Non-determinism in Probabilistic Timed Systems with General Distributions

Mario Bravetti [1] and Alessandro Aldini [2]

Dipartimento di Scienze dell'Informazione,
University of Bologna, Mura Anteo Zamboni 7, 40127 Bologna, Italy

Abstract

In this paper we address the problem of adequately handling non-deterministic choices in Generalised Semi-Markov Processes (GSMPs), i.e. probabilistic timed systems where durations of delays are expressed by means of random variables with a general probability distribution. In particular we want the probabilistic duration of a delay not to be decided all at once when the delay starts, but step by step in each system state (in the theory of GSMPs this corresponds to recording spent lifetimes instead of residual lifetimes of delays). In this way an adversary cannot take decisions a priori, based on the knowledge he may get about the future behavior of the system. In order to accomplish this, we consider Interactive Generalised Semi-Markov Processes (IGSMPs). We start by formalizing the class of well-named IGSMP models and the class of Interactive Stochastic Timed Transition Systems (ISTTSs) which are both closed under CSP parallel composition and hiding. Then, we introduce a semantics for IGSMPs which maps well-named IGSMP models onto ISTTSs by recording spent lifetimes of delays. Finally, we show that two weakly bisimilar IGSMPs give rise to two weakly bisimilar semantic models and that our semantic mapping is compositional with respect to both CSP parallel composition and hiding.

1 Introduction

The importance of modeling the behavior of concurrent systems with respect to time has been widely recognized [18,17,3,10,5]. Moreover due to the fact that either systems are frequently described at a high level of abstraction, or the temporal behavior of some system component is inherently probabilistic (e.g. transmission time of a message through a network), it is important

[1] Email: bravetti@cs.unibo.it
[2] Email: aldini@cs.unibo.it

This is a preliminary version. The final version is considered for publication in Electronic Notes in Theoretical Computer Science
URL: www.elsevier.nl/locate/entcs

that the modeling paradigm employed allows for the specification of probabilistic time. To this aim several modeling techniques have been defined to specify systems including activities with probabilistic exponentially distributed duration [18,17,3,10,5]. These approaches have the advantage to be easily tractable from both the modeling and analysis viewpoint since the underlying performance models are just simple Markov Chains. The price to pay is a strong limitation in the expressiveness of these modeling paradigms, since even fixed (non probabilistic) durations cannot be represented. Some previous efforts have been made in order to develop models for general distributions [16,2,9,24,6,14]. In particular in [8] we have recognized that a formalism expressing systems with generally distributed delays should originate from probabilistic models which are well-founded from the viewpoint of probability theory. More precisely, we have considered Generalised Semi-Markov Processes (GSMPs), i.e. probabilistic timed systems where durations of delays are expressed by means of random variables with a general probability distribution. A GSMP describes the temporal behavior of a system by using *elements*, which act similarly as clocks of a Timed Automata (see e.g. [23]). In particular the temporal delays in the evolution of a system are represented by clocks (elements) whose duration is determined by an associated generally distributed random variable. In this way the temporal behavior of the system is "guided" by the events of start and termination of clocks (elements). Following the idea of [17], where the same problem is attacked for exponential distributions, we have introduced in [6] the possibility of specifying systems as the parallel composition of subsystems described by GSMPs, by developing the calculus of Interactive Generalized Semi-Markov Processes (IGSMPs).

An IGSMP represents the behavior of a component by employing both *standard action transitions*, representing the interactive behavior of the component, and *clock start transitions* and *clock termination transitions*, representing the timed probabilistic behavior of the component. Action transitions are just standard CCS/CSP transitions: when several action transitions are enabled in an IGSMP state, the choice among them is just performed nondeterministically and when IGSMPs are composed in parallel they synchronize following the CSP [19] approach, where the actions belonging to a given set S are required to synchronize. Clock start transitions are labeled with a clock name and a weight and represent the event of start of a temporal delay whose probabilistic duration is given by the distribution associated with the clock. When several clock start transitions are enabled in an IGSMP state, the choice among them is performed probabilistically according to the weights of the transitions. Clock termination transitions are labeled with a clock name and represent the event of termination of the corresponding temporal delay. A system stays in a state enabling several termination transitions until one of the temporal delays currently in execution terminates and the corresponding transition is performed.

Introducing non-determinism in probabilistic systems with general distributions causes new problems to arise with respect to the classical theory of GSMPs. Such problems arise when we consider the interplay of non-deterministic choices and the probabilistic behavior of clocks when IGSMPs are actually executed. Following the classical approach of discrete event simulation (see e.g. [12]), in the instant a clock starts, the clock is set to a temporal value sampled from its duration distribution. As time passes clock counts down and it terminates when it reaches value zero. From a technical viewpoint this means that, while the GSMP proceeds from state to state, we keep track of the quantity of time that clocks must still spend in execution (the *residual lifetimes* of the clocks). This approach to the execution of an IGSMP, which has been previously applied in [14] to systems including non-determinism and generally distributed time, has the drawback that an adversary can base its decisions (concerning non-deterministic choices) on the knowledge obtained a priori about the future behavior of the system, e.g. the information about the quantity of time that a delay will spend in execution.

In this paper we consider a new alternative approach to the execution of systems including non-determinism and generally distributed time which adequately handles non-deterministic choices. The idea is that we want the probabilistic duration of a generally distributed delay not to be decided all at once when the delay starts, but step by step in each system state. More precisely, this is realized by keeping track of the quantity of time spent by clocks in execution (*spent lifetimes* of clocks), and by evaluating, when a new IGSMP state is entered, the distribution of the residual duration of the clock from (i) the duration distribution associated with the clock, and (ii) the time it has already spent in execution. Such an approach, which is based on recording spent lifetimes instead of residual lifetimes, is adherent to the classical behavior of Timed Automata [23] where clocks are increased (and not decreased) while time passes. Besides it indeed solves the problem of executing a system with non-deterministic choices because, since the residual duration of clocks is sampled in every state traversed by the IGSMP, the adversary cannot gain a priori knowledge on the system behavior. Finally, considering spent lifetimes instead of residual lifetimes is correct also from a probabilistic viewpoint, because in probability theory the two approaches are both valid alternative ways to interpret a GSMP [13]. It is worth noting that the choice of adopting this alternative approach for representing the execution of an IGSMP is conceptual and not at all related with the technical differences between the formalism considered in [14] and IGSMPs. We could apply the technique used in [14] to IGSMPs as well.

Similarly as in [14], based on our approach to the execution of an IGSMP, we produce a semantics for IGSMPs which maps an IGSMP onto a transition system where: (i) the passage of time is explicitely represented by transitions labeled with numeric time delays and (ii) duration probability distributions are turned into infinitely branching probabilistic choices which lead to states performing numeric time delays with different durations. Differently from [14] we express semantic models of IGSMPs by means of "interactive" probabilistic timed transition systems which can be themselves composed and we develop a semantic mapping which is compositional with respect to parallel composition and hiding.

More precisely, we start (in Sect. 2) by formalising the model of IGSMPs and the model of well-named IGSMPs (a canonical form for IGSMPs which makes it simple to establish weak bisimulation over IGSMPs). With respect to [6], where well-named IGSMPs are defined as the class of semantic models obtained from the terms of a process algebra, in this paper we characterize well-named IGSMPs directly as a class of transition systems. Moreover we show that the class of well-named IGSMPs is closed with respect to CSP parallel composition and hiding and we introduce a notion of weak bisimulation over well-named IGSMPs. Then, (in Sect. 3) we introduce the model of Interactive Stochastic Timed Transition Systems (ISTTSs) which include: *standard action transitions*, representing the interactive behavior of a system component, *numeric time transitions* representing a fixed temporal delay, and *probabilistic transitions* (expressed by means of probability spaces) representing (infinitely branching) probabilistic choices. Moreover we show that the class of ISTTSs is closed with respect to CSP parallel composition and hiding and we introduce a notion of weak bisimulation over ISTTSs. Moreover, (in Sect. 4) we present the semantics for IGSMPs which maps IGSMPs onto ISTTSs and we show that weakly bisimilar IGSMPs give rise to weakly bisimilar semantic models and that the semantic mapping is compositional with respect to both CSP parallel composition and hiding. Finally, (in Sect. 5) we report some concluding remarks. The proofs of the results in this paper can be found in [4].

2 Interactive Generalized Semi-Markov Process

In this section we will present the model of Interactive Generalized Semi-Markov Processes (IGSMPs) and of well-named Interactive Generalized Semi-Markov Processes: a canonical form for IGSMPs which introduces some constraints on clock names and makes it simple to establish equivalence over IGSMPs. We first briefly introduce some basic notions about GSMPs, and then we discuss in depth the model of IGSMPs and well-named IGSMPs.

2.1 The GSMP Model

The class of generalized semi-Markov processes (GSMPs) has been introduced by Matthes (1962) in [21] and represents the temporal behavior of a system through elements (or clocks) each with an associated duration probability distribution (element lifetime). What characterizes GSMPs (e.g. with respect to Semi-Markov Processes) is the possibility of having multiple *active elements* in a state, so that when an active element terminates (*it dies*) a state change occurs and the other elements continue their life in the following state, thus carrying over their residual duration.

Definition 2.1 A *generalized semi-Markov process* (GSMP) is a stochastic process defined on a set of states $\{s \mid s \in \mathcal{S}\}$ as follows. In each state s there is a set of active elements e taken from a set El. The set El is partitioned into two sets El' ed El^* with $El = El' \cup El^*$. If $e \in El'$ the element e has an exponentially distributed lifetime, if instead $e \in El^*$ it has an arbitrarily distributed lifetime. Whenever in a state s an active element e dies, the process moves to the state $s' \in \mathcal{S}$ with a given probability $P(s, e, s')$.

In GSMPs the following restrictions are considered [21]:

- When the process moves from a state to another, no more than one element of El^* can be born or die contemporaneously.
- The active elements of El^* that do not die in a state keep their residual duration.

A GSMP can be analyzed through simulative techniques and/or mathematical techniques (based on phase-type approximation or insensitivity [21]) in order to obtain performance measures of a system.

2.2 The IGSMP Model

The model of Interactive Generalized Semi-Markov Processes extends that of Generalized Semi-Markov Processes by expressing in addition to GSMP clocks (or elements) execution, also the execution of standard actions which can synchronize and have a zero duration. Such an approach, which is inspired from [17], is also quite usual in real-time process algebras [23] where transitions representing temporal delays are distinguished from standard action transitions which are performed in zero time. As far as probabilistic delays are concerned, they are modeled as in GSMPs by means of clocks C whose duration is expressed through general probability distributions. In the following we will distinguish different clocks used in an IGSMP through "names", where C_n denotes the clock with name n. In an IGSMP the execution of a clock C_n is represented by means of two events: the event of clock start C_n^+ followed by the relative event of clock termination C_n^-. Therefore in an IGSMP we have three types of transitions: standard action transitions representing action execution, clock start transitions representing events C_n^+ and clock termination transitions representing events C_n^-. When a transition C_n^+ is performed by the IGSMP the clock C_n starts and continues its execution in every state traversed by the IGSMP. Whenever the clock C_n terminates, then the IGSMP executes the corresponding termination transition C_n^-. In particular, since, as in GSMPs, each started clock C_n which has not terminated yet must continue its execution in each state traversed by the IGSMP, all such states must have an outgoing transition C_n^-. Obviously clocks which can be simultaneously under execution in an IGSMP state must have different names (even if they have the same duration distribution), so that the event of termination of a clock C_n^- is always uniquely related to the corresponding event of start of the same clock C_n^+. Similarly as GSMPs, IGSMPs can also express probabilistic choices. This is obtained by associating with each start transition C_n^+ a weight $w \in \mathbb{R}^+$. In this way when a state of the IGSMP enables several clock start transitions $\langle C_n^+, w \rangle$, the choice of the clock to be started is performed probabilistically according to the weights w of the transitions. For instance, a state enabling two transitions labeled with $\langle C_n^+, w \rangle$ and $\langle C_{n'}^+, w' \rangle$ respectively starts clock C_n with probability $w/(w + w')$ and starts clock $C_{n'}$ with probability $w'/(w + w')$. On the other hand, similarly as in [17], IGSMPs also have, in addition to GSMPs, the capability of expressing non-deterministic choices. This because, as in standard labeled transition systems deriving from CCS/CSP terms, in the states of an IGSMP action transitions are just non-deterministically chosen. In particular alternative transitions labeled with invisible τ actions represent internal non-deterministic choices which are performed in zero time and can never be "resolved" through synchronization with other system components. On the contrary, visible actions a in an IGSMP are seen as incomplete actions which wait for a synchronization with other system components (they represent potential interaction with the environment). Therefore the choice of such actions in any IGSMP state is governed by an external form of non-determinism, as their execution completely depends on the environment. Note that since we adopt a CSP synchronization policy for IGSMPs which produces visible actions from the synchronization of visible actions (thus allowing for multiway synchronization) the only way to turn an incomplete action in a complete one is by means of a hiding operator, which turns visible actions into τ actions. Similarly as in [17] an IGSMP represents a *complete system* only when it does not include any transition labeled by a visible action. This approach differs from that of the stochastic automaton model of [14], where two different kinds of semantics have to be defined in order to describe the *actual behavior* of closed systems and the *potential behavior* of open systems. In our approach both the potential and the actual behavior of the system are represented within the same model and complete systems are obtained by hiding all the actions of the model. Note that IGSMPs representing complete systems may still include non-determinism due to multiple internal τ transitions enabled in the same state (internal non-determinism). Therefore, adversaries (or schedulers) play an important role in the performance analysis of IGSMPs in that they allow internal non-determinism to be removed from an IGSMP thus turning it into a GSMP.

More precisely, in an IGSMP we have four different kinds of state:

- *silent states*, enabling invisible action transitions τ and (possibly) visible action transitions a only. In such states the IGSMP just performs a non-deterministic choice among the τ transitions in zero time and may potentially interact with the environment through one of the visible actions (see e.g. Fig. 1.a).

- *probabilistic states*, enabling $\langle C_n^+, w\rangle$ transitions and (possibly) visible action transitions a only. In such states the IGSMP just performs a probabilistic choice among the clock start transitions in zero time and may potentially interact with the environment through one of the visible actions (see e.g. Fig. 1.b).
- *timed states*, enabling C_n^- transitions and (possibly) visible action transitions a only. In such states the IGSMP executes all the clocks labeling the outgoing termination transitions according to their residual duration distribution. The clock that terminates first determines the transition to be performed. Note that since, as in GSMPs, we assume that clocks cannot terminate at the same instant, we always have a unique clock terminating before the other ones (see e.g. Fig. 1.c). While the IGSMP sojourns in the state, it may (at any time) potentially interact with the environment through one of the outgoing visible action transitions.
- *waiting states*, enabling standard visible actions only or no transition at all. In such states the IGSMP sojourns indefinitely. It may, at any time, potentially interact with the environment through one of the outgoing visible action transitions (see e.g. Fig. 1.d).

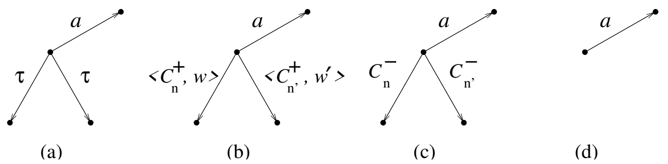

Fig. 1. Some examples of possible states of an IGSMP

In the following we present the formal definition of Interactive Generalized Semi-Markovian Transition System (IGSMTS), then we will define Interactive Generalized Semi-Markov Process as IGSMTSs possessing an initial state. Formally, we denote with PDF the set of probability distribution functions over $\mathbb{R}$ ranged over by $f, g, \ldots$ and with PDF^+ the set of probability distribution functions over $\mathbb{R}$ such that $f(x) = 0$ for $x < 0$ (representing duration distributions). Weights, belonging to $\mathbb{R}^+$, are ranged over by $w, w', \ldots$. Moreover, we denote the set of standard action types used in a IGSMTS by Act, ranged over by $\alpha, \alpha', \ldots$. As usual Act includes the special type τ denoting internal actions. The set $Act - \{\tau\}$ is ranged over by $a, b, \ldots$. The set of clocks of an IGSMTS is denoted by $\mathcal{C} = \{C_n \mid n \in \mathcal{C}Names\}$, where $\mathcal{C}Names$ is a set of clock names. Given a set $\mathcal{C}$, we denote with $\mathcal{C}^+ = \{\langle C_n^+, w\rangle \mid C_n \in \mathcal{C}, w \in \mathbb{R}^+\}$ the set of events denoting the starting of a clock and $\mathcal{C}^- = \{C_n^- \mid C_n \in \mathcal{C}\}$ the set of events denoting the termination of a clock. Let $\mathcal{C}^+ \cup \mathcal{C}^-$ be ranged over by $\theta, \theta', \ldots$. The set of states of an IGSMTS is denoted by Σ, ranged over by $s, s', \ldots$. We assume the following abbreviations that will make the definition of IGSMTSs easier. Let us suppose that $T \subseteq (\Sigma \times Labels \times \Sigma)$ is a transition relation, where $Labels$ is a set of transition labels, ranged over by l. We use $s \xrightarrow{\;l\;} s'$ to stand for $(s, l, s') \in T$, $s \xrightarrow{\;l\;}$ to stand for $\exists s' : s \xrightarrow{\;l\;} s'$, and

$s \stackrel{l}{\not\longrightarrow}$ to stand for $\nexists s' : s \stackrel{l}{\longrightarrow} s'$.

Definition 2.2 An Interactive Generalized Semi-Markovian Transition System (IGSMTS) is a tuple $\mathcal{G} = (\Sigma, \mathcal{C}, D, Act, T_+, T_-, T_a)$ with

- Σ a set of states,
- $\mathcal{C}$ a set of clocks,
- $D : \mathcal{C} \longrightarrow PDF^+$ a function that assigns a duration probability distribution function to each clock,
- Act a set of standard actions,
- $T_+ \subseteq (\Sigma \times \mathcal{C}^+ \times \Sigma)$, $T_- \subseteq (\Sigma \times \mathcal{C}^- \times \Sigma)$, and $T_a \subseteq (\Sigma \times Act \times \Sigma)$ three transition relations representing clock start and termination events and action execution, respectively, such that: [3]

  1 $\forall s \in \Sigma.$
  $$s \stackrel{\tau}{\longrightarrow} \implies \nexists \theta.\, s \stackrel{\theta}{\longrightarrow}$$
  2 $\forall s \in \Sigma.$
  $$\exists C_n, w.\, s \xrightarrow{\langle C_n^+, w\rangle} \implies \nexists C_{n'}.\, s \xrightarrow{C_{n'}^-}$$
  3 $\exists \mathcal{S} : \Sigma \longrightarrow \mathcal{P}(\mathcal{C})$ the *active clock function*, such that $\forall s \in \Sigma$.

  $a)$ - $s \stackrel{\alpha}{\longrightarrow} s' \implies \mathcal{S}(s') = \mathcal{S}(s)$

  - $s \xrightarrow{\langle C_n^+, w\rangle} s' \implies \mathcal{S}(s') = \mathcal{S}(s) \cup \{C_n\}$

  - $s \xrightarrow{C_n^-} s' \implies C_n \in \mathcal{S}(s) \;\wedge\; \mathcal{S}(s') = \mathcal{S}(s) - \{C_n\}$

  $b)$ $\exists C_n, w.\, s \xrightarrow{\langle C_n^+, w\rangle} \implies C_n \notin \mathcal{S}(s)$

  $c)$ $C_n \in \mathcal{S}(s) \;\wedge\; s \stackrel{\tau}{\not\longrightarrow} \;\wedge\; \nexists C_{n'}, w.\, s \xrightarrow{\langle C_{n'}^+, w\rangle} \implies s \xrightarrow{C_n^-}$

  4 $\forall s \in \Sigma.$
  $$s \xrightarrow{\langle C_n^+, w\rangle} s' \implies act(s') \subseteq act(s)$$
  where the *enabled action function* $act : \Sigma \longrightarrow \mathcal{P}(Act)$ is defined by $act(s) = \{\alpha \mid s \stackrel{\alpha}{\longrightarrow}\}$.

Definition 2.3 An Interactive Generalized Semi-Markov Process (IGSMP) is a tuple $\mathcal{G} = (\Sigma, \mathcal{C}, D, Act, T_+, T_-, T_a, s_0)$, where $s_0 \in \Sigma$ is the initial state of the IGSMP and $(\Sigma, \mathcal{C}, D, Act, T_+, T_-, T_a)$ is an IGSMTS such that function $\mathcal{S}$ in item 3 of Definition 2.2 also satisfies $\mathcal{S}(s_0) = \emptyset$.

The constraints over transition relations T_+, T_- and T_a guarantee that each state of the IGSMP belongs to one of the four kind of states above. In particular, the first requirement says that if a state can perform internal τ actions then it cannot perform events of clock starts or clock terminations. Such

[3] For the sake of readability here and in the rest of the paper we assume the following operator precedence when writing constraints for transition relations: existential quantifier > "and" operator > implication.

a property derives from the assumption of *maximal progress*: the possibility of performing internal actions prevents the execution of delays. The second requirement says that if a state can perform clock start events then it cannot perform clock termination events. Such a property derives from the assumption of *urgency of delays*: clock start events cannot be delayed but must be performed immediately, hence they prevent the execution of clock termination transitions. The third requirement checks that clock starting and termination transitions are consistent with the set of clocks that should be in execution in each state of the IGSMP. This is done by defining a function $\mathcal{S}$ which maps each state onto the expected set of clocks in execution, i.e. the set of clocks which have started but not terminated yet. In particular, in the initial state s_0 such a set is empty. The constraint a) defines the construction rule of the active clock set for each state reachable from s_0. In the case of a transition from a state s to a state s' labeled with an standard action, the active clocks of s' stem from the active clocks of s, as no clock can be terminated given that a standard action has been performed. If a transition from s to s' is labeled with a clock start event $\langle C_n^+, w\rangle$, then s' inherits the active clock set of s and adds to this set the started clock C_n. Finally, in the case of a transition from s to s' labeled with a clock termination event C_n^-, s' inherits the active clock set of s without such a terminated clock C_n. Constraints b) and c) concern the legality of the outgoing transitions of a state. In particular, the former says that a the name of a clock labeling a starting transition must be fresh (i.e. no clock with such a name must be currently in execution). The latter says that each state without τ and $\langle C_n^+, w\rangle$ outgoing transitions must have a $C_{n'}^-$ outgoing transition for each active clock $C_{n'}$. This definition preserves both the maximal progress and the urgency of delays assumptions and, in each state where it is possible, guarantees the possibility of terminating each delay that is still active. The fourth requirement of Definition 2.2 implements the following constraint over the structure of IGSMPs which makes their theory simpler. The unique role of clock start transitions in an IGSMP must be to lead to a timed state where the started clocks are actually executed, hence the execution of such transitions cannot cause new behaviors to be performable by the IGSMP. Such a constraint is satisfied by the semantic models of terms of the calculus of IGSMPs introduced in [6]. Formally, we require that the set of action transitions enabled after a clock start transition is a subset of (or equal to) the set of action transitions enabled before such a transition. This guarantees that no new behaviors can be introduced by clock start transitions because: (i) no new behavior beginning with a τ transition can be executable after a clock start transition (states enabling clock start transitions cannot enable τ transitions), and (ii) every potential behavior beginning with a transition a executable after a clock start transition can never be actually executed by hiding a, because before the clock start transition there is a potential behavior beginning with the same action a, which, when hidden, preempts the clock start (see the following Sect. 2.5 about the hiding of IGSMPs).

2.3 The Well-Named IGSMP Model

The model of well-named IGSMPs represents a canonical form for IGSMPs which introduces some constraints on clock names and makes it simple to develop an equivalence notion over IGSMPs which matches clocks with the same duration distribution. Well-named IGSMPs are exactly the class of semantic models obtained from the terms of the process algebra introduced in [6]. Here we will characterize well-named IGSMPs directly as a class of transition systems.

The constraint on the use of clock names in an IGSMP that we consider concerns the names k which are used for clocks when they start. As we already explained the name used for a starting clock must be fresh, i.e. no clock with such a name must be currently in execution. The requirement that we now add is that the new clock name which is used must depend from the duration distribution f associated with the starting clock and from the names of the clocks (with the same distribution f) already in execution, according to a fixed rule. In particular, we take the set of clock names to be defined by $\mathcal{C}Names = (PDF^+ \times \mathbb{N}^+)$, where "$f, i$" is a name for a clock with associated distribution f. The name "f, i" which is used for a starting clock must be such that i is the least $i \in \mathbb{N}^+$ which is not used in the name of any clock with the same distribution f already in execution. Note that, similarly as for standard ST models [1,7,11,15], using just duration distributions as clock names is not sufficient because indexes $i \in \mathbb{N}^+$ are needed in order to uniquely relate the clock termination event to the corresponding clock start event, even in the situation where several clocks with the same duration distribution are simultaneously executed (this is also observed in [8]).

Since in a well-named IGSMP names for clocks cannot be chosen arbitrarily and the clock names which are considered make it clear by themselves which is the duration distribution associated with a clock, with respect to IGSMTSs (Definition 2.2), in the definition of well-named IGSMTSs we omit set $\mathcal{C}$ and function D.

Definition 2.4 A well-named Interactive Generalized Semi-Markovian Transition System is a tuple $\mathcal{G} = (\Sigma, Act, T_+, T_-, T_a)$ where Σ and Act are defined as in Definition 2.2, while the definition of the transition relations T_+, T_- and T_a is obtained from that given in Definition 2.2 by substituting the constraint $b)$ of item 3 with:

$$b) \quad \exists C_{f,i}, w.\, s \xrightarrow{\langle C^+_{f,i}, w\rangle} \implies i = \min\{j \mid j \in \mathbb{N}^+,\, C_{f,j} \notin \mathcal{S}(s)\}$$

Note that the new version of constraint $b)$ guarantees that the name used for a starting clock is always fresh as required by the old version of constraint $b)$ (see Definition 2.2).

Definition 2.5 A well-named Interactive Generalized Semi-Markov Process is a tuple $\mathcal{G} = (\Sigma, Act, T_+, T_-, T_a, s_0)$, where $s_0 \in \Sigma$ is the initial state of the well-named IGSMP and $(\Sigma, Act, T_+, T_-, T_a)$ is a well-named IGSMTS such that function $\mathcal{S}$ in item 3 of Definition 2.2 also satisfies $\mathcal{S}(s_0) = \emptyset$.

As an important remark, we would like to point out that, since the rule expressed by constraint b) of Definition 2.5 reuses the indexes i of terminated clocks, each IGSMP with a finite set of states can be transformed into a well-named IGSMP with a finite set of states, by renaming clocks.

2.4 Parallel of Well-Named IGSMPs

Now, we address the problem of defining parallel composition à la CSP [19] of well-named IGSMPs, where the standard actions of a given set S are required to synchronize and the synchronization of two actions of type a is again an action of type a.

Intuitively, it should be clear that when composing in parallel two IGSMPs, a suitable renaming of the clocks is necessary in order to obtain a IGSMP, i.e. preserve the requirements on transition relations of Definition 2.3. Indeed composing in parallel two IGSMPs could lead to some conflict concerning the identification of the clocks of the composed model through names. More precisely, we have to cope with a name conflict whenever two clocks with the same name "f, i" are simultaneously in execution in both IGSMPs. In such a case the same name identifies two different clocks by compromising the relationship between the start and termination events of the two clocks. When considering well-named IGSMPs instead of just IGSMPs we have in addition the problem of preserving the rule for the name of starting clocks expressed by constraint b) of Definition 2.5.

The solution that we adopt consists in using l and r (left and right) as references to the two well-named IGSMPs $\mathcal{G}', \mathcal{G}''$ which are composed in parallel with $\mathcal{G}' \|_S \mathcal{G}''$ and relating each clock name locally used in $\mathcal{G}'$ (or $\mathcal{G}''$) to the well-named IGSMP $\mathcal{G}'$ (or $\mathcal{G}''$) through the reference l (or r). In this way C_{f,l_i} (C_{f,r_i}) denotes the clock $C_{f,i}$ executed by $\mathcal{G}'$ ($\mathcal{G}''$). In order to obtain a well-named IGSMP, when building the composed model, such "extended" names are renamed so that the rule for the name of starting clocks expressed by constraint b) of Definition 2.5 is satisfied. For instance, let us suppose that both $\mathcal{G}'$ and $\mathcal{G}''$ execute a clock with the same duration distribution f. For both well-named IGSMPs in isolation we represent such an event by activating the clock $C_{f,1}$. Somehow in the composed model we have to distinguish such clocks through names because they can be simultaneously in execution. Let us suppose that in $\mathcal{G}' \|_S \mathcal{G}''$ the first delay with distribution f that starts is the one executed by $\mathcal{G}'$. According to the well-naming rule in the composed model such a clock must get name "$f, 1$". Hence we map $C_{f,1}$ to the "extended" name of the clock $C_{f,1}$ executed by $\mathcal{G}'$, thus creating the following mapping:

$$C_{f,1} \longrightarrow C_{f,l_1}$$

denoting that the first clock with distribution f of the composed model $C_{f,1}$ corresponds to the first clock with distribution f of the lefthand well-named IGSMP. Then, if the second clock to be executed is the clock $C_{f,1}$ belonging to the righthand well-named IGSMP, in the composed model we create the fresh name "$f,2$" (according to the well-naming rule) and have in addition the following mapping:

$$C_{f,2} \longrightarrow C_{f,r_1}$$

In Table 1 we present an example of execution of a composed model $\mathcal{G}' \parallel_S \mathcal{G}''$ by showing how the mapping function (between the clock names of the composed model $\mathcal{G}' \parallel_S \mathcal{G}''$ and the corresponding clock names locally used in $\mathcal{G}'$ and $\mathcal{G}''$) for clocks with distribution f evolves.

Well-named IGSMPs	*Composed Model*	*Mapping Function*
$\mathcal{G}'$ *starts* $C_{f,1}$	$\mathcal{G}' \parallel_S \mathcal{G}''$ *starts* $C_{f,1}$	$C_{f,1} \longrightarrow C_{f,l_1}$
$\mathcal{G}''$ *starts* $C_{f,1}$	$\mathcal{G}' \parallel_S \mathcal{G}''$ *starts* $C_{f,2}$	$C_{f,1} \longrightarrow C_{f,l_1}$ $C_{f,2} \longrightarrow C_{f,r_1}$
$\mathcal{G}''$ *starts* $C_{f,2}$	$\mathcal{G}' \parallel_S \mathcal{G}''$ *starts* $C_{f,3}$	$C_{f,1} \longrightarrow C_{f,l_1}$ $C_{f,2} \longrightarrow C_{f,r_1}$ $C_{f,3} \longrightarrow C_{f,r_2}$
$\mathcal{G}''$ *ends* $C_{f,1}$	$\mathcal{G}' \parallel_S \mathcal{G}''$ *ends* $C_{f,2}$	$C_{f,1} \longrightarrow C_{f,l_1}$ $C_{f,3} \longrightarrow C_{f,r_2}$
$\mathcal{G}'$ *starts* $C_{f,2}$	$\mathcal{G}' \parallel_S \mathcal{G}''$ *starts* $C_{f,2}$	$C_{f,1} \longrightarrow C_{f,l_1}$ $C_{f,2} \longrightarrow C_{f,l_2}$ $C_{f,3} \longrightarrow C_{f,r_2}$

Table 1
Renaming of the clocks in $\mathcal{G}' \parallel_S \mathcal{G}''$

By following such a procedure, we build the composed model by dynamically storing all current mappings between the clock names of the composed model and the local clock names of the two well-named IGSMPs by employing a table (mapping function) for each distribution f. In general, when a clock C_{f_i} with distribution f is started by one of the two composed well-named IGSMPs, we do the following: (i) we choose the first index j for the distribution f which is unused in the composed model (by checking the table related to the duration probability distribution f), and we use the name "f,j" for the clock in the composed model; (ii) we add to the table related to distribution f the mapping $C_{f,j} \longrightarrow C_{f,l_i}$ if the clock is executed by the lefthand well-named

IGSMP or $C_{f,j} \longrightarrow C_{f,r_i}$ if the clock is executed by the righthand well-named IGSMP. When a clock C_{f_i} with distribution f is terminated by one of the two composed well-named IGSMPs, we do the following: (i) we establish the name "f, j" associated with the terminating clock in the composed model by checking the table related to distribution f (it must include $C_{f,j} \longrightarrow C_{f,l_i}$ if the clock is executed by the lefthand well-named IGSMP or $C_{f,j} \longrightarrow C_{f,r_i}$ if the clock is executed by the righthand well-named IGSMP); (ii) we remove from the table related to the duration probability distribution f the mapping for the name "f, j" of the composed model.

Now we formally define the parallel composition $\mathcal{G}_1 \parallel_S \mathcal{G}_2$ of two well-named IGSMPs $\mathcal{G}_1$ and $\mathcal{G}_2$, where the synchronization set S is a subset of $Act - \{\tau\}$.

We denote with $Loc = \{l, r\}$, ranged over by loc the set of locations, where l stands for left and r for right. We denote a mapping function, whose elements are pairs (j, loc_i), with $mapf$ which ranges over the set $MapF$ of partial bijections from $\mathbb{N}^+$ to $Loc \times \mathbb{N}^+$. Moreover, a global mapping M is a relation from PDF^+ to $\mathbb{N}^+ \times (Loc \times \mathbb{N}^+)$ such that $\forall f \in PDF^+ . M_f \in MapF$ [4], i.e. M is a global mapping including a mapping function for each different duration distribution. We denote the set of global mappings M by $\mathcal{M}$. In the following we use the shorthand $f : (j, loc_i)$ for $(f, (j, loc_i)) \in M$. Finally we make use of the auxiliary function $n : MapF \longrightarrow \mathbb{N}^+$ that computes the new index to be used for a clock name according to the well-naming rule, by choosing the minimum index not used by the other clocks with the same distribution already in execution, i.e. $n(mapf) = min\{k \mid k \notin dom(mapf)\}$.

Definition 2.6 The parallel composition $\mathcal{G}_1 \parallel_S \mathcal{G}_2$ of two well-named IGSMPs $\mathcal{G}_1 = (\Sigma_1, Act, T_{+,1}, T_{-,1}, T_{a,1}, s_{0,1})$ and $\mathcal{G}_2 = (\Sigma_2, Act, T_{+,2}, T_{-,2}, T_{a,2}, s_{0,2})$, with S being the synchronization set, is the tuple $(\Sigma, Act, T_+, T_-, T_a, (s_{0,1}, s_{0,2}, \emptyset))$ with

- $\Sigma = \Sigma_1 \times \Sigma_2 \times \mathcal{M}$ the set of states,
- $T_+ \subseteq (\Sigma \times \mathcal{C}^+ \times \Sigma)$, $T_- \subseteq (\Sigma \times \mathcal{C}^- \times \Sigma)$, and $T_a \subseteq (\Sigma \times Act \times \Sigma)$ are the least transition relations, such that $\forall (s_1, s_2, M) \in \Sigma$.

1_l $s_1 \xrightarrow{\alpha} s_1',\ \alpha \notin S \implies (s_1, s_2, M) \xrightarrow{\alpha} (s_1', s_2, M)$

2 $s_1 \xrightarrow{a} s_1' \wedge s_2 \xrightarrow{a} s_2',\ a \in S \implies$
$(s_1, s_2, M) \xrightarrow{a} (s_1', s_2', M)$

3_l $s_1 \xrightarrow{\langle C^+_{f,i}, w\rangle} s_1' \wedge s_2 \stackrel{\tau}{\not\longrightarrow} \implies$
$(s_1, s_2, M) \xrightarrow{\langle C^+_{f,n(M_f)}, w\rangle} (s_1', s_2, M \cup \{f : (n(M_f), l_i)\})$

4_l $s_1 \xrightarrow{C^-_{f,i}} s_1' \wedge s_2 \stackrel{\tau}{\not\longrightarrow} \wedge \not\exists C_{g,h}, w.\, s_2 \xrightarrow{\langle C^+_{g,h}, w\rangle} \wedge f : (j, l_i) \in M \implies$
$(s_1, s_2, M) \xrightarrow{C^-_{f,j}} (s_1', s_2, M - \{f : (j, l_i)\})$

[4] Given a relation M from A to B, we denote with M_a the set $\{b \in B \mid (a, b) \in M\}$.

and also the symmetric rules $\mathbf{1_r}, \mathbf{3_r}, \mathbf{4_r}$ referring to the local transitions of $\mathcal{G}_2$, which are obtained from the rules $\mathbf{1_l}, \mathbf{3_l}, \mathbf{4_l}$ by exchanging the roles of states s_1 (s_1') and s_2 (s_2') and by replacing l_i with r_i, hold true.

- $(s_{0,1}, s_{0,2}, \emptyset) \in \Sigma$ the initial state

Each state $s \in \Sigma$ of the composed model is represented by a triple including a pair of states ($s_1 \in \Sigma_1$ and $s_2 \in \Sigma_2$) and an auxiliary memory M containing all the mappings currently active in such a state. Rules **1** (**2**) describe the behavior of the composed model in the case of a standard action α performed by one (or both, via a synchronization) well-named IGSMPs, when $\alpha \notin S$ ($\alpha \in S$). Rules **3** and **4** define the behavior of the composed model in the case of delays locally performed by components. When in $\mathcal{G}_1$ ($\mathcal{G}_2$) occurs a transition labeled with $\langle C^+_{f,i}, w\rangle$, denoting the beginning of a delay with duration distribution f, then the new index $n(M_f)$ is determined for identifying the action at the level of the composed model, and the new mapping $f : (n(M_f), l_i)$ ($f : (n(M_f), r_i)$) is added to M. Conversely, when in $\mathcal{G}_1$ ($\mathcal{G}_2$) occurs a transition labeled with $C^-_{f,i}$, denoting the termination of a clock with duration distribution f, the particular clock with index j associated to l_i (r_i) in M_f terminates at the level of the composed model, and the index j becomes available. Note that the negative clauses in the premises enforce the maximal progress and the urgency of delays assumptions.

Theorem 2.7 *Let $\mathcal{G}_1$ and $\mathcal{G}_2$ be two well-named IGSMPs. Then for each $S \subseteq Act - \{\tau\}$, $\mathcal{G}_1 \,\|_S\, \mathcal{G}_2$ is a well-named IGSMP.*

2.5 Hiding of Well-Named IGSMPs

Now, we address the problem of defining hiding of well-named IGSMPs, where the standard actions of a given set L are turned into invisible τ actions.

As we already explained, the capability of hiding actions make it possible to turn visible "incomplete" actions into invisible "complete" ones, thus giving the possibility of building a complete system from several system components. In particular while a visible action transition (as long as it is enabled) can delay indefinitely before being performed, when such an action is turned into an invisible action it must be executed in zero time.

Now we formally define the hiding $\mathcal{G}/L$ of a well-named IGSMP $\mathcal{G}$, where the set L of the visible actions to be hidden is a subset of $Act - \{\tau\}$.

Definition 2.8 The hiding $\mathcal{G}/L$ of a well-named IGSMP $\mathcal{G} = (\Sigma, Act, T_{+,1}, T_{-,1}, T_{a,1}, s_0)$ with L being the set of visible actions to be hidden is the tuple $(\Sigma, Act, T_+, T_-, T_a, s_0)$ where $T_+ \subseteq (\Sigma \times \mathcal{C}^+ \times \Sigma)$, $T_- \subseteq (\Sigma \times \mathcal{C}^- \times \Sigma)$, and $T_a \subseteq (\Sigma \times Act \times \Sigma)$ are the least set of transitions, such that $\forall s \in \Sigma$. [5]

[5] In order to distinguish transition of $T_{+,1}$, $T_{-,1}$ and $T_{a,1}$ from transitions of T_+, T_- and T_a we denote the former with "$\longrightarrow_1$" and the latter simply with "$\longrightarrow$".

$\mathbf{1}\ s \xrightarrow{\alpha}_1 s',\ \alpha \notin L \implies s \xrightarrow{\alpha} s'$

$\mathbf{2}\ s \xrightarrow{a}_1 s',\ a \in L \implies s \xrightarrow{\tau} s'$

$\mathbf{3}\ s \xrightarrow{\theta}_1 s' \wedge\ \nexists a \in L.\, s \xrightarrow{a}_1 \implies s \xrightarrow{\theta} s'$

Rules **1** and **2** are standard. Rule **3** says that the effect of the hiding operator over states of $\mathcal{G}$ which enable standard actions in L is to preempt all clock related transitions according to the maximal progress assumption.

Theorem 2.9 *Let $\mathcal{G}$ be a well-named IGSMP. Then for each $L \subseteq Act - \{\tau\}$, $\mathcal{G}/L$ is a well-named IGSMP.*

2.6 Equivalence of Well-Named IGSMPs

Now we will recall the notion of weak probabilistic bisimulation over IGSMPs which has been introduced in [6]. In particular weak bisimulation matches the execution of clocks with the same duration distribution similarly as in the dynamic approach of [7], deals with probabilistic choices similarly as in [20], and abstracts from standard τ actions similarly as in [22]. Such an equivalence is shown in [6] to be a congruence with respect to both parallel composition and hiding.

In our context we express cumulative probabilities by aggregating weights.

Definition 2.10 Let $\mathcal{G} = (\Sigma, Act, T_+, T_-, T_a)$ be a well-named IGSMTS.The function $TW : \Sigma \times PDF^+ \times \mathcal{P}(\Sigma) \longrightarrow \mathbb{R}^+ \cup \{0\}$, which computes the aggregated weight that a state $s \in \Sigma$ reaches a set of states $I \in \mathcal{P}(\Sigma)$ by starting a delay with duration distribution $f \in PDF^+$ is defined as: [6]

$$TW(s, f, I) = \sum \{\!|\, w \mid \exists i \in \mathbb{N}^+, s' \in I.\ s \xrightarrow{\langle C^+_{f,i}, w\rangle} s' \,|\!\}$$

Let $NPAct = Act \cup \mathcal{C}^-$, the set of non-probabilistic actions, be ranged over by σ. Let $\stackrel{\sigma}{\Longrightarrow}$ denote $(\xrightarrow{\tau})^* \xrightarrow{\sigma} (\xrightarrow{\tau})^*$, i.e. a sequence of transitions including a single σ transition and any number of τ transitions. Moreover, we define $\stackrel{\hat{\sigma}}{\Longrightarrow}\ =\ \stackrel{\sigma}{\Longrightarrow}$ if $\sigma \neq \tau$ and $\stackrel{\hat{\tau}}{\Longrightarrow}\ = (\xrightarrow{\tau})^*$, i.e. a possibly empty sequence of τ transitions.

Definition 2.11 Let $\mathcal{G} = (\Sigma, Act, T_+, T_-, T_a)$ be a well-named IGSMTS. An equivalence relation β on Σ is a *weak bisimulation* iff $s_1\ \beta\ s_2$ implies

- for every $\sigma \in NPAct$ and $s'_1 \in \Sigma$,

$$s_1 \xrightarrow{\sigma} s'_1 \text{ implies } s_2 \stackrel{\hat{\sigma}}{\Longrightarrow} s'_2 \text{ for some } s'_2 \text{ with } s'_1\ \beta\ s'_2,$$

[6] We use $\{\!|$ and $|\!\}$ to denote multiset parentheses. The summation of an empty multiset is assumed to yield 0. Since the method for computing the new index of a delay f that starts in a state P is fixed, we have that several transitions f^+ leaving P have all the same index i.

- $s_2 \overset{\hat{\tau}}{\Longrightarrow} s_2'$ for some s_2' such that, for every $f \in PDF^+$ and equivalence class I of β,
$$TW(s_1, f, I) = TW(s_2', f, I)$$

Two states s_1 and s_2 are weakly bisimilar, denoted by $s_1 \approx s_2$, iff (s_1, s_2) is included in some weak bisimulation. Two well-named IGSMPs $(\mathcal{G}_1, s_{0,1})$ and $(\mathcal{G}_2, s_{0,2})$ are weakly bisimilar, if their initial states $s_{0,1}$ and $s_{0,2}$ are weakly bisimilar in the well-named IGSMTS obtained with the disjoint union of $\mathcal{G}_1$ and $\mathcal{G}_2$.

3 Interactive Stochastic Timed Transition Systems

In this section we introduce Interactive Stochastic Timed Transition Systems (ISTTSs) that will be used in the next section to define a semantics for IGSMPs. We first briefly introduce some basic notions about probability spaces.

3.1 Probability Spaces

In this section we recall some basic notions related to measure theory and we introduce some notation that will be used in the rest of the paper.

Definition 3.1 A *σ-algebra* on a set Ω, denoted by $\mathcal{F}$, is a family of subsets of Ω that contains Ω and is closed under complementation and countable union. The elements of a σ-algebra $\mathcal{F}$ are called *measurable sets*. The pair $(\Omega, \mathcal{F})$ is called a *measurable space*.

Definition 3.2 The *Borel σ-algebra* on a set Ω with a topology, denoted by $\mathcal{B}(\Omega)$, is defined to be the *σ-algebra* generated by the open subsets (or equivalently, by the closed subsets) of Ω.

Definition 3.3 A *finite measure* μ on a measurable space $(\Omega, \mathcal{F})$ is a function that assigns a non-negative real value to each element of $\mathcal{F}$, such that $\mu(\emptyset) = 0$ and, supposed $\{C_i\}_{i \in I}$, with $I \subseteq \mathbb{N}$, to be a family of disjoint elements of $\mathcal{F}$, $\mu(\cup_{i \in I} C_i) = \sum_{i \in I} \mu(C_i)$. The triple $(\Omega, \mathcal{F}, \mu)$ is called a *measure space*. If we have in addition that $\mu(\Omega) = 1$, then the triple $(\Omega, \mathcal{F}, \mu)$ is also called a *probability space*.

We now define some operations over measure spaces and probability spaces.

Definition 3.4 Let $(\Omega, \mathcal{F}, \mu)$ be a measure space and let f be a function defined on Ω, then $f(\Omega, \mathcal{F}, \mu)$ denotes the triple $(f(\Omega), \{C \subseteq f(\Omega) \mid f^{-1}(C) \in \mathcal{F}\}, \mu')$, where $\forall C \subseteq f(\Omega).\ \mu'(C) = \mu(f^{-1}(C))$.

It is easy to verify that, since $(\Omega, \mathcal{F}, \mu)$ is a measure space, $f(\Omega, \mathcal{F}, \mu)$ is a measure space as well. Such a measure space is called the measure space *induced* by f from $(\Omega, \mathcal{F}, \mu)$. Moreover if $(\Omega, \mathcal{F}, \mu)$ is a probability space, then $f(\Omega, \mathcal{F}, \mu)$ is a probability space as well.

Definition 3.5 Let $(\Omega, \mathcal{F}, \mu)$ be a measure space and let p be a positive real number, then $p \cdot (\Omega, \mathcal{F}, \mu)$ denotes the triple $(\Omega, \mathcal{F}, \mu')$, where $\forall C \subseteq \Omega.\ \mu'(C) = p \cdot \mu(C)$.

It is easy to verify that, since $(\Omega, \mathcal{F}, \mu)$ is a measure space, $p \cdot (\Omega, \mathcal{F}, \mu)$ is a measure space as well.

Definition 3.6 Let $(\Omega', \mathcal{F}', \mu')$ and $(\Omega'', \mathcal{F}'', \mu'')$ be two measure spaces, then $(\Omega', \mathcal{F}', \mu') + (\Omega'', \mathcal{F}'', \mu'')$ denotes the triple $(\Omega' \cup \Omega'', \{C \subseteq \Omega' \cup \Omega'' \mid C \cap \Omega' \in \mathcal{F}' \wedge C \cap \Omega'' \in \mathcal{F}''\}, \mu)$, where $\forall C \subseteq \Omega' \cup \Omega''.\ \mu(C) = \mu'(C \cap \Omega') + \mu''(C \cap \Omega'')$.

It is easy to verify that, since $(\Omega', \mathcal{F}', \mu')$ and $(\Omega'', \mathcal{F}'', \mu'')$ are measure spaces, $(\Omega', \mathcal{F}', \mu') + (\Omega'', \mathcal{F}'', \mu'')$ is a measure space as well. Moreover, considered a set of probability spaces $\{(\Omega_i, \mathcal{F}_i, \mu_i)\}_{i \in I}$, with $I \subseteq \mathbb{N}$ finite index set, and a set $\{p_i\}_{i \in I}$ of positive real numbers such that $\sum_{i \in I} p_i = 1$, we have that $\sum_{i \in I} p_i \cdot (\Omega_i, \mathcal{F}_i, \mu_i)$ is a probability space.

Definition 3.7 Let $(\Omega', \mathcal{F}', \mu')$ and $(\Omega'', \mathcal{F}'', \mu'')$ be two measure spaces, then $(\Omega', \mathcal{F}', \mu') \cdot (\Omega'', \mathcal{F}'', \mu'')$ denotes the triple $(\Omega' \times \Omega'', \{C' \times C'' \mid C' \in \mathcal{F}' \wedge C'' \in \mathcal{F}''\}, \mu')$, where $\forall C' \subseteq \Omega', C'' \subseteq \Omega''.\ \mu'(C' \times C'') = \mu'(C') \cdot \mu''(C'')$.

It is easy to verify that, since $(\Omega', \mathcal{F}', \mu')$ and $(\Omega'', \mathcal{F}'', \mu'')$ are measure spaces, $(\Omega', \mathcal{F}', \mu') \cdot (\Omega'', \mathcal{F}'', \mu'')$ is a measure space as well. Moreover, if $(\Omega, \mathcal{F}, \mu)$ is a probability space, then $(\Omega', \mathcal{F}', \mu') \cdot (\Omega'', \mathcal{F}'', \mu'')$ is a probability space as well.

We now show that a probability distribution function on real numbers defines a unique probability space over the Borel σ-algebra of real numbers.

Theorem 3.8 *Let $F \in PDF$ be a probability distribution function on $\mathbb{R}$. There is a unique probability measure P on $\mathcal{B}(\mathbb{R})$ such that $\forall a, b \in \mathbb{R}, a < b.\ P(\,(a, b]\,) = F(b) - F(a)$.*

Finally, we present a notion of equivalence over measure spaces which relates measure spaces with different domains by assuming that they assign measure 0 to the every set of elements not included in their domain.

Definition 3.9 Let $(\Omega', \mathcal{F}', \mu')$ and $(\Omega'', \mathcal{F}'', \mu'')$ be measure spaces. We say that $(\Omega', \mathcal{F}', \mu')$ is equivalent to $(\Omega'', \mathcal{F}'', \mu'')$, written $(\Omega', \mathcal{F}', \mu') \approx (\Omega'', \mathcal{F}'', \mu'')$, if $\forall C' \in \mathcal{F}'.\ C' \cap \Omega'' \in \mathcal{F}'' \wedge \mu''(C' \cap \Omega'') = \mu'(C')$ and $\forall C'' \in \mathcal{F}''.\ C'' \cap \Omega' \in \mathcal{F}' \wedge \mu'(C'' \cap \Omega') = \mu''(C'')$.

Note that the definition above implies that if $(\Omega', \mathcal{F}', \mu') \approx (\Omega'', \mathcal{F}'', \mu'')$ then both $\Omega' - \Omega'' \in \mathcal{F}'$ with $\mu'(\Omega' - \Omega'') = 0$ and $\Omega'' - \Omega' \in \mathcal{F}''$ with $\mu''(\Omega'' - \Omega') = 0$.

3.2 The ISTTS Model

In this section we formally introduce Interactive Stochastic Timed Transition Systems (ISTTS) which include three type of transitions: *standard action transitions*, representing the interactive behavior of a system component, *probabilistic transitions* (expressed by means of probability spaces) representing (infinitely branching) probabilistic choices and *numeric time transitions* representing a fixed temporal delay.

As far as standard actions are concerned they have exactly the same behavior as in IGSMPs. In ISTTS non-deterministic choices can arise not only from transitions labeled with standard visible actions (like in IGSMPs), but also from transitions representing the passage of time. As usual in the real time literature (see e.g. [23]), several timed transition leaving a state offer the possibility to the observer to choose the amount of time after which he wants to observe the status of the system.

In ISTTS we have two different kinds of state:

- *silent states* which are exactly like in IGSMPs.
- *probabilistic states* enabling probabilistic transitions, expressed by a probability space PS, and (possibly) visible action transitions a only. In such states the ISTTS just chooses a new state in zero time according to the probability space and may potentially interact with the environment through one of its visible actions (see e.g. Fig. 2.a).
- *timed states* enabling numeric timed transitions t and (possibly) visible action transitions a only. In such states the ISTTS just performs a non-deterministic choice among the numeric timed transitions (which cause the amount of time labeling the transition to pass) and may potentially interact with the environment through one of its visible actions (see e.g. Fig. 2.b).

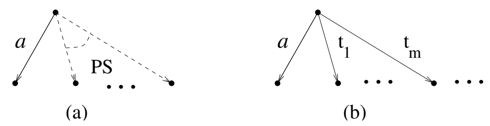

Fig. 2. Some examples of possible states of an ISTTS

In the following we present the formal definition of Interactive Stochastic Timed Transition System (ISTTS), then we will define Rooted Interactive Stochastic Timed Transition Systems as ISTTSs possessing an initial state. Formally, given a time domain $TD \subseteq \mathbb{R}^+ \cup \{0\}$, we use $t, t', \ldots$, representing time values, to range over TD.

Definition 3.10 An Interactive Stochastic Timed Transition System (ISTTS) is a tuple $\mathcal{D} = (\Sigma, TD, Act, P, T_t, T_a)$ with

- Σ a set of possibly infinite states,
- TD a time domain, i.e. the set of possible values over which the labels of the numeric timed transitions range,

- Act a set of standard actions,
- $P : \Sigma' \rightarrow PS(\Sigma - \Sigma')$, where $\Sigma' \subset \Sigma$ and $PS(\Sigma'')$ denotes the family of probability spaces $(\Sigma''', \mathcal{F}, \mu)$ over sets of states $\Sigma''' \subseteq \Sigma''$, the probabilistic transition relation which associates a probability space with some of the states of the ISTTS; and $T_t \subseteq (\Sigma \times TD \times \Sigma)$ and $T_a \subseteq (\Sigma \times Act \times \Sigma)$ two transition relations representing time passage and action execution, respectively. P, T_t and T_a must be such that $\forall s \in \Sigma$.
  - $s \xrightarrow{\tau} \implies s \notin dom(P) \wedge \nexists t. s \xrightarrow{t}$
  - $s \in dom(P) \implies \nexists t. s \xrightarrow{t}$
  - $s \xrightarrow{\tau} \vee \exists t. s \xrightarrow{t} \vee s \in dom(P)$

Definition 3.11 A Rooted Interactive Stochastic Timed Transition System (RISTTS) is a tuple $\mathcal{D} = (\Sigma, TD, Act, P, T_t, T_a, s_0)$, where $s_0 \in \Sigma$ is the initial state and $(\Sigma, TD, Act, P, T_t, T_a)$ is an ISTTS.

The meaning the constraints over transition relations is the following. The first requirement says that (similarly as in IGSMPs) if a state that can perform internal τ actions then it cannot perform neither probabilistic transitions nor timed transitions (*maximal progress* assumption). The second requirement says that (similarly as in IGSMPs) if a state that can perform probabilistic transitions then it cannot perform timed transitions (*urgency of choices* assumption). The third requirement says that (similarly as in IGSMPs) we cannot have states where time is not allowed to pass (time deadlocks).

3.3 Parallel of Rooted ISTTSs

Now we define, similarly as for IGSMPs, the parallel composition à la CSP of RISTTSs.

In such a parallel composition the discrete timed transitions of the composed RISTTSs are constrained to synchronize, so that the same amount of time passes for both systems, i.e. when time advances for one RISTTS it must also advance for the other RISTTS.

Definition 3.12 The parallel composition $\mathcal{D}_1 \,\|_S\, \mathcal{D}_2$ of two RISTTSs $\mathcal{D}_1 = (\Sigma_1, TD, Act, P_1, T_{t,1}, T_{a,1}, s_{0,1})$ and $\mathcal{D}_2 = (\Sigma_2, TD, Act, P_2, T_{t,2}, T_{a,2}, s_{0,2})$, with $S \subset Act - \{\tau\}$ being the synchronization set, is the tuple $(\Sigma, TD, Act, P, T_t, T_a, (s_{0,1}, s_{0,2}))$ with:

- $\Sigma = \Sigma_1 \times \Sigma_2$ the set of states
- P the partial function defined over $\Sigma_1 \times \Sigma_2$ obtained from P_1 and P_2 as follows: $\forall s_1 \in \Sigma_1, s_2 \in \Sigma_2$.

$$\begin{array}{ll} P(s_1,s_2) = Id^1_{s_2}(P_1(s_1)) & \text{if } s_1 \in dom(P_1) \wedge s_2 \xrightarrow{t} \\ P(s_1,s_2) = Id^2_{s_1}(P_2(s_2)) & \text{if } s_2 \in dom(P_2) \wedge s_1 \xrightarrow{t} \\ P(s_1,s_2) = P(s_1)\cdot P(s_2) & \text{if } s_1 \in dom(P_1) \wedge s_2 \in dom(P_2) \\ P(s_1,s_2) \text{ is not defined} & \text{otherwise} \end{array}$$

with $Id^1_{s_2} : \Sigma_1 \longrightarrow (\Sigma_1 \times \{s_2\})$ defined by $\forall s \in \Sigma_1 . Id_{s_2}(s) = (s, s_2)$ and $Id^2_{s_1} : \Sigma_2 \longrightarrow (\{s_1\} \times \Sigma_2)$ defined by $\forall s \in \Sigma_2 . Id_{s_1}(s) = (s_1, s)$.

- $T_t \subseteq (\Sigma \times TD \times \Sigma)$ and $T_a \subseteq (\Sigma \times Act \times \Sigma)$ the least transition relations, such that

  $\mathbf{1_l}$ $s_1 \xrightarrow{\alpha} s'_1,\ \alpha \notin S \implies (s_1,s_2) \xrightarrow{\alpha} (s'_1,s_2)$

  $\mathbf{1_r}$ $s_2 \xrightarrow{\alpha} s'_2,\ \alpha \notin S \implies (s_1,s_2) \xrightarrow{\alpha} (s_1,s'_2)$

  2 $s_1 \xrightarrow{a} s'_1 \wedge s_2 \xrightarrow{a} s'_2,\ a \in S \implies (s_1,s_2) \xrightarrow{a} (s'_1,s'_2)$

  3 $s_1 \xrightarrow{t} s'_1 \wedge s_2 \xrightarrow{t} s'_2 \implies (s_1,s_2) \xrightarrow{t} (s'_1,s'_2)$

- $(s_{0,1}, s_{0,2}) \in \Sigma$ the initial state.

When evaluating the probability spaces associated by function P to the states of the composed model we make use of induced probability spaces (see Definition 3.4) and we enforce the maximal progress assumption. Moreover we produce a single "global" probability space whenever both RISTTSs engage in probabilistic choices (we assume that choices are performed independently). When evaluating action transitions we just make use of standard rules. Finally we require timed transitions to synchronize.

Theorem 3.13 *Let $\mathcal{D}_1$ and $\mathcal{D}_2$ be two RISTTSs. Then for each $S \subseteq Act - \{\tau\}$, $\mathcal{D}_1 \,\|_S\, \mathcal{D}_2$ is a RISTTS.*

3.4 Hiding of Rooted ISTTSs

Now we define, similarly as for IGSMPs, the hiding of RISTTSs.

Definition 3.14 The hiding $\mathcal{D}/L$ of a RISTTS $\mathcal{D}_1 = (\Sigma, TD, Act, P_1, T_{t1}, T_{a1}, s_0)$, with $L \subset Act - \{\tau\}$ being the set of visible actions to be hidden, is the tuple $(\Sigma, TD, Act, P, T_t, T_a, s_0)$, with:

- P the partial function obtained from P_1 by removing from its domain those states (and the associated probability spaces) which enable at least one transition labeled with an action in L
- $T_t \subseteq (\Sigma \times TD \times \Sigma)$ and $T_a \subseteq (\Sigma \times Act \times \Sigma)$ the least transition relations, such that $\forall s \in \Sigma$. [7]

  1 $s \xrightarrow{\alpha}_1 s',\ \alpha \notin L \implies s \xrightarrow{\alpha} s'$

  2 $s \xrightarrow{a}_1 s',\ a \in L \implies s \xrightarrow{\tau} s'$

[7] In order to distinguish transition of $T_{w,1}$, $T_{t,1}$ and $T_{a,1}$ from transitions of T_w, T_t and T_a we denote the former with "$\longrightarrow_1$" and the latter simply with "$\longrightarrow$".

3 $s \xrightarrow{t}_1 \wedge \;\not\exists a \in L.\, s \xrightarrow{a}_1 \implies s \xrightarrow{t}$

Similarly as for IGSMPs, in the definition of the hiding operator in addition to standard rules we make use of rules which enforce the maximal progress assumption.

Theorem 3.15 *Let $\mathcal{D}$ be a RISTTS. Then for each $L \subseteq Act - \{\tau\}$, $\mathcal{D}/L$ is a RISTTS.*

3.5 Equivalence of Rooted ISTTSs

Now we introduce a notion of weak bisimulation for RISTTSs which constitutes an extension of the approach of [20] to probability spaces and abstracts from standard τ actions similarly as in [22].

Given an equivalence relation β on a set Σ and a set $I \subseteq \Sigma$, we first define the function $EC_{I,\beta} : I \to \Sigma/\beta$ which maps each state $s \in I$ into the corresponding equivalence class $[s]_\beta$ in Σ.

Definition 3.16 Let $\mathcal{D} = (\Sigma, TD, Act, P, T_t, T_a)$ be an ISTTS. An equivalence relation β on Σ is a *weak bisimulation* iff $s_1 \; \beta \; s_2$ implies

- for every $\alpha \in Act$,
  $$s_1 \xrightarrow{\alpha} s_1' \text{ implies } s_2 \stackrel{\hat{\alpha}}{\Longrightarrow} s_2' \text{ for some } s_2' \text{ with } s_1' \; \beta \; s_2',$$
- for every $t \in TD$,
  $$s_1 \xrightarrow{t} s_1' \text{ implies } s_2 \xrightarrow{t} s_2' \text{ for some } s_2' \text{ with } s_1' \; \beta \; s_2',$$
- $s_2 \stackrel{\hat{\tau}}{\Longrightarrow} s_2'$ for some s_2' such that, denoted $P(s_1) = (\Sigma_1, \mathcal{F}_1, \mu_1)$ and $P(s_2') = (\Sigma_2, \mathcal{F}_2, \mu_2)$, we have that $EC_{\Sigma_1,\beta}(P(s_1)) \approx EC_{\Sigma_2,\beta}(P(s_2'))$

Two states s_1 and s_2 are weakly bisimilar, denoted by $s_1 \approx s_2$, iff (s_1, s_2) is included in some weak bisimulation. Two RISTTSs $(\mathcal{D}_1, s_{0,1})$ and $(\mathcal{D}_2, s_{0,2})$ are weakly bisimilar, if their initial states $s_{0,1}$ and $s_{0,2}$ are weakly bisimilar in the ISTTS obtained with the disjoint union of $\mathcal{D}_1$ and $\mathcal{D}_2$.

In the last item we exploit induced probability spaces (see Definition 3.4) and equivalence between probability spaces (see Definition 3.9) to check that states s_1 and s_2' have the same aggregated probability to reach the same equivalence classes.

4 A Semantics for Interactive Generalized Semi-Markov Processes

In this section we present a semantics for well-named Interactive Generalized Semi-Markov Processes which maps them onto Interactive Stochastic Timed Transition Systems. Such a semantics explicitely represents the passage of time by means of transitions labeled with numeric time delays and turns probability distributions of durations into infinitely branching probabilistic choices which lead to states performing numeric time delays with a different duration. In particular, differently from [14] where a technique based on *residual lifetimes of clocks* is used, the states of the semantics of an Interactive Generalized Semi-Markov Process encode the *spent lifetimes of clocks*. This means that, in a timed state of the IGSMP where several clocks $C_{n_1} \dots C_{n_k}$ are in execution, the time delay originated by a clock C_{n_i} is determined according to its residual distribution of duration which is evaluated from (i) its associated duration distribution and (ii) its spent lifetime. Once we have sampled a time value t_i from the residual duration distribution of each clock C_{n_i}, we just take the minimum $t_{\min}$ of the sampled values and we consider the clock $C_{n_{\min}}$ which sampled such a time value. Such a "winning clock" is the clock that terminates in the timed state of the IGSMP. After this event the other clocks (which are still in execution) carry over their spent lifetimes, which now is given by $t'_i = t_i + t_{\min}$. Since, according to this approach, the residual duration of a clock is re-sampled in each IGSMP state until it terminates, an adversary (or scheduler) which resolves non-deterministic choices in an IGSMP cannot gain information about the future behavior of the system on which to base its decisions.

Example 4.1 Let us consider the IGSMP depicted in Fig. 3, where three temporal delays are started by activating three clocks C_{n_1}, C_{n_2}, and C_{n_3}. In particular, we concentrate on the case in which C_{n_2} is the first clock to terminate.

In Fig. 4 we show the semantics of the IGSMP of Fig. 3 obtained by following an approach similar to that of [14], which encodes in each state the *residual lifetimes of clocks*. Each state is enriched with the set of active clocks together with their residual lifetimes. In state $\langle s_0, \emptyset \rangle$ (where no clock is active) three numeric time delays t_1, t_2, and t_3 are sampled and associated with the lifetime of the clocks C_{n_1}, C_{n_2}, and C_{n_3}, respectively. Depending on which is the clock $C_{n_{\min}}$ sampling the minimum time value t_{min} in state $\langle s_0, \emptyset \rangle$, we move to one of three different classes of states, one for each possible winning clock. Afterwards, a temporal transition labeled with a numeric time value t between 0 and t_{min} is taken, and each residual duration is accordingly modified by subtracting t_{min} from the residual lifetime of each clock. For the sake of readability in Fig. 4 we just depict one trace leading from s_0 to a state s_1 which belongs to the class of states for which C_{n_2} is the winning clock (i.e. t_2 is t_{min}), and then from s_1 to the state s_2 via the transition labeled with the time value t_2, so that in s_2 the clock C_{n_2} is terminated. In state s_2 the residual lifetimes of the remaining active clocks C_{n_1} and C_{n_3} are $t_1 - t_{min}$ and $t_3 - t_{min}$ respectively. By exploiting this information an adversary may already know which clock between C_{n_1} and C_{n_3} will terminate first and consequently guide the nondeterministic choice in state s_2.

In Fig. 5 we show the semantics of the IGSMP of Fig. 3 obtained by

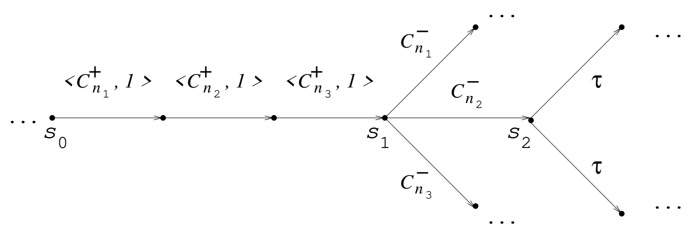

Fig. 3. Example of an IGSMP

following the approach that we adopt in this paper, which is based on the *spent lifetimes of clocks*. Each state is enriched with: (i) the set of active clocks together with their spent lifetimes, and (ii) a pair $C_n : t$ containing the time value sampled by the winning clock in a timed state of the IGSMP and the clock name. The latter field is set to "$-$" whenever the IGSMP is not in a timed state. The sampling executed in state $\langle s_0, \emptyset, - \rangle$ leads to a state where the three starting clocks are associated with the spent lifetime 0 (because the corresponding transition does not represent a passage of time but simply the result of the sampling), and the winning clock C_n and its sampled value are reported too. As in the case of Fig. 4, in Fig. 5 we just report one trace leading from s_0 to a state s_1 which belongs to the class of states for which C_{n_2} is the winning clock (i.e. C_{n_2} is $C_{n_{min}}$ and t_2 is its sampled value), and then from s_1 to the state s_2 via the transition labeled with the value t_2, so that in s_2 the clock C_{n_2} is terminated. In state s_2 the spent lifetimes of the remaining active clocks C_{n_1} and C_{n_3} are both equal to t_2, and their residual durations depend on both such a value and the duration distribution associated with the clocks. Since, according to this approach, the time to termination of clocks C_{n_1} and C_{n_3} is re-sampled, an adversary cannot gain in advance any information about the future behavior of the system and he cannot exploit this information when resolving the nondeterministic choice in state s_2.

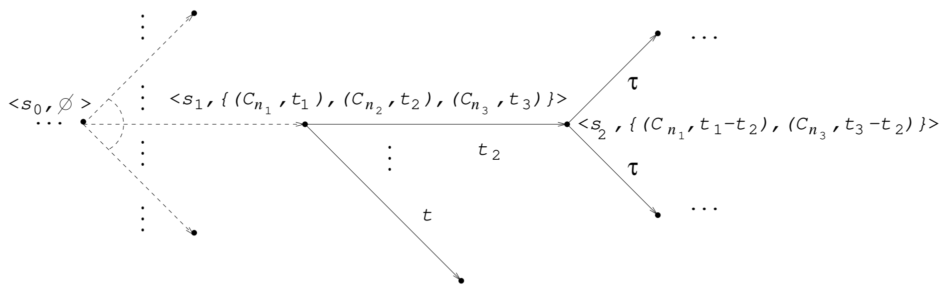

Fig. 4. Example of semantics based on residual lifetimes

In the following we introduce some preliminary definitions which are needed to define the semantics of IGSMPs.

Definition 4.2 Given a duration probability distribution $f \in PDF^+$ and a time value $t \in \mathbb{R}^+ \cup \{0\}$, we denote by $[f \mid t]$ the residual duration distribution of a clock C_n with duration distribution f which, after t time units from when it started, has not terminated yet (t is its spent lifetime). More formally, if T

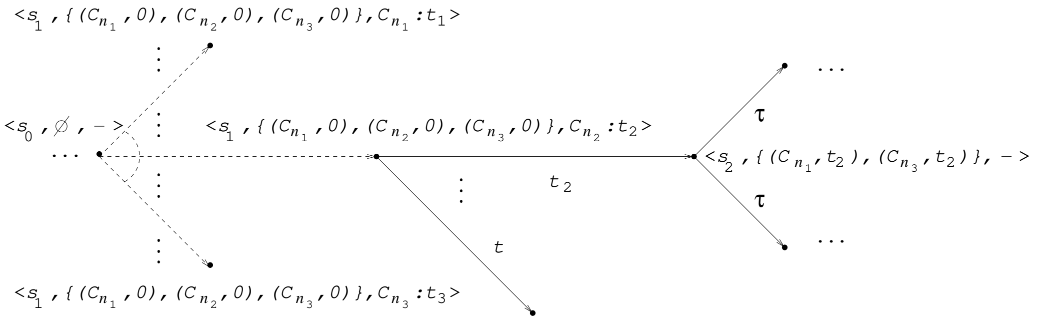

Fig. 5. Example of semantics based on spent lifetimes

is a random variable with distribution f, i.e. $\forall t' \in \mathbb{R}.\ f(t') = P(T \leq t')$, then $[f \mid t]$ is the probability distribution defined as follows. For all $t' \in \mathbb{R}$ we have that:

$$[f \mid t](t') = P(T \leq t' + t \mid T > t)$$

Theorem 4.3 *Given $f \in PDF^+$ and $t \in \mathbb{R}^+ \cup \{0\}$, we have that for all $t' \in \mathbb{R}^+ \cup \{0\}$:*

$$[f \mid t](t') = \frac{f(t+t') - f(t)}{1 - f(t)}$$

Consider a family of probability distribution functions $f_1, \ldots, f_k \in PDF$. We denote by $\mathcal{R}(f_1, \ldots, f_k)$ the probability space $\prod_{i=1\ldots k}(\mathbb{R}, \mathcal{B}(\mathbb{R}), P_i)$, where P_i is the unique probability measure on $\mathcal{B}(\mathbb{R})$ obtained from f_i (see Theorem 3.8).

Definition 4.4 Let the residual duration distribution of the set of clocks $C_{n_1}, \ldots, C_{n_k}$ in execution in an IGSMP state be $f_1, \ldots, f_k$, i.e. the probability that a certain tuple of residual durations $(t_1, \ldots, t_k)$ is sampled from the clocks is described by the probability space $\mathcal{R}(f_1, \ldots, f_k)$. For each $I \subseteq \{1, \ldots, k\}$ such that $|I| \geq 2$, the event $Term(I)$ of contemporaneous termination of the clocks $\{C_{n_i} \mid i \in I\}$ in execution is the following measurable subset of the sample space $\mathbb{R}^k$:

$$Term(I) = \{(t_1, \ldots, t_k) \mid \exists t.\ (\forall i \in I.\ t_i = t) \wedge (\forall i \notin I.\ t_i > t\}$$

Since in an IGSMP clocks in execution in a state cannot terminate at the same time instant (see Sect. 2.1) we have that each event $Term(I)$ of contemporaneous termination of a subset $\{C_{n_i} \mid i \in I\}$ of the clocks in execution $C_{n_1}, \ldots, C_{n_k}$ occurs with probability 0. More formally, we have that in each state of an IGSMP, if $(\mathbb{R}^k, \mathcal{F}, P)$ is the probability space $\mathcal{R}(f_1, \ldots, f_k)$ expressing the residual duration of the clocks $C_{n_1}, \ldots, C_{n_k}$ in execution in the state, for each $I \subseteq \{1, \ldots, k\}$ such that $|I| \geq 2$, we have $P(Term(I)) = 0$. We exploit this fact in order to reduce the domain of the probability space for a set of active clocks. In particular instead of considering the entire $\mathcal{R}(f_1, \ldots, f_k)$ we can just restrict to consider $\breve{\mathcal{R}}(f_1, \ldots, f_k)$ defined as follows.

Definition 4.5 $\breve{\mathcal{R}}(f_1, \ldots, f_k)$ is the triple $(\breve{\mathbb{R}}^k, \breve{\mathcal{F}}, \breve{P})$ defined as follows. Let $(\mathbb{R}^k, \mathcal{F}, P)$ be the probability space $\mathcal{R}(f_1, \ldots, f_k)$, then we have:

- $\breve{\mathbb{R}}^k = \mathbb{R}^k - \bigcup_{I \subseteq \{1,\ldots,k\}, |I| \geq 2} \mathit{Term}(I)$
- $\breve{\mathcal{F}} = \{E \subseteq \mathcal{F} \mid E \subseteq \breve{\mathbb{R}}^k\}$
- $\breve{P} = \{(E, p) \mid E \in \breve{\mathcal{F}} \wedge (E, p) \in P\}$

Theorem 4.6 *Let* $(\mathbb{R}^k, \mathcal{F}, P)$ *be the probability space* $\mathcal{R}(f_1, \ldots, f_k)$*. If* $\forall I \subseteq \{1, \ldots, k\}.\ |I| \geq 2 \Rightarrow P(\mathit{Term}(I)) = 0$*, then* $\breve{\mathcal{R}}(f_1, \ldots, f_k)$ *is a probability space.*

We are now in a position to formally define the semantics of an IGSMP.

Definition 4.7 The semantics of an IGSMP $\mathcal{G} = (\Sigma, \mathcal{C}, D, \mathit{Act}, T_+, T_-, T_a, s_0)$ is the RISTTS $[\![\mathcal{G}]\!] = (\Sigma', \mathbb{R}^+ \cup \{0\}, \mathit{Act}, P, T_t, T_a, s'_0)$ where:

- $\Sigma' = (\Sigma \times \mathit{Spent} \times \mathit{Sample})$ is the set of states of the RISTTS, where *Spent*, ranged over by v, is the set of partial functions from $\mathcal{C}$ to $\mathbb{R}^+ \cup \{0\}$, expressing the time already spent in execution by the clocks currently in execution in the IGSMP (clocks in the domain of *Spent*), and *Sample*, ranged over by *sample*, is the set $(\mathcal{C} \times (\mathbb{R}^+ \cup \{0\})) \cup \{-\}$, where a pair (C_n, t), also written $C_n : t$, denotes that the IGSMP is currently executing a set of clocks and that clock C_n has sampled the minimum residual time delay with t being the value of such a delay; while "$-$" denotes that started clocks are not under execution (e.g. the IGSMP is in a choice state or in a silent state).
- $\mathbb{R}^+ \cup \{0\}$ is the time domain: we consider continuous time.
- *Act* is the set of standard actions considered in the IGSMP.
- P, which associates a probability space (expressing next state probability) to some of the states in Σ', is defined to be the least partial function on Σ' satisfying the operational rules in the first part of Table 2.
- T_t is the set of timed transitions which are defined as the least relation over $\Sigma' \times (\mathbb{R}^+ \cup \{0\}) \times \Sigma'$ satisfying the operational rules in the second part of Table 2.
- T_a is the set of action transitions which are defined as the least relation over $\Sigma' \times \mathit{Act} \times \Sigma'$ satisfying the operational rules in the third part of Table 2.
- $s'_0 = \langle s_0, \emptyset, - \rangle$ is the initial state of the RISTTS, where the IGSMP is in the initial state and no clock is in execution.

In Table 2 we make use of the following notation. Given $v \in \mathit{Spent}$, we define $v - C_n$ to be the partial function obtained from v by removing C_n (and

$(P1)$	$\dfrac{(\exists C_n.\ s \xrightarrow{C_n^-}) \ \wedge\ \{C_{n_1},\ldots,C_{n_k}\} = dom(v)}{P(\langle s,v,-\rangle) = Sample^{\{\mathbf{n}_i\}}_{s,v}(\ \breve{\mathcal{R}}([D(C_{n_1}) \mid v(C_{n_1})],\ldots,[D(C_{n_k}) \mid v(C_{n_k})])\ )}$
$(P2)$	$\dfrac{(\exists C_n, w.\ s \xrightarrow{<C_n^+,w>}\ ) \ \wedge\ Pr = \{\ (\ <C_n,s'>,\ w/TW(s)\ )\ \mid\ s \xrightarrow{<C_n^+,w>} s'\ \}}{P(\langle s,v,-\rangle) = \sum_{<C_n,s'>\in dom(Pr)} Pr(<C_n,s'>) \cdot P(\langle s', v \cup \{(C_n,0)\}, -\rangle)}$
$(T1)$	$\langle s,v,C_n\!:\!t\rangle \xrightarrow{t'} \langle s, v+t', -\rangle \qquad 0 \le t' < t$
$(T2)$	$\dfrac{s \xrightarrow{C_n^-} s'}{\langle s,v,C_n\!:\!t\rangle \xrightarrow{t} \langle s', (v - C_n) + t, -\rangle}$
$(T3)$	$\dfrac{(\not\exists \theta.\ s \xrightarrow{\theta}) \ \wedge\ s \stackrel{\tau}{\not\longrightarrow}}{\langle s,v,-\rangle \xrightarrow{t} \langle s,v,-\rangle} \qquad t \ge 0$
$(A1)$	$\dfrac{s \xrightarrow{\alpha} s'}{\langle s,v,-\rangle \xrightarrow{\alpha} \langle s',v,-\rangle}$
$(A2)$	$\dfrac{s \xrightarrow{a} s'}{\langle s,v,C_n\!:\!t\rangle \xrightarrow{a} \langle s',v,-\rangle}$
	$TW(s) = \sum\{\!\mid w \mid \exists C_n.\ s \xrightarrow{<C_n^+,w>}\ \mid\!\}$
	$Sample^{\{\mathbf{n}_i\}}_{s,v}(t_1,\ldots,t_k) = \langle s,v,C_{n_{min}}\!:\!t_{min}\rangle$
	where *min* is the only index i such that: $\mathrm{t_i} = \min_{\mathrm{j}\in\{1,\ldots,\mathrm{k}\}} \mathrm{t_j}$

Table 2
Semantic rules for IGSMPs

the associated value) from its domain. We define $v + t$, with $t \in \mathbb{R}^+ \cup 0$, to be the partial function obtained from v by adding t to the time value associated with each clock in the domain of v. We use the notation $\{\mathbf{n}_i\}$ to stand for $\{\mathbf{n}_i\}_{i=1\ldots k}$, representing the sequence of names $n_1, \ldots n_k$ (in Table 2 the length k of the sequence is always clarified by the context in which $\{\mathbf{n}_i\}$ is used). Finally in the forth part of Table 2 we define two auxiliary functions. The function $TW : \Sigma \longrightarrow \mathbb{R}^+ \cup \{0\}$ computes the overall weight of the clock start transitions leaving a state of an IGSMP. Moreover, given a sate of the IGSMP $s \in \Sigma$, a partial function mapping active clock into their spent lifetimes $v \in Spent$, and a sequence $\{n_1, \ldots, n_k\}$ of clock indexes, the function

$Sample^{\{\mathbf{n}_i\}}_{s,v}$ maps a tuple $(t_1, \ldots, t_k)$ of time values sampled by clocks into the corresponding state $\langle s, v, C_{n_{\min}} : t_{\min}\rangle$ reached in the RISTTS, where *min* is the index of the clock which sampled the least time value. Note that function $Sample^{\{\mathbf{n}_i\}}_{s,v}$ is used in Table 2 for deriving (via induction, see Definition 3.4) a probability space over the states of the RISTTS from the probability space $\breve{\mathcal{R}}([D(C_{n_1}) \mid v(C_{n_1})], \ldots, [D(C_{n_k}) \mid v(C_{n_k})])$ over residual durations sampled by active clocks in a state of the IGSMP.

Theorem 4.8 *Let $\mathcal{G}'$, $\mathcal{G}''$ be two well-named IGSMPs. If $\mathcal{G}' \approx \mathcal{G}''$ then $[\![\mathcal{G}']\!] \approx [\![\mathcal{G}'']\!]$.*

The following theorems show that the semantics of well-named IGSMPs is indeed compositional.

Theorem 4.9 *Let $\mathcal{G}'$, $\mathcal{G}''$ be two well-named IGSMPs. For each $S \subseteq Act - \{\tau\}$ we have $[\![\mathcal{G}']\!] \parallel_S [\![\mathcal{G}'']\!] \approx [\![\mathcal{G}' \parallel_S \mathcal{G}'']\!]$.*

Theorem 4.10 *Let $\mathcal{G}$ be a well-named IGSMP. For each $L \subseteq Act - \{\tau\}$ we have $[\![\mathcal{G}]\!]/L \approx [\![\mathcal{G}/L]\!]$.*

5 Conclusion

Dealing with non-determinism in probabilistic systems with general distributions raises a series of problems, including the correct management of the residual durations of generally distributed delays in system states and the interplay of non-deterministic choices and probabilistic behaviors of temporal delays. The former problem can be solved by representing the temporal behavior of a system by using clocks (as in Timed Automata [23]) or elements (as in GSMPs [21]) whose durations are associated with generally distributed random variables. In particular we can correctly manage the residual durations of active clocks (elements) in system states with two different approaches which are borrowed from the theory of GSMPs: one based on spent clock lifetimes and one based on residual clock lifetimes. In this paper we have shown how to apply the former approach to the specification and analysis of concurrent systems including generally distributed delays, instead of using the latter approach as previously done in the literature [14]. In the former approach (similarly as in Timed Automata [23]) states are enriched with spent lifetimes of clocks and for each timed state where a clock C_n is active, the residual duration of C_n is sampled depending on both its spent lifetime and its associated duration distribution. In the latter approach (similarly as in classical Discrete Event Simulation [12]), the lifetime of each clock is sampled all at once at the clock start event, and states are enriched with residual lifetimes of clocks directly determining their residual duration. As we have shown, the drawback of the approach based on residual lifetimes, with respect to the one we propose, is that an adversary which is in charge of solving non-determinism may get information about the future system behavior since the duration of delays is decided a priori.

Our approach has been formalized by starting from the theory of Interactive GSMPs [6]. We first have characterized IGSMPs as a class of transition systems and then we have introduced the class of the Interactive Stochastic Timed Transition Systems (ISTTSs), which are both closed with respect to CSP parallel and hiding operators. Then we have used ISTTSs to define a compositional semantics for IGSMPs which realizes the approach based on spent lifetimes mentioned above.

References

[1] L. Aceto, M. Hennessy, *"Adding Action Refinement to a Finite Process Algebra"*, in Information and Computation 115:179-247, 1994

[2] M. Ajmone Marsan, A. Bianco, L. Ciminiera, R. Sisto, A. Valenzano, *"A LOTOS Extension for the Performance Analysis of Distributed Systems"*, in IEEE/ACM Trans. on Networking 2:151-164, 1994

[3] M. Bernardo, *"Theory and Application of Extended Markovian Process Algebra"*, Ph.D. Thesis, University of Bologna (Italy), 1999

[4] M. Bravetti, A. Aldini, *"Non-determinism in Probabilistic Timed Systems with General Distributions"*, Technical Report UBLCS-2001-08, University of Bologna (Italy), July 2001

[5] M. Bravetti, M. Bernardo, *"Compositional Asymmetric Cooperations for Process Algebras with Probabilities, Priorities, and Time"*, in Proc. of the *1st Int. Workshop on Models for Time-Critical Systems (MTCS 2000)*, ENTCS 39(3), State College (PA), 2000

[6] M. Bravetti, R. Gorrieri, *"The Theory of Interactive Generalized Semi-Markov Processes"*, to appear in Theoretical Computer Science

[7] M. Bravetti, R. Gorrieri, *"Deciding and Axiomatizing Weak ST Bisimulation for a Process Algebra with Recursion and Action Refinement"*, to appear in ACM Transactions on Computational Logic

[8] M. Bravetti, M. Bernardo, R. Gorrieri, *"Towards Performance Evaluation with General Distributions in Process Algebras"*, in Proc. of the *9th Int. Conf. on Concurrency Theory (CONCUR '98)*, LNCS 1466:405-422, 1998

[9] E. Brinksma, J.P. Katoen, R. Langerak, D. Latella, *"A Stochastic Causality-Based Process Algebra"*, in Computer Journal 38:553-565, 1995

[10] P. Buchholz, *"Markovian Process Algebra: Composition and Equivalence"*, in Proc. of the *2nd Int. Workshop on Process Algebra and Performance Modelling (PAPM '94)*, pp. 11-30, Erlangen (Germany), 1994

[11] N. Busi, R.J. van Glabbeek, R. Gorrieri, *"Axiomatizing ST Bisimulation Equivalence"*, in Proc. of the *IFIP Working Conf. on Programming Concepts, Methods and Calculi (PROCOMET '94)*, pp. 169-188, 1994

[12] C.G. Cassandras, *"Discrete Event Systems. Modeling and Performance Analysis"*, Aksen Associates, Irwin, 1993

[13] D.R. Cox, *"The Analysis of non-Markovian Stochastic Processes by the Inclusion of Supplementary Variables"*, in Proc. of the Cambridge Philosophical Society 51:433-440, 1955

[14] P.R. D'Argenio, *"Algebras and Automata for Timed and Stochastic Systems"*, Ph.D. Thesis, Univ. Twente, 1997

[15] R.J. van Glabbeek, F.W. Vaandrager, *"Petri Net Models for Algebraic Theories of Concurrency"*, in Proc. of the *Conf. on Parallel Architectures and Languages Europe (PARLE '87)*, LNCS 259:224-242, 1987

[16] N. Götz, U. Herzog, M. Rettelbach, *"TIPP - A Stochastic Process Algebra"*, in Proc. of the *1st Workshop on Process Algebras and Performance Modelling (PAPM '93)*, pp. 31-36, Edinburgh (UK), 1993

[17] H. Hermanns, *"Interactive Markov Chains"*, Ph.D. Thesis, Univ. Erlangen-Nürnberg, 1998

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

[19] C.A.R. Hoare, *"Communicating Sequential Processes"*, Prentice Hall, 1985

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

[21] K. Matthes, *"Zur Theorie der Bedienungsprozesse"*, in Trans. of the *3rd Prague Conf. on Information Theory, Stat. Dec. Fns. and Random Processes*, pp. 513-528, 1962

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

[23] X. Nicollin, J. Sifakis, S. Yovine, *"Compiling Real-Time Specifications into Extended Automata"*, in IEEE Trans. on Software Engineering, 18(9):794-804, 1992

[24] C. Priami, *"Stochastic π-Calculus with General Distributions"*, in *Proc. of the 4th Workshop on Process Algebras and Performance Modelling (PAPM '96)*, CLUT, pp. 41-57, Torino (Italy), 1996