Automatica 76 (2017) 177–182

Contents lists available at ScienceDirect

Automatica

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

Brief paper

Control synthesis for stochastic systems given automata specifications defined by stochastic sets[☆]

Maryam Kamgarpour, Tony A. Wood, Sean Summers, John Lygeros

Automatic Control Laboratory, Department of Information Technology and Electrical Engineering, Swiss Federal Institute of Technology (ETH), Zürich, Switzerland

ARTICLE INFO

Article history:
Received 26 November 2014
Received in revised form
16 September 2016
Accepted 19 September 2016

Keywords:
Stochastic
Dynamics
Control synthesis
Hybrid
Automaton
Reachability

ABSTRACT

The problem of control synthesis to maximize the probability of satisfying automata specifications for systems with uncertainty is addressed. Two types of uncertainty are considered; stochasticity in the dynamical system and in the sets defining the specifications. We model the uncertain dynamical sets as stochastic set processes. We show that the optimal control policy can be computed by solving a reachability problem for a hybrid stochastic system, which evolves on product state spaces of the automaton, stochastic sets, and the dynamical system. We derive an approximation to the stochastic set processes to alleviate the complexity of reachability computation. A case study illustrates the framework and the solution approach.

1. Introduction

With increasing autonomy in several domains spanning from robotics and transportation to energy systems, the need for control synthesis for complex specifications in uncertain environments increases. To define complex specifications for a dynamical system, one can use formal languages from computer science, such as linear temporal logic (LTL). In deterministic systems, LTL verification for a continuous state system can be cast as automata verification after deriving a finite state bisimulation of the system (Tabuada & Pappas, 2006). For stochastic systems one needs to resort to probabilistic bisimulations to derive a finite state equivalent system (Abate, Prandini, Lygeros, & Sastry, 2008). Temporal logic verification has been applied to stochastic systems modeled by finite state Markov chains (De Alfaro, 1998; Kress-Gazit, Wongpiromsarn, & Topcu, 2011; Lahijanian, Andersson, & Belta, 2011; Wolff, Topcu, & Murray, 2011). For Markov processes with uncountable state spaces specifications given by deterministic finite state automata have been verified for autonomous (Abate, Katoen, & Mereacre, 2011) and for controlled systems (Kamgarpour, Summers, & Lygeros, 2013; Tkachev, Mereacre, Katoen, & Abate, 2013). For this class of systems, PCTL model checking has been addressed in Lahijanian, Andersson, and Belta (2015) and Ramponi, Chatterjee, Summers, and Lygeros (2010).

In this paper, we consider automata-based control synthesis for a Markov decision process. In addition to stochasticity in the system dynamics, we consider that the sets defining the automaton alphabet and thus the specification are uncertain. The motivation is to address applications in which a dynamical system interacts with a partially known environment. As such, the locations of the safe sets or target sets are not known *a priori*. This problem has been receiving increasing attention in temporal logic motion planning. In Guo, Johansson, and Dimarogonas (2013), Maly, Lahijanian, Kavraki, Kress-Gazit, and Vardi (2013) and Wongpiromsarn, Topcu, and Murray (2010) the motion plan derived from a specification is revised online based on measurements of the environment. In Chen, Tůmová, and Belta (2012), Cizelj, Ding, Lahijanian, Pinto, and Belta (2011) and Ulusoy, Wongpiromsarn, and Belta (2014) temporal logic specifications are verified for a deterministic dynamical system interacting with stochastic agents in the environment. The difference of this work with the above past works is in consideration of stochastic systems with uncountable state spaces, and in the approach to model the uncertainties in the environment.

☆ This work was supported partially by SNF grants numbered 2000211_37876 and 141836. The material in this paper was partially presented at the Hybrid Systems: Computation and Control (HSCC 2013) Conference, April 8–11, 2013, Philadelphia, USA. This paper was recommended for publication in revised form by Associate Editor Bart De Schutter under the direction of Editor Ian R. Petersen.

E-mail addresses: mkamgar@control.ee.ethz.ch (M. Kamgarpour), woodt@control.ee.ethz.ch (T.A. Wood), ssummers@control.ee.ethz.ch (S. Summers), lygeros@control.ee.ethz.ch (J. Lygeros).

http://dx.doi.org/10.1016/j.automatica.2016.10.013
0005-1098/

We model uncertain sets capturing a specification on a Markov decision process as stochastic set processes (Summers, Kamgarpour, Lygeros, & Tomlin, 2011). In Summers, Kamgarpour, Tomlin, and Lygeros (2013) we solved the problem of reachability given stochastic set processes defining safe and target sets. The framework was applied to aircraft motion planning in hazardous weather (Summers et al., 2011), camera surveillance networks (Raimondo, Kariotoglou, Summers, & Lygeros, 2011) and an emergency rescue mission (Wood, Summers, & Lygeros, 2013). The contributions of this paper are as follows. First, we provide a framework to formulate automata specifications with stochastic set processes. Second, we show that similar to Abate et al. (2011), Kamgarpour et al. (2013) and Tkachev et al. (2013), we can cast automata verification as a reachability problem. Third, we derive an approximation to the stochastic set processes to alleviate the complexity of reachability computation. The problem formulation and solution approach are illustrated with a case study.

2. Dynamical system and specification models

Let $X \subseteq \mathbb{R}^n$ and $U \subset \mathbb{R}^m$ be Borel sets representing the state and input spaces, respectively. For a space S, let $\mathcal{B}(S)$ denote the set of Borel subsets of S. The stochastic dynamical system is described by:

$$x_{t+1} \sim \tau^X(B|x_t, u_t), \quad t = 0, 1, \ldots$$

where $x_t \in X$ and $u_t \in U$ are the state and input at time t, and $B \in \mathcal{B}(X)$. The function $\tau^X : \mathcal{B}(X) \times X \times U \to [0, 1]$ is a Borel measurable stochastic kernel, that is, $\tau^X(B|\cdot)$ is a measurable function on $X \times U$ for each $B \in \mathcal{B}(X)$ and $\tau^X(\cdot|x, u)$ is a probability measure on X for each (x, u). The interpretation is that the state x_{t+1} is sampled from the probability distribution $\tau^X(\cdot|x_t, u_t)$.

We consider specifications on the trajectory $\{x_t\}_{t=0}^N$ defined in terms of reaching or avoiding given subsets of X in a finite time horizon $N \in \mathbb{N}$. Each of these subsets are either known or are described by a stochastic set process defined below (Summers et al., 2013).

Definition 1 (*Stochastic Set Process*). Let $Y \subseteq \mathbb{R}^p$, $p \in \mathbb{N}$ be a parameter space and $\gamma : Y \to \mathcal{B}(X)$ be a set valued map. Let $\tau^Y : \mathcal{B}(Y) \times Y \to [0, 1]$ be a Borel measurable stochastic kernel, which assigns to each $y \in Y$ a probability measure $\tau^Y(\cdot|y)$ on the Borel space $\mathcal{B}(Y)$. A *stochastic set process* is defined by the map γ, the initial condition $y_0 \in Y$ and the Markov process for evolution of the parameter $y_{t+1} \sim \tau^Y(B|y_t)$, $B \in \mathcal{B}(Y)$.

An example of a stochastic set process is an ellipse in two dimensional space whose center and eccentricity evolve according to a given probability distribution (Summers et al., 2011). Examples in the contexts of surveillance and search and rescue in uncertain environments are provided in Raimondo et al. (2011) and Wood et al. (2013).

In order to systematically define the linear time specifications that involve multiple safety and reachability objectives we use the framework of finite state automata (Clarke, Grumberg, & Peled, 2001).

Definition 2 (*Automaton*). A finite state automaton is a tuple $\mathcal{A} = (Q, Q^I, Q^F, \Sigma, \Delta)$, where Q is a finite set of n_q states; $Q^I \subset Q$ is a set of initial states; $Q^F \subset Q$ is a set of final states; Σ is a finite alphabet; $\Delta \subset Q \times \Sigma \times Q$ is a transition relation.

Let $w = (w_0, \ldots, w_N)$ with $w_t \in \Sigma$ for $t = 0, 1, \ldots, N$, be a sequence referred to as a *word*. Let $q_{-1} \in Q^I$ be an initial state of the automaton. Automaton $\mathcal{A}$ *accepts* w if there exists a sequence of automaton states $(q_0, q_1, \ldots, q_N)$ such that $(q_{t-1}, w_t, q_t) \in \Delta$ for $t = 0, 1, \ldots, N$, and $q_N \in Q^F$. By linking an automaton alphabet and its transition relation to a given stochastic system, we obtain an automaton $\mathcal{A}_s$, which encodes specifications on the system trajectory $\{x_t\}_{t=0}^N$.

For each automaton state $j \in Q$, let $\gamma^{ij} : Y \to \mathcal{B}(X)$ for $i = 1, \ldots, n_j$ denote a number of parameterized sets, which determine the transition of the automaton from state j to state i. In the product space $X \times Y$, define $K^{ij} := \{(x, y) \mid x \in \gamma^{ij}(y)\}$. Consequently, $x \in \gamma^{ij}(y) \iff (x, y) \in K^{ij}$. Let $A = \cup_{j=1}^{n_q} \cup_{i=1}^{n_j} K^{ij}$. The automaton alphabet is given as $\Sigma := 2^A$ and its transition relation is $\Delta := \{(j, \sigma, i) \mid \sigma = \{K^{ij}\}, \forall i, j \in Q\}$. Given $\{x_t\}_{t=0}^N$, $\{y_t\}_{t=0}^N$, a labeling function $L : X \times Y \to \Sigma$ returns the subsets of A to which the pair (x, y) belongs and thus, generates a word $\{L(x_t, y_t)\}_{t=0}^N \in \Sigma^N$. This word enables the transitions of the automaton as allowed by Δ. For any final state $q \in Q^F$, define $(q, X \times Y, q) \in \Delta$, that is, each final automaton state is absorbing. Denote the resulting automaton by $\mathcal{A}_s$.

Assumption 1. For each $j \in Q$, the sets $\{K^{ij}\}_{i=1}^{n_j}$ partition $X \times Y$.

Lemma 1. *Under Assumption 1, automaton $\mathcal{A}_s$ is deterministic and non-blocking.*

Proof. Since $\cup_{i=1}^{n_j} K^{ij} = X \times Y$ for every automaton state j, every $(x, y) \in X \times Y$ belongs to a set K^{ij}. Thus, there exists a σ with $(i, \sigma, j) \in \Delta$ and the automaton is non-blocking. In addition, since $\{K^{ij}\}_{i=1}^{n_j}$ partition the state space, they are disjoint. Given this and the fact that $(j, \sigma, i) \in \Delta \iff \sigma = \{K^{ij}\}$, for every j there exists a unique i such that $(j, \sigma, i) \in \Delta$. □

The automaton needs to be deterministic to ensure a well-defined hybrid stochastic kernel on the product spaces $Q \times X \times Y$, as per solution approach of Section 3.

Definition 3 (*Specification*). The trajectory $\{x_t\}_{t=0}^N$ satisfies a specification given by automaton $\mathcal{A}_s$ if there exists a sequence of automaton states $(q_0, q_1, \ldots, q_N)$ such that $(q_{t-1}, L(x_t, y_t), q_t) \in \Delta$ for $t = 0, \ldots, N$, with $q_{-1} \in Q^I$, and $q_N \in Q^F$.

Given that Q^F is absorbing the specification is satisfied at the first time t, at which q_t reaches Q^F. The indexing of q_{-1} is a convention so that the specification is satisfied at time 0 if q_0 with $(q_{-1}, L(x_0, y_0), q_0)$ lies in Q^F.

For a set S, let S^t be the Cartesian product of S with itself t times. Denote $H_t := (X \times Y)^t$ as the history of the dynamical system and the stochastic set parameters from time 0 to time t. A *history dependent policy* is defined as a sequence $\pi = (\pi_0, \pi_1, \ldots, \pi_{N-1})$, $\pi_t : H_t \to U$. The control synthesis objective is stated as follows.

Problem. Find a policy $\pi_t : H_t \to U$, $t = 0, \ldots, N-1$, $H_t = (X \times Y)^t$, that maximizes the probability of satisfying the specification given by automaton $\mathcal{A}_s$.

3. Solution approach

3.1. Control synthesis as a reachability problem

Let $S = Q \times X \times Y$ denote the hybrid state space consisting of the discrete automaton states Q, the dynamical system state X, and the set parameter space Y. Define a discrete stochastic kernel $\tau^q : Q \times Q \times X \times Y \to [0, 1]$:

$$\tau^q(i|j, x, y) = \mathbf{1}_{i'}(i), \tag{1}$$

where $i' \in Q$ satisfies $(j, L(x, y), i') \in \Delta$. It follows from Assumption 1 that $\sum_{i \in Q} \tau^q(i|j, x, y) = 1$ and this construction results in a well-defined stochastic kernel.