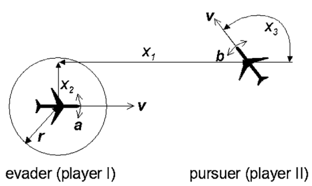
ABCD-CPS: Accurate Booleanization of Continuous Dynamics for Cyber-Physical systems

Archit Gupta and Jaijeet Roychowdhury
The Department of Electrical Engineering and Computer Sciences,
University of California, Berkeley

The pervasiveness of Cyber-Physical Systems (CPS) is shaping both the role and the nature of their interactions with humans. Increasing acceptance of CPS into safety-critical applications like autonomous driving, surveillance, rescue operations, robotic surgery, *etc.*, has elevated the need for safety verification for these systems.

To meet the growing demand for formal safety guarantees for these CPS, several attempts have been made to bridge the gap between complex physical processes that constitute a real system and the existing formal verification frameworks. To mention a few of the existing approaches, [1, 2] describe some of the methods that are employed to either come up with discrete abstractions for a set of Ordinary Differential Equations (ODEs) or specify reachable sets to ascertain safety guarantees. Invariably in all these cases, several simplifications are made by hand to reduce the size of the original system to a small one, which is then tractable for the aforementioned methods to proceed.



(a) original problem

$$\dot{x} = \frac{d}{dt}\begin{bmatrix}x_1\\x_2\\x_3\end{bmatrix} = \begin{bmatrix}-v_a + v_b\cos x_3 + a x_2\\ v_b \sin x_3 - a x_1\\ b - a\end{bmatrix} = f(x,a,b).$$

(b) simplification

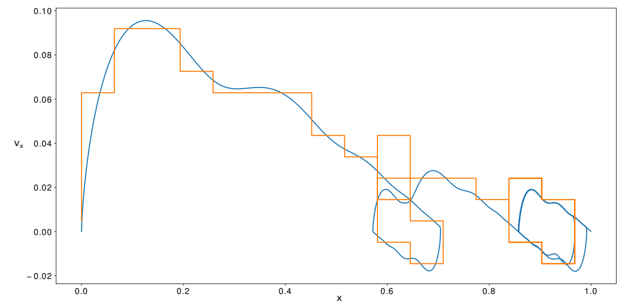
Fig. 1: Existing verification framework for air-collision avoidance [1]

Figure 1, for example, shows the problem of air-collision avoidance for two aircrafts. Large simplifications have to be made (Figure 1(b)) to make the problem tractable for applying the methods in [1]. The original equation system for, say, a basic model of a quadcopter consists of 12 variables for each aircraft, meaning that the equations in Figure 1(b) entail significant simplification of the original system. In any formal verification problem, the fidelity of the underlying model that represents the actual system is of utmost importance for the proposed "proofs" or "counter-examples" to a property to make sense.

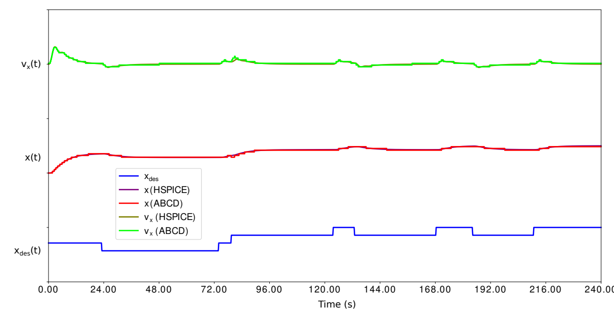
In this work, we apply Accurate Booleanization of Continuous Dynamics (ABCD) [3] to the problem of CPS-verification. ABCD, a technique developed over the last few years by our group, has been successfully applied for debugging Analog-Mixed Signal (AMS) bugs in a variety of non-trivial circuits like charge-pump, delay line, Analog-to-Digital Converter (ADC), Digital-to-Analog Converter (DAC), D-latch, interconnect networks *etc.*. The key idea is to traverse the state space of a continuous-time system for a few input trajectories and to use these traversals to construct a discrete abstraction.

For a majority of CPS, an underlying dynamical system is governed by a discrete component like a digital controller, or interestingly, in some other cases, a logical algorithm. Automatically booleanizing, or more generally speaking, discretizing, the underlying dynamical system sets up the way for reliable counter-example generation for several proposed safety mechanisms like air-collision avoidance which draw a large amount of research interest today.

Figure 2 shows the preliminary results that we have obtained by applying ABCD for translating a complete model of a quadcopter [4, 5]. The model used for translation incorporates various effects like the force/torque equations, aerodynamic drag, motor dynamics, altitude stabilization, path-tracking controller, *etc.*, and is automatically translated to a low dimensional discrete/boolean model using ABCD.



(a) state-space



(b) time-domain

Fig. 2: Application of ABCD to the system of equations for a quadcopter. Comparing the ABCD-generated model against the original model for a random input waveform.

References

[1] Ian M Mitchell, Alexandre M Bayen, and Claire J Tomlin. A time-dependent Hamilton-Jacobi formulation of reachable sets for continuous dynamic games. *IEEE Transactions on automatic control*, 50(7):947–957, 2005.

[2] Dieky Adzkiya, Bart De Schutter, and Alessandro Abate. Finite abstractions of max-plus-linear systems. *IEEE Transactions on Automatic Control*, 58(12):3039–3053, 2013.

[3] A. V. Karthik, S. Ray, P. Nuzzo, A. Mishchenko, R. K. Brayton, and J. Roychowdhury. ABCD-NL: Approximating continuous non-linear dynamical systems using purely Boolean models for analog/mixed-signal verification. pages 250–255, January 2014.

[4] Teppo Luukkonen. Modelling and control of quadcopter. *Independent research project in applied mathematics, Espoo*, 2011.

[5] Zongyu Zuo. Trajectory tracking control design with command-filtered compensation for a quadrotor. *IET control theory & applications*, 4(11):2343–2355, 2010.