Input/Output Stochastic Automata
Compositionality and Determinism

Pedro R. D'Argenio[1], Matias David Lee[2], and Raúl E. Monti[1(✉)]

[1] CONICET, Universidad Nacional de Córdoba, Córdoba, Argentina
{dargenio,rmonti}@famaf.unc.edu.ar
[2] LIP, Université de Lyon, CNRS, ENS de Lyon, Inria, UCBL, Lyon, France

Abstract. Stochastic automata provide a way to symbolically model systems in which the occurrence time of events may respond to any continuous random variable. We introduce here an input/output variant of stochastic automata that, once the model is closed —i.e., all synchronizations are resolved—, the resulting automaton does not contain non-deterministic choices. This is important since fully probabilistic models are amenable to simulation in the general case and to much more efficient analysis if restricted to Markov models. We present here a theoretical introduction to input/output stochastic automata (IOSA) for which we (i) provide a concrete semantics in terms of non-deterministic labeled Markov processes (NLMP), (ii) prove that bisimulation is a congruence for parallel composition both in NLMP and IOSA, (iii) show that parallel composition commutes in the symbolic and concrete level, and (iv) provide a proof that a closed IOSA is indeed deterministic.

1 Introduction

The difficulty of the modeling and analysis of a system grows rapidly with the size and complexity of the system itself. In this sense the advantages of compositional approaches to modeling complex systems are unquestionable: they facilitate systematic design and the interchange of components, enable compositional analysis and help for the compact representation of state spaces and other ways of attacking the state explosion problem. Compositional modeling allows the designer to focus on the modeling of the rather discernible operational behaviour of the components and the evident synchronization among them (compare to the difficulty of figuring out the whole behaviour in a monolithic model).

If these models are aimed at performance and dependability analysis, there is a need to consider general distributions. Although (negative) exponential distributions yield analytically tractable models (namely, continuous time Markov chains), and are useful for many applications, they are not realistic for modeling many phenomena. Phenomena such as timeouts in communication protocols, hard deadlines in real-time systems, human response times or the variability of the delay of sound and video frames (so-called jitter) in modern multi-media

Supported by ANPCyT PICT-2012-1823 and SeCyT-UNC 05/BP12 and 05/B497.

M. Fränzle and N. Markey (Eds.): FORMATS 2016, LNCS 9884, pp. 53–68, 2016.
DOI: 10.1007/978-3-319-44878-7_4

communication systems are typically described by non-memoryless distributions such as uniform, log-normal, or Weibull distributions.

To attack the compositional modeling of this type of systems stochastic process algebras with general continuous distributions have been devised (see e.g. [4] and references therein), and notably the modeling language MODEST [3]. The problem with all these languages is that they introduce non-determinism. In general, it is not possible to analyze generally distributed stochastic processes, let alone if they are also non-deterministic. However, deterministic stochastic processes can be simulated using discrete event simulation. Simulation is instead not feasible in general if the models are non-deterministic. (Though there are approaches to simulate Markov decission processes either by recognizing spurious non-determinism [2,16] or by sampling schedulers [9], it is not clear how these techniques scale to continuous settings.)

Starting from the notion of stochastic automata [7,8], we restrict this framework to obtain input/output stochastic automata (IOSA). While stochastic automata were constructed to naturally accept the non-determinism interacting with continuous probabilities, we designed IOSA so that parallel composition works naturally and, moreover, the system becomes fully probabilistic (i.e., it does not contain non-determinism) as soon as the system is closed (i.e. all interactions are resolved). Thus, we split actions into input and output and let them behave in a reactive and generative manner respectively (see [15] for the concepts of reactive and generative transitions), following ideas proposed in [22]. Since outputs behave generatively, we let their occurrence time be controlled by a random variable (encoded in a *clock*). As inputs are reactive, they are passive and hence their occurrence time can only depend on their interaction with outputs. Thus, IOSA combines in a single model the two interpretations of stochastic automata (either as open or as closed systems [7,8].)

The paper presents a theoretical introduction to IOSA. For this, we present the model in Sect. 3 and give its concrete semantics in terms of non-deterministic labeled Markov processes (NLMP) [10,21]. Next (Sect. 4) we define the parallel composition on IOSA and show that the model is closed under composition. We also define parallel composition on NLMPs and show that, when it is well defined, bisimulation is a congruence for parallel composition on NLMPs. Moreover, we prove that parallel composition commutes in the symbolic (IOSA) and concrete (NLMP) level through isomorphism and as a corollary have that bisimulation is a congruence for parallel composition on IOSAs. In Sect. 5, we define precisely what we mean by a deterministic IOSA, show several properties of the underlying NLMP, and prove that a closed IOSA (i.e., a IOSA without input actions) is indeed deterministic. In addition, we provide the essential background on measure theory in Sect. 2, and conclude the paper in Sect. 6.

2 Preliminaries on Measure Theory

In this section, we recall some fundamental notions of measure theory that will be useful throughout the paper.

Given a set S and a collection Σ of subsets of S, we call Σ a *σ-algebra* iff $S \in \Sigma$ and Σ is closed under complement and denumerable union. By $\sigma(\mathcal{G})$ we denote the *σ-algebra generated by* the family $\mathcal{G} \subseteq 2^S$, i.e., the minimal σ-algebra containing $\mathcal{G}$. Each element of $\mathcal{G}$ is called a *generator* and $\mathcal{G}$ is called the *generator set*. We call the pair (S, Σ) a *measurable space*. A *measurable set* is a set $Q \in \Sigma$. Let (L, Λ) and (S, Σ) be measurable spaces. A *measurable rectangle* is a set $A \times B$ with $A \in \Lambda$ and $B \in \Sigma$. The *product σ-algebra* on $L \times S$ is the smallest σ-algebra containing all measurable rectangles, and is denoted by $\Lambda \otimes \Sigma$. The *coproduct σ-algebra* $\Lambda \oplus \Sigma$ of L and S is defined in the disjoint union $L \uplus S$ and it is generated by the set $\Lambda \cup \Sigma$.

A function $\mu : \Sigma \to [0,1]$ is a *probability measure* if (i) it is σ-additive, i.e. $\mu(\bigcup_{i\in\mathbb{N}} Q_i) = \sum_{i\in\mathbb{N}} \mu(Q_i)$ for all countable family of pairwise disjoint measurable sets $\{Q_i \mid i \in \mathbb{N}\} \subseteq \Sigma$, and (ii) $\mu(S) = 1$. By δ_a we denote the Dirac probability measure concentrated in $\{a\}$. Given measures μ and μ' on (L, Λ) and (S, Σ) respectively, the product measure $\mu \times \mu'$ on the product space $(L \times S, \Lambda \otimes \Sigma)$ is defined as the unique measure such that $(\mu \times \mu')(A \times B) = \mu(A) \cdot \mu'(B)$ for all $A \in \Lambda$ and $B \in \Sigma$. Any measure μ on (L, Λ) can be naturally extended into a measure $\hat{\mu}$ in the coproduct space $(L \uplus S, \Lambda \oplus \Sigma)$ by taking $\hat{\mu}(A) = \mu(A \backslash S)$, and similarly for measures on (S, Σ). Let $\Delta(S)$ denote the set of all probability measures over the measurable space (S, Σ). We let μ, μ', μ_1,... range over $\Delta(S)$. Let (S_1, Σ_1) and (S_2, Σ_2) be two measurable spaces. A function $f : S_1 \to S_2$ is said to be *measurable* if for all $Q_2 \in \Sigma_2$, $f^{-1}(Q_2) \in \Sigma_1$, i.e., its inverse image maps measurable sets to measurable sets. In this case we denote $f : (S_1, \Sigma_1) \to (S_2, \Sigma_2)$.

A σ-algebra is *Borel* if it is generated by the set of all open sets in a topology. Particularly, the Borel σ-algebra on the real line is $\mathcal{B}(\mathbb{R}) = \sigma(\{(a, b) \mid a, b \in \mathbb{R} \text{ and } a < b\})$. Similarly, $\mathcal{B}([0,1])$ is the Borel σ-algebra on the interval $[0,1]$ generated by the open sets in the interval $[0,1]$.

There is a standard construction by Giry [14] to endow $\Delta(S)$ with a σ-algebra as follows: $\Delta(\Sigma)$ is defined as the σ-algebra generated by the sets of probability measures $\Delta^{\geq p}(Q) \doteq \{\mu \mid \mu(Q) \geq p\}$, with $Q \in \Sigma$ and $p \in [0,1]$. We let ξ range over $\Delta(\Sigma)$.

To give structure to non-determinism on NLMP, we will use hit σ-algebras [10] on $\Delta(\Sigma)$. Thus, the hit σ-algebra $H(\Delta(\Sigma))$ is defined to be the minimal σ-algebra containing all sets $H(\xi) \doteq \{\zeta \in \Delta(\Sigma) \mid \zeta \cap \xi \neq \varnothing\}$ with $\xi \in \Delta(\Sigma)$.

3 Input/Output Stochastic Automata (IOSA)

Stochastic automata [7,8] use clock variables to control and observe the passage of time. Since in our context the time at which events occur is random, clocks are in fact random variables. When a clock is set, it takes a random value whose probability depends on the distribution function of the clock. As time evolves, clocks count down synchronously, i.e., all do so at the same rate. When a clock reaches the value zero, "the clock expires" and this may enable some events. Starting from the notion of stochastic automata, we restrict this framework to

obtain IOSA. We split actions into inputs and outputs and let them behave in a reactive and generative manner respectively (see [15] for the concepts of reactive and generative transitions), somehow following ideas proposed in [22]. We could also think that inputs are externally controlled actions and outputs are locally controlled actions. Precisely because of this, the occurrence time of output actions is controlled by a random variable, while inputs are passive and hence their occurrence time can only depend on their interaction with outputs. A set of restrictions which we will explain later ensures that, almost surely, no two outputs actions are enabled at the same time.

Definition 1. *An input/output stochastic automaton (IOSA for short) is a structure* $(\mathcal{S}, \mathcal{A}, \mathcal{C}, \rightarrow, \mathcal{C}_0, s_0)$*, where* $\mathcal{S}$ *is a (denumerable) set of states,* $\mathcal{A}$ *is a (denumerable) set of labels partitioned into disjoint sets of input labels* $\mathcal{A}^I$*, and output labels* $\mathcal{A}^O$*,* $\mathcal{C}$ *is a (finite) set of clocks such that each* $x \in \mathcal{C}$ *has associated a continuous probability measure* μ_x *on* $\mathbb{R}$ *(hence* $\mu_x(d) = 0$ *for any* $d \in \mathbb{R}$*) also satisfying that* $\mu_x(\mathbb{R}_{>0}) = 1$*,* $\rightarrow \subseteq \mathcal{S} \times \mathcal{C} \times \mathcal{A} \times \mathcal{C} \times S$ *is a transition function,* $\mathcal{C}_0$ *is the set of clocks that are initialized in the initial state, and* $s_0 \in \mathcal{S}$ *is the initial state. In addition a IOSA should satisfy the following constraints:*

(a) *If* $s \xrightarrow{C,a,C'} s'$ *and* $a \in \mathcal{A}^I$*, then* $C = \varnothing$.
(b) *If* $s \xrightarrow{C,a,C'} s'$ *and* $a \in \mathcal{A}^O$*, then* C *is a singleton set.*
(c) *If* $s \xrightarrow{\{x\},a_1,C_1} s_1$ *and* $s \xrightarrow{\{x\},a_2,C_2} s_2$ *then* $a_1 = a_2$*,* $C_1 = C_2$ *and* $s_1 = s_2$.
(d) *If* $s \xrightarrow{\{x\},a,C} s'$ *then, for every transition* $t \xrightarrow{C_1,b,C_2} s$*, either* $x \in C_2$*, or* $x \notin C_1$ *and there exists a transition* $t \xrightarrow{\{x\},c,C_3} t'$.
(e) *If* $s_0 \xrightarrow{\{x\},a,C} s$ *then* $x \in C_0$.
(f) *For every* $a \in \mathcal{A}^I$ *and state* s*, there exists a transition* $s \xrightarrow{\varnothing,a,C} s'$.
(g) *For every* $a \in \mathcal{A}^I$*, if* $s \xrightarrow{\varnothing,a,C_1} s_1$ *and* $s \xrightarrow{\varnothing,a,C_2} s_2$*,* $C_1 = C_2$ *and* $s_1 = s_2$.

The occurrence of an action is controlled by the expiration of clocks. Thus, whenever $s \xrightarrow{\{x\},a,C} s'$ and the system is in state s, output action a will occur once the value of clock x reaches 0. At this point, the system moves to state s' setting the values of every clocks $y \in C$ to a value sampled according to the distribution μ_y. For input transitions $s \xrightarrow{\varnothing,a,C} s'$, the behaviour is similar, only that its occurrence can potentially occur at any time which will become definite once the action interacts with an output.

Restriction (a) states that every input is reactive and hence their occurrence is controlled by the environment. Hence no internal clock controls its occurrence. Restriction (b) states that each output is generative (or locally controlled) so it has associated a clock which determines its occurrence time. We also limit the set to exactly one clock, to have a clean definition. Restriction (c) forbids that a single clock enables two different transitions, otherwise two output actions would become enable simultaneously. Besides, notice that if clocks are used when they have already expired they would immediately enable the respective output transition, which may lead to a simultaneous enabling if the system arrives to a

states with two expired clocks enabling two different transitions. Restrictions (d) and (e) ensure that a clock would never be used when it has already expired. Particularly (d) states that an enabling clock x at state s should either be set on arrival ($x \in C_2$) or it has not been used immediately before ($x \notin C_1$) but should be also enabling on the immediately preceding state. Since clocks are set by sampling from a continuous random variable, the probability that the values of two different clocks are equal is 0. This last fact, together with restrictions (c), (d) and (e), guarantees that almost never two different output transitions are enabled at the same time. Restrictions (f) and (g) are usual restrictions on I/O-like automata: (f) ensures that outputs are not blocked in a composition, and (g) that determinism is preserved after composition.

The semantics of IOSA is defined in terms of NLMP [10,21]. An NLMP is a generalization of probabilistic transition systems with continuous domain. More particularly, it extends LMP [11] with *internal* non-determinism.

Definition 2. *A* non-deterministic labeled Markov process *(NLMP for short) is a structure* $(\boldsymbol{S}, \Sigma, \{\mathcal{T}_a \mid a \in \mathcal{L}\})$ *where* Σ *is a* σ*-algebra on the set of states* $\boldsymbol{S}$*, and for each label* $a \in \mathcal{L}$ *we have* $\mathcal{T}_a : \boldsymbol{S} \to \Delta(\Sigma)$ *is measurable from* Σ *to the hit* σ*-algebra* $H(\Delta(\Sigma))$*.*

The formal semantics of a IOSA is defined by an NLMP with two classes of transitions: one that encodes the discrete steps and contains all the probabilistic information introduced by the sampling of clocks, and other describing the time steps, that only records the passage of time synchronously decreasing the value of all clocks. In order to simplify the definition, we assume that the set of clocks has a particular order and their current values follow the same order in a vector.

Definition 3. *Given a IOSA* $\mathcal{I} = (\mathcal{S}, \mathcal{A}, \mathcal{C}, \to, \mathcal{C}_0, s_0)$ *with* $\mathcal{C} = \{x_1, \ldots, x_N\}$*, its semantics is defined by the NLMP* $\mathcal{P}(\mathcal{I}) = (\boldsymbol{S}, \mathscr{B}(\boldsymbol{S}), \{\mathcal{T}_a \mid a \in \mathcal{L}\})$ *where*

- $\boldsymbol{S} = (\mathcal{S} \cup \{\mathsf{init}\}) \times \mathbb{R}^N$, $\mathcal{L} = \mathcal{A} \cup \mathbb{R}_{>0} \cup \{\mathsf{init}\}$*, with* $\mathsf{init} \notin \mathcal{S} \cup \mathcal{A} \cup \mathbb{R}_{>0}$
- $\mathcal{T}_{\mathsf{init}}(\mathsf{init}, \vec{v}) = \{\delta_{s_0} \times \prod_{i=1}^{N} \mu_{x_i}\}$,
- $\mathcal{T}_a(s, \vec{v}) = \{\mu_{\vec{v},C',s'} \mid s \xrightarrow{C,a,C'} s', \bigwedge_{x_i \in C} \vec{v}(i) \leq 0\}$*, for all* $a \in \mathcal{A}$*, where* $\mu_{\vec{v},C',s'} = \delta_{s'} \times \prod_{i=1}^{N} \overline{\mu}_{x_i}$ *with* $\overline{\mu}_{x_i} = \mu_{x_i}$ *if* $x_i \in C'$ *and* $\overline{\mu}_{x_i} = \delta_{\vec{v}(i)}$ *otherwise, and*
- $\mathcal{T}_d(s, \vec{v}) = \{\delta^{-d}_{(s,\vec{v})} \mid 0 < d \leq \min\{\vec{v}(i) \mid \exists a \in \mathcal{A}^O, C' \subseteq \mathcal{C}, s' \in S : s \xrightarrow{\{x_i\},a,C'} s'\}\}$ *for all* $d \in \mathbb{R}_{\geq 0}$*, where* $\delta^{-d}_{(s,\vec{v})} = \delta_s \times \prod_{i=1}^{N} \delta_{\vec{v}(i)-d}$.

The state space is the product space of the states of the IOSA with all possible clock valuations. A distinguished initial state init is added to encode the random initialization of all clocks (it would be sufficient to initialize clocks in C_0 but we decided for this simplification). Such encoding is done by transition $\mathcal{T}_{\mathsf{init}}$. The state space is structured in the usual Borel σ-algebra. The discrete step is encoded by $\mathcal{T}_a$, with $a \in \mathcal{A}$. Notice that, at state $(s, \vec{v})$, the transition $s \xrightarrow{C,a,C'} s'$ will only take place if $\bigwedge_{x_i \in C} \vec{v}(i) \leq 0$, that is, if the current values of all clocks in C are not positive. For the particular case of the input actions this will always

be true. The next actual state would be determined randomly as follows: the symbolic state will be s' (this corresponds to $\delta_{s'}$ in $\mu_{\vec{v},C',s'} = \delta_{s'} \times \prod_{i=1}^{N} \overline{\mu}_{x_i}$), any clock not in C' preserves the current value (hence $\overline{\mu}_{x_i} = \delta_{\vec{v}(i)}$ if $x_i \notin C'$), and any clock in C' is set randomly according to its respective associated distribution (hence $\overline{\mu}_{x_i} = \mu_{x_i}$ if $x_i \in C'$). The time step is encoded by $\mathcal{T}_d(s,\vec{v})$ with $d \in \mathbb{R}_{\geq 0}$. It can only take place at d units of time if there is no output transition enabled at the current state within the next d time units (this is verified by condition $0 < d \leq \min\{\vec{v}(i) \mid \exists a \in \mathcal{A}^O, C' \subseteq \mathcal{C}, s' \in S : s \xrightarrow{\{x_i\},a,C'} s'\}$). In this case, the system remains in the same symbolic state (this corresponds to δ_s in $\delta^{-d}_{(s,\vec{v})} = \delta_s \times \prod_{i=1}^{N} \delta_{\vec{v}(i)-d}$), and all clock values are decreased by d units of times (represented by $\delta_{\vec{v}(i)-d}$ in the same formula).

We still need to show that $\mathcal{P}(\mathcal{I})$ is indeed an NLMP. For this we have to prove that $\mathcal{T}_a$ maps into measurable sets in $\Delta(\mathscr{B}(\mathbf{S}))$ (Lemma 4), and that $\mathcal{T}_a$ is a measurable function for every $a \in \mathcal{L}$ (Lemma 5).

Lemma 4. *$\mathcal{T}_a(s,\vec{v}) \in \Delta(\mathscr{B}(\boldsymbol{S}))$ for all $a \in \mathcal{L}$ and $(s,\vec{v}) \in \boldsymbol{S}$.*

Proof. The proof makes use of Lemma 3.1 in [10], from which we know that for all $\mu \in \Delta(\mathbf{S})$, $\{\mu\} \in \Delta(\mathscr{B}(\mathbf{S}))$ (since $\mathscr{B}(\mathbf{S})$ is generated by a discrete π-system).

Notice that for any $\vec{v} \in \mathbb{R}^N$, $\mathcal{T}_{\mathsf{init}}(\mathsf{init},\vec{v})$ is a singleton set and hence measurable. Similarly, notice that for every $d \in \mathbb{R}$, $s \in \mathcal{S}$, and $\vec{v} \in \mathbb{R}^N$, $\mathcal{T}_d(s,\vec{v})$ is either a singleton set or the empty set, and hence measurable. Finally, since there is only a denumerable number of transitions in a IOSA, for every $a \in \mathcal{A}$, $s \in \mathcal{S}$, and $\vec{v} \in \mathbb{R}^N$, $\mathcal{T}_a(s,\vec{v})$ is a denumerable union of singleton sets, and hence also measurable. □

Lemma 5. *For all $a \in \mathcal{L}$, T_a is measurable from $\mathscr{B}(\boldsymbol{S})$ to $H(\Delta(\mathscr{B}(\boldsymbol{S})))$.*

Proof. We need to show that for every $a \in \mathcal{L}$ and every $\xi \in \Delta(\mathscr{B}(\mathbf{S}))$, $\mathcal{T}_a^{-1}(H(\xi)) = \{(s,\vec{v}) \mid \mathcal{T}_a(s,\vec{v}) \cap \xi \neq \varnothing\}$ is measurable.

We divide the proof in three cases depending on the nature of the label on the transition function. First, notice that $\mathcal{T}^{-1}_{\mathsf{init}}(H(\xi)) = \{\mathsf{init}\} \times \mathbb{R}^N$ if $\delta_{s_0} \times \prod_{i=1}^{N} \mu_{x_i} \in \xi$ and $\mathcal{T}^{-1}_{\mathsf{init}}(H(\xi)) = \varnothing$ otherwise, and both sets are measurable.

We analyze now the case of $a \in \mathcal{A}$, for which we can calculate

$$\begin{aligned}\mathcal{T}_a^{-1}(H(\xi)) &= \{(s,\vec{v}) \mid \{\mu_{\vec{v},C',s'} \mid s \xrightarrow{C,a,C'} s', \textstyle\bigwedge_{x_i \in C} \vec{v}(i) \leq 0\} \cap \xi \neq \varnothing\} \\ &= \bigcup_{s \xrightarrow{C,a,C'} s'} \{(s,\vec{v}) \mid \textstyle\bigwedge_{x_i \in C} \vec{v}(i) \leq 0\} \cap \{(s,\vec{v}) \mid \mu_{\vec{v},C',s'} \in \xi\}\end{aligned}$$

Since the union is denumerable, it is sufficient to prove that the two intersecting sets are measurable. First, notice that $\{(s,\vec{v}) \mid \bigwedge_{x_i \in C} \vec{v}(i) \leq 0\} = \{s\} \times \prod_{i=1}^{N} V_i$ where $V_i = (-\infty, 0]$ if $x_i \in C$ and $V_i = \mathbb{R}$ otherwise. Hence, it is measurable.

For the second case, define $f_{C',s'} : \mathbb{R} \to \Delta(\mathbf{S})$ by $f_{C',s'}(\vec{v}) = \mu_{\vec{v},C',s'}$. Then $\{(s,\vec{v}) \mid \mu_{\vec{v},C',s'} \in \xi\} = \{(s,\vec{v}) \mid f_{C',s'}(\vec{v}) \in \xi\} = \{s\} \times f^{-1}_{C',s'}(\xi)$. So, it only remains to prove that $f_{C',s'}$ is a measurable function. Using [20, Lemma 3.6], we

only have to prove that $f^{-1}_{C',s'}(\Delta^{\geq q}(A \times \prod_{i=1}^{N} V_i))$ with $A \subseteq \mathbf{S}$ and $V_i \in \mathscr{B}(\mathbb{R})$, $1 \leq i \leq N$, is measurable, for which we can calculate

$$\begin{aligned} f^{-1}_{C',s'}(\Delta^{\geq q}(A \times \textstyle\prod_{i=1}^{N} V_i)) &= \{\vec{v} \mid \mu_{\vec{v},C',s'}(A \times \textstyle\prod_{i=1}^{N} V_i) \geq q\} \\ &= \{\vec{v} \mid s' \in A, (\textstyle\prod_{x_i \in C'} \mu_{x_i})(\textstyle\prod_{x_i \in C'} V_i) \geq q, \forall x_i \notin C' : \vec{v}(i) \in V_i\} \end{aligned}$$

Then, if $s' \in A$ and $(\prod_{x_i \in C'})(\prod_{x_i \in C'} V_i) \geq q$, $f^{-1}_{C',s'}(\Delta^{\geq q}(A \times \prod_{i=1}^{N} V_i)) = \prod_{i=1}^{N} \overline{V_i}$ with $\overline{V_i} = \mathbb{R}$ if $x_i \in C'$, $\overline{V_i} = V_i$ if $x_i \notin C'$, or $f^{-1}_{C',s'}(\Delta^{\geq q}(A \times \prod_{i=1}^{N} V_i)) = \varnothing$ otherwise, and in both cases the sets are measurable.

For the case of $d \in \mathbb{R}$, notice that

$$\begin{aligned} \mathcal{T}_d^{-1}(H(\xi)) = \; & \{(s,\vec{v}) \mid \delta^{-d}_{(s,\vec{v})} \in \xi\} \cap \\ & \{(s,\vec{v}) \mid 0 < d \leq \min\{\vec{v}(i) \mid \exists a \in \mathcal{A}^O, C' \subseteq \mathcal{C}, s' \in S : s \xrightarrow{\{x_i\},a,C'} s'\} \end{aligned}$$

The second set is equal to $\mathbf{S} \times \prod_{i=1}^{N} V_i$ where $V_i = [d, \infty)$ if $s \xrightarrow{\{x_i\},a,C'} s'$, and $V_i = \mathbb{R}$ otherwise. Hence it is measurable. For the first set, define $f_d : \mathbf{S} \to \Delta(\mathbf{S})$ by $f_d(s,\vec{v}) = \delta^{-d}_{(s,\vec{v})}$. Then $\{(s,\vec{v}) \mid \delta^{-d}_{(s,\vec{v})} \in \xi\} = f_d^{-1}(\xi)$ and hence it suffices to show that f_d is measurable. So, we have to prove that $f_d^{-1}(\Delta^{\geq q}(Q))$ is measurable for any $Q \in \mathscr{B}(\mathbf{S})$. But $f_d^{-1}(\Delta^{\geq q}(Q)) = \{(s,\vec{v}) \mid \delta^{-d}_{(s,\vec{v})}(Q) \geq q\} = \{(s,\vec{v}) \mid (s,\vec{v}-d) \in Q \wedge q = 1\}$. That is $f_d^{-1}(\Delta^{\geq q}(Q)) = \{(s,\vec{v}) \mid (s,\vec{v}-d) \in Q\}$ if $q = 1$ or $f_d^{-1}(\Delta^{\geq q}(Q)) = \varnothing$ otherwise, and in both cases the sets are measurable. □

4 Composition and Bisimulation as a Congruence

In this section we define parallel composition of IOSAs and show that IOSAs are closed for parallel composition. We also show that bisimulation is a congruence for the parallel composition and we achieve it through defining parallel composition on NLMPs.

Since we intend outputs to be autonomous (or locally controlled), we do not allow synchronization between outputs. Besides, we need to avoid name clashes on the clock, so that the intended behaviour of each component is preserved and moreover, to ensure that the resulting composed automata is indeed a IOSA. Thus we require to compose only *compatible* IOSAs.

Definition 6. *Two IOSAs $\mathcal{I}_1$ and $\mathcal{I}_2$ are said to be compatible if they do not share output actions nor clocks, i.e. $\mathcal{A}_1^O \cap \mathcal{A}_2^O = \varnothing$ and $\mathcal{C}_1 \cap \mathcal{C}_2 = \varnothing$.*

Definition 7. *Given two compatible IOSAs $\mathcal{I}_1$ and $\mathcal{I}_2$, the parallel composition $\mathcal{I}_1||\mathcal{I}_2$ is a new IOSA $(\mathcal{S}_1 \times \mathcal{S}_2, \mathcal{A}, \mathcal{C}, \rightarrow, \mathcal{C}_0, s_0^1||s_0^2)$ where (i) $\mathcal{A}^O = \mathcal{A}_1^O \cup \mathcal{A}_2^O$ (ii) $\mathcal{A}^I = (\mathcal{A}_1^I \cup \mathcal{A}_2^I) \setminus \mathcal{A}^O$ (iii) $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2$ (iv) $\mathcal{C}_0 = \mathcal{C}_0^1 \cup \mathcal{C}_0^2$ and $\rightarrow$ is the smallest relation defined by rules in Table 1 where we write $s||t$ instead of (s,t).*

The previous definition is only structural. We need to show that the seven restrictions that define IOSAs also hold.

Table 1. Parallel composition on IOSAs

$$\frac{s_1 \xrightarrow{C,a,C'}_1 s_1'}{s_1||s_2 \xrightarrow{C,a,C'} s_1'||s_2}\ a \in \mathcal{A}_1 \backslash \mathcal{A}_2 \quad (1) \qquad \frac{s_2 \xrightarrow{C,a,C'}_2 s_2'}{s_1||s_2 \xrightarrow{C,a,C'} s_1||s_2'}\ a \in \mathcal{A}_2 \backslash \mathcal{A}_1 \quad (2)$$

$$\frac{s_1 \xrightarrow{C_1,a,C_1'}_1 s_1' \quad s_2 \xrightarrow{C_2,a,C_2'}_2 s_2'}{s_1||s_2 \xrightarrow{C_1 \cup C_2, a, C_1' \cup C_2'} s_1'||s_2'} \quad (3)$$

Theorem 8. *Let $\mathcal{I}_1$ and $\mathcal{I}_2$ be two compatible IOSAs. Then $\mathcal{I}_1||\mathcal{I}_2$ is indeed a IOSA.*

Proof. The proof of restrictions (a), (b), (f), (e), and (g) follow by straightforward inspection on the rules, considering that $\mathcal{I}_1$ and $\mathcal{I}_2$ also satisfy the respective restriction, and doing some case analysis. Since $\mathcal{I}_1$ and $\mathcal{I}_2$ are compatible, restriction (c) also follows by inspecting the rules taking into account, in addition, that $\mathcal{I}_1$ and $\mathcal{I}_2$ satisfy restriction (g).

So, we only focus on (d). Suppose $s_1||s_2 \xrightarrow{\{x\},a,C} s_1'||s_2'$. We analyze the case in which $a \in \mathcal{A}_1$ and $x \in \mathcal{C}_1$. The other is symmetric. Moreover, we only consider the case in which $a \in \mathcal{A}_1 \cap \mathcal{A}_2$ since the case $a \in \mathcal{A}_1 \setminus \mathcal{A}_2$ follows similarly.

In this case, we have that $s_1 \xrightarrow{\{x\},a,C_1}_1 s_1'$, $s_2 \xrightarrow{\varnothing,a,C_2}_2 s_2'$, and $C = C_1 \cup C_2$. Let $t_1||t_2 \xrightarrow{C',b,C''} s_1||s_2$. We distinguish three cases:

(i) Suppose $b \in \mathcal{A}_1 \setminus \mathcal{A}_2$. Then $t_1 \xrightarrow{C',b,C''} s_1$ and $t_2 = s_2$. Because $\mathcal{I}_1$ satisfies (d), then either $x \in C''$, or $x \notin C'$ and there exist $t_1 \xrightarrow{\{x\},c,C_3}_1 t_1'$. Hence $x \in C''$, or $x \notin C'$ and there exist t_2' and C_3' such that $t_1||t_2 \xrightarrow{\{x\},c,C_3'} t_1'||t_2'$ (which may occur either by rule (1) or (3) if $c \in \mathcal{A}_1 \cap \mathcal{A}_2$).

(ii) If $b \in \mathcal{A}_2 \setminus \mathcal{A}_1$, then $t_2 \xrightarrow{C',b,C''}_2 s_2$ and $t_1 = s_1$. Notice that $C', C'' \subseteq \mathcal{C}_2$ and hence $x \notin C'$ and $x \notin C''$. Moreover, since $\mathcal{I}_2$ is input enabled (restriction (f)), $t_2 \xrightarrow{\varnothing,a,C_3}_2 t_2'$ for some C_3 and t_2'. Then, by rule (3), $s_1||t_2 \xrightarrow{\{x\},a,C_1 \cup C_3} s_1'||t_2'$ which proves this case.

(iii) If $b \in \mathcal{A}_1 \cap \mathcal{A}_2$, then, by rule (3), $t_1 \xrightarrow{C_1',b,C_1''}_1 s_1$, $t_2 \xrightarrow{C_2',b,C_2''}_2 s_2$, $C' = C_1' \cup C_2'$ and $C'' = C_1'' \cup C_2''$. Because $\mathcal{I}_1$ satisfies (d), then either $x \in C_1''$, or $x \notin C_1'$ and there exist $t_1 \xrightarrow{\{x\},c,C_3}_1 t_1'$. If $x \in C_1''$, then $x \in C'$ partially proving this case. If instead $x \notin C_1'$ and there exist $t_1 \xrightarrow{\{x\},c,C_3}_1 t_1'$, then $x \notin C''$ (since $x \notin C_2''$ by compatibility), and there exist t_2' and C_3' such that $t_1||t_2 \xrightarrow{\{x\},c,C_3'} t_1'||t_2'$ (which may occur either by rule (1) or (3) if $c \in \mathcal{A}_1 \cap \mathcal{A}_2$), finally proving this case. □

To prove that bisimulation is a congruence on IOSAs, we first define a parallel composition on NLMPs, prove congruence in this setting, and then show

that the semantics of the parallel composition of two IOSAs is isomorphic to the parallel composition of the semantics of each IOSA. From this, it follows that bisimulation is also a congruence for the parallel composition of IOSAs. An important consideration is that NLMPs are not closed for parallel composition [13] in general. So we will need to require that the parallel composition of NLMPs is also an NLMP as a hypothesis of the congruence theorem on NLMP.

Definition 9. *Let* $\mathcal{P}_i = (\boldsymbol{S}_i, \Sigma_i, \{\mathcal{T}_a^i \mid a \in \mathcal{L}_i\})$, $i \in \{1,2\}$, *be two NLMPs. We define the parallel composition by* $\mathcal{P}_1||\mathcal{P}_2 = (\boldsymbol{S}_1 \times \boldsymbol{S}_2, \Sigma_1 \otimes \Sigma_2, \{\mathcal{T}_a \mid a \in \mathcal{L}_1 \cup \mathcal{L}_2\})$ *where, writing* $s_1||s_2$ *instead of* (s_1, s_2),

(i) $\mathcal{T}_a(s_1||s_2) = \{\mu_1 \times \delta_{s_2} \mid \mu_1 \in \mathcal{T}_a^1(s_1)\}$, *if* $a \in \mathcal{L}_1 \setminus \mathcal{L}_2$,
(ii) $\mathcal{T}_a(s_1||s_2) = \{\delta_{s_1} \times \mu_2 \mid \mu_2 \in \mathcal{T}_a^2(s_2)\}$, *if* $a \in \mathcal{L}_2 \setminus \mathcal{L}_1$, *and*
(iii) $\mathcal{T}_a(s_1||s_2) = \{\mu_1 \times \mu_2 \mid \mu_1 \in \mathcal{T}_a^1(s_1), \mu_2 \in \mathcal{T}_a^2(s_2)\}$, *if* $a \in \mathcal{L}_1 \cap \mathcal{L}_2$.

Probabilistic bisimulation was introduced by Larsen and Skou [18] in a discrete setting and adapted to a continuous setting like NLMP in [10,11]. The idea behind the bisimulation equivalence is that from two equivalent states, an a-transition should lead with equal probability to any measurable aggregate of equivalence classes (properly speaking, to any measurable set that results from an arbitrary union of equivalence classes).

Given a relation $R \subseteq \mathbf{S} \times \mathbf{S}$, a set $Q \subseteq \mathbf{S}$ is *R-closed* if $R(Q) \subseteq Q$. If R is symmetric, Q is R-closed iff for all $s, t \in S$ such that $s\ R\ t$, $s \in Q \Leftrightarrow t \in Q$. Using this definition, a symmetric relation R can be lifted to an equivalence relation in $\Delta(\mathbf{S})$ as follows: $\mu\ R\ \mu'$ iff for every R-closed $Q \in \Sigma$, $\mu(Q) = \mu'(Q)$.

Definition 10. *A relation* $R \subseteq \boldsymbol{S} \times \boldsymbol{S}$ *is a* bisimulation *on the NLMP* $\mathcal{P} = (\boldsymbol{S}, \Sigma, \{\mathcal{T}_a \mid a \in \mathcal{L}\})$ *if it is symmetric and for all* $a \in \mathcal{L}$, $s\ R\ t$ *implies that for all* $\mu \in \mathcal{T}_a(s)$, *there is* $\mu' \in \mathcal{T}_a(t)$ *s.t.* $\mu\ R\ \mu'$. *We say that* $s, t \in S$ *are* bisimilar, *denoted by* $s \sim t$, *if there is a bisimulation* R *such that* $s\ R\ t$.

We know that $\sim$ is an equivalence relation [10]. The next theorem states that $\sim$ is a congruence for parallel composition whenever the resulting composition is indeed an NLMP.

Theorem 11. *Let* $\mathcal{P}_i = (\boldsymbol{S}_i, \Sigma_i, \{\mathcal{T}_a^i \mid a \in \mathcal{L}_i\})$ $i \in \{1,2\}$, *be two NLMPs. If* $\mathcal{P}_1||\mathcal{P}_2$ *is an NLMP, then for all* $s_1, s_1' \in \boldsymbol{S}_1$ *and* $s_2 \in \boldsymbol{S}_2$, *if* $s_1 \sim s_1'$, *then* $s_1||s_2 \sim s_1'||s_2$ *and* $s_2||s_1 \sim s_2||s_1'$.

Proof. We only prove that $s_1||s_2 \sim s_1'||s_2$. The other case is symmetric. Let $R \subseteq \mathbf{S}_1 \times \mathbf{S}_1$ be a bisimulation relation. Define $R' \subseteq (\mathbf{S}_1 \times \mathbf{S}_2) \times (\mathbf{S}_1 \times \mathbf{S}_2)$ by $R' = \{(s_1||s_2, s_1'||s_2) \mid (s_1, s_1') \in R, s_2 \in \mathbf{S}_2\}$. We prove that R' is a bisimulation by doing case analysis on the definition of the transition relation in the parallel composition.

Suppose in general that $s_1||s_2\ R'\ s_1'||s_2$, and consider the case in which $\mathcal{T}_a(s_1||s_2)$ results from (i) in Definition 9. Let $\mu_1 \times \delta_{s_2} \in \mathcal{T}_a(s_1||s_2)$ with $\mu_1 \in \mathcal{T}_a^1(s_1)$. Since $s_1\ R\ s_1'$, there exists $\mu_1' \in \mathcal{T}_a^1(s_1')$ such that $\mu_1\ R\ \mu_1'$. Let $Q \in$

$\Sigma_1 \otimes \Sigma_2$ be R'-closed and define $Q|_{s_2} = \{s_1 \mid s_1||s_2 \in Q\}$. $Q|_{s_2}$ is measurable in Σ_1 [1], and can be easily proven to be R-closed. Now we can calculate:

$$\begin{aligned}(\mu_1 \times \delta_{s_2})(Q) = \ & (\mu_1 \times \delta_{s_2})(Q|_{s_2} \times \{s_2\}) = \mu_1(Q|_{s_2}) \\ \overset{(*)}{=} \ & \mu_1'(Q|_{s_2}) = (\mu_1' \times \delta_{s_2})(Q|_{s_2} \times \{s_2\}) = (\mu_1' \times \delta_{s_2})(Q)\end{aligned}$$

where equality $(*)$ follows from $\mu_1 \ R \ \mu_1'$, and hence $(\mu_1 \times \delta_{s_2}) \ R' \ (\mu_1' \times \delta_{s_2})$.

Case (ii) in Definition 9 follows with a similar analysis, so we focus on case (iii). Let $\mu_1 \times \mu_2 \in \mathcal{T}_a(s_1||s_2)$ with $\mu_1 \in \mathcal{T}_a^1(s_1)$. Since $s_1 \ R \ s_1'$, there exists $\mu_1' \in \mathcal{T}_a^1(s_1')$ such that $\mu_1 \ R \ \mu_1'$. Let $Q \in \Sigma_1 \otimes \Sigma_2$ be R'-closed. Using Fubini's theorem [1], we calculate:

$$\begin{aligned}(\mu_1 \times \mu_2)(Q) = \ & \int_{\mathbf{S}_2}\int_{\mathbf{S}_1} 1_Q(x,y)\ d\mu_1(x)\ d\mu_2(y) = \int_{\mathbf{S}_2}\int_{\mathbf{S}_1} 1_{Q|_y}(x)\ d\mu_1(x)\ d\mu_2(y) \\ = \ & \int_{\mathbf{S}_2} \mu_1(Q|_y)\ d\mu_2(y) \overset{(*)}{=} \int_{\mathbf{S}_2} \mu_1'(Q|_y)\ d\mu_2(y) = (\mu_1' \times \mu_2)(Q)\end{aligned}$$

where 1_Q is the usual characteristic function, and $(*)$ follows from $\mu_1 \ R \ \mu_1'$. Therefore $(\mu_1 \times \mu_2) \ R' \ (\mu_1' \times \mu_2)$. □

Next, we prove that the semantic interpretation of IOSAs and parallel composition commutes, that is, that the NLMP resulting from interpreting a parallel composition of two IOSAs is isomorphic to the parallel composition of the two NLMPs interpreting each of the IOSAs.

Theorem 12. *Given two IOSAs $\mathcal{I}_1$ and $\mathcal{I}_2$, there is an isomorphism between (the reachable parts of) $\mathcal{P}(\mathcal{I}_1||\mathcal{I}_2)$ and $\mathcal{P}(\mathcal{I}_1)||\mathcal{P}(\mathcal{I}_2)$.*

Proof. Let N and M be the number of clocks in $\mathcal{I}_1$ and $\mathcal{I}_2$, respectively. Let $\mathbf{S} = ((\mathcal{S}_1 \times \mathcal{S}_2) \cup \{\mathsf{init}\}) \times \mathbb{R}^{N+M}$ and $\mathbf{S}' = ((\mathcal{S}_1 \times \mathbb{R}^N) \times (\mathcal{S}_2 \times \mathbb{R}^M)) \cup ((\{\mathsf{init}\} \times \mathbb{R}^N) \times (\{\mathsf{init}\} \times \mathbb{R}^M))$ be the states of $\mathcal{P}(\mathcal{I}_1||\mathcal{I}_2)$ and $\mathcal{P}(\mathcal{I}_1)||\mathcal{P}(\mathcal{I}_2)$, respectively[1]. The isomorphism is given by function $f : \mathbf{S} \to \mathbf{S}'$ defined by $f(\mathsf{init}, \vec{v}_1\vec{v}_2) = (\mathsf{init}, \vec{v}_1)||(\mathsf{init}, \vec{v}_2)$, and $f((s_1||s_2), \vec{v}_1\vec{v}_2) = (s_1, \vec{v}_1)||(s_2, \vec{v}_2)$ for all $s_1 \in \mathcal{S}_1$, $s_2 \in \mathcal{S}_2$, and vectors $\vec{v}_1$ and $\vec{v}_2$ which represent valuations on the sets of clocks $\mathcal{C}_1$ and $\mathcal{C}_2$ respectively. f is clearly bijective, and it can be proved straightforwardly that both f and f^{-1} are measurable (i.e. f is *bimeasurable*). From this, it follows that the measurable spaces $(\mathbf{S}, \mathscr{B}(\mathbf{S}))$ and $(\mathbf{S}', \mathscr{B}(\mathbf{S}'))$ are isomorphic.

Following [12], f induces a map $\Delta f : \Delta(\mathbf{S}) \to \Delta(\mathbf{S}')$ defined by $\Delta f(\mu) = \mu \circ f^{-1}$. It is not difficult to prove that Δf is bijective and bimeasurable. Hence, $(\Delta(\mathbf{S}), \Delta(\mathscr{B}(\mathbf{S})))$ and $(\Delta(\mathbf{S}'), \Delta(\mathscr{B}(\mathbf{S}')))$ are isomorphic.

[1] Strictly speaking, $\mathcal{P}(\mathcal{I}_1)||\mathcal{P}(\mathcal{I}_2)$ should also contain states of the form $(s, \vec{v}_1)||(\mathsf{init}, \vec{v}_2)$ and $(\mathsf{init}, \vec{v}_1)||(s, \vec{v}_2)$ with $s \neq \mathsf{init}$. Nonetheless, these states are not reachable. Thus, we do not consider them since otherwise the result would not be strictly an isomorphism and it would only add irrelevant technical problems to the proof.

We can lift f a second time to obtain an isomorphism on hit σ-algebras. Define[2] $Hf : \Delta(\mathscr{B}(\mathbf{S}')) \to \Delta(\mathscr{B}(\mathbf{S}))$ by $Hf = (\Delta f)^{-1}$. Again Hf can be proven to be bijective and bimeasurable and hence, $(\Delta(\mathscr{B}(\mathbf{S})), H(\Delta(\mathscr{B}(\mathbf{S}))))$ and $(\Delta(\mathscr{B}(\mathbf{S}')), H(\Delta(\mathscr{B}(\mathbf{S}'))))$ are isomorphic.

Now, it is not difficult to see that for all $a \in \mathcal{L}$, $\mathcal{T}_a(r) = Hf(\mathcal{T}'_a(f(r)))$ for all $r \in \mathbf{S}$ where $\mathcal{T}_a$ and $\mathcal{T}'_a$ are the transition functions on $\mathcal{P}(\mathcal{I}_1||\mathcal{I}_2)$ and $\mathcal{P}(\mathcal{I}_1)||\mathcal{P}(\mathcal{I}_2)$, respectively. This proves that both NLMPs are isomorphic. □

Given two NLMPs $\mathcal{P}_1$ and $\mathcal{P}_2$ with the same set of labels, the definition of bisimulation can be extended to states in the different NLMPs by constructing the NLMP induced by the coproduct σ-algebra. The NLMP $\mathcal{P}_1 \oplus \mathcal{P}_2$ is defined by the structure $(\mathbf{S}_1 \uplus \mathbf{S}_2, \Sigma_1 \oplus \Sigma_2, \{\mathcal{T}_a \mid a \in \mathcal{L}\})$ where, for all $s \in \mathbf{S}_1 \uplus \mathbf{S}_2$ and $a \in \mathcal{L}$, $\mathcal{T}_a(s) = \mathcal{T}^1_a(s)$ if $s \in \mathbf{S}_1$ and $\mathcal{T}_a(s) = \mathcal{T}^2_a(s)$ if $s \in \mathbf{S}_2$. Thus, if s_1 and s_2 are states of $\mathcal{P}_1$ and $\mathcal{P}_2$ respectively, $s_1 \sim s_2$ whenever they are bisimilar in $\mathcal{P}_1 \oplus \mathcal{P}_2$.

By [12, Proposition 3.6], the next corollary follows immediately from Theorem 12.

Corollary 13. *For any $\vec{v}_1$ and $\vec{v}_2$ representing valuations of clocks in $\mathcal{I}_1$ and $\mathcal{I}_2$, resp., $(\mathsf{init}, \vec{v}_1\vec{v}_2) \sim (\mathsf{init}, \vec{v}_1)||(\mathsf{init}, \vec{v}_2)$ and $((s_1||s_2), \vec{v}_1\vec{v}_2) \sim (s_1, \vec{v}_1)||(s_2, \vec{v}_2)$.*

We say that two IOSAs $\mathcal{I}_1$ and $\mathcal{I}_2$ are bisimilar, notation $\mathcal{I}_1 \sim \mathcal{I}_2$ whenever $(\mathsf{init}, \vec{v}_1) \sim (\mathsf{init}, \vec{v}_2)$ for any vectors $\vec{v}_1$ and $\vec{v}_2$ representing the valuations of clocks in $\mathcal{I}_1$ and $\mathcal{I}_2$, respectively.

Then, the fact that bisimulation equivalence is a congruence on IOSAs follows from Theorem 11 and Corollary 13 and it is stated in the following theorem.

Theorem 14. *Let $\mathcal{I}_1$ and $\mathcal{I}_2$ be two IOSAs such that $\mathcal{I}_1 \sim \mathcal{I}_2$. Then, for any IOSA $\mathcal{I}_3$, $\mathcal{I}_1||\mathcal{I}_3 \sim \mathcal{I}_2||\mathcal{I}_3$ and $\mathcal{I}_3||\mathcal{I}_1 \sim \mathcal{I}_3||\mathcal{I}_2$.*

5 Closed IOSAs are Deterministic

A *closed* IOSA is a IOSA in which all synchronizations have been resolved through parallel composition. Therefore, it has no input actions (i.e. $\mathcal{A}^I = \varnothing$).

In this section we show that a closed IOSA is deterministic in the sense that it is amenable for discrete event simulation or, in case all its clocks are exponentially distributed random variables, also amenable for analysis as a continuous time Markov chain. We will say that a IOSA is deterministic if almost surely at most one discrete transition is enabled at every time point. To avoid referring explicitly to time, we say instead that a IOSA is deterministic if it almost never reaches a state in which two different discrete transitions are enabled.

[2] Note that the domain and image of Hf appear apparently inverted. This is necessary in [12] since they only deal with morphisms, and we are following their definitions. In our case, we could have also defined a direct map from $\Delta(\mathscr{B}(\mathbf{S}))$ to $\Delta(\mathscr{B}(\mathbf{S}'))$ since Δf is bimeasurable, namely $H(f^{-1}) = (\Delta(f^{-1}))^{-1}$.

Definition 15. *A IOSA $\mathcal{I}$ is* deterministic *whenever in $\mathcal{P}(\mathcal{I}) = (\boldsymbol{S}, \mathscr{B}(\boldsymbol{S}), \{\mathcal{T}_a \mid a \in \mathcal{L}\})$, a state $(s, \vec{v}) \in \boldsymbol{S}$ such that $\bigcup_{a \in \mathcal{A} \cup \{\mathsf{init}\}} \mathcal{T}_a(s, \vec{v})$ contains at least two different probability measures, is almost never reached from any $(\mathsf{init}, \vec{v}') \in \boldsymbol{S}$.*

By "almost never" we mean that the measure of the set of all paths leading to a state $(s, \vec{v}) \in \mathbf{S}$ such that $\bigcup_{a \in \mathcal{A} \cup \{\mathsf{init}\}} \mathcal{T}_a(s, \vec{v})$ contains at least two elements is 0. A strictly formal definition of this requires a series of definitions related to schedulers and measures on paths in NLMPs which is not crucial for the developing of the result. (For a formal definition of scheduler and probability measures on paths in NLMPs see [21, Chap. 7].)

The previous definition only makes sense if $\mathcal{P}(\mathcal{I})$ satisfies *time additivity*, *time determinism*, and *maximal progress* [23]. Particularly, by maximal progress we understand that time cannot progress if an output transition is enabled.

Theorem 16. *For a IOSA $\mathcal{I}$, its semantics $\mathcal{P}(\mathcal{I}) = (\boldsymbol{S}, \mathscr{B}(\boldsymbol{S}), \{\mathcal{T}_a \mid a \in \mathcal{L}\})$ satisfies, for all $(s, \vec{v}) \in \boldsymbol{S}$, $a \in \mathcal{A}^O$ and $d, d' \in \mathbb{R}_{>0}$,*

maximal progress: $\mathcal{T}_a(s, \vec{v}) \neq \varnothing \;\Rightarrow\; \mathcal{T}_d(s, \vec{v}) = \varnothing$
time determinism: $\mu, \mu' \in \mathcal{T}_d(s, \vec{v}) \;\Rightarrow\; \mu = \mu'$, *and*
time additivity: $\delta^{-d}_{(s,\vec{v})} \in \mathcal{T}_d(s, \vec{v}) \wedge \delta^{-d'}_{(s,\vec{v}-d)} \in \mathcal{T}_{d'}(s, \vec{v} - d) \;\Leftrightarrow\; \delta^{-(d+d')}_{(s,\vec{v})} \in \mathcal{T}_{d+d'}(s, \vec{v})$.

Proof. Notice that if $\mathcal{T}_a(s, \vec{v}) \neq \varnothing$, with $a \in \mathcal{A}^O$, then there exists a transition $s \xrightarrow{\{x_j\}, a, C'} s'$ such that $\vec{v}(j) \leq 0$. Suppose by contradiction that $\mathcal{T}_d(s, \vec{v}) \neq \varnothing$, then $0 < d \leq \min\{\vec{v}(i) \mid \exists a \in \mathcal{A}^O, C' \subseteq \mathcal{C}, s' \in S : s \xrightarrow{\{x_i\}, a, C'} s'\} \leq \vec{v}(j) \leq 0$, which is a contradiction.

Time determinism is immediate by Definition 3 since either $\mathcal{T}_d(s, \vec{v}) = \{\delta^{-d}_{(s,\vec{v})}\}$ or $\mathcal{T}_d(s, \vec{v}) = \varnothing$.

For time additivity, let $\hat{d} = \min\{\vec{v}(i) \mid \exists a \in \mathcal{A}^O, C \subseteq \mathcal{C}, s' \in \mathcal{S} : s \xrightarrow{\{x_i\}, a, C} s'\}$. Suppose $\delta^{-d}_{(s,\vec{v})} \in \mathcal{T}_d(s, \vec{v})$ and $\delta^{-d'}_{(s,\vec{v}-d)} \in \mathcal{T}_{d'}(s, \vec{v} - d)$. By Definition 3, $0 < d \leq \hat{d}$ and $0 < d' \leq \hat{d} - d$, i.e. $0 < d + d' \leq \hat{d}$. Thus $\delta^{-(d+d')}_{(s,\vec{v})} \in \mathcal{T}_{d+d'}(s, \vec{v})$. Suppose now that $\delta^{-(d+d')}_{(s,\vec{v})} \in \mathcal{T}_{d+d'}(s, \vec{v})$. Then $0 < d + d' \leq \hat{d}$ and thus $0 < d \leq \hat{d}$ and $0 < d' \leq \hat{d} - d$, which implies that $\delta^{-d}_{(s,\vec{v})} \in \mathcal{T}_d(s, \vec{v})$ and $\delta^{-d'}_{(s,\vec{v}-d)} \in \mathcal{T}_{d'}(s, \vec{v} - d)$. □

The following is the main theorem of this section.

Theorem 17. *Every closed IOSA is deterministic.*

The rest of the section is devoted to proving this theorem. From now on, we work with the closed IOSA $\mathcal{I} = (\mathcal{S}, \mathcal{C}, \mathcal{A}, \rightarrow, s_0, \mathcal{C}_0)$, with $|\mathcal{C}| = N$, and its semantics $\mathcal{P}(\mathcal{I}) = (\mathbf{S}, \mathscr{B}(\mathbf{S}), \{\mathcal{T}_a \mid a \in \mathcal{L}\})$. We recall that IOSAs only admit sampling clock values from continuous random variables, which is essential for the validity of Theorem 17.

For every state $s \in \mathcal{S}$, let $\mathit{active}(s) = \{x \mid s \xrightarrow{\{x\}, a, C} s'\}$ be the set of active clocks at state s. By Definition 1(d) it follows that $\mathit{active}(s') \subseteq (\mathit{active}(s) \backslash \{x\}) \cup C$ whenever $s \xrightarrow{\{x\}, a, C} s'$.

The idea of the proof of Theorem 17 is to show that the property that all active clocks have non-negative values and they are different from each other is almost surely an invariant of $\mathcal{I}$, and that at most one transition is enabled in every state satisfying such invariant. Formally, the invariant is the set

$$\begin{aligned}\mathsf{Inv} = &\{(s,\vec{v}) \mid \ s \in \mathcal{S}, \vec{v}(i) \neq \vec{v}(j), \text{ and } \vec{v}(i) \geq 0 \\ &\text{for all } x_i, x_j \in \mathit{active}(s) \text{ with } i \neq j\} \cup (\{\mathsf{init}\}\times\mathbb{R}^N) \end{aligned} \tag{4}$$

therefore, its complement set is

$$\begin{aligned}\mathsf{Inv}^c = \ &\{(s,\vec{w}) \mid s \in \mathcal{S}, \vec{w}(i) = \vec{w}(j) \text{ for some } x_i, x_j \in \mathit{active}(s) \text{ with } i \neq j\} \\ \cup \ &\{(s,\vec{w}) \mid s \in \mathcal{S}, \vec{w}(i) < 0 \text{ for some } x_i \in \mathit{active}(s)\} \end{aligned} \tag{5}$$

The next lemma states that Inv^c is almost never reached in one step from a state satisfying the invariant.

Lemma 18. *For all $(s,\vec{v}) \in \mathsf{Inv}$, $a \in \mathcal{L}$, and $\mu \in \mathcal{T}_a(s,\vec{v})$, $\mu(\mathsf{Inv}^c) = 0$.*

Proof. We proceed analyzing by cases, according a is init, in $\mathcal{A}$, or in $\mathbb{R}_{>0}$.

For $a = \mathsf{init}$, we only consider states of the form $(\mathsf{init},\vec{v})$ since $\mathcal{T}_{\mathsf{init}}(s,\vec{v}) \neq \varnothing$ iff $s = \mathsf{init}$. So, let $\mu \in \mathcal{T}_{\mathsf{init}}(\mathsf{init},\vec{v})$. Then $\mu = \delta_{s_0} \times \prod_{i=1}^N \mu_{x_i}$. Since each μ_{x_i} is a continuous probability measure (hence the likelihood that two clocks are set to the same value is 0) and $\mu_{x_i}(\mathbb{R}_{>0}) = 1$, then $\mu(\mathsf{Inv}^c) = 0$.

For $a \in \mathcal{A}$, take $\mu \in \mathcal{T}_a(s,\vec{v})$ with $(s,\vec{v}) \in \mathsf{Inv}$. Notice that $s \in \mathcal{S}$. By Definition 3 and because $\mathcal{I}$ is closed, there exists $s \xrightarrow{\{x\},a,C} s'$ with $\vec{v}(i) \leq 0$ and $\mu = \mu_{\vec{v},C,s'} = \delta_{s'} \times \prod_{i\in I} \mu_{x_i} \times \prod_{j\in J} \delta_{\vec{v}(j)}$ where $I = \{i \mid x_i \in C\}$ and $J = \{j \mid x_j \notin C\}$.

For each $x_i, x_j \in \mathit{active}(s')$ define $\mathsf{Inv}^c_{ij} = \{(s'',\vec{w}) \mid s'' \in \mathcal{S}, \vec{w}(i) = \vec{w}(j)\}$ whenever $i \neq j$, and $\mathsf{Inv}^c_i = \{(s'',\vec{w}) \mid s'' \in \mathcal{S}, \vec{w}(i) < 0\}$. Notice that $\mathsf{Inv}^c = \bigcup \mathsf{Inv}^c_{ij} \cup \bigcup \mathsf{Inv}^c_i$ and, since the unions are finite, $\mu(\mathsf{Inv}^c) = 0$ iff $\mu(\mathsf{Inv}^c_{ij}) = 0$ and $\mu(\mathsf{Inv}^c_i) = 0$, for every i, j. In the following, we show this last statement.

Let $x_i \in \mathit{active}(s')$. Then $x_i \in (\mathit{active}(s)\backslash\{x\})\cup C$. If $x_i \in C$, then $\mu(\mathsf{Inv}^c_i) = 0$ because $\mu_i(\mathbb{R}_{\geq 0}) = 1$. If instead $x_i \in \mathit{active}(s)\backslash\{x\}$, then $\mu(\mathsf{Inv}^c_i) = 0$ because $\delta_{\vec{v}(i)}(\mathbb{R}_{\geq 0}) = 1$, since $(s,\vec{v}) \in \mathsf{Inv}$ and hence $\vec{v}(i) \geq 0$.

Let $x_i, x_j \in \mathit{active}(s')$ with $i \neq j$. Then $x_i, x_j \in (\mathit{active}(s)\backslash\{x\})\cup C$. If $x_i \in C$ then μ_i is a continuous probability measure and hence $\mu(\mathsf{Inv}^c_{ij}) = 0$. Similarly if $x_j \in C$. If instead $x_i, x_j \in \mathit{active}(s)\backslash\{x\}$, then $\delta_{\vec{v}(i)} \neq \delta_{\vec{v}(j)}$ because $(s,\vec{v}) \in \mathsf{Inv}$ and hence $\vec{v}(i) \neq \vec{v}(j)$. Therefore $\mu(\mathsf{Inv}^c_{ij}) = 0$. This proves that $\mu(\mathsf{Inv}^c) = 0$ for this case.

Finally, take $d \in \mathbb{R}_{>0}$ and suppose that $\mathcal{T}_d(s,\vec{v}) = \{\delta^{-d}_{(s,\vec{v})}\}$ with $(s,\vec{v}) \in \mathsf{Inv}$. Notice that $s \in \mathcal{S}$. By Definition 3, $0 < d \leq \min\{\vec{v}(k) \mid s \xrightarrow{\{x_k\},a,C'} s', a\in\mathcal{A}^O\}$ and $\delta^{-d}_{(s,\vec{v})} = \delta_s \times \prod_{i=1}^N \delta_{\vec{v}(i)-d}$. We take sets Inv^c_{ij} and Inv^c_i as before and follow a similar reasoning. For $x_i \in \mathit{active}(s)$, $\vec{v}(i)-d \geq \min\{\vec{v}(k) \mid s \xrightarrow{\{x_k\},a,C'} s', a\in\mathcal{A}^O\} - d \geq 0$ and hence $\delta_{\vec{v}(i)-d}(\mathbb{R}_{\geq 0}) = 1$. Therefore $\mu(\mathsf{Inv}^c_i) = 0$. For $x_i, x_j \in \mathit{active}(s)$ with $i\neq j$, $\delta_{\vec{v}(i)-d} \neq \delta_{\vec{v}(j)-d}$ because

$(s, \vec{v}) \in \mathsf{Inv}$ and hence $\vec{v}(i) \neq \vec{v}(j)$. So $\mu(\mathsf{Inv}^c_{ij}) = 0$. This proves that $\mu(\mathsf{Inv}^c) = 0$ for this case, and hence the lemma. □

From Lemma 18 we have the following corollary.

Corollary 19. *The set* Inv^c *is almost never reachable in* $\mathcal{P}(\mathcal{I})$.

The proof of the corollary requires, again, the definitions related to schedulers and measures on paths in NLMPs. We omit it here since the proof eventually boils down to directly applying Lemma 18 and seeing that the measure of all paths leading to a state in Inv^c is 0 for all possible schedulers.

The next lemma states that any state in the invariant Inv has at most one discrete transition enabled.

Lemma 20. *For all* $(s, \vec{v}) \in \mathsf{Inv}$, *the set* $\mathit{enabled}(s, \vec{v}) = \bigcup_{a \in \mathcal{A} \cup \{\mathsf{init}\}} \mathcal{T}_a(s, \vec{v})$ *is either a singleton set or the empty set.*

Proof. By Definition 3, $\mathit{enabled}(\mathsf{init}, \vec{v}) = \mathcal{T}_{\mathsf{init}}(s, \vec{v}) = \{\delta_{s_0} \times \prod_{i=1}^{N} \mu_{x_i}\}$, which proves this case. So, let $(s, \vec{v}) \in \mathsf{Inv}$ with $s \in \mathcal{S}$ and suppose that $\mathit{enabled}(s, \vec{v}) \neq \varnothing$. By Definition 3, there is at least one transition $s \xrightarrow{\{x_i\}, a, C} s'$ such that $\vec{v}(i) \leq 0$. Because, $(s, \vec{v}) \in \mathsf{Inv}$ and $x_i \in \mathit{active}(s)$, then $\vec{v}(i) = 0$ and for all $x_j \in \mathit{active}(s)$ with $i \neq j$, $\vec{v}(j) > 0$. Condition (c) in Definition 1 ensures that there is no other transition $s \xrightarrow{\{x_i\}, b, C'} s''$ and, as a consequence, $\mathit{enabled}(s, \vec{v})$ is a singleton set. □

Finally, the proof of Theorem 17 is a direct consequence of Corollary 19 and Lemma 20.

Proof (of Theorem 17). Let $\mathsf{En}_{\geq 2} = \{(s, \vec{v}) \in \mathbf{S} \mid |\mathit{enabled}(s, \vec{v})| \geq 2\}$. By Corollary 19, $\mathsf{En}_{\geq 2} \subseteq \mathsf{Inv}^c$. Therefore, by Lemma 20, $\mathsf{En}_{\geq 2}$ is almost never reachable. □

6 Conclusion

We introduced IOSA, a stochastic and compositional modeling formalism which turns to be deterministic when all synchronizations are resolved, i.e., the IOSA models a closed system. It supports arbitrary continuous probability distributions to model the stochastic timed behavior of a system. These characteristics make it highly suitable for modeling and simulating systems with more realistic results than Markov models such as CTMCs. Moreover, in case the model uses only exponential distributions, the closed IOSA is amenable to analysis as a CTMC.

As we have already mentioned, our work is related to [22]. This work presents an input/output variant of probabilistic automata where outputs are locally controlled, and hence their occurrence time is governed by exponential distributions, while inputs are externally controlled. Thus it also has the

generative/reactive view. In these settings, a closed system forms a CTMC. Our mathematical treatment and theirs is nonetheless very different since the memoryless nature of the exponential distribution can be encoded directly rather than through clocks. Also related to our work, it is the work on weak determinism by Crouzen [6, Chap. 8]. Rather than ensuring by construction that the model is deterministic, this work provides a technique based on Milner's [19, Chap. 11] that, by doing some static analysis, determines if a model, given as a composite I/O-IMC (an input/output variant of IMCs [17]), is weak bisimilar to a deterministic I/O-IMC. The technique may report false negatives.

Currently, we are using IOSA as input language for a discrete event simulation tool —a successor of Bluemoon [5]—that is being developed in our group, and plan to use it as an intermediate language to compile from graphical modeling languages.

Acknowledgments. We thank Pedro Sánchez Terraf for the help provided in measure theory, and Carlos E. Budde for early discussions on IOSAs.

References

1. Ash, R., Doléans-Dade, C.: Probability and Measure Theory. Academic Press, Cambridge (2000)
2. Bogdoll, J., Ferrer Fioriti, L.M., Hartmanns, A., Hermanns, H.: Partial order methods for statistical model checking and simulation. In: Bruni, R., Dingel, J. (eds.) FORTE 2011 and FMOODS 2011. LNCS, vol. 6722, pp. 59–74. Springer, Heidelberg (2011)
3. Bohnenkamp, H.C., D'Argenio, P.R., Hermanns, H., Katoen, J.: MODEST: a compositional modeling formalism for hard and softly timed systems. IEEE Trans. Softw. Eng. **32**(10), 812–830 (2006)
4. Bravetti, M., D'Argenio, P.R.: Tutte le algebre insieme: concepts, discussions and relations of stochastic process algebras with general distributions. In: Baier, C., Haverkort, B.R., Hermanns, H., Katoen, J.-P., Siegle, M. (eds.) Validation of Stochastic Systems. LNCS, vol. 2925, pp. 44–88. Springer, Heidelberg (2004)
5. Budde, C.E., D'Argenio, P.R., Hermanns, H.: Rare event simulation with fully automated importance splitting. In: Beltrán, M., Knottenbelt, W.J., Bradley, J.T. (eds.) Computer Performance Engineering. LNCS, vol. 9272, pp. 275–290. Springer International Publishing, Switzerland (2015)
6. Crouzen, P.: Modularity and Determinism in Compositional Markov Models. Ph.D. thesis, Universität des Saarlandes, Saarbrücken (2014)
7. D'Argenio, P.R.: Algebras and Automata for Timed and Stochastic Systems. Ph.D. thesis, University of Twente, Enschede (1999)
8. D'Argenio, P.R., Katoen, J.P.: A theory of stochastic systems part I: stochastic automata. Inf. Comput. **203**(1), 1–38 (2005)
9. D'Argenio, P.R., Legay, A., Sedwards, S., Traonouez, L.: Smart sampling for lightweight verification of Markov decision processes. STTT **17**(4), 469–484 (2015)
10. D'Argenio, P.R., Sánchez Terraf, P., Wolovick, N.: Bisimulations for nondeterministic labelled Markov processes. Math. Struct. Comput. Sci. **22**(1), 43–68 (2012)

11. Desharnais, J., Edalat, A., Panangaden, P.: Bisimulation for labelled Markov processes. Inf. Comput. **179**(2), 163–193 (2002)
12. Doberkat, E.E., Sánchez Terraf, P.: Stochastic non-determinism and effectivity functions. J. Logic Comput. (2015, to appear). doi:10.1093/logcom/exv049
13. Gburek, D., Baier, C., Klüppelholz, S.: Composition of stochastic transition systems based on spans and couplings. In: ICALP 2016. LIPICS (2016, to appear)
14. Giry, M.: A categorical approach to probability theory. In: Banaschewski, B. (ed.) Categorical Aspects of Topology and Analysis. Lecture Notes in Mathematics, vol. 915, pp. 68–85. Springer, Heidelberg (1982)
15. van Glabbeek, R.J., Smolka, S.A., Steffen, B.: Reactive, generative and stratified models of probabilistic processes. Inf. Comput. **121**(1), 59–80 (1995)
16. Hartmanns, A., Timmer, M.: Sound statistical model checking for MDP using partial order and confluence reduction. STTT **17**(4), 429–456 (2015)
17. Hermanns, H.: Interactive Markov Chains: and the Quest for Quantified Quality. Springer, Heidelberg (2002)
18. Larsen, K.G., Skou, A.: Bisimulation through probabilistic testing. Inf. Comput. **94**(1), 1–28 (1991)
19. Milner, R.: Communication and Concurrency. Prentice-Hall Inc., Upper Saddle River (1989)
20. Viglizzo, I.: Coalgebras on Measurable Spaces. Ph.D. thesis, Indiana University, Argentina (2005)
21. Wolovick, N.: Continuous Probability and Nondeterminism in Labeled Transition Systems. Ph.D. thesis, Universidad Nacional de Córdoba, Argentina (2012)
22. Wu, S., Smolka, S.A., Stark, E.W.: Composition and behaviors of probabilistic I/O automata. Theor. Comput. Sci. **176**(1–2), 1–38 (1997)
23. Yi, W.: Real-time behaviour of asynchronous agents. In: Baeten, J.C.M., Klop, J.W. (eds.) CONCUR '90 Theories of Concurrency: Unification and Extension. LNCS, vol. 458, pp. 502–520. Springer, Heidelberg (1990)