2007 Mediterranean Conference on Control and
Automation, July 27 - 29, 2007, Athens - Greece

Topological Superposition of Abstractions of Stochastic Processes

Manuela L. Bujorianu*, Marius C. Bujorianur†
*University of Twente/Faculty EWI, Enschede, The Netherlands
†University of Kent/Computing Laboratory, Canterbury, UK

***Abstract*— In this paper, we present a sound integration mechanism for Markov processes that are abstractions of stochastic hybrid systems (SHS). In a previous work, we have defined a very general model of SHS and we proved that the realization of an SHS is a Markov process. Moreover, we have developed a verification strategy for the reachability analysis problem. We develop further this line of research by making verification modularly. To achieve this, the state space is decomposed into regions that might share a common border. An abstraction can be constructed on each region and the abstraction method can vary from one region to another. We show how these abstractions can be integrated to provide an abstraction for the entire system. We illustrate this technique for the reachability analysis problem.**

Keywords: Markov processes, stochastic hybrid system, reachability analysis, superposition.

I. Introduction

The use of randomisations makes possible a very expressive modelling of hybrid systems, but the price to be paid is an extremely complex verification process. This issue is addressed, in this work, by exploiting the idea of modularity. The modular (or compositional) verification has become recently a topic of intensive investigations. The peculiar structure of SHS and the inherent high level mathematics involved suggest that the modular verification should be related to the topological structure of the large, mathematically complex state spaces of these systems. Unfortunately, there is a fundamental obstacle in composing subsystems verified by different methods. There is no result to guarantee that inconsistencies will not appear when superimposing topological subspaces of the state space. Moreover, in many situations, it is useful to have an entire system abstraction instead of a sheaf of abstractions of system projections on topological subsets.

The main contribution of this paper is to propose a method of checking consistency of different system abstractions when the state space has been topologically partitioned. Moreover, we construct the entire system abstraction from its projections.

Further, we consider the case when a property of interest spans over the partition of the state space (a cross-cutting concern). For example, in stochastic reachability analysis (SRA), it is necessary to provide an upper bound for the probability of hitting a given state set starting from an initial state. In [5], it is shown that this problem characterizes the reachability analysis for performance properties in the fluid models of computer networks. In the verification process, a partition is created such that all components share the point of interest at the border. Also, in each component, there is a projection of the target set. Now, suppose that the stochastic reachability problem is solved in each local abstraction by a specific method. The previously described construction gives a global abstraction, but it does not give a global upper bound for the probability of interest. We give a mathematical result that relates the global probability with the local abstraction probabilities via superposition gauges, solving in this way the global SRA problem.

The paper is structured as follows. In the next section we give a short background and we formulate the problem treated in this work. In Section III, we present the mathematical principles underpinning the definition of local abstractions associated to a system. In Section IV, we show how the integration process can be effectively constructed and we prove that this is a common simulation of the local abstraction processes. Then, we apply this theory to stochastic hybrid systems in Section V. The paper ends with some conclusions.

II. The Mathematical Framework

In this section, we briefly present the mathematical environment for our approach. For the reader with less background in stochastic analysis, we point out the fact that we present a rather general concept of continuous (time/ space) Markov process defined on a Hausdorff topological space. This process might be thought of as a natural extension of the concept of continuous time Markov chain to the case when the state space is *not discrete* and the trajectories are 'continuous' (not continuous functions as in mathematical analysis). To this process, one can naturally associate a *semigroup* of linear operators (formula (1) below) on the space of bounded measurable functions defined on the process state space.

A. Background

Let S be a Polish or an 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 S equipped with its Borel σ-algebra $\mathcal{B}$. Let $\mathbf{B}(S)$ be the Banach space of all bounded measurable numerical functions on S.

Formally, let $X = (\Omega, \mathcal{F}, \mathcal{F}_t, x_t, P, P_x)$ be a strong Markov process on S [10]. The sample probability space is $(\Omega, \mathcal{F}, P)$. The trajectories of X are modelled by a family of S-valued random variables (x_t), which, as

1-4244-1282-X/07/$25.00 ©2007 IEEE

functions of time, can have some continuity properties (as the càdlàg property, i.e. right continuous with left limits). The stochastic analysis identifies different parameterizations (like infinitesimal generator, operator semigroup/resolvent) that characterize in an abstract sense the evolutions of a Markov process [10].

Let $\mathcal{P} = (P_t)_{t>0}$ denote the family of linear *operators* associated to X, which maps $\mathbf{B}(S)$ into itself given by

$$P_t f(x) = \int f(y) p_t(x, dy) = E_x f(x_t), \forall x \in S \quad (1)$$

where (p_t) is the transition probability function and E_x is the expectation w.r.t. P_x.

To the semigroup $\mathcal{P}$ given by (1), one can associate its infinitesimal generator $\mathcal{L}$. The *infinitesimal generator* of $\mathcal{P}$ is the possibly unbounded linear operator $\mathcal{L}$

$$\mathcal{L}f = \lim_{t \searrow 0} \frac{P_t f - f}{t} \quad (2)$$

The domain $D(\mathcal{L})$ is the subspace of $\mathbf{B}(S)$ for which this limit exists. $\mathcal{L}$ is the derivative of P_t at $t = 0$.

B. Problem Formulation

Suppose we have given $n \in \mathbb{N}$ ($n \geq 2$) strong Markov processes $\widehat{X}_i$ with the state spaces $\widehat{S}_i$, for $i = 1, ..n$. Each space $\widehat{S}_i$ is equipped with its Borel σ-algebra $\mathcal{B}(\widehat{S}_i)$. In our terminology $\widehat{X}_i$ will be called *abstraction processes*.

Let us consider a strong Markov process X with the state space $(S, \mathcal{B}(S))$. We assume that the process X is 'simulated' by the abstraction processes locally. Then, the research problem, which derives from here is *to integrate the local abstraction processes in order to obtain a global process* that simulates the whole process X.

Formally, assume there exist a partition of the state space S with the closed sets

$$S = \cup_{i=1}^{n} F_i,\ int(F_i) \cap int(F_j) = \emptyset \text{ if } i \neq j, \quad (3)$$

and n surjective continuous maps $\psi_i : S \to \widehat{S}_i$, $i = 1, .., n$ such that $\psi_i^{-1}(\psi_i(F_i)) = F_i$.

The sets F_i can be thought of as the closures of the modes of the SHS, H.

The natural hypothesis, which we impose, is that the maps ψ_i satisfy the *zigzag morphism condition* in the sense of [6], i.e. for each $i = 1, .., n$, the process $\widehat{X}_i$ on the set $\psi_i(F_i)$ simulates the process X on F_i.

The problem is how to construct an *integration process* $\widetilde{\mathbf{X}}$ defined on $\widetilde{\mathbf{S}} = \cup_{i=1}^{n} \psi_i(F_i)$, which is still a Markov process and behaves as $\widehat{X}_i$ on $\psi_i(F_i)$, $i = 1, .., n$. This process will represent a *global abstraction* of X.

III. Region Abstractions

In this section we define the mathematical properties that a local abstraction of an SHS should have. Let us denote by S the system state space and by $\widehat{S}$ the state space of its abstraction. For the most examples of SHS, S is a Polish space. We assume the same about $\widehat{S}$.

Abstraction map. The *abstraction map* that relates S and $\widehat{S}$ is continuous surjective map $\psi : S \to \widehat{S}$. The nature of the abstraction is reflected by the mathematical properties of this map. It is desirable that these properties to capture the computational simulation of system into its abstraction. Such mathematical characterizations are given in terms of open maps and zigzag morphisms. The last characterization will be used in this paper.

Superposition space. Consider now the following situation. The verifiers have identified a set of states that the system may reach when it is performing a specific task. The continuous features of the system give rise to the necessity that this set to be considered topologically closed. It will be denoted by F. Formally, let $F \subseteq S$ be a closed subset of the state space S. Naturally, the topological space S is then decomposed in two components: the closed set F and its complement $S \backslash F$. Using the abstraction map ψ, we define the *superposition topological space* as $\widetilde{S} := (S \backslash F) \cup \psi(F)$, this being a disjoint union.

It is natural to assume that the F is 'maximal' w.r.t. ψ (in the abstraction process no extra states are added), i.e.

$$\psi^{-1}(\psi(F)) = F. \quad (4)$$

Since ψ is an abstraction map, we are not assuming that ψ is one to one. Condition (4) ensures that ψ can be restricted as a surjective map from F to $\psi(F)$.

Local abstraction. Suppose that our system dynamics is described by a stochastic process X with the state space S. Mathematically, X is a strong Markov process $X = (x_t, P^x)$ (we use, here, a short notation for X) on the probability space $(\Omega, \mathcal{F})$, with the state space S and the transition semigroup (P_t). The local abstraction of X on F will be given by another stochastic process $\widehat{X}$. Formally, $\widehat{X}$ is another strong Markov process $\widehat{X} = (\widehat{x}_t, \widehat{P}^x)$ defined on the probability space $(\widehat{\Omega}, \widehat{\mathcal{F}})$, with the state space $\widehat{S}$ and the transition semigroup $(\widehat{P}_t)$.

The goal of this section is to obtain a *local abstraction* of X, which behaves like $\widehat{X}$ when it is in $\psi(F)$ and like X in the rest of $\widetilde{S}$.

Definition 1: A *local abstraction* of X on F is an $\widetilde{S}$-valued process $\widetilde{X}$ such that: (i) its restriction to $S \backslash F$ coincides with X; (ii) its restriction to $\psi(F)$ coincides with $\widehat{X}$.

In construction of a local abstraction of X, we have been inspired by [9]. In the cited paper, it is presented a construction of a Markov process $\widetilde{X}$ on $\widetilde{S}$ by pinching X to $\psi \circ X$ when X is in F, but keeping the initial dynamics of X when it evolves in $S \backslash F$. The corner stone of this construction is what happens when $\widetilde{X}$ leaves $S \backslash F$ and enters $\psi(F)$ or viceversa.

Superposition space as a quotient space. The projection associated with an abstraction map is a function that shows how the abstraction works on the state set of interest, leaving invariant the other states. The projection map associated to ψ is a function $\pi : S \to \widetilde{S}$ given by

$$\pi := I \cdot \mathbf{1}_{S \backslash F} + \psi \mathbf{1}_F \quad (5)$$

Here, by $\mathbf{1}_A$ we denote the indicator function of a measurable set A and I is the identity function. Clearly, the projection map is the restriction of ψ on F and leaves unchanged the elements of $S \backslash F$.

The 'pinching' map π is injective on $S\backslash F$, i.e. no pinching occurs on $S\backslash F$, but is not generally injective on F. The space $\widetilde{S}$ is provided with the topology induced by π. The projection map π induces an equivalence relation $\mathcal{R}$

$$x\mathcal{R}y \Leftrightarrow \pi(x) = \pi(y) \tag{6}$$

The space $\widetilde{S}$ can be thought of as the quotient topological space S under the equivalence relation $\mathcal{R}$. Denote by $[x]$ the equivalence of $x \in S$ w.r.t. $\mathcal{R}$ defined by (6). $[x]$ is a measurable set of S.

We assume that $\widetilde{S}$ with this topology is a Polish space. The topology of $\widetilde{S}$ is equivalent to the trace topology of S on $S\backslash F$ and to the trace topology of $\widehat{S}$ on $\psi(F)$. The map π identifies the points on the boundary of $S\backslash F$ (in the topology of S) with the points on the boundary of $\psi(F)$ (in the topology of $\widehat{S}$) [9]. The Borel σ-algebra of $\widetilde{S}$ is composed by those measurable sets of $\mathcal{B}(S)$ closed under the equivalence relation $\mathcal{R}$.

From now on, we consider S, $\widetilde{S}$ and $\widehat{S}$ endowed with their Borel σ-algebras $\mathcal{B}(S)$, $\mathcal{B}(\widetilde{S})$, and, respectively, $\mathcal{B}(\widehat{S})$.

Dually, there exists a natural continuous map $\phi : \widetilde{S} \to \widehat{S}$

$$\phi := \psi \mathbf{1}_{S\backslash F} + I \cdot \mathbf{1}_{\psi(F)} \tag{7}$$

which leaves invariant the elements of $\psi(F)$ and further 'applies ψ' to the elements of $\psi(F)$.

From the formulas (5) and (7), we obtain obviously that

$$\psi = \phi \circ \pi. \tag{8}$$

Let us consider the lattices $\mathbf{B}(S)$, $\mathbf{B}(\widetilde{S})$ and respectively $\mathbf{B}(\widehat{S})$ of bounded real-valued measurable defined on S, $\widetilde{S}$ and respectively $\widehat{S}$. The abstraction map ψ can be lifted to map elements of these lattices by defining the *-map as follows: $\psi^* : \mathbf{B}(\widehat{S}) \to \mathbf{B}(S)$, $\psi^* f = f \circ \psi$. Similarly, for the projection π and its dual ϕ we can define the *-maps. The *-operation acts as an adjoint operation, i.e. $\pi^* \circ \phi^* = \psi^*$.

Lemma 1: ψ^* can be restricted to $\mathbf{B}(\psi(F))$ with values in $\mathbf{B}(F)$.

Compatibility hypotheses. A general problem in component composition (like architectural documents, software artifacts, formal specifications, mathematical models) is the compatibility of the communication infrastructure (that could be interfaces, share variables, a topological boundary, etc). In our case, this problem arises in the construction of the local abstraction at the border of F.

First, we have to impose some compatibility conditions of the abstraction map ψ and the dynamics of the processes X and $\widehat{X}$. The process $\widehat{X}$ must simulate the process X on F. This means that the abstraction map has to 'preserve' the transition probabilities of the two processes. Mathematically, ψ should be a *zigzag morphism* [6], i.e.

$$P_t \psi^* = \psi^* \widehat{P}_t. \tag{9}$$

Remark 1: The zigzag morphism condition (9), known as the Dynkin intertwining relation, appears for the first time in the context of Markov chains in [8]. This implies that the finite dimensional distributions of $\psi \circ X$ under P^x are the same as those of $\widehat{X}$ under $\widehat{P}^{\psi(x)}$ for any $x \in S$. The condition (9) says that ψ is a *Markov function* [4], i.e. $\psi \circ X$ is still a Markov process [11].

Using Lemma 1, it can be easily shown that the zigzag condition (9) is true locally on the set F.

Lemma 2: The zigzag morphism condition (9) remains true for the semigroups of the restriction of X to F and the restriction of $\widehat{X}$ to $\psi(F)$.

The main problem, in composing X and $\widehat{X}$, is the compatibility of the dynamics of the two processes at the border of F. Concretely, it appears when the local abstraction process $\widetilde{X}$, which should be soundly constructed, passes the border of F or $\psi(F)$ (which are identified in the topology of $\widetilde{S}$). If $\widetilde{X}$ would start in $\widehat{x} \in \partial_{\widetilde{S}}(S\backslash F) = \partial_{\widetilde{S}}\psi(F)$, since $\psi^{-1}\{\widehat{x}\}$ might contain more than one point in S, it is unclear where to jump in $S\backslash F$ if it decides to continue its evolution in $S\backslash F$.

We address this problem by introducing the *superposition gauges* that consider both topologies in the abstraction state space and the stochastic dynamics. A superposition gauge makes a 'smooth' common topological border realizing the sequential composition of trajectories from different subspaces. In its mathematical incarnation a superposition gauge is a probability kernel $k : \widehat{S} \times \mathcal{B}(S) \to \mathbb{R}$.

In the construction of the desired process $\widetilde{X}$, this probability kernel should give the location where to jump in $S\backslash F$, if, for example, it starts on the boundary of $S\backslash F$ and $\psi(F)$ and decides to make an excursion in $S\backslash F$. Therefore, some additional compatibility conditions w.r.t. the abstraction map should characterise, as well, a superposition gauge. The definition of a superposition gauge has to encompass these conditions, as follows.

Definition 2: A superposition gauge is a probability kernel $k : \widehat{S} \times \mathcal{B}(S) \to \mathbb{R}$, subject to the following properties: (i) $k(\widehat{x}, \psi^{-1}(\widehat{x})) = 1$, for all $\widehat{x} \in \widehat{S}$; (ii) $k(\psi(x), [x]) = 1$, for all $x \in S$.

The superposition gauge k can be lifted to act between the 'logic state formulas' of the two processes. Concretely, integrating w.r.t. the measure $k(\widehat{x}, \cdot)$, one can define a linear operator $K : \mathbf{B}(S) \to \mathbf{B}(\widehat{S})$ by

$$(Kf)(\widehat{x}) := \int f(y) k(\widehat{x}, dy). \tag{10}$$

The relation (10) shows in a natural way how to pass from the statements about the process X to statements about the simulator process $\widehat{X}$.

Remark 2: Definition 2 of the superposition gauge says that, for each $\widehat{x} \in \widehat{S}$ the probability measure $k(\widehat{x}, \cdot)$ is supported by $\psi^{-1}(\widehat{x})$. Therefore, we can restrict the action of K to $\mathbf{B}(F)$ having values in $\mathbf{B}(\psi(F))$.

Until now, we have imposed only compatibility relations between the dynamics of the two processes and the abstraction map. Naturally, it is required to impose compatibility relations between the superposition gauge and the process dynamics.

Assumption 1: Assume that the semigroups (P_t) and $(\widehat{P}_t)$ commute with K, i.e.

$$KP_t = \widehat{P}_t K. \tag{11}$$

This assumption ensures that if X has the initial probability distribution $k(\widehat{x},\cdot)$, then $\psi\circ X$ is a Markov process with the initial state equal to $\widehat{x}$ [11]. Note that the right hand side of (11), applied to an $f\in\mathbf{B}(S)$, is the integral of Kf given by (10) w.r.t. the transition probability function of $\widehat{X}$ (i.e. $\widehat{p}_t(\widehat{x},\widehat{E})=\widehat{P}_t 1_{\widehat{E}}(\widehat{x})$).

Remark 3: [9] The definition of the superposition gauge, the zigzag morphism condition and the compatibility relation (11) together imply

$$K\psi^* = I, \tag{12}$$

$$\widehat{P}_t = KP_t\psi^* \tag{13}$$

The relations (11), (12), and (13) represent the *Rogers-Pitman intertwining relations* [11].
Condition (12) is a natural compatibility condition between the abstraction map and the superposition gauge.

Remark 4: The zigzag morphism condition (9) and Remark 2 imply that the equality (11) remains true if it is restricted to $\mathbf{B}(F)$.

Suppose now we have given all the mathematical objects discussed in this section: the process X and $\widehat{X}$, state space S and $\widehat{S}$, the closed set $F\subseteq S$, the abstraction map ψ and the superposition gauge k. Then we can conclude with the existence of a local abstraction as follows.

Theorem 3: If ψ satisfies the zigzag condition (9), the superposition gauge k satisfies the compatibility condition (11), then there exists a local abstraction $\widetilde{X}$ of X on the closed set F w.r.t. the gauge k.

At this point of the presentation, we need to investigate the expression of the infinitesimal generator of a local abstraction. The expression of the infinitesimal generator of the local abstraction process will be used later for the verification purposes, treated in this paper. Roughly speaking, the infinitesimal generator of the local abstraction $\widetilde{X}$ of X on the closed set F w.r.t. the gauge k is equal with the infinitesimal generator of X on $S\backslash F$ and with the infinitesimal generator of $\widehat{X}$ composed with K on $\psi(F)$. These equalities take place via the *-map associated to the projection map π. The formal result is a version of the Proposition 4.1 from [9], for the case when the processes involved are not necessarily Feller [10].

IV. Superposition of Region Abstractions

In the previous section we have defined a local abstraction and proved some existence result. Obviously, a system that is verified only on a topological subset of its state space can be partly trusted. Usually, the state space is decomposed in a topological cover (in this case, a partition with closed sets). Then, a natural problem that arises is to ask how the abstraction process looks like on the union of this partition, i.e. to construct a system on the entire abstraction state space. This construction is presented in the current section. The section ends with an algorithm to construct the abstraction process from the local abstraction processes.

Process Local Abstractions. Let us consider the strong Markov processes X with the semigroup (P_t) and the state space S partitioned with a finite cover of closed sets $(F_i)_{i=1,..,n}$ as in (3).

For $i=1,..,n$, let us consider: (i) $\widehat{X}_i$ some the strong Markov processes with the semigroup $(\widehat{P}_t^i)$ and the state spaces $\widehat{S}_i$, which give, respectively, the local abstraction of X on F_i; (ii) the abstraction maps ψ_i, as in the Subsection II-B, satisfying the zigzag morphism condition (9) and the condition (4) w.r.t. F_i.
Since each ψ_i, $i=1,..,n$ is a zigzag morphism, and the condition (4) w.r.t. F_i holds, we have that the restriction of $\widehat{X}_i$ on $\psi_i(F_i)$ simulates the restriction of X on F_i.
All the arguments from the Section III have shown that the methodology to construct new Markov processes, which exhibit a required behavior on a certain set, needs only: 1. the local values of a *zigzag morphism*, and 2. a *superposition gauge* satisfying some compatibility relations w.r.t. the process dynamics.
Now we have to iterate the superposition construction developed in Section III. At each step i, we construct a new local abstraction (a new Markov process), which behaves like the initial process X on $X\backslash(F_1\cup F_2\cup...\cup F_i)$ and like the process $\widehat{X}_k$ on $\psi_k(F_k)$, for $k=1,..,i$. We have to define recursively the quotient spaces and the projection maps.
In the first step, we define $\widetilde{S}_1=(S\backslash F_1)\cup\psi_1(F_1)$ and the *projection map* associated to ψ_1 as $\pi_1:S\to\widetilde{S}_1$ given by $\pi_1:=I\cdot\mathbf{1}_{S\backslash F_1}+\psi\mathbf{1}_{F_1}$, i.e. pointwisely, π_1 is defined as: $\pi_1(x)=\begin{cases} x & \text{if } x\in S\backslash F_1\\ \psi_1(x) & \text{if } x\in F_1.\end{cases}$
Then, we define recursively, for $i=2,..,n$, the spaces $\widetilde{S}_i=(\widetilde{S}_{i-1}\backslash F_i)\cup\psi_i(F_i)$ and the projection maps $\pi_i:\widetilde{S}_{i-1}\to\widetilde{S}_i$ given by $\pi_i:=I\cdot\mathbf{1}_{\widetilde{S}_{i-1}\backslash F_i}+\psi_i\mathbf{1}_{F_i}$.
Let Π_i the composition of the projection maps until the ith step, i.e. $\Pi_i=\pi_i\circ\pi_{i-1}\circ...\circ\pi_1:S\to\widetilde{S}_i$, for $i=1,..,n$.
It is clear that $\Pi_i=I\cdot\mathbf{1}_{S\backslash(F_1\cup...\cup F_i)}+\sum_{k=1}^i\psi_k\mathbf{1}_{F_k}$.
The spaces $\widetilde{S}_i$ will be endowed with the topologies generated by the projection maps π_i. We assume that $\widetilde{S}_i$ with these topologies are Polish spaces. It is clear that $\widetilde{S}=\widetilde{S}_n=\cup_{i=1}^n\psi_i(F_i)$, and the *global projection map* $\Pi=\Pi_n:S\to\widetilde{S}$,

$$\Pi=\sum_{k=1}^n\psi_k\mathbf{1}_{F_k} \tag{14}$$

does not depend on the composition order.

Our goal is to construct the *global abstraction process* from the local abstractions, which should be a new Markov process $\widetilde{\mathbf{X}}$ on $\widetilde{S}$, which behaves like $\widehat{X}_i$ on $\psi_i(F_i)$, $i=1,..,n$. To complete the construction of $\widetilde{\mathbf{X}}$, we need to describe how the dynamics of $\widetilde{\mathbf{X}}$ 'jump' from one component location to another one.
Taking into consideration the results of Section III, to accomplish this construction, we need to give some *superposition gauges*, i.e. some probabilistic kernels $k_i:\widehat{S}_i\times\mathcal{B}(S)\to\mathbb{R}$, $i=1,..,n$; that describe the jumping mechanism at the boundary of $\psi_i(F_i)$. Similar to (11), some compatibility conditions should be imposed:

Assumption 2: Assume that each k_i, $i=1,..,n$ is a superposition gauge satisfying the compatibility relation of Assumption 1.

In order to be able to use the local abstraction construction presented in the Section III, we need to define

recursively the following *auxiliary gauges* (probability kernels): 1. $\widetilde{k}_1 = k_1$, 2. $\widetilde{k}_i : \widehat{S}_i \times \mathcal{B}(\widetilde{S}_{i-1}) \to \mathbb{R}, \widetilde{k}_i(\widehat{x}, \cdot) = k_i(\widehat{x}, \Pi_{i-1}^{-1}(\cdot))$, for $i = 2, .., n$ and for all $\widehat{x} \in \widehat{S}_i$.

Proposition 4: For each $i = 2, .., n$, the restriction of the kernels $\widetilde{k}_i$ to $\psi_i(F_i) \times \mathcal{B}(S \backslash (F_1 \cup ... \cup F_{i-1}))$ is a superposition gauge and satisfies the compatibility condition of the Assumption 1.

The algorithm to construct the global abstraction process $\widetilde{\mathbf{X}}$ consists in the iteration of the methodology presented in Section III. The Remarks 2-4 allow us to use at each step only the restrictions $\psi_i : F_i \to \psi_i(F_i)$ because the necessary Assumption 1 remains true. To construct the global abstraction process, one needs only the restrictions $\psi_i : F_i \to \psi_i(F_i)$ and the appropriate restrictions of the kernels $\widetilde{k}_i$, $i = 1, .., n$. Succinctly, the construction of $\widetilde{\mathbf{X}}$ can be given as the following algorithm.

Algorithm

Set $k = 0$, $F_k = \emptyset$ and $Y_k = S \backslash F_k$.

Repeat

$k = k + 1$

Choose $F_k \subset Y_{k-1}$ and the corresponding zigzag morphism ψ_k restricted to F_k. {It can be any F_i, $i = 1, .., n$ after re-indexing partition (3)}

Construct a process $\widetilde{X}_k$, which behaves as X on $Y_{k-1} \backslash F_k$, and as $\widehat{X}_i$ on $\psi_i(F_i)$, $i = 1, ..k$. {Use the method presented in Section III.}

Then $Y_k = Y_{k-1} \backslash F_k$.

Until

$Y_k = \emptyset$.

The zigzag morphism condition and the above reasoning allow us to write down the following result.

Proposition 5: The global abstraction process $\widetilde{\mathbf{X}}$ is a strong Markov process with the state space $\widetilde{\mathbf{S}} = \cup_{i=1}^{n} \psi_i(F_i)$.

Infinitesimal Generator. One of the main mathematical results of this paper is related to the generator of the integration process $\widetilde{\mathbf{X}}$. This generator will be further used to solve the reachability problem of the global abstraction process. It will be used to give the expression of the mean exit time associated to a target set in the space of the global abstraction process. Moreover, it can help to compute the transition probabilities of the integration process using the Kolmogorov backward equation.

Lemma 6: For all $i = 2, .., n$ we have: $\widetilde{K}_i : \mathbf{B}(\widetilde{S}_{i-1}) \to \mathbf{B}(\widehat{S}_i)$; $\widetilde{K}_i \widetilde{f} = K_i(\Pi_{i-1}^* \widetilde{f})$.

Notation. If $\widetilde{f} \in \mathbf{B}(\widetilde{\mathbf{S}})$ then its restriction to $\psi_i(F_i)$, i.e. $\widetilde{f}|_{\psi_i(F_i)} \in \mathbf{B}(\psi_i(F_i))$, is denoted by $\widetilde{f}_i$, for , $i = 1, .., n$. K_i and ψ_i are appropriate restrictions, i.e. $K_i : \mathbf{B}(F_i) \to \mathbf{B}(\psi_i(F_i))$; $\psi_i : F_i \to \psi_i(F_i)$, and the restriction of $(\Pi^* f)$ to F_i is denoted by f_i, where Π^* is the adjoint of the global projection defined by (14) and $\widetilde{f} \in \mathbf{B}(\widetilde{\mathbf{S}})$.

Theorem 7: Let $\widetilde{\mathbf{X}}$ and $\widehat{X}_i$ have the respective generators $\widetilde{\mathcal{L}}$ and $\widehat{\mathcal{L}}_i$, that have domains, respectively, $D(\widetilde{\mathcal{L}})$ and $D(\widehat{\mathcal{L}}_i)$, $i = 1, .., n$. The expression of the generator $\widetilde{\mathcal{L}}$ is

$$\widetilde{\mathcal{L}} \widetilde{f} = \sum_{i=1}^{n} \widehat{\mathcal{L}}_i K_i f_i \mathbf{1}_{\psi_i(F_i)} \tag{15}$$

for all $\widetilde{f} \in \mathbf{B}(\widetilde{\mathbf{S}})$, where and $\widehat{\mathcal{L}}_i$ is understood as the generator of the restriction of $\widehat{X}_i$ to $\psi_i(F_i)$ (i.e. it is applied to the extension of $\widetilde{f}_i$ with value 0 on $\widehat{S}_i \backslash \psi_i(F_i)$).

V. Mode Abstractions of Stochastic Hybrid Systems

A. Stochastic Hybrid System Definition

Let us consider a SHS, H [3]. Formally, a SHS is defined as a tuple $H = (Q, \mathcal{X}, \mathbf{F}, R, \lambda)$:

- Q is a countable or a finite set of discrete states;
- $\mathcal{X} : Q \to \mathbb{R}^{d(.)}$ maps each $q \in Q$ into a mode (an open subset) M^q of $\mathbb{R}^{d(q)}$, where $d(q)$ is the Euclidean dimension of the corresponding mode;
- $\mathbf{F} : Q \to \mathcal{F}$ specifies the continuous evolution of the automaton in terms of differential equations (ordinary/stochastic differential equations whose set is denoted by $\mathcal{F}$) over the continuous state x^q for each mode;
- $R = (R^q)_{q \in Q}$ is a family of probability kernels $R^q : \overline{M}^q \times \bigcup_{j \in Q} \mathcal{B}(M^j) \to [0, 1]$;
- $\lambda : \bigcup_{j \in Q} \overline{M}^j \to \mathbb{R}^+$ is a transition rate function[1].

The executions of an SHS can be described as follows: start with an initial point $y_0 \in M^q$, follow a continuous trajectory described by the restriction of $\mathbf{F}$ to M^q, jump when this trajectory hits the boundary or according with the transition rate λ. The jumping time is the minimum of the boundary hitting time and the time, which is exponentially distributed with the transition rate λ. From each mode q, the post-jump locations are given the probability kernel R^q. Under standard assumptions, for each initial condition $y \in \bigcup_{j \in Q} M^j$, the possible trajectories starting from y, form a stochastic process. Moreover, under standard assumptions [3], for all initial conditions y, the executions of an SHS make up a Markov process.

B. Mode Abstraction Superposition

The simplest way to apply to an SHS the methodology of composing local abstractions developed in the Section IV, is to suppose that the continuous evolution of each mode is simulated through an abstraction map by a simpler stochastic process. Then, the problem becomes how to construct the superposition gauges needed in the construction of the global abstraction.

Let us consider a SHS H, as in the previous subsection, with a finite set of discrete states Q ($card(Q) = n$). In order to have the condition (3) satisfied, the elements of each mode M^i are labelled by i, i.e. $M^i = \{(i, u) | u \in D^i(\text{open}) \subset \mathbb{R}^{d(i)}\}$. Supose we have given, for each $i \in Q$, an abstraction map $\psi_i : \mathbb{R}^{d(i)} \to \widehat{S}_i$ such that it can be restricted to $\psi_i : \overline{M}^i \to \psi_i(\overline{M}^i)$. The space $\widehat{S}_i$ represents the state space of a Markov process $\widehat{X}_i$, which simulates the continuous evolution of H on the mode M^i that describes a dynamical system or a diffusion process X_i. The process $\widehat{X}_i$ might be a continuous time Markov chain or a step process, etc. The abstraction map should satisfy the zigzag condition (9), i.e. it has to 'commute' with the transition probabilities of the two processes. Moreover, ψ_i has to be *compatible with the transition rate* λ restricted

[1] which gives the distributions of the jump times.

to $\overline{M}^i$, $\psi_i(i,u) = \psi_i(i,v) \Rightarrow \lambda(i,u) = \lambda(i,v)$, i.e. λ is constant on the equivalence classes induced by ψ_i. The abstraction map ψ_i should be compatible with the transition kernel R^i, i.e.

$$\psi_i(i,u) = \psi_i(i,v) \Rightarrow R^i((i,u),\cdot) = R^i((i,v),\cdot) \quad (16)$$

We assume, as well, that $R^i((i,u),\cdot)$ is supported by $\psi_i^{-1}[\psi_i(i,u)]$, i.e. the following condition holds:

$$R^i((i,u),\psi_i^{-1}[\psi_i(i,u)]) = 1 \quad (17)$$

Now, the superposition gauge k_i is defined using R^i such that ψ_i 'commutes' also with k_i, i.e.

$$k_i(\psi_i(i,u),A) = R^i((i,u),\psi_i^{-1}(A)), A \in \mathcal{B}(\psi_i(\overline{M}^i)) \quad (18)$$

Conditions (16) and (17) ensure that k_i is well defined and is indeed a superposition gauge in the sense of Def.2. The kernel k_i must satisfy also the compatibility condition (11) with the dynamics of the processes X_i and $\widehat{X}_i$. This condition can be written in terms of the infinitesimal generators of these processes (which are known in the most cases). Taking into consideration the expression of k_i given by (18), the main difficulty that derives from here is how to choose the simulator process $\widehat{X}_i$, which has to behave nicely w.r.t. the continuous evolution of H in the mode M^i and the discrete transitions from M^i described by R^i. The choose of $\widehat{X}_i$ depends on the ability of the developer to use possible methods to discretize diffusion processes or dynamical systems. The main achievement is that the theory developed in Section IV allows us to work with local abstractions that can be integrated then in a global abstraction of the entire system.

VI. Modular Stochastic Reachability

Probabilistic reachability analysis has known a rapid development in the recent years [1]. Efficient algorithms have been constructed for both discrete and continuous time, but discrete state processes. The continuous time continuous space case resisted to reachability analysis mainly because of mathematical complexity and of the radically different structure of the model.

In this section, we propose a stochastic version of the probabilistic reachability analysis. In [1], the distinction probabilistic/ stochastic is the distinction discrete/ continuous w.r.t. time. We apply this distinction w.r.t. the nature of the state space. In the verification of performability properties [5], the elementary statements are the same as in stochastic reachability analysis [7].

In the stochastic case, verification can take advantage of the statistical tools. In our case, the statistical reasoning involves the expectations of the first hitting times.

Suppose that $\widetilde{\mathbf{X}}$ is a global abstraction of an SHS, constructed using the algorithm described in Section IV. To address the stochastic reachability [7], assume that we have given a set $\widetilde{A} \in \mathcal{B}(\widetilde{\mathbf{S}})$ and a (finite or infinite) time horizon $T \in [0,\infty]$. In our case, $\widetilde{A} = \cup_{i=1}^n \psi_i(A_i)$, $A_i = \psi_i^{-1}(\widetilde{A} \cap \psi_i(F_i)) \subset F_i$. Let us to define: $Reach_T(\widetilde{A}) = \{\omega \in \Omega \mid \exists t \in \mathcal{T} : x_t(\omega) \in \widetilde{A}\}$, where $\mathcal{T} = [0,T]$ or $[0,\infty)$, depending on the time horizon T. The reachability analysis problem consists of determining the probabilities of such a set or, alternatively, computing the *mean of the first hitting time* $T_{\widetilde{A}}$, given by

$$T_{\widetilde{A}} = \inf\{t > 0 | x_t \in \widetilde{A}\}. \quad (19)$$

Theorem 8: The expectation of $T_{\widetilde{A}}$ denoted by $E_{\widetilde{x}}(T_{\widetilde{A}})$ is related by the hitting time expectations of the local abstractions by formula

$$E_{\widetilde{x}}(T_{\psi_i(A_i)}) = K_i\{[E_{\widetilde{x}}(T_{\widetilde{A}})]_i\},\ \widetilde{x} \in \psi_i(F_i) \quad (20)$$

where $T_{\psi_i(A_i)}$ is the first hitting time of $\psi_i(A_i)$ for the process $\widehat{X}_i$ and $[E_{\widetilde{x}}(T_{\widetilde{A}})]_i$ is the restriction of $\Pi^*\{E_{\widetilde{x}}(T_{\widetilde{A}})\}$ to F_i.

VII. Conclusions

In this paper, we have considered a verification methodology for SHSs. The complex state space of an SHS, which is usually a topological space, is decomposed into a partition of closed subspaces. The system is projected on each subspace and each projection is verified according to a specific procedure (reachability analysis, Markov chain discretisation). The output resulted from each verification is called an abstraction. Until now, these different abstractions were treated in an ad hoc manner. In this work, we have proposed a consistency check method of these abstractions and the sound mechanism of the superimposing them.

We have also proved the result relating the expectation of the hitting time of a target set in the global abstraction to the corresponding ones in the local abstractions. Using, the stochastic reachability analysis method from [5], this result can be used for compositional stochastic reachability analysis in diverse models including fluid Petri nets and other fluid models of distributed systems.

References

[1] Baier, C., Haverkort, B.R., Hermanns, H., Katoen, J.-P.: *Validation of Stochastic Systems - A Guide to Current Research*. Springer LNCS **2925** (2004).

[2] Blom, H.A.P., Lygeros, J. (Eds.): "*Stochastic Hybrid Systems: Theory and Safety Critical Applications*". LNCIS **337** (2006).

[3] Bujorianu, M.L., Lygeros, J.: *Towards Modelling of General Stochastic Hybrid Systems*. In [2]: 3-30.

[4] Bujorianu, M.L., Blom, H.A.P., Hermanns, H.: *Functional Abstractions of Stochastic Hybrid Systems*. Proc. IFAC Conf. ADHS (2006).

[5] Bujorianu, M.L., Bujorianu, M.C.: *A reachability analysis Strategy for a Class of Performance Properties of Fluid Stochastic Models*. Proc. EPEW'06, LNCS (2006): 93-107.

[6] Bujorianu, M.L., Lygeros, J., Bujorianu, M.C.: *Bisimulation for General Stochastic Hybrid Systems*. Proc. of HSCC'05, LNCS **3414** (2005): 198-216.

[7] Bujorianu, M.L.: *Extended Stochastic Hybrid Systems and their Reachability Problem*. Proc. of HSCC'04, LNCS **2993** (2004): 234-249.

[8] Dynkin, E.B.: "*Markov Processes*". Vol.1. Springer (1965).

[9] Evans, S.N, Sowers, R.B.: *Pinching and Twisting Markov Processes*. Ann. Prob. **31** (1) (2003): 486-527.

[10] Ethier, S.N., Kurtz, T.G.: "*Markov Processes: Characterization and Convergence*". John Wiley (1986).

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

[12] Prandini, M., Hu, J.: *A Stochastic Approximation Method for Reachability Computation*. In [2]: 107-139.