Computer Languages, Systems & Structures 47 (2017) 44–61

Contents lists available at ScienceDirect

Computer Languages, Systems & Structures

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

Automatic synthesis of k-inductive piecewise quadratic invariants for switched affine control programs[☆]

Assalé Adjé, Pierre-Loïc Garoche[*]

Onera, The French Aerospace Lab, France and Université de Toulouse, Toulouse, France

ARTICLE INFO

Article history:
Received 22 May 2015
Received in revised form
28 November 2015
Accepted 4 December 2015
Available online 17 December 2015

Keywords:
Formal verification
Static analysis
Piecewise affine systems
Piecewise quadratic Lyapunov functions

ABSTRACT

Among the various critical systems that are worth to be formally analyzed, a wide set consists of controllers for dynamical systems. Those programs typically execute an infinite loop in which simple computations update internal states and produce commands to update the system state. Those systems are yet hardly analyzable by available static analysis method, since, even if performing mainly linear computations, the computation of a safe set of reachable states often requires quadratic invariants.

In this paper we consider the general setting of a piecewise affine program; that is a program performing different affine updates on the system depending on some conditions. This typically encompasses linear controllers with saturations or controllers with different behaviors and performances activated on some safety conditions.

Our analysis is inspired by works performed a decade ago by Johansson et al., and Morari et al., in the control community. We adapted their method focused on the analysis of stability in continuous-time or discrete-time settings to fit the static analysis paradigm and the computation of invariants, that is over-approximation of reachable sets using piecewise quadratic Lyapunov functions.

This approach has been further extended to consider k-inductive properties of reachable traces (trajectories) of systems.

The analysis has been implemented in Matlab and shown very good experimental results on a very large set of synthesized problems.

1. Introduction

With the success of Astrée [4], static analysis in general and abstract interpretation in particular are now seriously considered by industrials from the critical embedded system community, and more specifically by the engineers developing and validating controllers. The certification norms concerning the V&V of those software have also evolved and now enable the use of such methods in the development process.

These controller software are meant to perform an infinite loop in which values of sensors are read, a function of inputs and internal states is computed, and the value of the result is sent to actuators. In general, in the most critical applications, the controllers used are based on a simple linear update with minor non-linearities such as saturations, i.e. enforcing bounds, or specific behaviors when some conditions are met. The controlled systems range from aircraft flight commands,

[☆] This work has been partially supported by an RTRA/STAE BRIEFCASE project grant, the ANR projects INS-2012-007 CAFEIN, and ASTRID VORACE.

[*] Corresponding author.

E-mail addresses: assale.adje@onera.fr (A. Adjé), pierre-loic.garoche@onera.fr (P.-L. Garoche).

http://dx.doi.org/10.1016/j.cl.2015.12.002
1477-8424/© 2015 Elsevier Ltd. All rights reserved.

guidance algorithms, engine control from any kind of device optimizing performance or fuel efficiency, control of railway infrastructure, fan control in tunnels, etc.

It is therefore of utmost importance to provide suitable analyses to verify these controllers. One of the approaches is to rely on quadratic invariants, such as the digital filters abstract domain of Feret [10], since, according to Lyapunov's theorem, any globally asymptotically stable linear system admits a quadratic Lyapunov function. Unfortunately, this theorem does not hold in the presence of disjunction, such as saturation. Moreover checking stability of piecewise systems is undecidable [25].

In static analysis, dealing with disjunction is an import concern. When the join of two abstract element is imprecise, one can consider the disjunctive completion of the domain [11]. This process enriches the set of abstract elements with new ones, but the cost, i.e. the number of new elements, could be exponential in the number of initial elements. Concerning relation abstract domains, one should mention the tropical polyhedra of Allamigeon [2] in which an abstract element characterizes a finite disjunction of zones [21]. However concerning quadratic properties, no static analysis actually performs the automatic computation of disjunctive quadratic invariants.

The goal of this paper is to propose such a computation: produce a disjunctive quadratic invariant as a sub-level of a piecewise quadratic Lyapunov function. Because of the undecidability of the problem, this search is heuristic, but shown to perform well in our experiments.

1.1. Related works

Most relational abstractions used in the static analysis community rely on a linear representation of relationship between variables, e.g. polyhedra [7], octagons [22], zonotopes [12] are not join-complete. Integrating constraints in invariants generation was developed in [9] but for computing linear invariants. As mentioned above, the tropical polyhedra domain [2] admits some disjunctions since it characterizes a family of properties encoded as finite disjunction of zones.

Concerning non-linear properties, the need for quadratic invariant was addressed a decade ago with ellipsoidal abstract domains for simple linear filters [10] and more recently for non-linear template domains [8] and policy iteration based static analysis [13].

More recently, techniques used in the control community have been used to synthesize appropriate quadratic templates using SDP solvers and Lyapunov functions [28].

The proposed technique addresses a family of systems well beyond the ones handled by the mentioned methods. In general, a global quadratic invariant is not enough to bound the reachable value of the considered systems, hence none of these could succeed.

On the control community side, Lyapunov based analysis is typically used to show the good behavior of a controlled system: it is globally asymptotically stable (GAS), i.e. when time goes to infinity the trajectories of the system goes to 0. Since about a decade SDP solvers, i.e. convex optimization algorithms for semi-definite programming, have reached a level of maturity that enable their use to compute quadratic Lyapunov functions. On the theory side, variants of quadratic Lyapunov functions such as the papers motivating our work – Johansson and Rantzer [27,15] as well as Mignone, Ferrari-Trecate and Morari [20] – addressed the study of piecewise linear systems for proving the GAS property.

Another related approach is the line of works supported by Lee and Dullerud [19,17,18] in which the problem is the ability to synthesize a stable controller for a piecewise system. Their approach relies on the computation of a piecewise quadratic Lyapunov for a subset of feasible transitions of the system, considering a bounded fixed number of switches between system behaviors.

In general, computing a safe superset of reachable states, as needed when performing static analysis, is not a common question for control theorist. They would rather address the related notions of controllability or stability under perturbations. In most cases, either the property considered or the technique used relies on the existence of such a bound over reachable state; which we aim to compute in static analysis.

1.2. Contributions

Our contribution is threefold and based on the method of Johansson and Mignone used to prove the GAS property of a piecewise linear system:

- we detailed the method in the discrete setting, computing a piecewise quadratic Lyapunov function of a *discrete-time system*;
- we adapted it to compute an invariant over reachable states of the analyzed system;
- we showed the applicability of the proposed method to a wide set of generated examples.

This paper is an extended version of [1] considering the expression of relationships between quadratic invariants along program traces as inspired by Lee and Dullerud. This approach proposed can be considered as a lift of previous method to k-induction [29,16].