A theory for the semantics of continuous systems with stochastic and structural non-determinism*

Carlos E. Budde

FaMAF, Universidad Nacional de Córdoba – CONICET

cbudde@famaf.unc.edu.ar

Abstract

We report an approach to modelling the semantics of complex systems, comprising non-deterministic and stochastic behaviour inside continuous domains. The theory is based on the mathematical field of measure theory, and extends labelled Markov processes (LMP) with internal non-determinism. We show how the bisimulation relation can be understood in different manners, and mention the known boundaries between the different resulting definitions. We also review a variant of Hennessy-Milner logic that provides logical characterizations of some of these bisimulations.

1 Introduction

The description of complex systems involving physical or biological components usually requires modelling involved continuous behaviour induced by variables such as time, distance, temperature, etc. Situations showing both non-deterministic and stochastic behaviour naturally arise in these scenarios.

Mobile devices are a good example. They operate in discrete (memory hierarchy) as well as continuous (position, battery voltage, etc.) state spaces. The latter may be perturbed by the environment in a stochastically quantifiable way, and discrete probabilities may be used by internal algorithms. Moreover, the software operates over meshes of devices where the relative execution speeds are not known in advance, thus leading to unpredictable time interleavings. Observations of discrete values like buttons enabledness, and of continuous values like displayed roll angle in a cell phone, are part of these systems.

Examples of this kind exceed the modelling capabilities of Markov processes with continuous-state spaces or continuous time evolution (or both): they also need the consideration of non-determinism. Many formal frameworks have been defined to study them from a process algebra perspective (see [4] and references therein). A prominent work on this area, based on well understood mathematical foundations, is that of *labelled Markov processes (LMP)* [4,7,9]. However LMP theory does not consider *internal* non-determinism, i.e. non-determinism which can not be resolved by an external entity. This is a drawback since such behaviour immediately arises in the analysis of systems, e.g. when abstracting internal activity, or because of state abstraction techniques such as model checking.

Many variants of continuous Markov processes filling that gap have been defined. Following the approach of Desharnais, Panangaden, et al. [4, 7, 9, etc.] we extended LMP with internal non-determinism using measure theory. This led to our development of *non-deterministic labelled Markov processes (NLMP)* [2, 5, 6, 11]. Here we review a proper restriction of NLMP denominated *structured non-deterministic labelled Markov processes (SNLMP)*. This abstract is based on the research reported in [2, 3].

*Supported by ANPCyT project PICT 2012-1823, SeCyT-UNC project 05/B497 and program 05/BP02, and EU 7FP grant agreement 295261 (MEALS).

2 Structured non-deterministic labelled Markov processes

SNLMP can be introduced as transition systems with stochastic and non-deterministic labelled transitions over a continuous state space. Moreover, structure must be imposed over the state and the label spaces, in order to obtain some basic desired properties. This is done by means of σ-algebras.

A *σ-algebra* on an arbitrary set S is a collection $\Sigma \subseteq 2^S$ closed under complement and denumerable union. Elements of Σ are called *measurable sets*, and (S, Σ) is a *measurable space*. A σ-additive function $\mu : \Sigma \to [0, 1]$ such that $\mu(S) = 1$ is called a *probability measure*. Let $\Delta(S)$ denote the set of all probability measures over (S, Σ), then $\Delta(\Sigma)$ is defined as the smallest σ-algebra containing all sets $\Delta^B(Q) \doteq \{\mu \in \Delta(S) \mid \mu(Q) \in B\}$, where $Q \in \Sigma$ and B is a Borel set in $[0, 1] \subseteq \mathbb{R}$. A function $f : S_1 \to S_2$ is *measurable* if the inverse image through f of a measurable set is also a measurable set.

Definition 1. *A* structured non-deterministic labelled Markov process *(SNLMP for short) is a structure $(S, \Sigma, L, \Lambda, T)$ where Σ is a σ-algebra on the set of states S, Λ is a σ-algebra on the set of labels L so that $\{a\} \in \Lambda$ for all $a \in L$, and $T : S \to \Lambda \otimes \Delta(\Sigma)$ is measurable.*

Due to the measurability requirement over T, we need to endow the codomain $\Lambda \otimes \Delta(\Sigma)$ with a σ-algebra. This is a key construction for the development of SNLMP theory, and of NLMP in general.

Definition 2. *Let $\lambda \in \Lambda$ and $\xi \in \Delta(\Sigma)$, then $H(\Lambda \times \Delta(\Sigma))$ is defined as the smallest σ-algebra containing all sets $H_{\lambda \times \xi} = \{\theta \in \Lambda \otimes \Delta(\Sigma) \mid \theta \cap (\lambda \times \xi) \neq \emptyset\}$.*

In Def. 1, transition function T maps each state $s \in S$ to a measurable set $T(s) \subseteq L \times \Delta(S)$ of labels and probability measures. If $(a, \mu) \in T(s)$ then a is an enabled action in s, and μ is a probability measure that s can reach through label a. In particular, internal non-determinism is encoded via the a-section of $T(s)$, denoted by $T(s)|_a$ and defined as the (possibly uncountable) set of measures $\{\mu \in \Delta(S) \mid (a, \mu) \in T(s)\}$. Notice this is the set of all measures reached from state s through action a.

Motivations for the various aspects of Def. 1 and 2 can be found in [2, 5, 11]. In particular the next example illustrates the need for the measurability restriction imposed over the transition relation T.

Example 1. *Let $S \doteq \{t\} \uplus [0, 1]$ and $L \doteq \{a, b\}$ be endosed with the standard Borel spaces, $T(t) \doteq \{(a, \mu)\}$ for fixed measure μ, and $\forall r \in [0, 1] : T(r) \doteq$* **if** *$(r \in V)$* **then** *$\{(b, \delta_1)\}$* **else** *$\emptyset$, where V is a Vitali set. Notice that $T(s)$ is measurable in $\Lambda \otimes \Delta(\Sigma)$ for all $s \in S$. Starting in t, suppose some scheduler (also "adversary" or "policy", see [11]) chooses to do 'a' first and 'b' second. Then the probability of such executions cannot be measured, as it requires to apply μ to the non-measurable set $T^{-1}(H_{\{a\} \times \Delta(S)}) = V$.* □

3 Bisimulation relation(s)

The original definition of bisimulation given by Larsen and Skou [8] has been generalized to a continuous setting (see e.g. [1, 7]). The resulting definitions closely resemble Larsen and Skou's, the only difference being that two measures are considered equivalent if they agree in every measurable union of equivalence classes induced by the relation.

In our theory this definition is instantiated using the a-section $T(\cdot)|_a$, which is a measurable function since $T(s)$ and $\{a\}$ are measurable as well. We also use the lifting over $\Delta(S)$ of a relation $R \subseteq S \times S$, defined as follows: given $\mu, \nu \in \Delta(S)$ then $\mu \, R \, \nu$ iff for every R-closed set $Q \in \Sigma$ it holds that $\mu(Q) = \nu(Q)$.

Definition 3. *A relation R is a* state bisimulation *on the SNLMP $(S, \Sigma, L, \Lambda, T)$, if it is symmetric and for all $s, t \in S$ and $a \in L$, $s R t$ implies that for every $\mu \in T(s)|_a$ there exists $\nu \in T(t)|_a$ s.t. $\mu R \nu$. We say states $s, t \in S$ are* state bisimilar*, denoted by $s \sim_s t$, if there is a state bisimulation R such that $s R t$.*

Relation $\sim_s$ is the largest state bisimulation and it is also an equivalence relation [5, 11].

The definition of state bisimulation is point-wise and not "event-wise" as one should expect in a measure-theoretic realm, since R has no measurability restrictions. Indeed, as shown in [4], a state bisimulation can distinguish more states than the underlying σ-algebra. In [4] a measure-theory aware notion of behavioural equivalence is presented. On the same lines here we define *event bisimulation* on SNLMP.

Definition 4. *An* event bisimulation *on the SNLMP* $(S, \Sigma, L, \Lambda, T)$ *is a sub-σ-algebra* Ξ *of* Σ *s.t.* $T : (S, \Xi) \to (\Lambda \otimes \Delta(\Sigma)\,,\ H(\Lambda \otimes \Delta(\Xi)))$ *is measurable.*

The notion of event bisimulation can be extended to relations: R is an event bisimulation if there exists an event bisimulation Ξ s.t. $R = \mathcal{R}(\Xi)$. More generally, two states $s, t \in S$ are called *event bisimilar*, denoted by $s \sim_e t$, if there is an event bisimulation Ξ such that $s\ \mathcal{R}(\Xi)\ t$. Just like for state bisimulation, relation $\sim_e$ is the largest event bisimulation and it is also an equivalence relation [2].

For SNLMP we define a third notion of behavioural equivalence which we call *hit bisimulation*. Rather than looking point-wise at probability measures as state bisimulations do, hit bisimulation follows the idea of Def. 2, and verifies that both $T(s)|_a$ and $T(t)|_a$ *hit* the same measurable sets of probability measures, considering only R-closed sets.

Definition 5. *A relation R is a* hit bisimulation *on the SNLMP* $(S, \Sigma, L, \Lambda, T)$ *if it is symmetric and for all $a \in L$, $sR\,t$ implies that for every $\xi \in \Delta(\Sigma(R))$, $T(s)|_a \cap \xi \neq \emptyset \Leftrightarrow T(t)|_a \cap \xi \neq \emptyset$. We say states $s, t \in S$ are* hit bisimilar*, denoted by $s \sim_h t$, if there is a hit bisimulation R such that $sR\,t$.*

Again here we have that $\sim_h$ is an equivalence relation and the largest of hit bisimulations. As it happens, hit bisimulation can be equivalently defined using intersections of whole measurable sets (i.e. $T(s) \cap \theta$) rather than restricting to single labels with $T(s)|_a$. For details see [2, Thm. 5.2].

Hit bisimulations relate to event bisimulations in different ways. In particular R is a hit bisimulation if and only if $\Sigma(R)$ is an event bisimulation. This is the result that leads to the fact that $\sim_h$ is also an event bisimulation, and hence $\sim_h \subseteq \sim_e$. On the other hand a state bisimulation is also a hit bisimulation, so an immediate consequence is that $\sim_s \subseteq \sim_h$, with proper inclusion in the general case. Interestingly, all three definitions coincide on *image denumerable* SNLMP (an SNLMP is image denumerable if for all $a \in L$ and $s \in S$ the set $T(s)|_a$ is denumerable).

4 Logical characterization

We provide a Hennessy-Milner-like logic for SNLMP that characterizes event bisimulation in general and all three notions under some conditions. The logic is related to that of Parma and Segala [10]. The main difference is that we consider two kinds of formula: φ productions are interpreted on states and ψ productions are interpreted on measures. Also, the action modality considers a measurable set of actions rather than a single label. The syntax is:

$$\varphi \ \equiv\ \top \mid \varphi_1 \wedge \varphi_2 \mid \langle\lambda\rangle\psi \qquad\qquad \psi \ \equiv\ \textstyle\bigvee_{i\in I} \psi_i \mid \neg\psi \mid [\varphi]_{\geqslant q}$$

where $\lambda \in \Lambda$, I is a denumerable index set, and $q \in \mathbb{Q} \cap [0, 1]$. In particular the modality $\langle a\rangle\psi$ of [5, 10] corresponds to $\langle\{a\}\rangle\psi$. We denote by $\mathcal{L}$ the set of all formulas generated by the first production and by $\mathcal{L}_\Delta$ the set generated by the second.

The semantics is defined with respect to SNLMP $(S, \Sigma, L, \Lambda, T)$ in the following way;

$$\begin{aligned} [\![\top]\!] &= S & [\![\textstyle\bigvee_{i\in I} \psi_i]\!] &= \textstyle\bigcup_i [\![\psi_i]\!] \\ [\![\varphi_1 \wedge \varphi_2]\!] &= [\![\varphi_1]\!] \cap [\![\varphi_2]\!] & [\![\neg\psi]\!] &= [\![\psi]\!]^{\mathsf{c}} \\ [\![\langle\lambda\rangle\psi]\!] &= T^{-1}(H_{\lambda\times[\![\psi]\!]}) & [\![[\varphi]_{\geqslant q}]\!] &= \Delta^{\geq q}([\![\varphi]\!]) \end{aligned}$$

Notice that $\langle\lambda\rangle\psi$ is satisfied at a state s whenever there is some measure μ reachable from s by an action in λ that satisfies ψ, and that $[\varphi]_{\geqslant q}$ is satisfied by a measure μ whenever $\mu([\![\varphi]\!]) \geqslant q$.

Sets $[\![\varphi]\!]$ and $[\![\psi]\!]$ are measurable in Σ and $\Delta(\Sigma)$ respectively, and it can be proved that $\mathcal{L}$ completely characterizes event bisimulation, i.e. $\mathcal{R}(\mathcal{L}) = \sim_{\mathrm{e}}$. Together with the previously discussed relations between the different bisimulations, this shows that state and hit bisimulation are sound for $\mathcal{L}$, i.e., they preserve the validity of formulas. Formally: $\sim_{\mathrm{s}} \subseteq \sim_{\mathrm{h}} \subseteq \sim_{\mathrm{e}} = \mathcal{R}(\mathcal{L})$.

These inclusions can not be reversed in general. Nevertheless, for image-finite processes over analytic spaces it can be proved that logic $\mathcal{L}$ is complete for state bisimilarity, and hence all bisimulation notions are the same inside said restricted setting. Therefore given an image-finite SNLMP $(S, \Sigma, L, \Lambda, T)$ where (S, Σ) is analytic, for all $s, t \in S$ we have that

$$s \sim_{\mathrm{s}} t \quad \Leftrightarrow \quad s \sim_{\mathrm{h}} t \quad \Leftrightarrow \quad s \sim_{\mathrm{e}} t \quad \Leftrightarrow \quad s \,\mathcal{R}(\mathcal{L})\, t \,.$$

5 Concluding remarks

In the general setting of NLMP, hit bisimulation is the preferred notion of behavioural equivalence. On the one hand, state bisimulation distinguishes non-measurable sets and therefore it distinguishes beyond the structure of the state space (see [5]). On the other hand, event bisimulation fails to distinguish (measurable sets of) deadlock states.

The lack of structure on the labels is the key in the counterexamples that show the differences between the bisimulations on NLMP. This motivated the introduction of SNLMP [2, 3, 11]. In this case we know that $\sim_{\mathrm{s}} \subseteq \sim_{\mathrm{h}}$, though it remains unclear if such inclusion is proper. The most pertinent question therefore is whether that is actually the case, and if so then how do these bisimulations differ. We do known however that $\sim_{\mathrm{h}} \neq \sim_{\mathrm{e}}$ [2, 3]. From a probabilistic point of view $\sim_{\mathrm{e}}$ seems the best choice, since the only events it fails to tell apart have measure zero. Still, there is not yet enough study on the subject to guarantee the distinguishing power of $\sim_{\mathrm{e}}$ suffices for general purposes.

References

[1] M. Bravetti and P.R. D'Argenio. Tutte le algebre insieme: Concepts, discussions and relations of stochastic process algebras with general distributions. In *Validation of Stochastic Systems*, volume 2925 of *LNCS*, pp. 44–88. Springer, 2004.

[2] C.E. Budde. No determinismo completamente medible en procesos probabilísticos continuos. Master's thesis, FaMAF, Universidad Nacional de Córdoba, 2012.

[3] C.E. Budde, P.R. D'Argenio, N. Wolovick, and P. Sánchez Terraf. A theory for the semantics of stochastic and non-deterministic continuous systems. *Submitted*, 2013.

[4] V. Danos, J. Desharnais, F. Laviolette, and P. Panangaden. Bisimulation and cocongruence for probabilistic systems. *Inf. & Comp.*, 204:503–523, 2006.

[5] P.R. D'Argenio, P. Sánchez Terraf, and N. Wolovick. Bisimulations for non-deterministic labelled Markov processes. *Mathematical. Structures in Comp. Sci.*, 22(1):43–68, February 2012.

[6] P.R. D'Argenio, N. Wolovick, P. Sánchez Terraf, and P. Celayes. Nondeterministic labeled Markov processes: Bisimulations and logical characterization. In *Proc. of QEST 2009*, pp. 11–20. IEEE Computer Society, 2009.

[7] J. Desharnais. *Labeled Markov Process*. PhD thesis, McGill University, 1999.

[8] K.G. Larsen and A. Skou. Bisimulation through probabilistic testing. *Inf. & Comp.*, 94(1):1–28, 1991.

[9] P. Panangaden. *Labelled Markov Processes*. Imperial College Press, 2009.

[10] A. Parma and R. Segala. Logical characterizations of bisimulations for discrete probabilistic systems. In *Proc. of FOSSACS 2007*, volume 4423 of *LNCS*, pp. 287–301. Springer, 2007.

[11] N. Wolovick. *Continuous probability and nondeterminism in labeled transaction systems*. PhD thesis, Universidad Nacional de Córdoba, 2012.