to each of which the induction hypothesis $\mathit{Rate}(E_1, a, l, C) = \mathit{Rate}(E_2, a, l, C)$ should be applicable. Actually, this is possible only for those classes which are reachable from the subterm E_1' of E_1 in the scope of the static operator, because for the other classes we would need a converse argument related to the transitions of the subterm E_2' of E_2 in the scope of the static operator. Similar to [5], in [4] it is proposed to solve the problem by splitting the proof into two symmetric parts and changing the induction assertion of the whole proof into $\mathit{Rate}(E_1, a, l, C) \leqslant \mathit{Rate}(E_2, a, l, C)$. The complete revised proof of Theorem 5.19 can be found in [4, 1].

The second error, discovered by Pedro D'Argenio and Holger Hermanns, is concerned with the congruence property w.r.t. the parallel composition operator of Theorem 5.14. Such a property does not hold in general. As an example, if we consider

$$E_1 \equiv \langle a, * \rangle.\underline{0} + \langle a, * \rangle.\langle b, \mu \rangle.\underline{0}$$

$$E_2 \equiv \langle a, * \rangle.\underline{0} + \langle a, * \rangle.\underline{0} + \langle a, * \rangle.\langle b, \mu \rangle.\underline{0}$$

$$F_1 \equiv \langle a, * \rangle.\langle a, * \rangle.\underline{0} \parallel_{\emptyset} \langle a, * \rangle.\langle b, \mu \rangle.\underline{0}$$

$$F_2 \equiv \langle a, * \rangle.\underline{0} \parallel_{\emptyset} \langle a, * \rangle.\underline{0} \parallel_{\emptyset} \langle a, * \rangle.\langle b, \mu \rangle.\underline{0}$$

$$G \equiv \langle a, \lambda \rangle.\underline{0}$$

we have that $E_1 \sim_{\mathrm{EMB}} E_2$ and $F_1 \sim_{\mathrm{EMB}} F_2$ by $E_1 \parallel_{\{a\}} G \not\sim_{\mathrm{EMB}} E_2 \parallel_{\{a\}} G$ and $F_1 \parallel_{\{a\}} G \not\sim_{\mathrm{EMB}} F_2 \parallel_{\{a\}} G$, because e.g. $\mathit{Rate}(E_1 \parallel_{\{a\}} G, a, 0, [\langle b, \mu \rangle.\underline{0}]_{\sim_{\mathrm{EMB}}}) = \lambda/2 \neq \lambda/3 = \mathit{Rate}(E_2 \parallel_{\{a\}} G, a, 0, [\langle b, \mu \rangle.\underline{0}\,]_{\sim_{\mathrm{EMB}}})$. The problem is that the way rate normalization works in the semantic rule of Table 1 for the parallel composition operator (i.e., counting the number of passive actions with which a given active action can be synchronized) is not compatible with the idempotence for passive actions captured by $\sim_{\mathrm{EMB}}$ (see Axiom $\mathscr{A}_4$ of Table 6).

As observed in [1], the result still holds for a class of terms characterizable in a semantic way. More precisely, $\sim_{\mathrm{EMB}}$ is a congruence w.r.t. the parallel composition operator for the class of EMPA terms allowing for the following restricted form of nondeterminism among passive actions of the same type: Whenever several passive actions of the same type can be synchronized with the same active action, the derivative terms of the passive actions must be equivalent. More formally, Theorem 5.14 holds for the class of guarded and closed EMPA terms

$$\mathscr{G}_{\Theta,\mathrm{rnd}} = \{E \in \mathscr{G}_\Theta \mid \forall F \in S_{E,\mathscr{I}}.RND(F)\}$$

where $S_{E,\mathscr{I}}$ is the state space of E and predicate $RND : \mathscr{G}_\Theta \rightarrow \{true,\ false\}$ is defined by structural induction as follows:

$$\begin{array}{rcl}
RND(\underline{0}) & & \\
RND(\langle a,\tilde{\lambda}\rangle.E) & & \\
RND(E/L) & \Leftarrow & RND(E) \\
RND(E[\varphi]) & \Leftarrow & RND(E) \\
RND(\Theta(E)) & \Leftarrow & RND(E) \\
RND(E_1 + E_2) & \Leftarrow & RND(E_1) \wedge RND(E_2) \\
RND(E_1 \parallel_S E_2) & \Leftarrow & RND(E_1) \wedge RND(E_2) \wedge \\
& & (\nexists a \in S. E_1 \xrightarrow{a,*} E_1' \wedge E_1 \xrightarrow{a,*} E_1'' \wedge \\
& & \quad E_2 \xrightarrow{a,\tilde{\lambda}} E_2' \wedge \tilde{\lambda} \neq * \wedge \\
& & \quad E_1' \not\sim_{\mathrm{EMB}} E_1'') \wedge \\
& & (\nexists a \in S. E_1 \xrightarrow{a,\tilde{\lambda}} E_1' \wedge \tilde{\lambda} \neq * \wedge \\
& & \quad E_2 \xrightarrow{a,*} E_2' \wedge E_2 \xrightarrow{a,*} E_2'' \wedge \\
& & \quad E_2' \not\sim_{\mathrm{EMB}} E_2'') \\
RND(A) & \Leftarrow & RND(E) \qquad \text{if } A \stackrel{\Delta}{=} E
\end{array}$$

The revised version of Theorem 5.14, whose complete proof can be found in [1], establishes that nondeterminism, priority, probability, and exponentially distributed time fit well together in EMPA as long as the nondeterminism is confined to the choice among passive actions of different types or, under certain conditions, of the same type. Despite the fact that such conditions are rather semantical in nature, a characterization of a subset of $\mathscr{G}_{\Theta,\mathrm{rnd}}$ which is easier to check may be set up by requiring that the derivative terms of passive actions of the same type are related by a more syntactical equivalence which approximates $\sim_{\mathrm{EMB}}$. As an example, one could adopt structural congruence over terms modulus associativity and commutativity of the alternative and parallel composition operators. This would be sufficient to single out a reasonable class of terms (including those in the case studies of [1]) for which the congruence property w.r.t. the parallel composition operator holds.

A different solution to the problem has been proposed in [3], where a generative–reactive (according to the terminology of [5]) variant of EMPA called $\mathrm{EMPA_{gr}}$ is introduced which rules out nondeterminism between passive actions of the same type. Exploiting the asymmetric form of synchronization between exponentially timed/immediate actions and passive actions typical of EMPA, the idea is that nondeterministic passive actions, whose rate is denoted by $*$, are turned into reactive prioritized-probabilistic passive actions, whose rate is denoted by $*_{l,w}$. According to the reactive approach, the priority levels and the weights associated with passive actions are used in $\mathrm{EMPA_{gr}}$ only to choose among passive actions of the same type, thus confining nondeterminism to the choice among passive actions of different types and avoiding discrepancies with the way rate normalization works. In [3] it is shown that $\sim_{\mathrm{EMB}}$ turns out to be a congruence w.r.t. the parallel composition operator for the whole $\mathrm{EMPA}_{\mathrm{gr}}$, which means that nondeterminism among passive actions of different types, priority, probability, and exponentially distributed time fit well together in $\mathrm{EMPA}_{\mathrm{gr}}$.

References

[1] M. Bernardo, Theory and application of extended Markovian process algebra, Ph.D. Thesis, University of Bologna, Italy, 1999 (http://www.di.unito.it/~ bernardo/).
[2] M. Bernardo, R. Gorrieri, A tutorial on EMPA: a theory of concurrent processes with nondeterminism, priorities, probabilities and time, Theoret. Comput. Sci. 202 (1998) 1–54.
[3] M. Bravetti, M. Bernardo, Compositional asymmetric cooperations for process algebras with probabilities, priorities, and time. Tech. Rep. UBLCS-2000-01, University of Bologna, Italy, 2000 (ftp.cs.unibo.it/pub/techreports).
[4] M. Bravetti, M. Bernardo, R. Gorrieri, A note on the congruence proof for recursion in Markovian bisimulation equivalence, Proc. 6th Int. Workshop on Process Algebra and Performance Modelling (PAPM 98), Nice, France, 1998, pp. 153–164.
[5] R. van Glabbeek, S.A. Smolka, B. Steffen, Reactive, generative and stratified models of probabilistic processes, Inform. and Comput. 121 (1995) 59–80.
[6] 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.
[7] K.G. Larsen, A. Skou, Bisimulation through Probabilistic Testing, Inform. and Comput. 94 (1991) 1–28.
[8] R. Milner, Communication and Concurrency, Prentice-Hall, Englewood Cliffs, NJ, 1989.