Input-output robustness for software systems

Paulo Tabuada, Ayca Balkan, Sina Caliskan, Yasser Shoukry, Rupak Majumdar

Cyber-Physical Systems Laboratory, Dept. of Electrical Engineering, UCLA
Max Plank Institute for Software Systems

UCLA

Introduction

- Cyber-Physical Systems (CPSs) are typically non-robust
  - a small deviation from the design assumptions can lead to a large deviation in the desired behavior;
- While robustness is well understood for continuous components, the same is not true for cyber components;
- We introduce a notion of robustness for cyber components, modeled as transducers, and study the associated verification and synthesis problems.

Transducer models for software

- We start with a set Σ of input symbols and a set Λ of output symbols;
- Σ^* and Λ^* denote the set of all finite strings obtained by concatenating elements of Σ and Λ, respectively;
- A transducer is a map $f : \Sigma^* \to \Lambda^*$ if for every $\sigma, \sigma' \in \Sigma^*$ for which $\sigma \preceq \sigma'$ we have $f(\sigma) \preceq f(\sigma')$ where $\preceq$ denotes the prefix partial order;
- A transducer offers an input/output view of software.

Input-Output Stability (IOS) as a notion of robustness

- Inspired by Grüne's notion of Input-to-State Dynamic Stability we propose the following notion of Input-Output Stability:

Definition

Given parameters $\gamma, \eta \in \mathbb{N}$, we say the transducer $f : \Sigma^* \to \Lambda^*$ is (γ,η)-*input-output stable* (or (γ,η)-IOS) w.r.t. the functions $I : \Sigma^* \to \mathbb{N}_0$ and $O : \Lambda^* \to \mathbb{N}_0$ if for each $\sigma \in \Sigma^*$ we have

$$O\left(f\left(\sigma\right)\right) \leq \max_{\sigma' \preceq \sigma} \left\{\gamma\, I\left(\sigma'\right) - \eta\left(|\sigma| - |\sigma'|\right)\right\}. \tag{1}$$

- The parameter γ is called the *robustness gain* and the parameter η is called the *rate of decay*;
- We say a transducer f is *input-output stable* (or IOS) w.r.t. (I, O) if there exist $\gamma, \eta \in \mathbb{N}$ such that f is (γ,η)-IOS w.r.t. (I, O);
- An IOS transducer satisfies two important properties:
  - bounded disturbances lead to bounded consequences, mathematically $O_\infty(f(\sigma)) \leq \gamma I_\infty(\sigma)$ where $O_\infty(\lambda) = \max_{\lambda' \preceq \lambda} O(\lambda)$ and $I_\infty(\lambda) = \max_{\lambda' \preceq \lambda} I(\lambda)$;
  - the effect of a sporadic disturbance disappears in finitely many steps.

Verification problems

(γ,η)-IOS Verification problem: given transducer f, input and output cost functions I and O respectively, and parameters γ and η, is the transducer f (γ,η)-IOS for I and O?

IOS Verification problem: given transducer f and input and output cost functions I and O respectively, does there exist γ and η such that f is (γ,η)-IOS for I and O? (If so, find such γ and η.)

Synthesis problem

- In order to discuss the synthesis problem we assume Σ to be of the form $\Sigma = \Sigma^c \times \Sigma^d$ where Σ is a set of *control* inputs and Σ^d is a set of *disturbance* inputs.
- A *controller* is a map:

$$C : \Sigma^* \times \Sigma^c \to \Sigma^c$$

  transforming the history of past inputs $\sigma \in \Sigma^*$ and a given control input request s^c into the control input $C(\sigma, s^c)$ to be provided to the system. We denote the closed loop system by f_C.
- We then have the following synthesis problem:

Synthesis problem: given transducer f, cost functions (I, O), and parameters (γ,η), does there exist a controller C such that f_C is (γ,η)-IOS w.r.t. (I, O)?

Finite-state (weighted) automata

- We will solve the verification and synthesis problems for finite-state (weighted) automata.

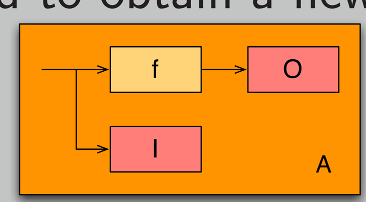
Definition

A finite-state automaton $A = (Q, q_0, \Sigma, \delta, \Lambda, H)$ consists of:
- a finite set of states Q;
- an initial state $q_0 \in Q$;
- a set of inputs Σ;
- a transition function $\delta : Q \times \Sigma \to Q$;
- a set of outputs Λ;
- and an output function $H : Q \to \Lambda$.

- A finite-state weighted automaton A is a finite-state automaton whose set of outputs or *weights* is $\mathbb{N}_0$ and whose output map satisfies $H(q_0) = 0$.
- A weighted automaton A *defines* the cost function $I_A(\sigma) = H(\delta^*(q_0, \sigma))$;

Solving the verification problems

- We assume that f is defined by a finite-state automaton and that both I and O are given by finite-state weighted automata.
- These automata are combined to obtain a new finite-state automaton A:



- We now consider the operator $F : M^Q \to M^Q$, where $M = \{0, 1, \ldots, \overline{m}\}$, $\overline{m} = \max_{q \in Q} H^I(q^I)$, defined by:

$$F(W)(q) = \max\left\{\gamma H^I(q), W(q), \min_{q' \in \mathrm{Pre}(q)} W(q') - \eta\right\}.$$

Theorem

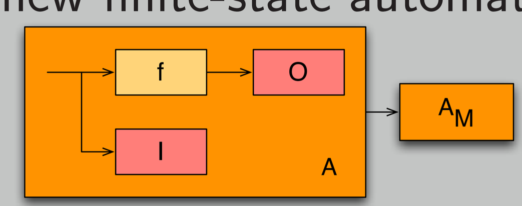
Let A^f be a finite-state automaton. Let A^I and A^O be finite-state weighted automata defining costs I and O, respectively. Given $\eta, \gamma \in \mathbb{N}$, the transducer defined by A^f is (γ,η)-IOS with respect to (I, O) iff the infimal fixed point of F, denoted by W^*, satisfies the following inequality for every $q \in Q$:

$$H^O(q) \leq W^*(q).$$

- Notice that our characterization gives a natural dynamic programming formulation for verification and a polynomial algorithm.
- The IOS verification problem admits a similar solution.

Solving the synthesis problems

- As before we construct a new finite-state automaton A':



  where A_M is a monitor for the IOS property in the following sense. If the input $\sigma \in \Sigma^*$ takes the initial state of A' to $(q, m) \in Q \times M$ then:

$$m = \max_{\sigma' \preceq \sigma}\{\gamma\, I(\sigma') - \eta(|\sigma| - |\sigma'|)\}.$$

- The synthesis problem is now equivalent to the problem of synthesizing a controller to render the following set invariant (computation of the largest controlled invariant set):

$$S = \{(q, m) \in Q \times M \mid H^O(q) \leq m\}$$

  is invariant.
- This problem can be solved in $O(|Q| \cdot |M| \cdot |\Sigma^c|)$ time.

Future work

- The next step is to combine this notion of robustness with existing notions for physical components in order to study the robustness of CPSs.

NSF award 1035916, CPS: Small: Towards robust cyber-physical systems