Algorithmic Verification of Stability of Hybrid Systems
Pavithra Prabhakar and Miriam García Soto
IMDEA Software Institute

Motivation

- Cyber Physical Systems (CPS): systems which combine control, communication and computation.
- Applications: aeronautics, automotive, manufacturing processes, robotics, medical devices and consumer appliances.
- Challenge: design methodology for building high-confidence systems.
- Unique feature: mixed discrete-continuous behaviour.
- Formal verification: a promising approach based on strong mathematical foundations.

Stability verification problem

Given a hybrid automaton, is it stable?

- Hybrid Automaton: model capturing the mixed discrete-continuous behaviour.
- Stability: small perturbations in the initial state/input of a system induce only small variations in the eventual behaviour of the system.

A Stable System

An Unstable System

An algorithmic framework

- Algorithmic: fully automated verification by a systematic state-space exploration.
- Deductive: verification by reduction to a theorem proving task, often requires substantial user input.

Abstraction: construct a simpler system; a modified predicate abstraction resulting in a finite weighted graph.

Model-checking: state-space exploration; check for the existence of cycles indicating instability.

Validation: check if counter-example corresponds to a bug; check if the cycle corresponds to a diverging infinite path (not a bounded model-checking problem).

Refinement: construct a more precise system; add more predicates.

Tool Architecture

AVERIST: Algorithmic VERifier for STability

References


