CO-EVOLUTION PRESERVING MODEL REDUCTION FOR UNCERTAIN CYBER-PHYSICAL SYSTEMS

Towards a Framework for Nanoscience

Manuela L. Bujorianu and Marius C. Bujorianu
School of Mathematics, University of Manchester, U.K.

Keywords: Cyber-physical systems, Adaptive bisimulation, Co-evolution, Stochastic model checking, Qualitative model reduction, Nanoscience.

Abstract: The problem of abstracting computational relevant properties from sophisticated mathematical models of physical environments has become crucial for cyber-physical systems. We approach this problem using Hilbertean formal methods, a semantic framework that offers intermediate levels of abstractions between the physical world described in terms of differential equations and the formal methods associated with theories of computation. Although, Hilbertean formal methods consider both deterministic and stochastic physical environments, in this paper, we focus on the stochastic case. The abstraction method can be used for verification, but also to improve the controller design and to investigate complex interactions between computation and physics. We define also a computational equivalence relation called adaptive model reduction, because it considers the co-evolution between a computation device environment and its physical environment during abstraction.

1 INTRODUCTION

The interaction between physics and computation can be very subtle. The research experience from areas like nanoscience (Hornyak e.a. 2008) and quantum computing (Accardi e.a. 2006), or from smart dust, shows that common principles can be distilled from these different worlds. At a larger scale, the general system theory provides a systematic repertoire of common properties of the physical and digital dynamical systems. This experiences give hope for a sound semantic framework for *cyber-physical systems* (CPS). The manifestos on CPS - see, for example(Tabuada 2006) - emphasize the need for a fundamentally new theoretical foundation. This foundation should be interdisciplinary and at the right level of abstraction: it should offer analytical tools to investigate physical models, and, at the same time, to be abstract enough to give semantics for models of computation.

In this paper, we consider *Hilbertian Formal Methods* (HFM) (Bujorianu, Bujorianu 2007a, 2007b) as a semantic framework for CPS modeling. HFM represent a logical framework that uses functional and stochastic analysis to construct logics for reasoning about qualitative properties of physical phenomena. These logics can be easily integrated with specification logics for automata. In this work, we focus more on the method part of HFM, and less on the formal aspects. In the HFM framework, we use hybrid systems to design an abstraction method that simplifies the physical models whilst the computational properties are simulated. Intuitively, the computational discrete steps are preserved, while the mathematical models of the continuous phenomena in the environment are drastically simplified.

The qualitative model reductions method we propose is a fundamental step towards *stochastic model checking* (SMC) (Bujorianu, Bujorianu 2006) for uncertain CPS. Stochastic model checking coincides with *probabilistic model checking* (Bujorianu, Katoen 2008) for Markov chains. In the case of continuous or hybrid stochastic dynamical systems, the SMC is a specialization of the *stochastic reachability analysis* (Bujorianu 2004) by means of computer science inspired *abstraction* (Bujorianu, Lygeros, Bujorianu 2005a) or *bisimulation methods* (Bujorianu, Lygeros, Bujorianu 2005b) , (Bujorianu, Bujorianu 2008b).

In the context of uncertain cyber-physical systems, we introduce a new concept of behavior equivalence called *adaptive bisimulation*. In the theory of concurrent discrete processes, bisimulation is a method for reducing the state space, while the tran-

Bujorianu M. and Bujorianu M. (2009).
CO-EVOLUTION PRESERVING ABSTRACT MODEL REDUCTION FOR UNCERTAIN CYBER-PHYSICAL SYSTEMS - Towards a Framework for Nanoscience.
In *Proceedings of the 6th International Conference on Informatics in Control, Automation and Robotics - Signal Processing, Systems Modeling and Control*, pages 39-46
DOI: 10.5220/0002217800390046

sitions are preserved. Using category theory the concept of bisimulation was defined for continuous and hybrid dynamical systems (Haghverdi, Tabuada, Pappas 2005). Based on the same categorical machinery, in (Bujorianu, Lygeros, Bujorianu 2005b), bisimulation has been defined for stochastic hybrid systems. However, in the context of uncertain CPS, the classical concept of bisimulation seems to be too strong (i.e., systems that are considered equivalent by a designer or by an observer, fail to be bisimilar). More appropriate concepts of behavioral equivalence, like approximate bisimulation and behavioral bisimulation have been proposed in (Bujorianu, Bujorianu, Blom 2008) and (Bujorianu, Lygeros, Bujorianu 2005a). Under *approximate bisimulation*, the trajectories of two randomized hybrid systems differ with a small distance, the measurement being done according with a suitable metric. For the *behavioral bisimulation*, two equivalent systems have the same probabilities of reaching some specific state sets. Although these bisimulation concepts are better in describing properties of systems that operate in physical environments, they do not imply the preservation of the interaction between computation and physics. The key point in defining such a bisimulation consists in modeling this interaction. In this paper, we model this interaction using an abstract measure called *energy*, which is a basic concept of HFM. The energy characterizes globally the cyber physical process, but also it can discriminate continuous (physical) evolutions, discrete (computational) transitions and control (the process killing, in order to start another one). This last aspect makes the difference between a CPS and a classical automaton: a computation device has the capability to influence its physical environment (and achieving *co-evolution* in this way). Naturally, the CPS bisimulation should be related to energy preservation. An intuitive illustration of adaptive bisimulation is given by the following scenario. During its evolution, a CPS may produce a change of its environment. Suppose that for the new dynamical system modeling the environment is classically bisimilar with the former one. Then, for an adaptive bisimilar CPS the computational component will exhibit a equivalent behavior.

The paper road map can be described as follows. The following section contains the mathematical setting. In Section 3 we formulate the stochastic model checking problem and we prove two results that make the problem solvable. In Section 4 we investigate the qualitative model reductions and bisimulations. The final section contains some short conclusions.

2 THE MATHEMATICAL FRAMEWORK

2.1 Uncertain Cyber-physical Systems

The theory of hybrid systems is a well-established modeling paradigm for embedded systems. Similarly, the theory of concurrent embedded hybrid systems (Bujorianu, Lygeros, Bujorianu 2005a) constitutes a suitable modeling framework for CPS. In the following an uncertain cyber-physical system is modeled as a randomized embedded hybrid system.

There are two major ways to randomize a continuous or hybrid dynamical system: In one approach, the concept of noise is used to model small random perturbations. The randomized system has trajectories that closely resemble those of the deterministic initial system. The noise based randomization is carried out using stochastic differential equations. When the influence of the random perturbation changes dramatically the system evolution, the randomization is carried out using stochastic kernels that replace the concept of reset maps from deterministic hybrid system models.

A Ucps $U = (Q, \mathcal{X}, F, R, \lambda)$ consists of

- a finite set of discrete variables Q;
- a map $\mathcal{X} : Q \to \mathbb{R}^{d(.)}$ that sends each $q \in Q$ into a mode (an open subset) X^q of $\mathbb{R}^{d(q)}$, where $d(q)$ is the Euclidean dimension of the corresponding mode;
- a map $F : Q \to 2^{\mathcal{F}_{SDE}}$ which specifies the continuous evolution of the automaton in terms of stochastic differential equations (SDE) over the continuous state x^q for each mode;
- a family of stochastic kernels $R = (R^q)_{q \in Q}$,

$$R^q : \overline{X}^q \times (\cup \mathcal{B}(X^j) | j \in Q \backslash \{q\}) \to [0,1];$$

- a transition rate function

$$\lambda : (\cup \overline{X}^j | j \in Q) \to \mathbb{R}^+, \quad (1)$$

which gives the distributions of the jump times.

The executions of a Ucps can be described as follows: start with an initial point $x_0 \in X^q$, follow a solution of the SDE associated to X^q, jump when this trajectory hits the boundary or according with the transition rate λ (the jump time is the minimum of the boundary hitting time and the time, which is exponentially distributed with the transition rate λ). Under standard assumptions, for each initial condition $x \in j \in Q \cup X^j$, the possible trajectories starting from x, form a stochastic process. Moreover, for all initial conditions x, the executions of a Ucps form the semantics, which can be thought of as a Markov process in a general setting. Let us consider $M = (\Omega, \mathcal{F}, \mathcal{F}_t, x_t, P_x)$ be the semantics of U. Under mild

assumptions on the parameters of U, M can be viewed as a family of Markov processes with the state space $(X,\mathcal{B})$, where X is the union of modes and $\mathcal{B}$ is its Borel σ-algebra. Let $\mathcal{B}^b(X)$ be the lattice of bounded positive measurable functions on X. The meaning of the elements of M can be found in any source treating continuous-parameter Markov processes (see, for example, (Davis 1993)). Suppose we have given a σ-finite measure μ on $(X,\mathcal{B})$.

In the following we give some operator characterizations of stochastic processes, which are employed in this paper to define a qualitative model reduction for Ucps.

2.2 Hilbertean Formal Methods

The HFM abstract away the analytical properties of deterministic and stochastic differential operators using the so called kernel operator (defined in the following). Using methods of functional analysis HFM elegantly generalize both deterministic and stochastic systems. In this work we focus on the stochastic case. Let us describe briefly the mathematical apparatus that is usually employed to study continuous time continuous space Markov processes.
The *transition probability function* is $p_t(x,A) = P_x(x_t \in A)$, $A \in \mathcal{B}$. This is the probability that, if $x_0 = x$, x_t will lie in the set A.
The *operator semigroup* $\mathcal{P}$ is defined by

$$P_t f(x) = \int f(y) p_t(x,dy) = E_x f(x_t), \forall x \in X,$$

where E_x is the expectation w.r.t. P_x.
The *operator resolvent* $\mathcal{V} = (V_\alpha)_{\alpha \geq 0}$ associated with $\mathcal{P}$ is

$$V_\alpha f(x) = \int_0^\infty e^{-\alpha t} P_t f(x) dt,$$

$x \in X$. Let denote by V the initial operator V_0 of $\mathcal{V}$, which is known as the *kernel operator* of the Markov process M. The operator resolvent $(V_\alpha)_{\alpha \geq 0}$ is the Laplace transform of the semigroup.
The *strong generator* $\mathcal{L}$ is the derivative of P_t at $t = 0$. Let $D(\mathcal{L}) \subset \mathcal{B}_b(X)$ be the set of functions f for which the following limit exists (denoted by $\mathcal{L} f$):

$$\lim_{t \searrow 0} \frac{1}{t}(P_t f - f).$$

In the HFM, there is developed a semantic framework for concurrent embedded systems constructed using energy forms. We specialize this theory for function spaces, reaching in this way the theory of Dirichlet forms (Ma, Rockner 1990).

A quadratic form $\mathcal{E}$ can be associated to the generator of a Markov process in a natural way.

Let $L^2(X,\mu)$ be the space of square integrable μ-measurable extended real valued functions on X, w.r.t. the natural inner product $< f,g >_\mu = \int f(x)g(x)d\mu(x)$.
The quadratic form $\mathcal{E}$:

$$\mathcal{E}(f,g) = - < \mathcal{L} f, g >_\mu, f \in D(\mathcal{L}), g \in L^2(X,\mu) \quad (2)$$

defines a closed form. This leads to another way of parameterizing Markov processes. Instead of writing down a generator one starts with a quadratic form. As in the case of a generator it is typically not easy to fully characterize the domain of the quadratic form. For this reason one starts by defining a quadratic form on a smaller space and showing that it can be extended to a closed form in subset of $L^2(\mu)$. When the Markov process can be initialized to be stationary, the measure μ is typically this stationary distribution (see (Davis 1993) p.111). More generally, μ does not have to be a finite measure.

A *coercive closed form* is a quadratic form $(\mathcal{E}, D(\mathcal{E}))$ with $D(\mathcal{E})$ dense in $L^2(X,\mu)$, which satisfies the: (i) closeness axiom, i.e. its symmetric part is positive definite and closed in $L^2(X,\mu)$, (ii) continuity axiom. $\mathcal{E}$ is called *bilinear functional energy* (BLFE) if, in addition, it satisfies the third axiom: (iii) contraction condition, i.e. $\forall u \in D(\mathcal{E})$, $u^* = u^+ \wedge 1 \in D(\mathcal{E})$ and $\mathcal{E}(u \pm u^*, u \mp u^*) \geq 0$.
For a the general theory of closed forms associated with Markov processes see (Ma, Rockner 1990).

Let $(\mathcal{L}, D(\mathcal{L}))$ be the generator of a coercive form $(\mathcal{E}, D(\mathcal{E}))$ on $L^2(X,\mu)$, i.e. the unique closed linear operator on $L^2(X,\mu)$ such that $1 - \mathcal{L}$ is onto, $D(\mathcal{L}) \subset D(\mathcal{E})$ and $\mathcal{E}(u,v) = < -\mathcal{L}u, v >$ for all $u \in D(\mathcal{L})$ and $v \in D(\mathcal{E})$. Let $(T_t)_{t>0}$ be the strongly continuous contraction semigroup on $L^2(X,\mu)$ generated by $\mathcal{L}$ and $(G_\alpha)_{\alpha>0}$ the corresponding strongly continuous contraction semigroup (which exist according to the Hille-Yosida theorem).

A right process M with the state space X is *associated* with a BLFE $(\mathcal{E}, D(\mathcal{E}))$ on $L^2(X,\mu)$ if the semigroup (P_t) of the process M is a μ-version[1] of the form semigroup (T_t). It has been proved (Albeverio, Ma, Rockner 1993) and (Ma, Rockner 1990) that only those BLFEs, which satisfy some regularity conditions can be associated with some right Markov processes and viceversa (Th.1.9 of (Albeverio, Ma, Rockner 1993)).

Prop. 4.2 from (Albeverio, Ma, Rockner 1993) states that two right Markov processes M and M' with state space X associated with a common quasi-regular BLFE $(\mathcal{E}, D(\mathcal{E}))$ are stochastically equivalent (Ma, Rockner 1990). That means a quasi-regular BLFE

[1] I.e., for all $f \in L^2(X,\mu)$ the function $P_t f$ is a μ-version (differs on a set of μ-measure zero) of $T_t f$ for all $t > 0$.

characterizes a class of stochastically equivalent right Markov processes.

Let $M = (\Omega, \mathcal{F}, \mathcal{F}_t, x_t, P_x)$ be a right Markov process with the state space X. Now assume that X is a Lusin space (i.e. it is homeomorphic to a Borel subset of a compact metric space) and $\mathcal{B}(X)$ or $\mathcal{B}$ is its Borel σ-algebra. Assume also that μ is a σ-finite measure on $(X, \mathcal{B})$ and μ is a stationary measure of the process M. Let $X^{\#}$ another Lusin space (with $\mathcal{B}^{\#}$ its Borel σ-algebra) and $F : X \to X^{\#}$ be a measurable function. Let $\sigma(F)$ be the sub-σ-algebra of $\mathcal{B}$ generated by F. If μ is a probability measure then the projection operator between $L^2(X, \mathcal{B}, \mu)$ and $L^2(X, \sigma(F), \mu)$ is the conditional expectation $E_\mu[\cdot|F]$. Recall that E_μ is the expectation defined w.r.t. P_μ and that $P_\mu(A) = \int P_x(A) d\mu$, $A \in \mathcal{F}$. We denote by $\mu^{\#}$ the image of μ under F, i.e. $\mu^{\#}(A^{\#}) = \mu(F^{-1}(A^{\#}))$, for all $A^{\#} \in \mathcal{B}^{\#}$. In general, anything associated with $X^{\#}$ will carry the #-superscript symbol in this section.

Let $\mathcal{E}$ be the BLFE on $L^2(X, \mu)$ associated to M. F induces a form $\mathcal{E}^{\#}$ on $L^2(X^{\#}, \mu^{\#})$ by

$$\mathcal{E}^{\#}(u^{\#}, v^{\#}) = \mathcal{E}(u^{\#} \circ F, v^{\#} \circ F); \quad (3)$$

for $u^{\#}, v^{\#} \in D[\mathcal{E}^{\#}]$, where

$$D[\mathcal{E}^{\#}] = \{u^{\#} \in L^2(X^{\#}, \mu^{\#}) | u^{\#} \circ F \in D[\mathcal{E}]\}. \quad (4)$$

It can be shown (see Prop.1.4 in (Iscoe, McDonald 1990)), under a mild condition on the conditional expectation operator $E_\mu[\cdot|F]$ that $\mathcal{E}^{\#}$ is a BLFE. If, in addition, $\mathcal{E}^{\#}$ is quasi-regular then we can associate it a right Markov process $M^{\#} = (\Omega, \mathcal{F}, \mathcal{F}_t, x_t^{\#}, P_x^{\#})$ with the state space $X^{\#}$. The process $M^{\#}$ is called the *induced Markov process* w.r.t. to the proper map F. If the image of M under F is a right Markov process then $x_t^{\#} = F(x_t)$. The process $M^{\#}$ might have some different interpretations like a refinement of discrete transitions structure, or an approximation of continuous dynamics or an abstraction of the entire process. It is difficult to find a practical condition to impose on F, which would guarantee that $\mathcal{E}^{\#}$, as defined by (3) and (4), is also quasi-regular. To circumvent this problem, it is possible to restrict the original domain $D[\mathcal{E}^{\#}]$ and impose some regularity conditions on F (for more details, see (Iscoe, McDonald 1990)).

Assumption 1. *Suppose that $\mathcal{E}^{\#}$ is a quasi-regular BLFE.*

3 THE STOCHASTIC MODEL CHECKING PROBLEM

Let us consider $M = (\Omega, \mathcal{F}, \mathcal{F}_t, x_t, P_x)$ a strong Markov process, which is the semantics of a UCPS. For this strong Markov process we address a verification problem consisting of the *stochastic reachability problem* defined as follows. Given a set $A \in \mathcal{B}(X)$ and a time horizon $T > 0$, let us to define (Bujorianu 2004):

$$\begin{aligned} Reach_T(A) &= \{\omega \in \Omega \mid \exists t \in [0,T] : x_t(\omega) \in A\} \\ Reach_\infty(A) &= \{\omega \in \Omega \mid \exists t \geq 0 : x_t(\omega) \in A\}. \quad (5) \end{aligned}$$

These two sets are the sets of trajectories of M, which reach the set A (the flow that enters A) in the interval of time $[0,T]$ or $[0,\infty)$.

The reachability problem consists of determining the probabilities of such sets. The reachability problem is well-defined, i.e. $Reach_T(A)$, $Reach_\infty(A)$ are indeed measurable sets. Then the probabilities of reach events are

$$P(T_A < T) \text{ or } P(T_A < \infty) \quad (6)$$

where $T_A = \inf\{t > 0 | x_t \in A\}$ and P is a probability on the measurable space $(\Omega, \mathcal{F})$ of the elementary events associated to M. P can be chosen to be P_x (if we want to consider the trajectories, which start in x) or P_μ (if we want to consider the trajectories, which start in x_0 given by the distribution μ).

Usually a target set A in the state space is a level set for a given function $F : X \to \mathbb{R}$, i.e. $A = \{x \in X | F(x) > l\}$ (F can be chosen as the Euclidean norm or as the distance to the boundary of E). The probability of the set of trajectories, which hit A until time horizon $T > 0$ can be expressed as

$$P(\sup F(x_t) | t \in [0,T]) > l. \quad (7)$$

Our goal is to *define a new stochastic process $M^{\#}$ such that the probabilities (6) are preserved.*

Ideally, since (6) can be written as (7), $F(x_t)$ would represent the best candidate for defining a possible qualitative model reduction for M, which preserves the reach set probabilities. The main difficulty is that $F(x_t)$ is a Markov process only for special choices of F (Rogers, Pitman 1981). The problem is how to choose F well.

Note, if $A^{\#}$ is open in $X^{\#}$ and $A = F^{-1}(A^{\#})$, then we consider the two first hitting times T_A (w.r.t. M) and $T_{A^{\#}}^{\#}$ (w.r.t. $M^{\#}$) of A and $A^{\#}$, respectively. Recall that $T_A = \inf\{t > 0 | x_t \in A\}$.

The following results show that the stochastic model checking problem is solvable for uncertain cps.

Proposition 1. *Under the assumption.1, if μ is a probability measure and $\xi = +\infty$ (M has no killing), then*

$$E_\mu \exp(-T_A) \leq E_{\mu^{\#}} \exp(-T_{A^{\#}}^{\#}) \quad (8)$$

where E_μ (resp. $E_{\mu^{\#}}$) is the expectation defined w.r.t. P_μ (resp. $P_{\mu^{\#}}$).

If M is the semantics of a UCPS U, given a target state set $A \in \mathcal{B}(X)$, then the goal in the stochastic reachability analysis is to compute the probability $P_\mu(T_A \leq T)$ for a finite horizon time $T > 0$. We now translate the relation (8) in terms of probability of the reachable sets.

Proposition 2. *Under the assumption.1, if μ is a probability measure, then*

$$\begin{aligned} P_\mu(T_A &\leq T) \leq eK \min\{T\mathcal{E}^\#(u^\#,u^\#) + && (9)\\ &< u^\#,u^\# >_{\mu^\#} | u^\# \in D(\mathcal{E}^\#),\ u^\# \geq 1, && (10)\\ &\mu^\# - a.e.\ on\ A^\#\} && (11) \end{aligned}$$

where $K > 0$ is the sector constant of $\mathcal{E}$.

4 ADAPTING VERIFICATION TO CO-EVOLUTION

The idea is to apply a "state space reduction" technique based on the general 'induced BLFEs' method to achieve qualitative model reductions for Ucps. With this technique, the semantics of Ucps are 'approximated' by a one-dimensional stochastic process with a much smaller state space.

4.1 Qualitative Model Reduction

The stochastic reachability definition gives the idea to introduce the following concept of qualitative model reduction for Ucps.

Definition 1. *Given a right Markov process M defined on the Lusin state space $(X,\mathcal{B})$, and $F : X \to \mathbb{R}$ a measurable weight function, suppose that assumption.1 is fulfilled. The process $M^\#$ associated to the induced BLFE $\mathcal{E}^\#$ under function F is called a qualitative model reduction of M.*

Let U be a UCPS and M its semantics. Suppose that M is a right Markov process defined on the Lusin state space $(X,\mathcal{B})$.

Definition 2. *Any UCPS $U^\#$ whose semantics is a qualitative model reduction of M is called a qualitative model reduction of U.*

Let U be a Ucps and M its semantics (that is a right Markov process, with the state space X).

Proposition 3. *If M is a diffusion then any qualitative model reduction $M^\#$ of M is a diffusion.*

Proposition 4. *If M is a jump process then any qualitative model reduction $M^\#$ of M is again a jump process.*

Proof. This statement can be obtained as a consequence of the abstract version of the *Kolmogorov backward equations* (Davis 1993)

$$\frac{\partial}{\partial t}P_t f(x) = LP_t f(x),\ P_0 f = f,\ f \in D(\mathcal{L}) \qquad (12)$$

and the equality (14). If the equations (12) are associated to an initial diffusion process (resp. jump process) then the relation (14) allow to obtain the fact that the transition probabilities of the induced process satisfy a similar equation, such that the induced process is still a diffusion process (resp. jump process). The same conclusion can be obtain using the stochastic calculus of BLFEs (Iscoe, McDonald 1990).■

Since the semantics of a Ucps is, in most cases, a stochastic process, which can be viewed an interleaving between some diffusion processes and a jump process (see (Bujorianu, Lygeros 2004) for a very general model for Ucps and its semantics as a Markov string), we can write the following result as a corollary of Prop.3.

Proposition 5. *Any qualitative model reduction of a Ucps is again a Ucps.*

Let $(\mathcal{L},D(\mathcal{L}))$ and $(\mathcal{L}^\#,D(\mathcal{L}^\#))$ be the generators of $\mathcal{E}$ and $\mathcal{E}^\#$, respectively. For the following results we suppose that the Ass.1 is fulfilled.

Proposition 6. *The generators $\mathcal{L}$ and $\mathcal{L}^\#$ are related as follows*

$$\mathcal{L}(u^\# \circ F) = \mathcal{L}^\# u^\# \circ F, \forall u^\# \in D(\mathcal{L}^\#) \qquad (13)$$

Theorem 7. *For all $A^\# \in \mathcal{B}^\#(X^\#)$ and for all $t > 0$ we have*

$$p_t^\#(Fx,A^\#) = p_t(x,F^{-1}(A^\#)) \qquad (14)$$

where $(p_t^\#)$ and (p_t) are the transition functions of $M^\#$ and M, respectively.

Proof. Let $F^\#$ be defined as $F^\# : \mathcal{B}^b(X^\#) \to \mathcal{B}^b(X)$; $F^\# u^\# = u^\# \circ F$. Then (13) becomes $(\mathcal{L} \circ F^\#)u^\# = (F^\# \circ \mathcal{L}^\#)u^\#, \forall u^\# \in D(\mathcal{L}^\#)$ $(**)$. For a strong Markov process, the opus of the kernel operator is the inverse operator of the infinitesimal generator of the process. Now, from $(**)$ we get a similar relation between the kernel operators V and $V^\#$ of the processes M and $M^\#$, i.e. $F^\# \circ V^\# = V \circ F^\#$ on $\mathcal{B}^b(X^\#)$, or

$$V^\# u^\# \circ F = V(u^\# \circ F), \forall u^\# \in \mathcal{B}^b(X^\#) \qquad (15)$$

since if $u^\# \in \mathcal{B}^b(X^\#)$ then $V^\# u^\# \in D(\mathcal{L}^\#)$. For $u^\# = 1_{A^\#}$ (the indicator function of $A^\#$), by the kernel operator integral definition, we obtain (14).■

Relation (15) implies the following corollary:

Corollary 8. *The semigroups $(P_t^\#)$ and (P_t) of $M^\#$ and M are related by*

$$P_t^\# u^\# \circ F = P_t(u^\# \circ F), \forall u^\# \in \mathcal{B}^b(X^\#). \qquad (16)$$

4.2 Adaptive Bisimulation

In this subsection we define a new concept of adaptive bisimulation for cps. This concept is defined as measurable relation, which induces equivalent BLFEs on the quotient spaces. In defining adaptive bisimulation, we do not impose the equivalence of the quotient processes, which might not have Markovian properties (Rogers, Pitman 1981), but we impose the equivalence of the qualitative model reductions (that can differ from the quotient processes) associated with the induced BLFEs, with respect to the projection maps.

Let $(X,\mathcal{B}(X))$ and $(Y,\mathcal{B}(Y))$ be Lusin spaces and let $\mathcal{R}\subset X\times Y$ be a relation such that $\Pi^1(\mathcal{R})=X$ and $\Pi^2(\mathcal{R})=Y$. We define the equivalence relation on X that is induced by the relation $\mathcal{R}\subset X\times Y$, as the transitive closure of $\{(x,x')|\exists y \text{ s.t. } (x,y)\in\mathcal{R} \text{ and } (x',y)\in\mathcal{R}\}$. Analogously, the induced (by $\mathcal{R}$) equivalence relation on Y can be defined. We write $X/_{\mathcal{R}}$ and $Y/_{\mathcal{R}}$ for the sets of equivalence classes of X and Y induced by $\mathcal{R}$. We denote the equivalence class of $x\in X$ by $[x]$. Let

$$\mathcal{B}^{\#}(X)=\mathcal{B}(X)\cap\{A\subset X|\text{ if } x\in A \text{ and } [x]=[x'] \text{ then } x'\in A\}$$

be the collection of all Borel sets, in which any equivalence class of X is either totally contained or totally not contained. It can be checked that $\mathcal{B}^{\#}(X)$ is a σ-algebra. Let $\pi_X: X\to X/_{\mathcal{R}}$ be the mapping that maps each $x\in X$ to its equivalence class and let

$$\mathcal{B}(X/_{\mathcal{R}})=\{A\subset X/_{\mathcal{R}}|\pi_X^{-1}(A)\in\mathcal{B}^{\#}(X)\}.$$

Then $(X/_{\mathcal{R}},\mathcal{B}(X/_{\mathcal{R}}))$, which is a measurable space, is called the quotient space of X w.r.t. $\mathcal{R}$. The quotient space of Y w.r.t. $\mathcal{R}$ is defined in a similar way. We define a bijective mapping $\psi: X/_{\mathcal{R}}\to Y/_{\mathcal{R}}$ as

$$\psi([x])=[y] \text{ if } (x,y)\in\mathcal{R} \text{ for some } x\in[x] \text{ and some } y\in[y].$$

We say that the relation $\mathcal{R}$ is *measurable* if X and Y if for all $A\in\mathcal{B}(X/_{\mathcal{R}})$ we have $\psi(A)\in\mathcal{B}(Y/_{\mathcal{R}})$ and vice versa, i.e. ψ is a homeomorphism. Then the real measurable functions defined on $X/_{\mathcal{R}}$ can be identified with those defined on $Y/_{\mathcal{R}}$ through the homeomorphism ψ. We can write $\mathcal{B}^b(X/_{\mathcal{R}})\overset{\psi}{\cong}\mathcal{B}^b(Y/_{\mathcal{R}})$. Moreover, these functions can be thought of as real functions defined on X or Y measurable w.r.t. $\mathcal{B}^{\#}(X)$ or $\mathcal{B}^{\#}(Y)$.

Assumption 2. *Suppose that $X/_{\mathcal{R}}$ and $Y/_{\mathcal{R}}$ with the topologies induced by projection mappings are Lusin spaces.*

Suppose we have given two right Markov processes M and W with the state spaces X and Y. Assume that μ (resp. ν) is a stationary measure of the process M (resp. W). Let $\mu/_{\mathcal{R}}$ (resp. $\nu/_{\mathcal{R}}$) the image of μ (resp. ν) under π_X (resp. π_Y). Let $\mathcal{E}$ (resp. $\mathcal{F}$) the quasi-regular BLFE corresponding to M (resp. W). The equivalence between the induced processes can be used to define a new bisimulation between Markov processes, as follows.

Definition 3. *Under assumptions 1 and 2, a measurable relation $\mathcal{R}\subset X\times Y$ is a bisimulation between M and W if the mappings π_X and π_Y define the same induced BLFE on $L^2(X/_{\mathcal{R}},\mu/_{\mathcal{R}})$ and $L^2(Y/_{\mathcal{R}},\nu/_{\mathcal{R}})$, respectively.*

This definition states that M and W are bisimilar if $\mathcal{E}/_{\mathcal{R}}=\mathcal{F}/_{\mathcal{R}}$. Here, $\mathcal{E}/_{\mathcal{R}}$ (resp. $\mathcal{F}/_{\mathcal{R}}$) is the induced BLFE of $\mathcal{E}$ (resp. $\mathcal{F}$) under the mapping π_X (resp. π_Y). Clearly, this can be possible iff $\mu/_{\mathcal{R}}=\nu/_{\mathcal{R}}$.

Assumption 3. *Suppose that $\mathcal{E}/_{\mathcal{R}}$ and $\mathcal{F}/_{\mathcal{R}}$ are quasi-regular BLFE.*

Denote the Markov process associated to $\mathcal{E}/_{\mathcal{R}}$ (resp. $\mathcal{F}/_{\mathcal{R}}$) by $M/_{\mathcal{R}}$ (resp. $W/_{\mathcal{R}}$).

Proposition 9. *Under assumptions 1, 2 and 3, M and W are stochastic bisimilar under $\mathcal{R}$ iff their qualitative model reductions $M/_{\mathcal{R}}$ and $W/_{\mathcal{R}}$ with respect to π_X and, respectively π_Y are $\mu/_{\mathcal{R}}$-equivalent.*

Let U and U' be two UCPSs, with the semantics M and W, strong Markov processes defined on the state spaces $(X,\mathcal{B}(X))$ and $(Y,\mathcal{B}(Y))$, respectively.

Definition 4. *U and U' are called bisimilar if there exist a bisimulation relation under which their semantics M and W are bisimilar*

4.3 An Example

Let us recall the chemically reacting system case study from (Singh, Hespanha 2005), where it is investigated using the theory of polynomial stochastic hybrid systems. Consider a system of n species X_j, $j=1,..,n$, inside a fixed volume V involved in K reactions of the form

$$(R_i)\, u_{ai}A_i+u_{i1}X_1+...+u_{in}X_n \xrightarrow{c_i} \nu_{i1}X_1+...+\nu_{in}X_n, \forall i \in \{1,...,K\}$$

where the species A_i have a constant number of molecules. The meaning and the assumptions about the coefficients of the reaction equation are given in (Singh, Hespanha 2005). c_i is a reaction parameter

which is used in defining the probability that a particular reaction takes place on $(t, t+dt)$. The system is characterized by the trivial dynamics $\dot{x}=0$, $x=[x_1,x_2,...,x_n]^T$, a family of K *reset maps* $x=\phi_i(x^-)$, $\phi_i:\mathbb{R}^n\to\mathbb{R}^n$, and a corresponding family of *transition intensities* $\lambda_i:\mathbb{R}^n\to[0,\infty)$, $\forall i=1,..,K$. For each $i=1,..,K$, the reset map ϕ_i and the corresponding λ_i is uniquely defined by the i^{th} reaction equation and given by $x\mapsto\phi_i(x)$, $\phi_i(x)=x+[\nu_{i1}-u_{i1},\nu_{i2}-u_{i2},...,\nu_{in}-u_{in}]^T$; $\lambda_i(x)=c_ih_i(x)$, where U_i represents the number of distinct molecular reactant combinations present in V at time t for the reaction R_i. The executions of such a system are defined in (Singh, Hespanha 2005).

Now we apply the method of qualitative model reduction to this process. We can show that executions of this cps form a particular kind of right Markov process called jump process (Davis 1993). The extended generator (Th.1 (Singh, Hespanha 2005)) is $(L\psi)(x)=\sum_{i=1}^K(\psi(\phi_i(x))-\psi(x))\lambda_i(x)$, $\psi\in D(L)$.

Let us consider a proper map $F:\mathbb{R}^n\to\mathbb{R}$ and write the generator of the induced process for
$\psi^\#\circ F$, $\psi^\#\in D(L^\#)$:
$L(\psi^\#\circ F)(x)=\sum_{i=1}^K(\psi^\#(F(\phi_i(x)))-\psi^\#(F(x)))\lambda_i(x)$

Define $\phi_i^\#:\mathrm{Im}F\to\mathbb{R}$ by $\phi_i^\#(Fx)=F(\phi_i(x))$ and $\lambda_i^\#:\mathrm{Im}F\to\mathbb{R}$ by $\lambda_i^\#(Fx)=\lambda_i(x)$. In order to have these two function well-defined we need to impose some compatibility conditions between F and reset maps ϕ_i and their corresponding transition intensities λ_i as follows: $Fx=Fx'\Rightarrow F(\phi_i(x))=F(\phi_i(x'))$ and $\lambda_i(x)=\lambda_i(x')$. This means that F preserves the jumps (reset maps and transition intensities), i.e. the pre-jump locations have the same image under F then the intensities of transition should be equal and the post-jump locations have the same image under F. Using (13), the generator of the induced process is

$$L^\#\psi^\#(x^\#) = \sum_{i=1}^K(\psi^\#(\phi_i^\#(x^\#))-\psi^\#(x^\#))\lambda_i^\#(x^\#);\quad x^\#=Fx;\ x\in X.$$

For simplicity, we suppose that the reactions R_i are reversible in time. Then the generator is self-adjoint (or Hermitian). The (symmetric) quasi-regular energy bilinear form on $L^2(\mathbb{R}^n,\mu)$ associated to the given process (with μ a stationary distribution) can be written

$\mathcal{E}(\psi,\varphi)=\sum_{i=1}^K\int_{\mathbb{R}^n}(\psi(\phi_i(x))-\psi(x))(\varphi(\phi_i(x))-\varphi(x))\lambda_i(x)\mu(dx)$

Then the induced energy bilinear form $\mathcal{E}^\#$ on $L^2(\mathbb{R},\mu^\#)$ (where $\mu^\#$ is the image of μ under F) w.r.t. F is

$$\begin{aligned}\mathcal{E}^\#(\psi^\#,\varphi^\#) &= \sum_{i=1}^K\int_{\mathbb{R}^n}[\psi^\#(\phi_i^\#(Fx))-\psi^\#(Fx)]\\ &\quad[\varphi^\#(\phi_i^\#(Fx))-\varphi^\#(Fx)]\lambda_i^\#(Fx)\\ &\quad\mu(dx)\\ &= \sum_{i=1}^K\int_{\mathbb{R}}[\psi^\#(\phi_i^\#(x^\#))-\psi^\#(x^\#)][\varphi^\#\\ &\quad(\phi_i^\#(x^\#))-\varphi^\#(x^\#)]\lambda_i^\#(x^\#)\mu^\#(dx^\#).\end{aligned}$$

Clearly, $\mathcal{E}^\#$ is associated to a jump process - thequalitative model reduction of the given process. In this particular case, the induced process is exactly the image under F of the initial jump process.

5 CONCLUSIONS

In this paper, we have used the concept of energy, which is a key ingredient of Hilbertean formal methods, to define qua;itative model reduction and behavioral equivalence for cyber-physical systems operating in random environments. Energy is a versatile analytical concept that characterizes in a subtle way the interaction between computation and physics, as well as their co-evolution.

Adaptive bisimulation means the energy preservation of the stochastic processes generated by the cyber-physical system evolutions. The energy concept can be also used to define qualitative model reductions for cyber-physical systems. Given an qualitative model reduction function that reduces the state space, we have defined a standard construction that associates a qualitative model reduction (called standard) on the reduced state space. The mathematical results from Section 4.1 show that the qualitative model reduction method preserves important analytic properties (related to HFM). Two uncertain CPS are adaptive bisimilar if they have the same energy. The theorem from Section 4.2 shows that two uncertain CPS are adaptive bisimilar iff their standard qualitative model reductions are equivalent as Markov processes.

We have formulated the stochastic model checking problem (a subproblem of stochastic reachability analysis, corresponding to the probabilistic model checking of Markov chains). We proved two results that show that the problem is solvable for uncertain cyber-physical systems. The mathematical results from Section 3 provide a upper bound for the reach set probabilities. In this way, one can prove that the probability of reaching a state in a certain set can be small enough.

The most closely related model is that of *stochastic hybrid automata* (Bujorianu 2004). These automata are not necessarily embedded systems and their hybrid behavior is often an internal feature (as for cars, aircraft, mobile robots and so on) rather than the interaction with a physical environment (a feature of embedded systems). Cyber-physical systems are also networked.

In following work we will refine the formal framework presented in this paper to be used for nanoscience.

ACKNOWLEDGEMENTS

This work was funded by the EPSRC project EP/E050441/1 CICADA.

REFERENCES

Accardi L., Ohya M., Watanabe N., 2006. *Quantum Information and Computing* World Scientific.

Albeverio, S., Ma, Z.M., Rockner, M., 1993. Quasi-regular Dirichlet Forms and Markov Processes. *J. of Functional Analysis* 111: 118-154.

Bujorianu, M.C., Bujorianu M.L., 2007a. Towards Hilbertean Formal Methods *Proc. of the 7th International Conference on Application of Concurrency to System Design ACSD* IEEE Press.

Bujorianu, M.C., Bujorianu, M.L., 2007b. An integrated specification framework for embedded systems, *Proc. of SEFM*, IEEE Press.

Bujorianu, M.C., Bujorianu M.L., 2008a. A Randomized Model for Communicating Embedded Systems. *Proceedings of the 16th Mediterranean Conference on Control and Automation*, IEEE Press.

Bujorianu, M.L., Bujorianu, M.C., 2008b. Bisimulation, Logic and Mobility for Markovian Systems, In: *Proc of 18th International Symposium on Mathematical Theory of Networks and Systems (MTNS08)*, SIAM.

Bujorianu, M.L., Bujorianu, M.C., Blom H., 2008. Approximate Abstractions of Stochastic Hybrid Systems, *Proc. of the 17th IFAC World Congress*, Elsevier.

Bujorianu, M.L., Katoen J., 2008. Symmetry reduction for stochastic hybrid systems. In: *Proc. of IEEE 47th Conference on Decision and Control*, IEEE press.

Bujorianu, M.L., Bujorianu, M.C. 2006. A Model Checking Strategy for a Performance Measure of Fluid Stochastic Models, In: *European Performance Engineering Workshop (EPEW)*, Springer LNCS 4054, pp. 93-107.

Bujorianu, M.L., Lygeros, J., 2004. General Stochastic Hybrid Systems: Modelling and Optimal Control. *Proc. 43th Conference in Decision and Control*, IEEE Press: 182-187.

Bujorianu, M.L. 2004. Extended Stochastic Hybrid Systems and their Reachability Problem. In *Hybrid Systems: Computation and Control*, Springer LNCS 2993: 234-249.

Bujorianu, M.L., Lygeros, J., Bujorianu, M.C., 2005a. Abstractions of Stochastic Hybrid System. *Proc. 44th Conference in Decision and Control*. IEEE Press.

Bujorianu, M.L., Lygeros, J., Bujorianu, M.C., 2005b. Bisimulation for General Stochastic Hybrid Systems. In *Proc. Hybrid Systems: Computation and Control*, Springer LNCS 3414: 198-216.

Davis, M.H.A. 1993. *Markov Models and Optimization* Chapman & Hall.

Ethier, S.N., Kurtz, T.G., 1986. *Markov Processes: Characterization and Convergence*. John Wiley and Sons.

Haghverdi, E., Tabuada, P., Pappas, G.J., 2005. Bisimulation Relations for Dynamical, Control and Hybrid Systems. *Theor. Comput. Science*, 342(2-3):229-261.

Hornyak, G., Dutta, J., Tibbals H.J., Rao A.K. 2008. *Introduction to Nanoscience* CRC Press.

Iscoe, I., McDonald, D., 1990. Induced Dirichlet Forms and Capacitary Inequalities. *Ann. Prob.* 18 (3): 1195-1221.

Ma, M., Rockner, M., 1990. *The Theory of (Non-Symmetric) Dirichlet Forms and Markov Processes* Springer Verlag.

Rogers, L.C.G., Pitman, J.W., 1981. Markov Functions. *Ann. Prob.*, 9 (4): 573-582.

Singh, A., Hespanha, J.P., 2005. Models for Multi-Specie Chemical Reactions Using Polynomial Stochastic Hybrid Systems. *Proc. of 44th Conference in Decision and Control*, IEEE Press.

Tabuada P. 2006. *Cyber-Physical Systems: Position Paper* presented at NSF Workshop on Cyber-Physical Systems.