A generic conformance notion

In general, determining that the outputs of the Model and the Implementation are "close enough", i.e. conformant, is application-dependent and relies on expertise and ad-hoc rules.

We propose \((T,J,t,\epsilon,\tau)\)-closeness as a generic conformance notion. This notion is appropriate for continuous-time, discrete-time, and hybrid-time systems.

Related work: distance between systems

- Input-Output Conformance (Tretmans) for discrete Labeled Transition Systems and Hybrid I/OCO (Van Osch) for Hybrid Transition Systems.
- Woelke et al. verify conformance to a specification (and not between systems)
- Modeling by Discrete Action Systems (Brandl et al.)
  - Directional Hausdorff distance (Abate et al.)
  - \((c,\tau)\)-similar traces (Quesel)
- Skorokhod metrics with bijective re-times (Caspi et al.) or set-valued re-times (Davoren)
- Approximate synchronization and bisimulation (Jullus et al.)

Benefits of \((T,J,t,\epsilon,\tau)\)-closeness as a generic notion of conformance:

- Only requires the ability to simulate the system — black boxes O.K.
- Can be tested early in the design cycle before all the instrumentation is in place for more targeted testing.
- Captures differences in timing characteristics as well as signal values
- Real-valued: can speak of a conformance degree and rank implementations based on how well they conform to the Model.

Conformance Testing as Falsification for Cyber-Physical Systems

Houssam Abbas(1), Bardh Hoxha(1), Georgios Fainekos(1), Jyotirmoy Deshmukh(2), James Kapinski(2) and Koichi Ueda(2)

\((T,J,t,\epsilon,\tau)\)-closeness

Consider two trajectories \(y\) and \(y'\) of \(\Sigma\) and \(\Sigma'\), respectively. Given \(T > 0, J > 0, t > 0, \epsilon > 0\), we say \(y\) and \(y'\) are \((T,J,t,\epsilon,\tau)\)-close if:

a) For all \((t,j)\) in the support of \(y\) s.t. \(t \leq T\) and \(j \leq J\), there exists \((s,j)\) in the support of \(y'\), such that \([t - s] < \tau\) and \([y(t,j) - y'(s,j)]\) < \(\epsilon\)

b) For all \((t,j)\) in the support of \(y'\) s.t. \(t \leq T\) and \(j \leq J\), there exists \((s,j)\) in the support of \(y\), such that \([t - s] < \tau\) and \([y'(t,j) - y(s,j)]\) < \(\epsilon\)

The largest \((\tau,\epsilon)\) such that all trajectories of \(\Sigma\) and \(\Sigma'\) are \((T,J,t,\epsilon,\tau)\)-close is the conformance degree between \(\Sigma\) and \(\Sigma'\).


Implemented in the S-TaLiRo Toolbox

- S-TaLiRo
  - Minimum Robustness
  - Falsifying Trajectory
  - Minimum Expected Robustness
  - Stochastic Optimization
  - Convex Optimization
- Simulink/Stateflow Simulation Engine (or hybrid automata simulator)
- Model Calibration

Conformance testing results

The \((\tau,\epsilon)\) pairs are partially ordered, so must fix one parameter and optimize the other.

We fix \(\tau\) and maximize \(\epsilon\), for pre-defined values of the horizon \((T,J)\).