Towards a Formal Framework for Multidimensional Codesign

Manuela L. Bujorianu[1] and Marius C. Bujorianu[2]

[1] *Faculty of Computer Science, Unversity of Twente, The Netherlands,*
email: L.M.Bujorianu@cs.utwente.nl
[2] *Computer Laboratory, University of Kent, UK,* email: M.C.Bujorianu@kent.ac.uk

Abstract. Multidimensional codesign is a recently proposed paradigm for integrating different system dimensions in sensor networks. Examples of such dimensions are logical and physical mobility, continuous and discrete transitions, deterministic and random evolutions and features resulting from their interaction, like deterministic and stochastic hybrid behaviours. In this paper, we propose a unifying computational model that considers multiple dimensions, inspired by the Hilbertian Formal Methods paradigm. We couple this model with an integration framework based on domain theory. In this framework new dimensions can be incrementally added, and we illustrate this technique by adding logical mobility to the computational model. The new model has a very promising modelling power, offering all formal ingredients of a neural network. We further investigate bisimulation for systems mixing physical and logical mobility. We identify and solve a compatibility problem between bisimulation relations arising from mobility and continuous behaviours.
Keywords: *distributed embedded systems, mobility, stochastic processes, bisimulation, domain theory.*

1 Introduction

Nowadays, anyone can easily observe an explosive development in distributed embedded systems like sensor networks, gene regulatory networks and other system biology areas. A general tendency in this development is the integration of very different features, like mobility, randomness, continuity and discrete / continuous mixed behaviors. Formal methods that should mathematically support this development are still largely focussed on one area or another. In this paper, we present two formal mechanisms for developing a formal framework, in which these various features can be investigated altogether. One mechanism consists of a unifying axiomatization of deterministic and stochastic automata, in the spirit of the recently introduced paradigm called Hilbertian formal methods [10, 11]. The second one proposes a generic technique based on the categorical domain theory for adding new features to an existing model. This mechanism constitutes a formal approach to a recent development paradigm called *multidimensional codesign* [16, 9]. In the limited space of this paper, we restrict our presentation to a class of systems that mix continuous evolutions with logical mobility. These systems appear especially in medical applications of embedded systems, where mathematical models based on differential equations abound. Concretely, networked systems of genes or sensors are difficult to investigate formally because the lack of a formal framework to integrate such features.

Continuous behaviors have been investigated formally mostly in the area of hybrid systems. In most applications, the continuous behaviors are associated with man made technical systems (like engines, transmission systems, etc.) and their mathematical description consists of rather very simple differential equations. In the case of embedded systems, the continuous evolutions of the environment often involve very complex mathematical descriptions. For example, in a meteo system, a continuous evolution is described by a system containing up to one hundred partial differential equations. In the case of a cardiac implant, the continuous evolutions are subject to randomized changes. The main difficulty in developing formal methods for such systems is given by their very different mathematical foundations. When probabilities are considered, fundamental system properties are lost, like the uniquely determined system trajectory by an initial state. The idea of considering two different approaches, one for the deterministic case and one for the stochastic, is not feasible in practice. The selection of the environment characteristics that should be considered by the embedded controller is subject to frequent changes. The interaction between different characteristics is often not entirely mathematically understood and the initial deterministic model turns into a stochastic one. In the case of two different formal approaches, the addition of new functionalities would involve a complete redesign and a replacement of the old controllers. That can be very costly, especially if, for example, the sensor network has been placed in a geographical position difficult to access (think at a military application) or if a gene network must be re-created (to obtain accurate biological cultures in genetics is still a very complex process). The first main contribution of this paper is a unifying semantic framework, in which both deterministic and stochastic environment behaviors can be modelled.

The second contribution of this paper focuses on the possibility to introduce logical mobility in the framework described above. We consider the categorical formalization of the π-calculus introduced and developed by Glynn Winskel and his co-authors [12]. This formalization relies on heavy categorical algebra and therefore we discuss only how Winskel's calculus can be used. In principle, Winskel's approach is constructed generically using an abstract model of computation specified as a category. The subtle point of this construction is that, in this category, a computational equivalence, described in terms of open maps must exist. When this category consists of labelled transition systems, as used in process algebra, the computational equivalence becomes the familiar concept of bisimulation. The mobile processes are then described as presheaves on this category. The computational equivalence between the mobile processes is then borrowed from this category via Yoneda embedding. We extend the behaviors of continuous systems with mobile processes by constructing suitable categories to replace this category. Obviously, there are many categories of continuous processes in the literature (especially in control theory), but these can not be used because the computational equivalence by open maps can not be defined. The main contribution of this paper is to construct a category of models of computation that unifies deterministic and stochastic evolutions and for which the open maps can be defined and generate an equivalence relation.

From a mathematical viewpoint, the paper follows two main streams. The first part uses intensively the general theory of Markov processes to introduce a unifying model of concurrent embedded systems and its concept of bisimulation. We show that this general concept of bisimulation subsumes the bisimulation of deterministic continuous and hybrid dynamical systems introduced and investigated by Tabuada e.a [19] using open maps. In the second part, an approach based on category theory enriches the previous model with first order mobility, such that the bisimulation relation for mobile processes is compatible with the stochastic bisimulation.

2 A quick tour on continuous processes

In this section we give some background of on Markov processes necessary to understand the contribution of this paper. As well, we present the class of semi-dynamical systems, which can be thought of as "Markov processes" that "degenerated" into determinism, or what "Markov processes" would be if its transition probabilities would be given by some Dirac distributions[1]. For studying Markov processes specific parameterization have been developed. When the process is deterministic these analytical tools characterize the semi-dynamical systems.

2.1 Markov Processes

The stochastic processes we consider here are randomized systems with a continuous state space, where the "noise" can be measured using transition probability measures. Markov processes form a subclass of stochastic systems for which, at any stage, future evolutions are conditioned only by the present state (in other words, they do not depend on the past).

The state space is denoted by X. The basic assumption is that one can reason about state change using probabilities. Then the state space should be a measurable space. Suppose that X is a Polish or analytic space. A Polish space is a topological space, which is a homeomorphic image of complete separable metric space. The continuous image of a Polish space is called an analytic space. We consider X equipped with its Borel σ-algebra $\mathcal{B}$ (i.e. the σ-algebra generated by all open sets). We adjoin an extra point Δ (the cemetery or deadlock point) to X as an isolated point, $X_\Delta = X \cup \{\Delta\}$. Let $\mathcal{B}(X_\Delta)$ be the Borel σ-algebra of X_Δ.

In the following, we will use intensively the set of all bounded measurable numerical functions on X denoted by $\mathbf{B}(X)$. Mathematically, this set can be thought of as a lattice (with the natural pointwise order between numerical functions, or as an additive monoid $S = (\mathbf{B}(X), +, 0)$. These functions can be thought as abstract states (configurations) of the given system or, some formulas in an appropriate logic. Moreover, $\mathbf{B}(X)$ is also a *Banach space* with respect to the sup-norm and the natural pointwise algebraic operations which give its linear structure.

A probability space $(\Omega, \mathcal{F}, P)$ is fixed and all $X-$valued random variables are defined on this probability space. The trajectories in the state space are modelled by a family of random variables (x_t) where t denotes the time. The reasoning about state change is carried out by a family of probabilities P_x one for each state $x \in X$. The construction is similar to the coalgebraic reasoning in the semantics of specification languages: the system behavior is described by given for each state the possible evolutions. For Markov processes, for each state x, the probability $P_x(x_t \in A)$ to reach a given set of state $A \subset X$ (provided that A is measurable) starting from x describes the system evolution. We remark two ingredients that make the difference from the deterministic case: the evolutions are described from an initial state to a set of final set (nondeterminism) and all we know is a probability to have such trajectories (uncertainty). This is the sense how a semigroup of operators (which will be defined in the following) is abstracting a Markov process.

Formally, let $M = (\Omega, \mathcal{F}, \mathcal{F}_t, x_t, P, P_x)$ be a strong Markov process (see the definition, for example, in [18]). Strong Markov property means that the Markov property is still true with respect to the stopping times of the process M. Recall that a $[0, \infty]$-valued function τ on Ω is called an $\{\mathcal{F}_t\}$-*stopping time* if $\{\tau \leq t\} \in \mathcal{F}_t, \forall t \geq 0$. In particular, any Markov chain is a strong Markov process. The trajectories of M are modelled by a family of X-valued random variables (x_t), which, as functions of time, can have some continuity properties (as the càdlàg property, i.e. right continuous with left limits). $\mathcal{F}_t$ is the σ-algebra generated by the random variables x_s, $s \leq t$, and it describes the history of the process up to the time t.
The stochastic analysis identifies concepts (like infinitesimal generator, semigroup of operators, resolvent of operators) that characterize in an abstract sense the evolutions of a Markov process. Under standard assumptions, all these concepts are equivalent, in the sense that given one concept then all the others can be constructed from it. For a detailed presentation of these

[1] Recall that the Dirac measure $\delta_x(A)$, for $x \in X$ and $A \in \mathcal{B}(X)$ is equal to 1 iff $x \in A$, and 0 otherwise.

notions and the connections between them, the reader can consult, for example, [18]. These tools can be further used to define a very general concept of bisimulation.

2.2 Deterministic dynamical systems

Markov processes are generalizations of semidynamical[2] in continuous time [28]. Note that these (semi-dynamical) systems are not supposed to be continuous. They might be thought of as restrictions of dynamical systems to the positive time interval.

Definition 1. *[21] A semi-dynamical system is a function* ϕ*:* $\mathbb{R}_+ \times X_\Delta \to X_\Delta$ *such that*
1. ϕ *is a measurable map; 2.* $\phi(0, x) = x$*;*
3. $\phi(t_1 + t_2, x) = \phi(t_1, \phi(t_2, x))$
4. $\phi(t, x) = \Delta \Rightarrow \phi(s, x) = \Delta, \forall s \geq t$*;*
5. $\phi(t, x) = \phi(t, y), \forall t > 0 \Rightarrow x = y$*.*

The *life time* of the system ϕ is the map $\zeta : X_\Delta \to [0, \infty]$ defined by $\zeta(x) = \inf\{t \geq 0 | \phi(t, x) = \Delta\}$. We can suppose without loosing the generality that for all $x \in X$ the life time $\zeta(x) > 0$. For each $x \in X$ the *trajectory* starting from x is

$$\Gamma_x = \{\phi(t, x) | t \in [0, \zeta(x))\}.$$

The semi-dynamical system ϕ is called *transient* if there exists $(A_n) \subset \mathcal{B}$ such that $X = \bigcup_{n \in \mathbb{N}} A_n$ and

$$\forall x \in X : m\{t \in [0, \infty) | \phi(t, x) \in A_n\} < \infty$$

where m is the Lebesgue measure.

2.3 A unifying framework

We can abstract away a set of common properties of Markov processes and semidynamical systems. These properties are defined less operational but rather algebraic. This unifying method derives from the so-called weak solutions of differential equations. For equations where solutions can not be computed, the existence and important analytic properties of the solutions can be established. The key point is to consider a larger space of elements that contains the solutions. A typical example of such a space constitutes $\mathbf{B}(X)$. The differential operator becomes then a linear operator on a subset of this large space. Again this operator is too complex and it is replaced by a time-indexed family of "approximating" simpler operators. This approximating family is the so-called semigroup of operators.

A family $\{P_t : \mathbf{B}(X) \to \mathbf{B}(X), t \geq 0\}$ of linear operators on $\mathbf{B}(X)$ is called *semigroup of operators* if the following conditions are satisfied:

- semigroup property: $P_t P_s = P_{t+s}$, $t, s \geq 0$;
- contraction property: $||P_t f|| \leq ||f||$, $f \in \mathbf{B}(X)$.

In addition, if $\lim_{t \to 0} P_t f = f$, then (P_t) is called *strongly continuous* semigroup.

This concept has enough components to allow us to define powerful analytic tools such as the operator resolvent and the infinitesimal generator.

To each operator semigroup $\mathcal{P} = (P_t)$ on the Banach space $\mathbf{B}(X)$, the following mathematical objects can be associated:

[2] dynamical system with pozitive time

1. The *resolvent of operators* $\mathcal{V} = (V_\alpha)_{\alpha\geq 0}$ associated to $\mathcal{P}$ is the Laplace transform of $\mathcal{P}$, given by formula
$$V_\alpha f(x) = \int_0^\infty e^{-\alpha t} P_t f(x) dt.$$
2. The *kernel operator,* denoted by V, is the initial operator V_0 of $\mathcal{V}$ (for $\alpha = 0$).
3. The *infinitesimal generator* of $\mathcal{P}$ is the possibly unbounded linear operator $\mathcal{A}$ defined by:
$$\mathcal{A}f = \lim_{t\searrow 0} \frac{P_t f - f}{t} \tag{1}$$
The domain $D(\mathcal{A})$ is the subspace of $\mathbf{B}(X)$ for which this limit exists.

Let us have a closer look on the infinitesimal generator. If (P_t) is a strongly continuous contraction semigroup then $D(\mathcal{A})$ is dense. In addition, $\mathcal{A}$ is closed, that is if $f_n \in D(\mathcal{A})$ converges to f and $\mathcal{A}f_n$ converges to g then $g \in D(\mathcal{A})$ and $\mathcal{A}f = g$.

The following definition is inspired by a condition from the Hille-Yosida theorem (Th. 2.6, Chapter 1 in [18]).

A linear operator $\mathcal{A}$ has the Hille-Yosida property if for all $\lambda > 0$, the operator $\lambda I - \mathcal{A}$ has an everywhere defined inverse $R(\lambda, \mathcal{A})$ such that $\|\lambda R(\lambda, \mathcal{A})\| \leq 1$ (To say $\lambda\ I - \mathcal{A}$ has an everywhere defined inverse means that the operator $\lambda\ I - \mathcal{A}$ is injective on the domain of $\mathcal{A}$ and that its range is all of X.)

We have now all ingredients to introduce an unifying concept for deterministic and stochastic continuous processes.

Definition 2. *An abstract continuous system (ACS) consists of:*

- *a state space X, with the structure of a Polish/analytic space;*
- *a bounded linear operator $\mathcal{A}$ on $\mathbf{B}(X)$ that is densely defined and has the Hille-Yosida property;*
- *an operator semigroup $\mathcal{P} = (P_t)$ on $\mathbf{B}(X)$ such that $\mathcal{A}$ is the infinitesimal generator associated to $\mathcal{P}$.*

The Hille-Yosida theorem gives necessary and sufficient conditions for a linear operator to be the generator of a strongly continuous, positive contraction semigroup. It results from the Hille-Yosida theorem that the last component of an ACS is superfluous because it can be derived from the second component. We decided to keep it in the definition motivated by practical reasons. The Hille-Yosida theorem is non-constructive and in the most practical situations the expression of the semigroup is known.

On the state space X of an ACS we can define a *preorder relation* $\prec$ as
$$x \prec y \Longleftrightarrow Vf(y) \leq Vf(x), \forall f \in \mathbf{B}(X), f \geq 0. \tag{2}$$

Now, let see how the framework looks like for a Markov process M.
Let $\mathcal{P} = (P_t)_{t>0}$ denote the family of linear *operators* associated to M, which maps $\mathbf{B}(X_\Delta)$ into itself given by
$$P_t f(x) = \int f(y) p_t(x, dy) = E_x f(x_t), \forall x \in X \tag{3}$$
where E_x is the expectation w.r.t. P_x. We make the standard assumption that $f(\Delta) = 0$. The Chapman-Kolmogorov property ensures that this family of operators has indeed the semigroup property. This is a strongly continuous semigroup of operators.

For each $t > 0$, the function $P_t f$ applied in a state $x \in X$ is the expectation of the image of the measurable function f applied to the states at the time t of those trajectories of the process that start in x at time 0. In other words, $P_t f$ describes the transition probability of the abstract state of the system at time t.

To the semigroup $\mathcal{P}$ given by (3), one can associate its operator resolvent $\mathcal{V}$ and its infinitesimal generator $\mathcal{A}$. Conversely, given an operator semigroup $\mathcal{P}$, one can check if it might be associated to a Markov process (for necessary and sufficient conditions to ensure that the semigroup can be interpreted as a semigroup of conditional expectations see Th. 2.2, Chapter 4, [18]). The importance of the infinitesimal generator for a Markov process is briefly explained in the following paragraph.

The evolution of a continuous time Markov process can be described in very much the same terms as those used for discrete time processes. Many difficulties may arise in the analysis, especially when the state space is infinite. The way out of these difficulties is too complicated to describe in detail here, and the reader should look elsewhere [18]. Even for continuous time Markov chains the things are quite difficult. The general scheme is as follows. For discrete-time processes the n-step transition probabilities can be written in a matrix form and expressed them in terms of the one-step matrix (usually denoted by $\mathbf{P}$ and called the *stochastic matrix* associated to a discrete time Markov chain). In continuous time there is no exact analogue of $\mathbf{P}$ since there is no implicit unit length of the time. The infinitesimal calculus offers one way to plug this gap. For example, for continuous time Markov chains there exists a matrix $\mathbf{G}$ (such that $P_t = \exp(t\mathbf{G})$), called the *generator* of the chain, which takes over the role of $\mathbf{P}$. For more general continuous time Markov processes (when the state space is infinite), the matrix $\mathbf{G}$ becomes the linear operator $\mathcal{A}$ defined by (1) using the operator semigroup given by (3).

The following assumption is essential for the mathematical reasoning presented in this paper.

Assumption 1 *Suppose that M is a* transient Markov process, *i.e. there exists a strict positive Borel measurable function q such that Vq is a bounded function.*

The transience of M means that for any Borel set E in X and for almost all trajectories there exists a finite stopping time t^* such that $x_t \notin E$ for all $t > t^*$ (for more explanations about the transience property see [14]).

Using (2), we can define a preorder relation $\prec_M$ associated to M. Intuitively, $\prec_M$ is the order on the trajectories of M. In particular, if M degenerates in a semi-dynamical system, $\prec_M$ is exactly the order relation on the trajectories.

Now we instantiate the framework with semi-dynamical systems. With every semi-dynamical system ϕ one can associate the *semigroup of operators* $\mathcal{P} = (P_t)_{t>0}$ defined by

$$P_t f(x) = f(\phi(t, x)) \tag{4}$$

for all functions $f \in \mathbf{B}(X_\Delta)$. The standard assumption $f(\Delta) = 0$ is in force. For each $t > 0$, the function $P_t f$ applied in a state $x \in X$ is the image of the measurable function f at that point corresponding to the time t of the flow $\phi(\cdot, x)$ (which starts in x at time 0). In other words, $P_t f$ describes the abstract state of the system at time t or how a logical formula f is changed after the time t.

If in the semigroup formula (4), we take $f = I_A$ with $A \in \mathcal{B}$ (the indicator function of a measurable set A) then $P_t I_A(x) = I_A(\phi(t, x))$, i.e. it takes the value one iff $\phi(t, x) \in A$, otherwise it is equal to zero (see [21] and the references therein, for more properties of the semigroup associated to a semi-dynamical system).

Remark 1. The semigroup formula (4) can be derived as a particular case of (3), taking the transition probabilities

$$p_t(x, \cdot) = \delta_{\phi(t,x)}(\cdot), t \geq 0$$

where $\delta_{\phi(t,x)}$ is the Dirac distribution corresponding to $\phi(t,x)$.

In a standard way, to the semigroup (4), one can associate its resolvent $\mathcal{V}$ and its generator $\mathcal{A}$.

Remark 2. If $A \in \mathcal{B}$ then $VI_A(x)$ is exact the Lebesgue measure of those moments of time $t \geq 0$ for which the trajectory Γ_x has a non-empty intersection with A.

We denote $x \prec_\phi y$ if there exists $t \in [0,\infty)$ such that $y = \phi(t,x)$. If the system under consideration is transient then $\prec_\phi$ is an *order relation* [21]. This order relation can be characterized using the initial resolvent kernel (Prop. 13 [5]) via (2).

3 Bisimulation in the Presence of Probability and Continuity

In this section we define a bisimulation concept for abstract continuous systems, organized in a category. We further instantiate this category for continuous time, continuous space Markov processes.

In the first subsection, we discuss a general view of the methodology for defining bisimulation for Markov processes. In the remainder of the section, this methodology will be generalized using operator parameterizations of stochastic processes, in order to make it applicable to a general category of Markov processes. The resulting concept of bisimulation will be compared with a concept of bisimulation via open maps (as introduced by Winskel et.a. [22]) for continuous dynamical system by P. Tabuada, G. Pappas et.a. - see [19] and its references) and of bisimulation for different classes of Markov chains (build on the ideas of Panangaden, Edalat e.a. [4, 17] and of Larsen and Skou [23]).

3.1 Algebraic concepts of bisimulation

For ACS, the open maps definition of bisimulation can not be adapted straightforward. The main problem is how to define the simulation morphisms and the open maps.

In a category, a semi-pullback means that, for any pair of morphisms $\varphi^1 : M^1 \to M$ and $\varphi^2 : M^2 \to M$ (M^1, M^2, M are objects in that category) there exists an object M^0 and morphisms $\pi^i : M^0 \to M^i$ ($i = 1, 2$) such that

$$\varphi^1 \circ \pi^1 = \varphi^2 \circ \pi^2.$$

We develop a concept of *unifying bisimulation* for ACS defined on Polish/analytic spaces, which can be instantiated with the bisimulation defined for different particular classes of Markov processes studied in the literature. A zigzag morphism between two ACS should 'commute' with the infinitesimal operators of the processes considered. Then the bisimulation relation is naturally given via zigzag morphism spans between ACS. Moreover, the category of ACS defined on Polish/analytic spaces with these zigzag morphisms as arrows has semi-pullback. Therefore, the bisimulation relation is an equivalence relation.

We also derive from the above bisimulation for ACS, a notion of bisimulation for (deterministic) semi-dynamical systems. For dynamical systems, we prove that our concept of zigzag morphism and the open map concept, defined in [19], are equivalent.

3.2 A Category of abstract continuous systems

We define the category **ACS** of abstract continuous systems, which has as:

1. objects - a countable set of ACS, defined on Polish/analytic spaces, denoted $S^1, S^2, ...$
2. arrows - zigzag morphisms, which will be defined in the following.

The aim of this subsection is to give an appropriate definition of these *zigzag morphisms* (and of *simulation morphisms*) between such processes, which will allow us to define a general concept of unifying bisimulation in this category.

The main difference with respect to the similar notions from [17], is that we require some *global conditions* written in terms of infinitesimal generators (associated to the ACSs considered) to be satisfied by these morphisms. Our choice is motivated by the fact that, in general, the transition probabilities depend on time and their computation, for each moment of time $t > 0$, is not practically possible.

Let S^1 and S^2 be two objects of **ACS**. The state space of S^1 (resp. S^2) is $X^{(1)}$ (resp. $X^{(2)}$). For any mapping $\psi : X^{(2)} \to X^{(1)}$, we denote by ψ^* the *action* of ψ on the their monoids of bounded measurable functions, i.e. $\psi^* : \mathbf{B}(X^{(1)}) \to \mathbf{B}(X^{(2)})$ given by

$$\psi^* f = f \circ \psi, \forall f \in \mathbf{B}(X^{(1)}) \tag{5}$$

Let $\mathcal{A}^1$ and $\mathcal{A}^2$ the infinitesimal generators of S^1 and S^2, with the domains $D(\mathcal{A}^1)$ and $D(\mathcal{A}^2)$, respectively. The following assumption is essential for defining the arrows in the category **ACS**.

Assumption 2 *If $f \in D(\mathcal{A}^1)$ then $\psi^* f \in D(\mathcal{A}^2)$, i.e. the twisted function ψ^* can action between the domains of the generators $\mathcal{A}^1$ and $\mathcal{A}^2$:*

$$\psi^* : D(\mathcal{A}^1) \to D(\mathcal{A}^2)$$

Definition 3. *A simulation morphism between the processes S^2 and S^1 (the process S^1 simulates the process S^2) is a measurable, monotone increasing, continuous application $\psi : X^{(2)} \to X^{(1)}$ such that it satisfies the Assumption 2 and*

$$\mathcal{A}^2 \circ \psi^* \leq \psi^* \circ \mathcal{A}^1$$

where $\mathcal{A}^1$ (resp. $\mathcal{A}^2$) is the infinitesimal generator associated to S^1 (resp. S^2) and ψ^* is given by (5).

Definition 4. *A surjective simulation morphism ψ between the processes S^2 and S^1 is called zigzag morphism if the condition from the Def. 3 holds with equality, i.e.*

$$\mathcal{A}^2 \circ \psi^* = \psi^* \circ \mathcal{A}^1 \tag{6}$$

Using the relationships between generator, operator semigroup and kernel operator (see, for example, [18]), we can prove the following result.

Proposition 1. *A surjective simulation morphism ψ between the processes S^2 and S^1 is a zigzag morphism iff for almost all $t \geq 0$ (i.e. except with a zero Lebesgue measure set of times) the following equality holds*

$$P_t^2 \circ \psi^* = \psi^* \circ P_t^1 \tag{7}$$

where (P_t^1) (resp. (P_t^2)) is the semigroup of operators associated to S^1 (resp. S^2).

The relation (7) is known in the literature by the name of *Dynkin intertwining relation* [15].

Corollary 1. *A surjective simulation morphism ψ between S^2 and S^1 is a zigzag morphism iff for almost all $t \geq 0$ (i.e. except with a zero Lebesgue measure set of times) and for all $E \in \mathbf{B}(X^{(1)})$ and $x^2 \in X^{(2)}$, the following equality holds*

$$p_t^2(x^2, \psi^{-1}(A)) = p_t^1(\psi(x^2), A) \tag{8}$$

where (p_t^1) (resp. (p_t^2)) is the transition probability functions associated to S^1 (resp. S^2).

This corollary illustrates that the simulating process can make all the transitions of the simulated process with the same transition probabilities than in the process being simulated. Moreover, this corollary illustrates that the zigzag morphism introduced in this section is a natural generalization of the similar concept defined for particular classes of Markov processes in [4, 17].
The monotony of a zigzag morphism ψ can be derived from the condition satisfied by a zigzag morphism. Roughly speaking, this means that whilst the process S^2 evolves from u to $\psi^{-1}(A)$ ($A \in \mathcal{B}(X^{(1)})$) on a trajectory with a given probability, the process S^1 evolves from $\psi(u)$ to A with the same probability.

3.3 Bisimulation

We consider the category **ACS** defined in the previous section. Then, we define the *bisimulation* between two processes in this category as the existence of a span of zigzag morphisms between them.

Definition 5. *Let S^1 and S^2 be two objects in* **ACS**. *S^1 is bisimilar to S^2 (written $S^1 \sim S^2$) if there exists a span of zigzag morphisms between them, i.e. there exists S^{12} (object in* **ACS***) and two zigzag morphisms ψ^1 and ψ^2 as follows: $X^{(1)} \stackrel{\psi^1}{\leftarrow} X^{12} \stackrel{\psi^2}{\rightarrow} X^{(2)}$.*

Theorem 1. *The category* **ACS** *has semi-pullbacks.*

Proof. Suppose that S^1, S^2, S are three ACS defined on the Polish/analytic spaces $X^{(1)}, X^{(2)}, X$, respectively. Assume that there exist two zigzag morphisms

$$\psi^1 : X^{(1)} \to X,\ \psi^2 : X^{(2)} \to X.$$

Our goal is to prove that there exists another object $S^0 \in$ **ACS** and two zigzag morphisms $\pi^1 : X^{(0)} \to X^{(1)}$ and $\pi^2 : X^{(0)} \to X^{(2)}$ such that the following diagram commutes

$$\begin{array}{ccccc} & & X^{(0)} & & \\ & \stackrel{\pi^1}{\swarrow} & & \stackrel{\pi^2}{\searrow} & \\ X^{(1)} & & & & X^{(2)} \\ & \underset{\psi^1}{\searrow} & & \underset{\psi^2}{\swarrow} & \\ & & X & & \end{array}$$

First step is to construct the desired ACS S^0. The state space of S^0 will be defined as

$$X^{(0)} = \{(x^1, x^2) | \psi^1(x^1) = \psi^2(x^2)\}.$$

Let now have a closer look at the space $X^{(0)}$:

– it is a nonempty space since ψ^1 and ψ^2 are supposed surjective,
– it is a topological space because it can be naturally equipped with the trace topology of the product topology on $X^{(1)} \times X^{(2)}$,
– it is a Polish/analytic space because it is a closed subset of the space $X^{(1)} \times X^{(2)}$. The product space $X^{(1)} \times X^{(2)}$ is a Polish/analytic space because it is the product of two such spaces.

Now we can define S^0 as the restriction to $X^{(0)}$ of $S^1 \otimes S^2$ (the product of S^1, S^2).

Denote by $\mathcal{A}^1$, $\mathcal{A}^2$ the infinitesimal generators associated with S^1 and S^2. According to [29], the product process $S^1 \otimes S^2$ (which is still an object in **ACS**) has the infinitesimal generator given by the smallest closed extension of the operator defined on $D(\mathcal{A}^1) \otimes D(\mathcal{A}^2)$ by Trotter formula [29]

$$\mathcal{A}(f \otimes g) = \mathcal{A}^1(f) \otimes g + f \otimes \mathcal{A}^2(g), \tag{9}$$

where $f \in D(\mathcal{A}^1)$ and $g \in D(\mathcal{A}^2)$. The domain of the generator $\mathcal{A}$ denoted by $D(\mathcal{A})$ includes $D(\mathcal{A}^1) \otimes D(\mathcal{A}^2)$. Note that we can use Trotter formula (9) because the operator semigroups of S^1 and S^2 are strongly continuous (as it results considering the Hille-Yosida theorem).
For all $f \in D(\mathcal{A})$ that vanish outside $X^{(0)}$, the generator of S^0 is related with the generator of $S^1 \otimes S^2$ by

$$\mathcal{A}^0 f = \mathcal{A}(f)$$

The second step is to find suitable zigzag morphisms π^1 and π^2. These can be taken as the projection maps. The surjectivity of π^1 or π^2 can be easily derived using the surjectivity of ψ^1 and ψ^2 and the definition of $X^{(0)}$.

Using Trotter formula (9), it follows that these projection maps are indeed zigzag morphisms. For example, for π^1, we have $\pi^{1*}f \in D(\mathcal{A}^0)$ if $f \in D(\mathcal{A}^1)$ (it depends only on x^1 and $\mathcal{A}^2$ does not change it). Then

$$\mathcal{A}^0(\pi^{1*}f)(x^1, x^2) = (\mathcal{A}^1 f)(\pi^1(x^1, x^2))$$

for all $(x^1, x^2) \in X^{(0)}$. The equality $\psi^1 \circ \pi^1 = \psi^2 \circ \pi^2$ trivially holds.□

An immediate corollary of the existence of semi-pullbacks in the category **ACS** is the following.

Proposition 2. *The bisimulation in the category* **ACS** *is an equivalence relation.*

Bisimulation is difficult to understand especially because of unavailability of the next state concept. In most cases, bisimulation has a computational understanding described in terms of next transition in each system. Random trajectories with discrete steps are treated globally using metrics, topologies, etc. When the continuous and probabilistic features interact new system properties emerge. Typical examples of this kind of properties are:

– a continuous or hybrid system trajectory is not uniquely determined anymore and
– the system may switch between possible trajectories according to some probability distributions. In this way, the trajectory space itself has contiguous properties.

The emerging properties make system analysis very difficult and their treatment requires a global approach based on topological and stochastic analysis methods. Therefore, the computational equivalence, usually implied by bisimulation for discrete and deterministic hybrid systems, needs to be explained in specific mathematical terms.

3.4 Particular cases

In this subsection we investigate the cases when all objects of **ACS** have the same type.

In the case when all objects are Markov processes we obtain a generalization **GMP** of the category defined in [7].

In the case of Markov models, we say that a Markov process M^1 *simulates* another Markov M^2 if there exists a surjective continuous morphism $\psi : X^2 \to X^1$ between their state spaces such that each transition probability on X^2 'is matched' by a transition probability on X^1. The meaning of this 'matching' is that for each measurable set $A \subset X^1$ and for each $u \in X^2$ we have

$$p_t^2(u, \psi^{-1}(A)) \leq p_t^1(\psi(u), A) \qquad \forall t \geq 0 \qquad\qquad (*)$$

where (p_t^2) and (p_t^1) are the transition functions corresponding to M^2, respectively to M^1. Such a morphism ψ is called *simulation morphism*. The open maps are replaced then by the *zigzag morphisms*, which are simulation morphism for which the above condition holds with equality.

For continuous time Markov processes, a simulation condition as before is hard to be checked because the time t runs in a 'continuous' set. Therefore, it is required to provide supplementary assumptions about the transition probabilities of the processes we are talking about. This kind of simulation morphisms and zigzag morphisms have been defined for some particular classes of Markov processes: for discrete/continuous time Markov chains [23], for labelled Markov processes and for step Markov processes (which are natural extensions of Markov chain to processes with continuous space), defined on Polish or analytic spaces (see [17] and the references therein). The categories considered there have, as objects, the above Markov models, and, as morphisms, the zigzag morphisms. Then the concept of bisimulation for these categories is given in a 'classical' way [22]. For example, two labelled Markov processes are probabilistically bisimilar if there exists a *span of zigzag morphisms* between them. Here, we underlie another reason why only some special kind of Markov processes is considered. This bisimulation relation is always reflexive and symmetric. But the transitivity of such a relation (the bisimulation should be an equivalence relation) is usually implied by the existence of *semi-pullbacks* in the Markov process category considered [22, 17].

In the categories of labelled or stationary Markov processes, the construction of the semi-pullback is strongly based on the stationarity property of the Markov processes considered [17]. In this case the transition probabilities do not depend on time! Then the construction mechanism of the semi-pullback in such categories of Markov processes is reduced to the construction of the semi-pullback in the category of transition probability functions and surjective transition probability preserving Borel maps (as morphisms in the respective category).

Our approach is more general and somehow more elegant. The unifying bisimulation has, by far, considerably many and more general instantiations. Moreover, the analytic machinery of generators is more readable compared with the lengthy technical arguments involving transition probabilities.

In the case when all objects are semi-dynamical systems, we obtain a new category **SD**. In fact, **SD** is a full subcategory of **ACS**.

Proposition 3. *A surjective simulation morphism $\psi : X^{(2)} \to X^{(1)}$ between two semi-dynamical systems ϕ^2 and ϕ^1 is a zigzag morphism if and only if*

$$\int_0^\infty P_t^2(\psi^* f)dt = \int_0^\infty \psi^*[(P_t^1 f)]dt, \forall f \in \mathbf{B}(X^{(1)}),\ f \geq 0, \tag{10}$$

where (P_t^1) and (P_t^2) are the semigroups of kernels associated to ϕ^1 and ϕ^2.

Proposition 4. *The condition (10) is equivalent with*

$$\psi(\phi^2(t,u)) = \phi^1(t,x) \ (m - a.e. \ w.r.t. \ t \geq 0) \tag{11}$$

for all $u \in X^{(2)}$ *such that* $x = \psi(u)$.

Corollary 2. *If* ψ *is a zigzag morphism between two semi-dynamical systems* ϕ^2 *and* ϕ^1 *then*

$$\psi(\Gamma_u^2) = \Gamma_{\psi u}^1$$

except a set of times with Lebesgue measure zero.

Proposition 5. *For dynamical systems a zigzag morphism is exactly an open map in the sense of [19].*

Proof. A zigzag morphism is monotone, i.e. if $u \prec_{\phi^2} v$ then $\psi u \prec_{\phi^1} \psi v$, or in other words if the system ϕ^2 evolves from u to v in the time t, then the system ϕ^2 evolves from ψu to ψv in the same period of time t. Therefore, it 'transforms trajectories in trajectories', and then it is an open map according to the characterization of open maps (Prop.11, [19]).

Therefore, the bisimulation for dynamical systems given in terms of zigzag morphisms is exactly the bisimulation given in terms of open maps [19].

In the light of the Corollary 2, a zigzag morphism ψ between two semi-dynamical systems ϕ^2 and ϕ^1 induces an equivalence relation (bisimulation) on the state of trajectories of ϕ^2 as follows:

Definition 6. *Two trajectories* Γ_u^2 *and* Γ_v^2 *are equivalent if and only if their initial points are bisimilar, i.e.* $\psi u = \psi v$.

4 Mobile Markovian Systems

4.1 A categorical concept of bisimulation for mobile processes

In a series of papers (see [12], [13] and the references therein) G. Winskel and coworkers defined a generic model of mobile processes, where each process is a presheaf.

We use the category theory notations from [1]. In particular, arrow composition, denoted by ;, is the sequential composition. For example, for two functions F, g this means $f;g = g \circ f$.

In the following we define the concept of bisimulation for presheaves.

A *preashef* over a category $\mathbf{P}$ is a functor from $\mathbf{P}$ to $\mathbf{Set}$, the category of sets and functions. The preasheaves over the same category, together with the natural transformations between them, form a category, denoted $\widehat{\mathbf{P}}$. This construction comes accompanied by the Yoneda lemma [1], which provides a functor

$$y_{\mathbf{P}} : \mathbf{P} \to \widehat{\mathbf{P}}, y_{\mathbf{P}}(A) = \mathbf{P}(\_, A)$$

which fully and faithfully embeds $\mathbf{P}$ into $\widehat{\mathbf{P}}$. Basically the Yoneda lemma ensures a preashef representation for every category $\mathbf{P}$: it can be regarded as a full subcategory of $\widehat{\mathbf{P}}$.

The bisimulation of mobile processes is the standard open bisimulation from open maps, as introduced in [22].

Now we give the definition of functors preserving open maps. Given two categories, $\mathbf{P}$ and $\mathbf{Q}$, and a functor F between them, an arrow $f : X \to Y$ is called $F-$open if, for every commuting square

$$\begin{array}{ccc} F(A) & \xrightarrow{\alpha} & X \\ F(g)\downarrow & & \downarrow f \\ F(B) & \xrightarrow[\beta]{} & Y \end{array}$$

there is an arrow $\gamma : F(B) \to X$ such that $F(g); \gamma = \alpha$ and $\gamma; f = \beta$. The isomorphisms are $F-$open and the all $F-$open maps form a subcategory. In it is proved [13] that an arrow between presheaves in $\widehat{\mathbf{P}}$ is $\mathbf{P}$-open iff it $y_{\mathbf{P}}$-open.

Two presheaves in $\widehat{\mathbf{P}}$ are called $\mathbf{P}$-bisimilar iff there is a span of surjective open maps between them.

An $\mathbf{P}-$indexed category, denoted $\mathbf{Q}^{\mathbf{P}}$, is formed by all functors of the shape $\mathbf{P} \to \mathbf{Q}$. Profunctors are indexed presheaves. A *profunctor* is a functor of the shape $F : \mathbf{P} \to \widehat{\mathbf{Q}}$. Profunctors compose and form a bicategory (i.e. there is an additional category on arrows), denoted $\mathbf{PR}$.

4.2 The integrated model

As a mobile process evolves, the ambient set of channel names may change. These channel names are modelled by the category $\mathbf{I}$ of finite sets (of names) and injective maps between them. To take account of this variability, we have to consider the semantic categories involved as indexed by $\mathbf{I}$.

The *object of names* $\mathbf{N}$ is the functor $\mathbf{N} : \mathbf{I} \to \mathbf{PR}$, that sends a set $S \in \mathbf{I}$ to the corresponding discrete category.

The category of *abstract continuous systems with names* is $\mathbf{ACS}^{\mathbf{I}\cdot}$.

Now the integrated model is obtained by including the category $\mathbf{ACS}$ in the domain equations that define the basic processes of π-calculus.

$$\begin{aligned} \mathbf{P} &= \mathbf{ACS}^{\mathbf{I}\cdot} \otimes \mathbf{Q} \\ \mathbf{Q} &\cong \mathbf{Q}_{\perp} + \mathbf{Out} + \mathbf{In} \\ \mathbf{Out} &= (\mathbf{N} \otimes \mathbf{N} \otimes \mathbf{Q}_{\perp}) + (\mathbf{N} \otimes (\delta\mathbf{Q})_{\perp}) \\ \mathbf{In} &= \mathbf{N} \otimes (\mathbf{N} \twoheadrightarrow \mathbf{Q})_{\perp} \end{aligned}$$

where $\otimes$ and $+$ denote the product, respectively the coproduct.

A method to solve the domain equations is presented in detail in [12]. Due to the lengthy and technical arguments, we have to recommend to the interested reader to consult that paper. We briefly describe the meaning of the solutions. The mobile processes are products of π-calculus processes and abstract continuous systems with names. The ACS can communicate values and the names of other channels. Therefore, the communication is first order and deterministic.

These types could be combined, for example, with the type subsystem corresponding to the name passing CCS. This construction has been investigated in [8], but the stochastic hybrid systems could exchange names of communication channels.

G. Winskel and co-workers have extended (see, for example, [25]) the preasheaves semantics to higher order mobile processes, as expressed in higher order π-calculus or the ambient calculus. Unfortunately, the integration mechanism must be changed in this case. The reason is given by the fact the higher order functions do not preserve open maps (see Section 2 for the definition). Winskel solution is to introduce a new language called HOPLA with an operational semantics derived from the preasheaves semantics. Then the bisimulation is defined using the operational semantics. A formal calculus for stochastic processes with mobile communication is subject to future investigations.

Examples of systems that mix continuous behaviours (deterministic or randomised) with software mobility abound. A trivial example is that of people travelling by car or by plane and use a mobile phone. Less trivial, imagine a mobile software that proceeds a secret security check in the pilots cabin. But the target application of this framework is the field of gene regulatory networks, making possible to integrate the existing approaches: stochastic π-calculus [3] and hybrid systems [2]. This integration will be realized in a following paper.

In [7], the authors have introduced a concept of bisimulation for stochastic hybrid systems (SHS). In [6], it is proved that the executions of an SHS form a Markov process on a Borel space, whose trajectories are right continuous with left limits. This paper proposes a different approach where the system properties are derived from the infinitesimal generator of a continuous process. The mathematical model of an embedded system is in general constructed starting with the differential equation characterizing the evolution of the environment. This differential equation gives rise to the expression of the generator. When probabilities are introduced, the resulted stochastic process is also called in the literature a random dynamical system (RDS). In the context of this paper, an RDS is simply a Markov process, alternatively defined using the associated generator. The expression of the generator is known for large classes of processes [18] including diffusions, step processes, Poisson processes, piecewise deterministic Markov processes and so on. In consequence, the concept of bisimulation from this paper is more adequate for these classes of processes. Summarizing this bisimulation is for controllers embedded in complex physical environments that exhibit mobile communication.

5 Final Remarks

Due to physical environment of embedded systems, it is natural to consider continuous feature representations in the system model (arising from the interaction with the environment). Randomization knows recent intensive applications in modelling and verification of embedded systems. The combination of these two paradigms gives rise to models with new and sophisticated mathematical characteristics that can obscure the understanding of computational concepts. In the current work, we have addressed this issue, by introducing a unifying framework, of abstract continuous systems, for systems with (partially) continuous behaviours, deterministic or stochastic.

Bisimulation is now well understood for discrete probabilistic automata [4] or deterministic hybrid systems [19], but it is far more complicated for the stochastic embedded systems. In this paper we have developed a unifying notion of bisimulation for different classes of embedded systems including semi-dynamical systems [5], [21] and strong Markov processes defined on Polish/analytic spaces with continuous time, which are non-stationary. We define a category for each class of systems. For the former category, the morphisms are the so-called zigzag morphisms, which are surjective continuous measurable functions between their state spaces which 'commutes' with the infinitesimal generators of the processes considered. We say that two Markov processes are bisimilar if there exists a span of zigzag morphisms between them.

The category of abstract continuous systems can be used in conjunction with a categorical semantics of π-calculus [12] to define systems mixing physical and logical mobility. The cornerstone of this construction is the concept of bisimulation, which must be equivalent with the one derived from open map [22] (and it must exist). The existence of open map bisimulation is proved for the category of abstract continuous systems. A proof theoretic approach to combine π-calculus and deterministic hybrid systems is presented in [27].

The mobile stochastic hybrid systems provide a very general semantic frameworks in which embedded systems can be studied. Examples could include sensor networks and air traffic control. Mobility allows system reconfiguration, which, combined with probabilities, provide the basic ingredients for randomized learning. This work puts the grounds for semantics of the most actual issues in ubiquitous computing: the self-* systems (abbreviation for features like reconfigurable, adaptive, learning, self-managed, etc. systems).

An extended version of this paper is available on www[3]. It includes more explanations, examples and background material.

References

1. Barr, M., Wells, C.: "*Category Theory for Computing Science*" Prentice Hall (1990).
2. Batt G., Belta C., Weiss R., *Model checking liveness properties of genetic regulatory networks*, 13th Int. Conf. TACAS, (2007).
3. Blossey R., Cardelli L., Phillips A.: *A Compositional Approach to the Stochastic Dynamics of Gene Networks*. T. Comp. Sys. Biology (2006): 99-122
4. Blute R., Desharnais J., Edalat A., Panangaden P.: *Bisimulation for labelled Markov processes.* In Proc. LICS'97, (1997):149–159.
5. Bucur, G., Bezzarga, M.: *Theorie du Potentiel pour les Systemes Semi-Dynamiques.* Rev. Roumaine Math. Pures Appl., 39, no.5 (1994) 439-456.
6. Bujorianu, M. L. ; Lygeros, J.: *Toward a general theory of stochastic hybrid systems. Stochastic hybrid systems*, Lecture Notes in Control and Inform. Sci., **337**(2006): 3–30.
7. Bujorianu, M.L., Lygeros, J., Bujorianu, M.C.: *Bisimulation for General Stochastic Hybrid Systems.* In [24]: 198-214.
8. Bujorianu, M.L., Bujorianu, M.C.: *Distributed Stochastic Hybrid Systems.* In [20].
9. Bujorianu, M.L., Bujorianu, M.C.: *Multi-dimensional codesign: towards an integration paradigm Research Report*, Department of Engineering, University of Cambridge, 2005.
10. Bujorianu M.C., Bujorianu M.L. *Towards Hilbertian Formal Methods* ACSD 2007, IEEE Press.
11. Marius C. Bujorianu, Manuela L. Bujorianu. *An Integrated Specification Framework for Embedded Systems* SEFM 2007, IEEE Press.
12. Cattani G.L., Stark I., Winskel G.: *Presheaf Models for the pi-Calculus.* 7th Conference on Category Theory and Computer Science, Springer LNCS 1290, 106-126, (1997)
13. Cattani G.L., Winskel G.: *Profunctors, Open Maps and Bisimulation.* MSCS, (2004).
14. Chung, K.L.: "Green, Brown and Probability", World Scientific (1995).
15. Dynkin, E.B.: "*Markov Processes*". Vol.1. Berlin Heidelberg New York: Springer (1965).
16. *Design, Implementation and Adaptation of Sensor Networks through Multi-dimensional Co-design* EPSRC Project EP/C014782/1 available as www.dcs.gla.ac.uk/dias/Files/CfS-Full-final.pdf
17. Edalat, A.: *Semi-pullbacks and Bisimulation in Categories of Markov Processes.* Math. Struct. in Comp. Science. **9** no.5 (1999): 523-543.
18. Ethier, S.N., Kurtz, T.G.: "*Markov Processes: Characterization and Convergence*". John Wiley (1986).
19. Haghverdi, E., Tabuada, P., Pappas, G.J.: *Open maps, alternating simulations and control synthesiss.* 15th International Conference on Concurrency Theory , Springer LNCS 3170, (2004): 466-480.
20. Horacek P., Simandl M., Zitek P. (Eds.), "*Proceedings of the 16th IFAC World Congres*" Elsevier Science Press, In press.
21. Hmissi, M.: *Semi-groupes Deterministes.* Sem. Th. Potentiel **9** (1989), Paris, in Lect. Notes in Math, (1393) 135-144.
22. Joyal, A., Nielsen, M., Winskel, G.: *Bisimulation from Open Maps.* Information and Computation, **127(2)** (1996) 164-185.
23. Larsen, K.G., Skou, A.: *Bisimulation through Probabilistic Testing.* Information and Computation, **94** (1991) 1-28.

[3] http://wwwhome.cs.utwente.nl/~manuela/aisha/mobility.pdf

24. Morari, M., Thiele, L. (Eds.), Proc. of *Hybrid Systems: Computation and Control*, 8th International Workshop, LNCS **3414** (2005)
25. Nygaard, M., Winskel, G. : *Domain Theory for Concurrency.* Theoretical Computer Science, May (2004).
26. Padulo, L., Arbib, M.A.: "*System Theory. A Unified State-Space Approach to Continuous and Discrete Systems*" W.B. Saunders Company, (1974).
27. Rounds W.C., Song H.: *The Phi-Calculus: A Language for Distributed Control of Reconfigurable Embedded Systems.* Proc of HSCC 2003, Springer LNCS 2623, (2003) 435-449.
28. Saperstone, S. H.: *"Semidynamical Systems in Infinite Dimensional Spaces ".* Springer Verlag (1981).
29. Trotter, H.F.: *On the Product of Semigroups of Operators.* Proc. Amer. Math. Soc. **10** (1959): 545-551.