Available online at www.sciencedirect.com

ScienceDirect

IFAC Papers Online CONFERENCE PAPER ARCHIVE

IFAC PapersOnLine 50-1 (2017) 7467–7474

Constructive analysis of control system stability

Pavel Osinenko * **Grigory Devadze** * **Stefan Streif** *

* *Laboratory for Automatic Control and System Dynamics; Technische Universität Chemnitz, 09107 Chemnitz, Germany*

Abstract: Stability of control systems is one of the central subjects in control theory. The classical asymptotic stability theorem states that the norm of the residual between the state trajectory and the equilibrium is zero in the limit. Unfortunately, it does not in general allow computing a rate of convergence, whereas proving exponential stability is notoriously complicated. This work proposes to revisit the asymptotic stability theory with the aim of computing convergence rates using constructive analysis which is a mathematical tool that realizes equivalence between certain theorems and computational algorithms. The overall goal of the current study matches with the trend for introducing formal verification tools into control theory. Besides existing approaches, constructive analysis, suggested within this work, can also be considered for formal verification of control systems. A computational example is provided that demonstrates extraction of a convergence certificate for a dynamical system.

Keywords: Dynamic stability, computational methods, formal verification

1. INTRODUCTION AND PROBLEM STATEMENT

System stability has been among the most crucial subjects of control theory. Traditionally, stability of control systems is analyzed within the Lyapunov theory (Lyapunov, 1992). The Lyapunov function method (also called second method of Lyapunov) lies in the heart of numerous controller designs found in literature. Besides stability, there is relatively new but important notion called formal correctness that is addressed within the so-called formal verification. Formal verification, i. e. verification of system's properties within some formal logic, recently started attracting much attention in the control engineering community (Platzer, 2012; Araiza-Illan et al., 2014; Althoff, 2014; Gao, 2014; Kong et al., 2014; Siddique et al., 2015; Chan et al., 2016). Formal correctness may be seen as a formal certificate ensuring that the behavior of the system matches with the designed one for the whole space of possible input conditions. As for the stability theory, it means providing a formal certificate, i. e., a certain mathematical construct, that assures boundedness or convergence of the system trajectories to the equilibrium. Incorrect functioning may drive the behavior away from the expected one. Consequences of failures may be as bad as damage to the devices and human health, not just deteriorated performance.

In investigation of system stability, one may be interested in answering the following questions: "What is a bound on the magnitude of a system trajectory starting from a given initial condition?", "How fast does the trajectory converge to the equilibrium?". The classical Lyapunov theory does not in general provide answers to these questions. For example, finding an appropriate Lyapunov function candidate and showing negative definiteness of its time derivative ensures "energy decay" in the system and, consequently, convergence. However, the theory does not provide a rate of convergence. Even though it shows that the limit of the metric between the system trajectory and the equilibrium is zero as time goes to infinity, it does not say how fast the said metric decays. This is due to the classical definition of a limit. The definition merely states what the "value at infinity" is, but does not provide any information on the rate of convergence. To deal with this problem, the concept of exponential stability is sometimes used instead, but it is harder to verify than asymptotic stability. Perhaps, using a different notion of a limit, which would necessarily "encode" a rate of convergence, might provide a practically useful framework for formal verification of control systems stability. This is the central question of the current study. In other words, what is necessary information to be provided within a Lyapunov function that allows "computing" the rate of convergence of the state trajectories?

The current study makes a proposal for addressing stability of control systems formally, i. e., providing formal certificates that assure stability of the system trajectories along with the respective rates of convergence. A formal stability certificate is, within the current study, a function of time which puts an upper bound on the metric between system trajectories and the equilibrium.

This work starts with a review of selected existing approaches to formal verification of control systems in Section 2 followed by a brief description of mathematical frameworks which may help address the stated problem (Section 3). A brief review of Lyapunov stability theory is given in Section 4. Section 5 is concerned with the analysis and design of an algorithm for computing formal certificates of asymptotic stability whereas Section 6 present a preliminary case study. As the main contribution of the current work, a proposal for formal verification of control systems stability within constructive analysis is

Peer review under responsibility of International Federation of Automatic Control.
10.1016/j.ifacol.2017.08.1520

considered that establishes correspondence between mathematical proof and algorithms as will be highlighted in Section 3.

2. SELECTED APPROACHES TO FORMAL VERIFICATION OF CONTROL SYSTEMS

Formal verification methods have gained attention in the control engineering community in the recent years and the proposed approaches are diverse. To demonstrate this, some selected approaches are briefly reviewed in this section. They can be tracked to as early as the work of Livadas and Lynch (1998) where formal verification for collision avoidance in hybrid systems was addressed. The major apparatus used were hybrid input-output automata. The work suggested a special abstract notion – called protector – to guarantee compliance with safety requirement. Correctness proof of the protector was established within the theory of hybrid input-output automata. Similar issues were addressed by Fränzle (1999) where formal logics of hybrid automata and the related reachability issues were investigated. Later, Mysore et al. (2005) applied formal logic of hybrid automata to systems biology. An important property of these two formal logic approaches was quantifier elimination, i. e., deriving formally true quantifier-free logical formulas. Another approach based on mixed logical dynamical systems and set-theoretic methods was presented in Andonov et al. (2015) and Rumschinski et al. (2012).

In their project dedicated to formal verification methods to the European Train Control System (ETCS), Platzer and Quesel (2009) also suggested to use quantifier elimination. The background formal system was differential dynamic logic. This is a first-order system for formalization of hybrid systems which can be generalized to formalize also differential equations. The ETCS was formalized and verified within the differential dynamic logic throughout an iterative process including the so-called controllability discovery, control refinement, safety convergence and liveness check steps. A more generalized and substantial description of the framework of differential dynamic logic applied to dynamical systems with an extensive set of examples was given in (Platzer, 2012). It is important to notice their background number field – the real closed field – that enables quantifier elimination (Tarski, 1998). Another application of differential dynamic logic can be found in (Loos et al., 2013) where they addressed safety of distributed aircraft systems. The works by Platzer et al. also offer a good literature review on the subject matter for an interested reader. Hybrid Hoare logic was used by Zou et al. (2013) to formally verify a control system within the Chinese train network. They claimed to better address parallelism and communication issues within their approach than the one based on differential dynamic logic. Automated theorem proving – performed by special software called proof assistants – also plays an important role in formal verification of control systems. For instance, Platzer (2008) developed automated theorem proving methods within their differential dynamic logic. Zou et al. (2013) used Isabelle for implementation of their control system formal verification based on Hybrid Hoare logic. A tool called Why3 coupled with MATLAB/Simulink was used in more recent works by Araiza-Illan et al. (2014, 2015) to perform simple stability checks of linear discrete systems with quadratic Lyapunov functions. Their method may be considered complimentary to the model verifiers available within MATLAB/Simulink. Gao (2014) mentioned several automated theorem proving software tools to be considered for implementation of formal verification of control systems – Coq, HOL Light, Isabelle, Lean. This work also indicated the importance of the question raised within the current study. It was suggested to address formal analysis of the theories like stability, including Lyapunov theory, observability, controllability, optimal, robust, and adaptive control. As a logical frameworks for computations, it was suggested to use the Type Two Theory of Effectivity developed by Weihrauch (see, for example, Weihrauch 1987, 1997, 2012). This theory will be briefly reviewed in Section 3. Gao (2014) also reviewed a solver called dReal for solving logical formulas in nonlinear dynamical systems theory. Siddique et al. (2015) used HOL Light in their formalization of photonic systems. Among other aspects, they formalized difference equations and z-transform within the proof assistant. A recent work by Bernardeschi and Domenici (2016) proposed to use the Prototype Verification System as the proof assistant for verification of a water level controller. Formalization of the behavior and safety requirement verification were carried out.

The Munich project on formal verification of cyber-physical systems is another representative example. Within it, Althoff (2014) extensively used reachability analysis with zonotopes for verification of power systems stability and automated road vehicles respectively. Kong et al. (2014) investigated applications of reachable sets to semi-algebraic dynamical systems with polynomial approximators of sets in Euclidean space as their central concept. They focused on inductive invariants which are certain properties of dynamical systems that hold from the initial state throughout the system trajectories. Chan et al. (2016) recently also addressed formal verification of cyber-physical systems using Coq proof assistant. In their work, they addressed formal verification within the Lyapunov stability theory. An ongoing European research project on formal verification of stability of embedded control systems (refer to CORDIS, 2014) is dedicated to algorithmic methods of correctness check and also demonstrates the importance of the questions raised within the current study. To summarize, the given review clearly indicates that application of different formal methods has certain merits for control theory. The software tools and logical foundations are diverse. However, a certain effort is required for a control systems engineer to start working with the mentioned techniques since they are loaded with background in pure logic that is not usually largely represented within engineering education. This also concerns the Weihrauch's computable analysis suggested as the major framework by Gao (2014).

In the next section, a brief description of computable analysis is provided. The next section also proposes another background mathematical foundation for formal analysis of control systems – constructive analysis – and it will be shown such an approach might have a certain merit. It is believed that constructive analysis might better match with the mathematical education a control engineer usu-