Bisimulation, Logic and Reachability Analysis for Markovian Systems

Manuela L. Bujorianu and Marius C. Bujorianu

***Abstract*— In the recent years, there have been a large amount of investigations on safety verification of uncertain continuous systems. In engineering and applied mathematics, this verification is called stochastic reachability analysis, while in computer science this is called probabilistic model checking (PMC). In the context of this work, we consider the two terms interchangeable. It is worthy to note that PMC has been mostly considered for discrete systems. Therefore, there is an issue of improving the application of computer science techniques in the formal verification of continuous stochastic systems.**

We present a new probabilistic logic of model theoretic nature. The terms of this logic express reachability properties and the logic formulas express statistical properties of terms. Moreover, we show that this logic characterizes a bisimulation relation for continuous time continuous space Markov processes. For this logic we define a new semantics using state space symmetries. This is a recent concept that was successfully used in model checking. Using this semantics, we prove a full abstraction result. Furthermore, we prove a result that can be used in model checking, namely that the bisimulation preserves the probabilities of the reachable sets.

Keywords: ***model theoretic probabilistic logic, Markov processes, bisimulation, symmetries, excessive functions, probabilistic model checking.***

I. Introduction

When the randomness and the continuity coexist in the system model, the safety verification gains an explosive complexity. We address this issue defining a logic, called *behaviour stochastic logic* (BSL), for model checking safety properties over continuous state spaces. In control engineering, this verification method is better known and developed under the name of stochastic reachability analysis.

Considering BSL, we introduce a natural concept of bisimulation. Two continuous Markov processes are considered bisimilar if they have the same reach set probabilities.
Recent advances in probabilistic model checking have been achieved using the state space symmetries [9]. We use space symmetries to define a new semantics for BSL. One main advantage of this new semantics is that we can refine the bisimulation concept. In practice, the probabilities are approximated and their equality is difficult to check. The most of current approaches consider a metric and ask that the transition probabilities are approximately equal. In our approach, we ask the equality only for the reach set probabilities associated to some sets selected using the symmetries. One advantage of this definition is that some transition probabilities might be different, but these differences should be 'compensated' when we consider global behaviors..

Manuela L. Bujorianu is with Faculty of Computer Science, Unversity of Twente, The Netherlands L.M.Bujorianu@cs.utwente.nl

Marius C. Bujorianu is with CICADA, Unversity of Manchester, The UK

Using state space symmetries, we establish two important results. One of them assures the full abstraction characterisation of this new logic. The second one opens the possibility of model checking BSL formulas.

II. Probabilistic Background and Main Hypotheses

Let us consider $M = (x_t, P_x)$ a strong Markov process with the state space X, and with underlying probability space $(\Omega, \mathcal{F}, P)$. X is equipped with its Borel σ-algebra (generated by the open sets), denoted by $\mathcal{B}(X)$. Recall that any process is adapted to the filtration it induces, i.e. $\mathcal{F}_t^0 = \sigma\{x_t, s \leq t\}$ for $t \in [0, \infty)$ and $\mathcal{F}^0 = \vee_t \mathcal{F}_t^0$. $(\mathcal{F}_t^0)$, called the *minimum admissible filtration* or the *natural filtration*. A process being adapted to a filtration just means, for each time, the filtration gives us enough information to find the value of the process. Let $\mathcal{F}$ and $\mathcal{F}_t$ be the appropriate completion of σ-algebras $\mathcal{F}^0$ and $\mathcal{F}_t^0$. $\mathcal{F}_t$ describes the history of the process up to the time t.

Technically, with any state $x \in X$ we can associate a natural probability space $(\Omega, \mathcal{F}, P_x)$ where P_x is a probability measure such that $P_x(x_t \in A)$ is $\mathcal{B}$-measurable in $x \in X$, for each $t \in [0, \infty)$ and $A \in \mathcal{B}$, and its initial probability distribution is

$$P_x(x_0 = x) = 1.$$

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 it is measurable w.r.t. the history of the process, i.e. $\{\tau \leq t\} \in \mathcal{F}_t, \forall t \geq 0$. In particular, any Markov chain is a strong Markov process. There exist cases when the simple Markov property does not imply the strong Markov property. This is because there could be subtle linkages between random times and the evolution of the process. If the time is discrete then the strong Markov property is implied by the ordinary Markov property.
We adjoin an extra point ∂ (the cemetery) to X as an isolated point, $X_\partial = X \cup \{\partial\}$. The existence of ∂ is assumed in order to have a probabilistic interpretation of $P_x(x_t \in X) < 1$, i.e. ∂ is the state where the process lies when it 'dies'. Then, the 'termination time' $\zeta(\omega)$ is the random time when the process M escapes to and is trapped at ∂.

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).
A transition function $p_t(x, \Gamma)$ is a *transition probability function* for a time homogeneous Markov process if $P\{x_{t+s} \in$

$\Gamma|\mathcal{F}_t\} = p_s(x_t, \Gamma)$, for all $s, t \geq 0$ and $\Gamma \in \mathcal{B}(X)$. The relation between the transition probabilities and the Wiener probabilities is given by $p_t(x, \Gamma) = P_x(x_t \in \Gamma)$, for all $t \geq 0$ and $\Gamma \in \mathcal{B}(X)$.

Borel Process

We suppose that the process M satisfies some regularity assumptions, as follows.

1. M paths are right-continuous with left limits (cadlag property), i.e. if all the paths $t \to x_t(\omega)$ are right continuous functions on $[0, +\infty)$ and have left-hand limits on $[0, \zeta)$ almost surely.

2. X is a separable metric space homeomorphic to a Borel subset of some compact metric space (X is called Lusin space), equipped with Borel σ-algebra $\mathcal{B}(X)$ or shortly $\mathcal{B}$. Let $\mathcal{B}(X_\partial)$ be the Borel σ-algebra of X_∂.

3. The operator semigroup of M maps $\mathbf{B}(X)$ into itself.

4. M is strong Markov process.

Hypotheses 2., 3., 4. mean that M is a Borel right process [11]. These assumptions are inspired by our work in stochastic hybrid systems [5]. Usually, the semantics of a stochastic hybrid system is such a process.

We have used the following concepts:

- The set $\mathbf{B}(X)$ is the Banach space, that is a complete linear normed space, of *bounded real measurable functions* defined on X, with the sup-norm $||\varphi|| = \sup_{x \in X} |\varphi(x)|$, $\varphi \in \mathbf{B}(X)$.
- On $\mathbf{B}(X)$, one can define the *semigroup of operators* (P_t), given by

$$P_t f(x) = E_x f(x_t) = \int f(y) p_t(x, dy), t \geq 0 \quad (1)$$

  where E_x is the expectation with respect to P_x and $p_t(x, A)$, $x \in X$, $A \in \mathcal{B}$ represent the transition probabilities. The semigroup property of (P_t) can be derived from the Chapman-Kolmogorov equations satisfied by the transition probabilities. The right-hand derivative of P_t for $t = 0$ is called the *infinitesimal operator* (or generator) of the process. The operator semigroup and the generator belong to the functional analysis characterisation of a Markov process.
- A function f is *excessive* with respect to the semigroup (P_t) if it is measurable, non-negative and $P_t f \leq f$ for all $t \geq 0$ and $P_t f \nearrow f$ as $t \searrow 0$.

Let $\mathcal{E}_M$ be the set of all excessive functions associated to M. According to the Blumenthal-Getoor-McKean theorem [6], the cone of excessive functions determines the process up to a time change. For a Markov process, the excessive functions play the role of the *superharmonic functions* from the theory of partial differential equations (for example, for the well known Laplacian Δ of the heating equation, a function f is superharmonic if $\Delta f \leq 0$).

For a better understanding of the concept of excessive function we instantiate M with a continuous-time Markov chain (CTMC), with a denumerable state space I and with the stochastic transition matrix $P(t) = (p_{ij}(t))$, where i and j range over I. Let us denote by $Q = (q_{ij})$ the right-hand derivative at $t = 0$ of $P(t)$. Q is called the generator (stochastic) matrix of the chain and each element q_{ij} represents the transition rate from i to j.

A sequence $C = \{C(i)\}$ of nonnegative finite numbers indexed by I is called a $P(t)$-excessive if $P(t)C \leq C$ for all t.

From [7], we can derive the following characterization of the excessive functions associated to a CTMC.

Proposition 1: C is $P(t)$-excessive if and only if $C \geq 0$ and $QC \leq 0$.

To the operator semigroup, one can associate the *kernel operator* or *Green kernel* as

$$Vf = \int_0^\infty P_t f dt, \; f \in \mathbf{B}(X) \quad (2)$$

The kernel operator is the inverse of the opposite of the infinitesimal operator associated to M. For a Markov chain, the kernel operator is the opposite of the inverse of its stochastic matrix. For any $f \in \mathbf{B}(X)$, $f \geq 0$; we call Vf the *potential* associated to f. The name of "potential" for F is justified by the fact that it has an analogous property with respect to the generator of the process, as the classical Newtonian potential with the distribution $f(x)$ with respect to the Laplace operator Δ. We denote by $\mathcal{P}_M$ the set of potentials. Each potential is itself an excessive function, i.e. $\mathcal{P}_M \subset \mathcal{E}_M$ [11]. The potentials will be used in the proof of Theorem 5. The excessive functions can be generated by *potentials*, using a (balayage) theorem due to Hunt [8].

Remark 1: The state space X can be chosen to be an analytic space (as the most general case), but we restrict ourself to the case of a Lusin space because we intend to apply the results of this paper to stochastic hybrid systems whose realizations have, in most of the cases, Lusin state spaces [4].

Transience

We assume also that M is *transient*. This means that there exists a strictly positive Borel function q such that Vq is bounded. The transience of M means that any process trajectory which will visit a Borel measurable set of the state space, it will leave it after a finite time.

Remark 2 (Illustration of kernel operator formula): If M is a discrete time Markov chain on a countable space X, then the kernel operator (or the Green function)

$$V(x, y) = \sum_{n=0}^{\infty} p^{(n)}(x, y) = \sum_{n=0}^{\infty} P_x[x_n = y] \quad (3)$$

where $p^{(n)}(x, y)$ represent the n-step transition probabilities and P_x is the law of the chain $\{x_n | n \geq 0\}$ when $x_0 = x$. The transience of M means that

$$V(x, y) < \infty, \forall x, y \in X.$$

The transience hypothesis guarantees that the cone $\mathcal{E}_M$ is rich enough to be used.

III. Behavioural Stochastic Logic

In this section, we propose a logic, called Behavioural Stochastic Logic (BSL), for specifying properties of general Markov processes defined as in Section 2. Although, in scope, this logic is similar to other probabilistic logics, its analytical models might look non-standard from the traditional formal methods perspective.

We specialise a variant of Larsen and Skou's probabilistic modal logic [10] for Borel right processes. Our approach differs fundamentally. The formulas of the logic are upper bounds for probabilities of reachable sets.

The syntax is constructed from a formal description of a Markov process. That means we have a logic language where we can specify concepts like probability space, random variables, transition probabilities.

The main design scheme is based on the following principles. The system is modelled by a general Markov process. The sets of states are coded by their indicator functions. Obviously, these are measurable bounded functions (elements of $\mathbf{B}(X)$). The application of the kernel operator on these functions generates the probabilities of the events that the system trajectories hit the respective sets. This spectacular interpretation has been actually researched, in the last half of the 20th century, starting with the pioneering work of Hunt [8].

The vocabulary of the logic is given by a family of measurable sets in a Lusin space. Each set is represented by its indicator function. For example, the interval $A = [0, 1/2]$ is represented, in the logic, by the function 1_A, which in each point x takes the value 1 if $0 \leq x \leq 1/2$ and the value 0 otherwise. The union of two disjoint sets A and B will be represented by the function $1_A + 1_B$. The intersection of two sets A and B will be represented by the function $\inf(1_A, 1_B)$. The complementary of the set A is represented by $1 - 1_A$.

We consider a linear space of bounded measurable functions, which is ranged over by the variable f. We define the *terms* by the following rules:

- the atomic terms are given by $\mathbf{1}$ or $\mho.f$, where $\mho$ is an '*action operator*'
- any other term is obtained from the atomic terms using:

$$g := \inf(g, g') | \sup_{n \in \mathbb{N}} g_n \tag{4}$$

The set of terms is denoted by $\mathcal{T}$.

A *formula* is a statement of the form $g \leq v$, where g is a term and v is a real number in $[0, 1]$. The other formulas are obtained using the usual boolean operators.

The semantics is defined as follows.
The semantic domain is necessarily a Markov process $M = (\Omega, \mathcal{F}, \mathcal{F}_t, x_t, P_x)$ satisfying the hypotheses of Section 2.

We consider only those bounded measurable functions that are indicator functions of measurable sets of states. For simplicity, consider a term, which contains only a bounded measurable function f. Intuitively, a term denotes a function that when applied to a state x provides the probability a trajectory, starting from x, reaches a set 'indicated' by f. The reachability problem is formulated relatively to several sets of states, then the term is formed with their indicator functions.

The interpretation of a term $f \in \mathcal{T}$ is a function $f : X \to \mathbb{R}$, which belongs to $\mathbf{B}(X)$. The interpretation $\Im$ of the atomic terms is given by:

$$\Im(\mathbf{1}) \quad = \mathbf{1} \ , \quad \Im(\mho.f) \quad = \mho.g$$

where, for all $x \in X$

$$\mathbf{1}(x) = 1, \ (\mho.g)(x) = \int [\int_0^\infty g(x_t(\omega))dt] P_x(d\omega)$$

The infimum and supremum are defined pointwise.
The following characterization of the action of $\mho$ to a term g is insightful

$$(\mho.g)(\cdot) = E.[\int_0^\infty g(x_t)dt] = \int_0^\infty P_t g(\cdot)dt = Vg(\cdot). \tag{5}$$

The terms are statistical statements about sets in the state space. An atomic term is the expectation of the random variable provided by the "visits" of a target set. In the discrete state space, this interpretation can be easily checked using formula (3).

Example 1: Consider the case of an aircraft for which we want to check that the probability to reach the sphere $S(u, 2)$ starting from an initial point x is less than 0.01. We can consider a Markov process in the Euclidean space modelling the aircraft dynamics. The probability is given by the following BSL formula

$$\mho.(1_{S(u,2)})(x) \leq 0.01$$

which in the above semantics means

$$E_x[\int_0^\infty 1_{S(u,2)}(x_t)dt] \leq 0.01.$$

This formula appears frequently in the mathematical models used in air traffic control (See, for example, the references of the recently completed EU Hybridge project[1]).

The BSL logic can be fruitfully applied to performance analysis. In [3], it is shown that the expressions (5), represent performance measures for the fluid models of communication networks. Here, the expressions (5) represent the semantics of BSL formulas. Moreover, in the cited paper, there is described a model checking strategy of the expressions (5) against strong Markov processes. Therefore, the BSL formulas characterise the model checking of performance measures.

IV. BSL semantics based on symmetries

Symmetry reduction is an efficient recently developed method [9] for explointing the occurence of replication in a model. The verification of a model can be then performed when a bisimilar quotient model, which is (up to factorially)

[1] http://www2.nlr.nl/public/hosted-sites/hybridge/

smaller. This is why, in this section, we explore the possibility of an alternative semantics of BSL based on symmetries. This new semantics is useful for extending the symmetries based model checking of Kwiatovska e.a. [9] to systems with continuous state components.

Let $\mathcal{S}(X)$ be the group of all homeomorphisms $\varphi : X \to X$, i.e. all bijective maps φ such that φ, φ^{-1} are $\mathcal{B}(X)$-measurable. When X is finite, $\mathcal{S}(X)$ is the set of (finite) permutations of X.

Any permutation[2] of X induces a permutation of the group of measurable functions (in particular of the terms) as follows. Let

$$* : \mathcal{S}(X) \to Perm[\mathbf{B}(X)]$$

be the *action* $\mathcal{S}(X)$ to $\mathbf{B}(X)$ defined by

$$*(\varphi) = \varphi^* : \mathbf{B}(X) \to \mathbf{B}(X)$$

where φ^* is the linear operator on $\mathbf{B}(X)$ given by

$$\varphi^* f = f \circ \varphi. \tag{6a}$$

The range of $*$ is included in $Perm[\mathbf{B}(X)]$ (the permutation group of $\mathbf{B}(X)$). This fact is justified by the invertibility of φ^*. The invertibility of φ^* can be derived from the bijectivity of $\varphi \in \mathcal{S}(X)$ because it is clear that

$$(\varphi^*)^{-1} = (\varphi^{-1})^*$$

Then φ^* can be thought of as a symmetry of $\mathbf{B}(X)$ for each φ given in the appropriate set.

Consider now a Markov process M, as in the Section 2. The excessive function cone $\mathcal{E}_M$ is clearly a semigroup included in $\mathbf{B}(X)$, but we can not define the action of $\mathcal{S}(X)$ to $\mathcal{E}_M$ using formula (6a) because the result of composition in (6a) is not always an excessive function.

Therefore it is necessary to consider some subgroups of permutations of the state space such that we can define the action of these subgroups on the semigroup of the excessive functions $\mathcal{E}_M$.

We consider the *maximal subgroup of permutations* of the state space X, denoted by $\mathcal{H}$, such that we can define the *action of* $\mathcal{H}$ to $\mathcal{E}_M$ denoted also by $*$

$$* : \mathcal{H} \to Perm[\mathcal{E}_M]$$

defined as the appropriate restriction of (6a). The elements of $\mathcal{H}$ 'preserve' through '$*$' the excessive functions (the weak solutions associated to the infinitesimal operator of the Markov process M), or in other words the stochastic specifications of the system.

In the spirit of [9], the elements of $\mathcal{H}$ are called *automorphisms*. Note that in [9], the automorphisms are permutations of the state space, which preserve the transition system relation. For the Markov chains, the automorphisms defined in [9] preserve the probability transition function. For the case of continuous-time continuous space Markov processes, a transition system structure is no longer available (the concept of next state is available only for Markov chains). Therefore, it should be the case that the definition of the concept of automorphism to be different: An automorphism must preserve the probabilistic dynamics of the system. To express formally this idea, we need to use global parameterizations of Markov processes different from transition probabilities, which are local and depend on time. This is the reason why we have defined these automorphisms as maps which preserve the excessive functions.

In particular, using the Proposition 1, it is easy to prove that the automorphisms defined for Markov chains in [9] preserve, as well, the excessive functions, i.e. are automorphisms in the sense of this paper.

Using $\mathcal{H}$, an equivalence relation $\mathcal{O} \subset X \times X$, called *orbit relation*, can be defined on the state space X as follows.

Definition 1: Two states x, y are in the same orbit, written $x\mathcal{O}y$, if and only if there exists an automorphism $\varphi \in \mathcal{H}$ such that $\varphi(x) = y$.

Let us denote by $[x]$ the equivalence class containing the point x in X. The equivalent classes of $\mathcal{O}$ are called *orbits.* It is clear that an orbit $[x]$ can be described as

$$[x] = \{\varphi(x) | \varphi \in \mathcal{H}\}.$$

Let $X/_{\mathcal{O}}$ denote the set of orbits, and let $\Pi_{\mathcal{O}}$ the canonical projection

$$\Pi_{\mathcal{O}} : X \to X/_{\mathcal{O}},\ \Pi_{\mathcal{O}}(x) = [x]. \tag{7}$$

The space $X/_{\mathcal{O}}$ will be equipped with the quotient topology by declaring a set $A \subset X/_{\mathcal{O}}$ to be open if and only if $\Pi_{\mathcal{O}}^{-1}(A)$ is open in X. It is clear now that $\Pi_{\mathcal{O}}$ is a continuous map with respect to the initial topology of X and the quotient topology of $X/_{\mathcal{O}}$.

Consider an automorphism $\varphi \in \mathcal{H}$.

Definition 2: A term g is called *φ-symmetric in* $x, y \in X$ if

$$\varphi(x) = y \Rightarrow g(x) = g(y). \tag{8}$$

The φ-symmetry property of a term gives rise to a new concept of *satisfaction* for a formula.

Definition 3: A formula $g \leq v$ is *equally satisfied* in $x, y \in X$ if there exists an automorphism $\varphi \in \mathcal{H}$ such that g is *φ-symmetric*.

V. Bisimulation

The computational equivalence of processes (or bisimulation) is the traditional tool for reducing the complexity of the system state space. In the observational case, the probabilistic bisimulation has been subject of intensive research. In the behavioural case, the stochastic bisimulation relation has been defined and investigated in a categorical setting in [5]. In the following, we refine this bisimulation for a class strong Markov processes in an analytical setting. Behavioural properties can be much more easily checked using a bisimilar system abstraction as illustrated in [4], [3].

For a continuous time continuous space Markov process M with the state space X, an equivalence relation $\mathcal{R}$ on X is a *(strong) bisimulation* if for $x\mathcal{R}y$ we have

$$p_t(x, A) = p_t(y, A), \forall t > 0, \forall A \in \mathcal{B}(X/_R) \tag{9}$$

[2]Here, permutation is used with the sense of one-to-one correspondence or bijection.

where $p_t(x, A)$, $x \in X$ are the transition probabilities of M and $\mathcal{B}(X/_R)$ represent the σ-algebra of measurable sets closed with respect to $\mathcal{R}$. This variant of strong bisimulation considers two states to be equivalent if their 'cumulative' probability to 'jump' to any set of equivalent classes (that this relation induces) is the same. The relation (9) is hard to be checked in practice since the time t runs continuously. Therefore, to construct a robust bisimulation relation on M it is necessary to use other characterising parameters of M, such that formula (9) can be derived as a consequence of this new bisimulation.

In the following we briefly present the concept of bisimulation defined in [4]. This concept is more robust because it can be characterized by an interesting pseudometric according to [4].

Let $E \in \mathcal{B}(X_\partial)$ be a measurable set and T_E its *first hitting time*. In the study of stochastic processes in mathematics, a hitting time (or first hit time) is a particular instance of a stopping time, the first time at which a given process "hits" a given subset of the state space. Formally, T_E is defined as

$$T_E = \inf\{t > 0 | x_t \in E\}.$$

Then, one can define the *hitting operator* associated to T_E on $\mathbf{B}(X)$ by

$$P_E f(x) = P_x[f(x_{T_E}) | T_E < \infty]. \tag{10}$$

If f is excessive, then so is $P_E f$. In particular,

$$P_E 1(x) = P_x[T_E < \infty]$$

is excessive for any $E \in \mathcal{B}(X_\partial)$. It can be shown that this function represents the probability measure of the set of process trajectories which hit the target set E, in infinite horizon time [4]. Formally, we have

$$P_x[T_E < \infty] = P_x[Reach(E)]$$

where, the set of trajectories is

$$Reach(E) = \{\omega \in \Omega | \exists t \in [0, \infty) \text{ s.t. } x_t(\omega) \in E\}.$$

Suppose we have given a Markov process M on the state space X, with respect to a probability space $(\Omega, \mathcal{F}, \mathbf{P})$. Assume that $\mathcal{R} \subset X \times X$ is an equivalence relation such that the quotient process $M|_\mathcal{R}$ is still a Markov process with the state space $X/_\mathcal{R}$, with respect to a probability space $(\Omega, \mathcal{F}, \mathbf{Q})$. That means that the projection map associated to $\mathcal{R}$ is a Markov function.

Definition 4: A relation $\mathcal{R}$ is called a behavioral bisimulation on X if for any $A \in \mathcal{B}(X/_\mathcal{R})$ we have that

$$\mathbf{P}[T_E < \infty] = \mathbf{Q}[T_A < \infty]$$

where $E = \Pi_\mathcal{R}^{-1}(A)$ (i.e. the reach set probabilities of the process M and $M|_\mathcal{R}$ are equal).

Our first major assumption is that $X/_\mathcal{O}$ is a Lusin space. Often, this assumption can be checked, but there are some cases when $X/_\mathcal{O}$ fails to be even a Hausdorff space (i.e. it is possible that two different orbits to share the same vicinity system). In these cases some minor modifications of X (changing, for example, the original topology) lead to a Hausdorff quotient space.

The main result of this section is that the orbit relation $\mathcal{O}$ is indeed a bisimulation relation defined on the state space X.

Theorem 2: The orbit relation $\mathcal{O}$ is a behavioral bisimulation (as in the Definition 4).

To prove this theorem we need some auxiliary results, which will be developed in the following.

Lemma 3: If $f \in \mathcal{E}_M$ and $\varphi \in \mathcal{H}$ then

$$P_E f = \varphi^*[P_F(\vartheta)] \tag{11}$$

where

$$F = \varphi(E);\ \vartheta = \varphi^{-1*} f$$

the action of '$*$' is given by (6a) and P_F is the hitting operator associated to F.

Remark 3: The equality (11) remains true for functions of the form $f_1 - f_2$ where f_1 and f_2 are excessive functions, and from there to arbitrary Borel measurable functions.

Proposition 4: Let $g : X/_\mathcal{O} \to \mathbb{R}$ be a $\mathcal{B}(X/_\mathcal{O})$-measurable and let $E = \Pi_\mathcal{O}^{-1}(A)$ for some $A \in \mathcal{B}(X/_\mathcal{O})$. Then the following equality holds

$$P_E = \varphi^* \circ P_A, \forall \varphi \in \mathcal{H} \tag{12}$$

applied to all functions f

$$f : X \to \mathbb{R},\ f = g \circ \Pi_\mathcal{O}.$$

Formula (12) shows that the function $P_E f$ (where $f = g \circ \Pi_\mathcal{O}$) is constant on the equivalent classes with respect to $\mathcal{O}$. Then it makes sense to define a collection of operators (Q_A) on $(X/_\mathcal{O}, \mathcal{B}(X/_\mathcal{O}))$ by setting

$$Q_A g([x]) = P_E(g \circ \Pi_\mathcal{O})(x) \tag{13}$$

where $E = \Pi_\mathcal{O}^{-1}(A)$. Proposition 4 allows to use any representative x of $[x]$ in the right side of (13). It easy to check that

$$Q_A Q_B = Q_B$$

if A and B are open sets of $X/_\mathcal{O}$ with $B \subset A$. Under some supplementary hypotheses one can construct a Markov process

$$M/_\mathcal{O} = (\Omega, \mathcal{F}, \mathcal{F}_t, [x]_t, Q_{[x]})$$

with these hitting operators [6].

Now, we have all the auxiliary results needed to prove the Theorem 2.

Proof of the Th.2. If $E = \Pi_\mathcal{O}^{-1}(A)$ for some $A \in \mathcal{B}(X/_\mathcal{O})$ and we let $g \equiv 1$ in (13) then, for all $x \in X$

$$P_x[T_E < \infty] = Q_{[x]}[T_A < \infty]. \tag{14}$$

Formula (14) illustrates the equality of the reach set probabilities, i.e. $\mathcal{O}$ is a bisimulation relation. ■

A. Logical Characterization of Bisimulation

Theorem 5 (Full Abstraction Theorem): Any two states $x, y \in X$ are bisimilar (through $\mathcal{O}$) if and only if, each BSL formula is equally satisfied in x, y.

Proof of the Th. 5.

Necessity:

$x\overline{\mathcal{O}}y$ implies that there exists $\overline{\varphi} \in \mathcal{H}$ such that $\overline{\varphi}(x) = y$. Since $\overline{\varphi} \in \mathcal{H}$, for all $g \in \mathbf{B}(X)$ we have from Lemma 3 (taking $E = \{\partial\}$ and $\overline{\varphi}\{\partial) = \partial$) that

$$Vg(x) = V(g \circ \overline{\varphi}^{-1})(\overline{\varphi}(x))$$

Or, taking $\varphi = \overline{\varphi}^{-1}$

$$Vg(x) = (Vg \circ \varphi)(x) \tag{15}$$

and using the fact any excessive function f is the limit of an increasing sequence of potentials (by Hunt theorem [2]) we can make the following reasoning. For a function $f \in \mathcal{E}_M$ there exists a sequence $(g_n) \subset \mathbf{B}(X)$ such that Vg_n is increasingly converging to f. Then, from (15), we obtain that

$$(f \circ \varphi)(x) = \uparrow \lim Vg_n(\varphi(x)) = \uparrow \lim Vg_n(x), \forall x \in X,$$

i.e., we get that

$$f(x) = (f \circ \varphi)(x), \forall f \in \mathcal{E}_M$$

Therefore, the evaluations of each stochastic specification (excessive function) f in x and y are equal when $x\mathcal{O}y$. Then the result is true also for $f \in \mathcal{T}$, since any measurable function can be represented as the difference of two excessive function.

Sufficiency:

In this case, we have to show that if for each $f \in \mathcal{T}$ there exists $\varphi \in \mathcal{H}$ such that (8) is true, then $x\mathcal{O}y$. This statement is straightforward. ∎

The Full Abstraction Theorem establishes that our model is correct and complete for the behavioural stochastic logic. It provides new insights to the bisimulation relation $\mathcal{O}$, as follows.

Two states are equivalent when, for all system trajectories passing them, some relevant probabilistic properties are evaluated to be the same. This computational copy of a state is given by the permutation φ from (8).

Corollary 6: The action of $\mathcal{H}$ to $\mathcal{E}_M$ can be restricted as the action of $\mathcal{H}$ to $\mathcal{P}_M$, i.e.

$$* : \mathcal{H} \times \mathcal{P}_M \to \mathcal{P}_M$$

given by (6a).

This corollary is a direct consequence of the fact that $\mathcal{P}_M$ generates the cone $\mathcal{E}_M$. Then in the definition of $\mathcal{O}$, we can work not with excessive functions, but with potentials. This means that we can give the following characterisation of the orbit relation.

Proposition 7: $x\mathcal{O}y$ if and only if they have the 'same potential', i.e. there exists $\varphi \in \mathcal{H}$ such that

$$Vf(x) = Vf(y), y = \varphi(x)$$

for all $f \in \mathbf{B}(X)$

Corollary 8: If $x\mathcal{O}y$ then there exists $\varphi \in \mathcal{H}$ such that $\varphi(x) = y$ and

$$p_t(x, \varphi^{-1}(A)) = p_t(y, A), \forall t \geq 0, \forall A \in \mathcal{B}.$$

VI. Conclusions

In this paper, we have proposed a *foundational* approach to specification and verification of behavioural stochastic models. To the authors' knowledge, this problem is new. For the logic, named *behavioural stochastic logic*, we construct a fully abstract model in a class of Markov processes. We borrow the specification methodology used for Petri nets. A net can describe the system structure, but also its behaviours (the processes). In our case, a system can be specified, for example, by a set of stochastic differential equations (SDEs) and a set of discrete transitions between them (see, for example, the concept of *stochastic hybrid systems* [5]). Behaviours (or processes) of this kind of systems are composed by solutions of SDEs. If the mathematical expressions of these solutions would be known, computational methods would be easier available. Instead, we have to comply with the behavioural (or analytical, non-constructive) way of reasoning from mathematics. The existence of a fully abstract model, but still very general and constructive, forms the basis for future automated reasoning systems.

Considering the efficient model checking methods based on symmetry reduction [9], it is natural to further investigate developing similar numerical methods for BSL.

References

[1] Borkar, V.S.: "*Probability Theory. An Advance Course.*" Springer Verlag, (1995).

[2] Boboc, N., Bucur, G., Cornea, A.: "*Order and Convexity in Potential Theory. H-Cones"*. Lecture Notes in Math, Vol. **853**, Springer Verlag (1992).

[3] Bujorianu, M.L., Bujorianu, M.C.: *A Model Checking Strategy for a Class of Performance Properties of Fluid Stochastic Models*. In M. Telek e.a. eds., Proceedings of 3rd European Performance Engineering Workshop, Springer LNCS, (2006)

[4] Bujorianu, M.L., Lygeros, J., Bujorianu, M.C.: *Abstractions of Stochastic Hybrid System.* Proc. 44th Conference in Decision and Control. IEEE Press (2005).

[5] Bujorianu, M.L., Lygeros, J., Bujorianu, M.C.: *Bisimulation for General Stochastic Hybrid Systems*. In [12]: 198-216.

[6] Blumenthal, R.M., Getoor, R.K.: "*Markov Processes and Potential Theory*", Academic Press, New York and London (1968).

[7] Chamberlain, M.W.: *The excessive functions of a continuous time Markov chain*. Ann. of Prob. **2** (6) (1974): 1075-1089.

[8] Hunt, G.A.: *Markov Processes and Potential I*, Illinois J.Math., **1** (1957): 44-93.

[9] Kwiatkowska, M., Norman, G., Parker, D.: *Symmetry Reduction for Probabilistic Model Checking*. In Proc. 18th International Conference on Computer Aided Verification (CAV'06), LNCS **4144**, (2006): 234-248.

[10] Larsen, K.G., Skou, A.: *Bisimulation through Probabilistic Testing*. Information and Computation, **94** (1991): 1-28.

[11] Meyer, P.-A.: "*Probability and Potential*". Blaisdell, Waltham Mass, (1966).

[12] Morari, M., Thiele, L. (Eds.): "*Proc. Hybrid Systems: Computation and Control*" 8th International Workshop, Springer LNCS 3414 (2005)