Automatica 49 (2013) 261–266

Contents lists available at SciVerse ScienceDirect

Automatica

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

Brief paper

Formal analysis of piecewise affine systems through formula-guided refinement☆

Boyan Yordanov [a,1], Jana Tůmová [a,2], Ivana Černá [b], Jiří Barnat [b], Calin Belta [c]

[a] Department of Mechanical Engineering, Boston University, United States

[b] Department of Informatics, Masaryk University, Czech Republic

[c] Department of Mechanical Engineering and Division of Systems Engineering, Boston University, United States

ARTICLE INFO

Article history:
Received 15 July 2011
Received in revised form
15 April 2012
Accepted 10 August 2012
Available online 23 October 2012

Keywords:
Piecewise linear analysis
Temporal logic
Verification
Biotechnology

ABSTRACT

We present a computational framework for identifying a set of initial states from which all trajectories of a piecewise affine (PWA) system with additive uncertainty satisfy a linear temporal logic (LTL) formula over a set of linear predicates in its state variables. Our approach is based on the construction and refinement of finite abstractions of infinite systems. We derive conditions guaranteeing the equivalence of an infinite system and its finite abstraction with respect to a specific LTL formula and propose a method for the construction of such formula-equivalent abstractions. While provably correct, the overall method is conservative and expensive. A tool for PWA systems implementing the proposed procedure using polyhedral operations and analysis of finite graphs is made available. Examples illustrating the analysis of PWA models of gene networks are included.

1. Introduction

Recently, there has been increasing interest in developing computational tools for temporal logic analysis and control of dynamical systems (Fainekos, Kress-Gazit, & Pappas, 2005; Kloetzer & Belta, 2008a; Tabuada & Pappas, 2006). In this paper, we focus on piecewise affine systems (PWA) that evolve along different discrete-time affine dynamics in different polytopic regions of the (continuous) state space. PWA systems are widely used, since they can approximate nonlinear dynamics with arbitrary accuracy, and are equivalent to other classes of hybrid systems (Heemels, De Schutter, & Bemporad, 2001). In addition, techniques for the identification of such models from experimental data are available (Juloski et al., 2005).

We are interested in developing a method for the analysis of PWA systems from LTL specifications that leads to more informative results than simple Yes/No answers. We consider the following problem: given a PWA system with additive, polytopic parameter uncertainties and an LTL formula over an arbitrary set of linear predicates in its state variables, find the largest region of initial states from which all trajectories of the system satisfy the formula. Our approach is based on the construction, iterative refinement and verification of finite abstractions inspired by LTL model checking (Baier, Katoen, & Larsen, 2008) and bisimulation-based refinement (Bouajjani, Fernandez, & Halbwachs, 1991). The construction of abstractions is enabled by our previous results (Yordanov & Belta, 2010), where we showed that finite quotients of PWA systems can be constructed by using polyhedral operations only. Our refinement procedure is guided by formula equivalence, i.e., at each iteration we aim at constructing a finite abstraction of the PWA system that satisfies exactly the same formula.

This work can be seen in the context of literature focused on the construction of finite quotients of infinite systems, and is related to Clarke et al. (2003), Pappas (2003) and Tabuada and Pappas (2006). The embedding of discrete-time systems into transition systems is inspired from Pappas (2003) and Tabuada and Pappas (2006). However, while the focus there is on characterizing the existence of bisimulation quotients or developing control strategies using such quotients for linear systems, in this work we consider an analysis problem and focus on the computation of finite quotients, which are equivalent to the original, infinite PWA system with respect to the satisfaction of a specific LTL formula. The related idea of defining CTL formula-specific equivalences coarser than bisimulation has been explored in Aziz, Shiple, Singhal, Brayton, and Sangiovanni-Vincentelli (2002) in the context of finite state

☆ This work was partially supported by grants ARO W911NF-09-1-0088, NSF CNS-0834260, and AFOSR FA9550-09-1-020 at Boston University and by grants LH11065,GD102/09/H042, and GAP202/11/0312 at Masaryk University. The material in this paper was partially presented at the 49th IEEE Conference on Decision and Control (CDC 2010), December 15–17, 2010, Atlanta, Georgia, USA. This paper was recommended for publication in revised form by Associate Editor Maurice Heemels under the direction of Editor Andrew R. Teel.

E-mail addresses: yordanov@microsoft.com (B. Yordanov), xtumova@fi.muni.cz (J. Tůmová), cerna@fi.muni.cz (I. Černá), barnat@fi.muni.cz (J. Barnat), cbelta@bu.edu (C. Belta).

[1] Currently with Biological Computation Group, Microsoft Research, Cambridge, UK.

[2] Currently with Department of Informatics, Masaryk University, Czech Republic.

0005-1098/$ – see front matter © 2012 Elsevier Ltd. All rights reserved.
doi:10.1016/j.automatica.2012.09.027

systems. A trace-equivalent quotient, which might be coarser than a bisimulation one, can be used to analyze an infinite system with any LTL formulas (e.g. see Henzinger, Majumdar, & Raskin, 2005). Instead, our method can lead to the construction of quotients that are even coarser but are equivalent with the infinite system with respect to a specific formula only. While we focus on the analysis of PWA systems, methods targeting other classes of infinite systems might also benefit from the construction of formula-equivalent quotients, provided that all operations required by the method can be implemented.

Our methods differ from counterexample-guided refinement (CEGAR) (Clarke et al., 2003) (a different strategy for specification-based refinement) in two ways. First, instead of performing many model checking steps, in this work we aim directly at the construction of formula-equivalent quotients. Second, we obtain more informative results by identifying satisfying and violating regions (i.e. regions of initial conditions from which all trajectories of the system satisfy or violate the specification). This resembles the construction and refinement of 3-valued abstractions (Bruns & Godefroid, 1999; Chechik & Ding, 2002). While the analysis of PWA systems for properties such as stability, invariance and reachability has been considered previously (Bemporad, Torrisi, & Morari, 2000), our approach allows greater expressivity through LTL specifications.

Compared to our previous approach to the analysis of PWA systems (Yordanov & Belta, 2010), in this paper we develop a more efficient procedure by constructing formula-equivalent abstractions coarser than bisimulation. In addition, we derive conditions under which the analysis results are exact although, in general, the overall procedure is still conservative. A preliminary version of this work was presented in Yordanov, Tumova, Belta, Cerna, and Barnat (2010), where only fixed parameter PWA systems were considered. In this paper, we extend the method from Yordanov et al. (2010) to handle uncertain parameter systems, while introducing additional optimizations to our analysis procedure. The algorithms presented here were implemented as a tool available at http://hyness.bu.edu/software.

2. Preliminaries and notation

We assume familiarity with the following notions (for details see, e.g., Baier et al., 2008) and only introduce some preliminaries.

A *transition system* is a tuple $T = (Q, \rightarrow, O, o)$, where Q is a (possibly infinite) set of states, $\rightarrow \subseteq Q \times Q$ is a transition relation, O is a finite set of observations, and $o : Q \rightarrow O$ is an observation map. We denote by $Pre_T(X) = \{x \in Q \mid \exists x' \in X,\ x \rightarrow x'\}$ the states that reach *region* $X \subseteq Q$ in one step. We denote the *language* of T starting from X as $\mathcal{L}_T(X)$ and use $\mathcal{L}_T$ for $\mathcal{L}_T(Q)$.

We use the graphical notation for the LTL operators (i.e. $\Box$ for always and $\Diamond$ for eventually). Given an LTL formula ϕ over O, we write $T(X) \models \phi$ if all the words from $\mathcal{L}_T(X)$ satisfy ϕ. Let $X_T^\phi = \{x \in Q \mid T(x) \models \phi\}$ denote the largest region of T satisfying ϕ. For a finite T, the set X_T^ϕ can be computed through model-checking (Baier et al., 2008).

We use $\sim_o$ to denote the equivalence relation induced by o over Q (i.e. for $x_1, x_2 \in Q$, $x_1 \sim_o x_2$ iff $o(x_1) = o(x_2)$) and $\sim_b$ to denote the coarsest, observation-preserving bisimulation. The quotient $T/_{\sim_o} = (Q/_{\sim_o}, \rightarrow_{\sim_o}, O, o_{\sim_o})$ simulates T, while T and $T/_{\sim_b}$ are bisimilar. This leads to the following relationships between the region X_T^ϕ for T and its quotients[3]

$$\mathrm{con}(X_{T/_{\sim_o}}^\phi) \subseteq \mathrm{con}(X_{T/_{\sim_b}}^\phi) = X_T^\phi. \tag{1}$$

A *Büchi automaton* is a tuple $\mathcal{B} = (S, S_0, O, \delta_\mathcal{B}, F)$ where S is a finite set of states, $S_0 \subseteq S$ is the set of initial states, O is the input alphabet, $\delta_\mathcal{B} : S \times O \rightarrow 2^S$ is a transition function and $F \subseteq S$ is the set of accepting states. For any LTL formula ϕ, a Büchi automaton denoted by $\mathcal{B}_\phi$ that accepts all and only words satisfying ϕ can be constructed. A *product automaton* $P = T \otimes \mathcal{B}_\phi$ is a Büchi automaton[4] $P = (S_P, S_{P0}, \delta_P, F_P)$ where $S_P = Q \times S$, $S_{P0} = Q \times S_0$, and $F_P = Q \times F$. P accepts all and only words from $\mathcal{L}_T$ satisfying ϕ. We denote the projection of states of P to states of T by $\alpha : S_P \rightarrow Q$ (i.e. for a state (x, s) of P, $\alpha((x, s)) = x \in Q$).

3. Problem formulation and approach

Let $\mathcal{X}_l,\ l \in L$ be a set of open polytopes in $\mathbb{R}^N$, where L is a finite index set, such that $\mathcal{X}_{l_1} \bigcap \mathcal{X}_{l_2} = \emptyset$ for all $l_1, l_2 \in L, l_1 \neq l_2$ and $\mathcal{X} = \cup_{l \in L} cl(\mathcal{X}_l)$ is a closed full-dimensional polytope in $\mathbb{R}^N$ ($cl(\mathcal{X}_l)$ denotes the topological closure of set $\mathcal{X}_l$). A discrete-time piecewise affine (PWA) system is defined as:

$$x_{k+1} = A_l x_k + b_l, \quad x_k \in \mathcal{X}_l,\ l \in L,\ k = 0, 1, \ldots, \tag{2}$$

where, for each mode $l \in L$, parameter b_l is uncertain but known to belong to a polyhedral region $B_l \subset \mathbb{R}^N$. We assume that $\mathcal{X}$ is an invariant for all trajectories of the system and matrix A_l is nonsingular for all $l \in L$.

We are interested in properties of (2) specified over the polytopes from its definition.[5] More specifically, given LTL formula ϕ over L we seek the largest initial region from which all trajectories of the PWA system satisfy ϕ. To formalize this problem, we define the semantics of PWA systems through a transition system embedding[6]:

Definition 1. Let $T_e = (Q_e, \rightarrow_e, O_e, o_e)$, where $Q_e = \cup_{l \in L} \mathcal{X}_l$; $x \rightarrow_e x'$ iff there exist $l \in L, b_l \in B_l$ such that $x \in \mathcal{X}_l$ and $x' = A_l x + b_l$; $O_e = L$; $o_e(x) = l$ iff $x \in \mathcal{X}_l$. Given $X \subseteq Q_e$, all trajectories of system (2) originating in X satisfy an LTL formula ϕ iff $T_e(X) \models \phi$.

From Definition 1, the main problem considered in this paper is formalized as the computation of $X_{T_e}^\phi$. Since T_e has an infinite number of states, it cannot be analyzed directly, which motivates us to consider the generalized problem:

Problem 1. Given an infinite transition system T and an LTL formula ϕ over its set of observations O, find X_T^ϕ.

We assume that the quotient $T/_{\sim_o}$ can be constructed (in Yordanov and Belta (2010) we showed that this is indeed the case for T_e). Then, the set $X_{T/_{\sim_o}}^\phi$ can be computed and used as in Eq. (1) to obtain an under-approximation of X_T^ϕ, leading to a conservative solution to Problem 1. The bisimulation algorithm (Bouajjani et al., 1991) can then be used to decrease this conservatism (a similar idea was applied in Chutinan and Krogh (2001) for ACTL). The equivalence relations $\sim_i$ produced at the i-th iteration of the bisimulation algorithm (i.e. $\sim_0 = \sim_o$ and $\sim_{i+1}$ refines $\sim_i$) provide approximations of X_T^ϕ with increasing accuracy (i.e. $\mathrm{con}(X_{T/_{\sim_i}}^\phi) \subseteq \mathrm{con}(X_{T/_{\sim_{i+1}}}^\phi)$). If the algorithm terminates at step k (which cannot be guaranteed for general infinite systems), the bisimulation $\sim_k = \sim_b$ leads to an exact solution as shown in Eq. (1).

[3] The *concretization* con() maps a region of a quotient to its corresponding region in the concrete system T.

[4] The singleton input alphabet of P is omitted.

[5] These polytopes can capture arbitrary linear predicates.

[6] Such a formalization was also used in Yordanov and Belta (2010) where several additional remarks were considered.