Automatica 55 (2015) 183–196

Contents lists available at ScienceDirect

Automatica

journal homepage: www.elsevier.com/locate/automatica

Symbolic models for stochastic switched systems: A discretization and a discretization-free approach[☆]

Majid Zamani[a,1], Alessandro Abate[b], Antoine Girard[c]

[a] Department of Electrical and Computer Engineering, Technische Universität München, 80333 Munich, Germany

[b] Department of Computer Science, University of Oxford, OX1 3QD, Oxford, United Kingdom

[c] Laboratoire Jean Kuntzmann, Université de Grenoble, 38041 Grenoble Cedex 9, France

ARTICLE INFO

Article history:
Received 9 July 2013
Received in revised form
5 July 2014
Accepted 26 February 2015

Keywords:
Stochastic hybrid systems
Stochastic switched systems
Formal synthesis
Finite abstractions
Symbolic models

ABSTRACT

Stochastic switched systems are a relevant class of stochastic hybrid systems with probabilistic evolution over a continuous domain and control-dependent discrete dynamics over a finite set of modes. In the past few years several different techniques have been developed to assist in the stability analysis of stochastic switched systems. However, more complex and challenging objectives related to the verification of and the controller synthesis for logic specifications have not been formally investigated for this class of systems as of yet. With logic specifications we mean properties expressed as formulae in linear temporal logic or as automata on infinite strings. This paper addresses these complex objectives by constructively deriving approximately equivalent (bisimilar) symbolic models of stochastic switched systems. More precisely, this paper provides two different symbolic abstraction techniques: one requires state space discretization, but the other one does not require any space discretization which can be potentially more efficient than the first one when dealing with higher dimensional stochastic switched systems. Both techniques provide finite symbolic models that are approximately bisimilar to stochastic switched systems under some stability assumptions on the concrete model. This allows formally synthesizing controllers (switching signals) that are valid for the concrete system over the finite symbolic model, by means of mature automata-theoretic techniques in the literature. The effectiveness of the results are illustrated by synthesizing switching signals enforcing logic specifications for two case studies including temperature control of a six-room building.

1. Introduction

Stochastic hybrid systems are dynamical systems comprising continuous and discrete dynamics interleaved with probabilistic noise and stochastic events (Blom & Lygeros, 2006). Because of their versatility and generality, methods for analysis and design of stochastic hybrid systems carry great promise in many safety-critical applications (Blom & Lygeros, 2006). Examples of such applications include power networks, automotive, finance, air traffic control, biology, telecommunications, and embedded systems. Stochastic *switched* systems are a relevant subclass of stochastic hybrid systems. They consist of a finite (discrete) set of modes of operation, each of which is associated with continuous probabilistic dynamics; further, their discrete dynamics, in the form of mode changes, are governed by a non-probabilistic control (switching) signal.

It is known (Liberzon, 2003) that switched systems can be endowed with global behaviors that are not characteristic of the behavior of any of their modes: for instance, global instability may arise by proper choice over time of the discrete switches between a set of stable modes. This is but one of the many features that makes switched systems theoretically interesting. With focus on *stochastic* switched systems, despite recent progresses on basic dynamical analysis focused on stability properties (Chatterjee & Liberzon, 2006), there are no notable results in the literature targeting more complex objectives, such as those dealing with verification or (controller) synthesis for logical specifications. Examples of those

☆ This work was partially supported by the European Commission MoVeS project FP7-ICT-2009-5 257005. The material in this paper was partially presented at the International Conference on Quantitative Evaluation of SysTems (QEST), August 27–30, 2013, Buenos Aires, Argentina. This paper was recommended for publication in revised form by Associate Editor Jan Komenda under the direction of Editor Ian R. Petersen.

E-mail addresses: zamani@tum.de (M. Zamani), alessandro.abate@cs.ox.ac.uk (A. Abate), Antoine.Girard@imag.fr (A. Girard).

[1] Tel.: +49 89 28923732; fax: +49 89 28923555.

http://dx.doi.org/10.1016/j.automatica.2015.03.004
0005-1098/

specifications include linear temporal logic or automata on infinite strings, and as such they are not amenable to classical approaches for stochastic processes.

A promising direction to investigate these general properties is the use of *symbolic models*. Symbolic models are abstract descriptions of the original dynamics, where each abstract state (or symbol) corresponds to an aggregate of states in the concrete system. When a finite symbolic model is obtained and is formally put in relationship with the original system, one can leverage automata-theoretic techniques for controller synthesis over the finite model (Maler, Pnueli, & Sifakis, 1995) to automatically synthesize controllers for the original system. Toward this goal, a relevant approach is the construction of finite-state symbolic models that are exactly *bisimilar* to the original system. Unfortunately, the class of continuous (-time and -space) dynamical systems admitting exactly bisimilar finite-state symbolic models is quite restrictive (Alur, Henzinger, Lafferriere, & Pappas, 2000; Lafferriere, Pappas, & Sastry, 2000) and in particular it covers mostly non-probabilistic models. The results in Bujorianu, Lygeros, and Bujorianu (2005) provide a notion of exact stochastic bisimulation for a class of stochastic hybrid systems, however, Bujorianu et al. (2005) does not provide any abstraction algorithm, nor does it look at the synthesis problem. Therefore, rather than requiring exact bisimilarity, one can resort to *approximate bisimulation* relations (Girard & Pappas, 2007), which introduce a natural metric between the trajectories of the abstract and the concrete models, and require boundedness in time of this distance.

The construction of approximately bisimilar symbolic models has been extensively studied for non-probabilistic control systems, possibly affected by disturbances (Majumdar & Zamani, 2012; Pola, Girard, & Tabuada, 2008; Pola & Tabuada, 2009) and references therein, as well as for non-probabilistic switched systems (Girard, Pola, & Tabuada, 2010). However, stochastic systems, particularly when endowed with hybrid dynamics, have only been scarcely explored. With focus on these models, a few existing results deal with abstractions of discrete-time stochastic processes (Abate, Amin, Prandini, Lygeros, & Sastry, 2007; Abate, D'Innocenzo, & Di Benedetto, 2011; Azuma & Pappas, 2010). Results for continuous-time models cover probabilistic rectangular hybrid automata (Sproston, 2011) and stochastic dynamical systems under some contractivity assumptions (Abate, 2009). Further, the results in Julius and Pappas (2009) only *check* the relationship between uncountable abstractions and a given class of stochastic hybrid systems via the notion of stochastic (bi)simulation function. However, these results do not provide any *construction* of approximations, nor do they deal with *finite* abstractions, and moreover appear to be computationally tractable only in the case where no input is present. The recent results in Zamani and Abate (2014) and Zamani, Mohajerin Esfahani, Majumdar, Abate, and Lygeros (2014) investigate the construction of finite bisimilar abstractions for continuous-time stochastic control systems, without any hybrid dynamics, and randomly switched stochastic systems, respectively, such that the discrete dynamics in the latter systems are governed by a random uncontrolled signal. Finally, the recently proposed techniques in Zamani, Tkachev, and Abate (2014) improve the ones in Zamani, Mohajerin Esfahani et al. (2014) by not requiring state space discretization but only input set discretization. However, these results only deal with stochastic control systems, without any hybrid dynamics. In summary, to the best of our knowledge there is no comprehensive work on the automatic construction of finite bisimilar abstractions for continuous-time stochastic switched systems in which the discrete dynamics are governed by a non-probabilistic control signal.

The main contributions of this work consist in showing the existence and the construction of approximately bisimilar symbolic models for incrementally stable stochastic switched systems using two different techniques: one requires state space discretization and the other one does not require any space discretization. Note that all the techniques provided in Abate (2009), Abate et al. (2007), Abate et al. (2011), Azuma and Pappas (2010), Girard et al. (2010), Majumdar and Zamani (2012), Pola et al. (2008), Pola and Tabuada (2009), Sproston (2011), Zamani and Abate (2014) and Zamani, Mohajerin Esfahani et al. (2014) are only based on the discretization of state sets. Therefore, they suffer severely from *the curse of dimensionality* due to gridding those sets, which is especially irritating for models with high-dimensional state sets. We also provide a simple criterion in which one can choose between the two proposed approaches the most suitable one (based on the size of the symbolic abstraction) for a given stochastic switched system. Another advantage of the second proposed approach here is that it allows one to construct symbolic models with probabilistic output values, resulting possibly in less conservative symbolic abstractions in comparison with the first proposed approach and with the ones in Zamani and Abate (2014), Zamani, Mohajerin Esfahani et al. (2014) allowing for non-probabilistic output values only. Furthermore, the second proposed approach here allows one to construct symbolic models for any given precision ε and any given sampling time, but the first proposed approach and the ones in Zamani and Abate (2014), Zamani, Mohajerin Esfahani et al. (2014) may not be applicable for a given sampling time.

Incremental stability is a property on which the main proposed results of this paper rely. This type of stability requires uniform asymptotic stability of every trajectory, rather than stability of an equilibrium point or a particular time-varying trajectory. In this work, we show the description of incremental stability in terms of a so-called common Lyapunov function or of multiple Lyapunov functions. The main results are illustrated by synthesizing controllers (switching signals) for two examples. First, we consider a room temperature control problem (admitting a common Lyapunov function) for a six-room building. We synthesize a switching signal regulating the temperature toward a desired level which is not tractable using the first proposed technique. The second example illustrates the use of multiple Lyapunov functions (one per mode) using the first proposed approach. A preliminary investigation on the construction of bisimilar symbolic models for stochastic switched systems using the first proposed approach (requiring state space discretization) appeared in Zamani and Abate (2013). In this paper we present a detailed and mature description of the results presented in Zamani and Abate (2013), including proofs, as well as proposing a second approach which does not require any space discretization.

2. Stochastic switched systems

2.1. Notation

The symbols $\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{R}^+$, and $\mathbb{R}_0^+$ denote the set of natural, nonnegative integer, integer, real, positive, and nonnegative real numbers, respectively. The symbols I_n, 0_n, and $0_{n\times m}$ denote the identity matrix, zero vector, and zero matrix in $\mathbb{R}^{n\times n}$, $\mathbb{R}^n$, and $\mathbb{R}^{n\times m}$, respectively. Given a set A, define $A^{n+1} = A \times A^n$ for any $n \in \mathbb{N}$. Given a vector $x \in \mathbb{R}^n$, we denote by x_i the ith element of x, and by $\|x\|$ the infinity norm of x, namely, $\|x\| = \max\{|x_1|, |x_2|, \ldots, |x_n|\}$, where $|x_i|$ denotes the absolute value of x_i. Given a matrix $P = \{p_{ij}\} \in \mathbb{R}^{n\times n}$, we denote by $\mathrm{Tr}(P) = \sum_{i=1}^{n} p_{ii}$ the trace of P. The *diagonal set* $\Delta \subset \mathbb{R}^n \times \mathbb{R}^n$ is defined as: $\Delta = \{(x, x) \mid x \in \mathbb{R}^n\}$.

The closed ball centered at $x \in \mathbb{R}^n$ with radius ε is defined by $\mathcal{B}_\varepsilon(x) = \{y \in \mathbb{R}^n \mid \|x - y\| \leq \varepsilon\}$. A set $B \subseteq \mathbb{R}^n$ is called a *box* if $B = \prod_{i=1}^{n}[c_i, d_i]$, where $c_i, d_i \in \mathbb{R}$ with $c_i < d_i$ for each $i \in \{1, \ldots, n\}$. The *span* of a box B is defined as $span(B) = \min\{|d_i - c_i| \mid i = 1, \ldots, n\}$. By defining $[\mathbb{R}^n]_\eta = \{a \in \mathbb{R}^n \mid a_i = k_i\eta, k_i \in \mathbb{Z}, i =$