Monitoring and Measuring Hybrid Behaviors

Tutorial

Dejan Ničković
AIT Austrian Institute of Technology GmbH.
Introduction

Cyber-Physical Systems

- Interconnected heterogeneous components
  - Digital, SW, analog
- Interactions with the physical environment
  - Sensors + actuators
- **Hybrid behaviors**
- Verification and validation is a challenge
- State-of-the-practice
  - Simulation and manual testing
  - Ad-hoc, error prone, tedious
Monitoring and Measuring Technology

- Rigourous
- Not ambiguous
- Automatic
- Scalable
- Reusable
Motivating Example

Distributed Systems Interface (DSI3)
- Automotive bus standard

Airbag System Overview
(Sensors <-> Controller <-> Actuators)

- Communication via *voltage* and *current* lines
Motivating Example

Distributed Systems Interface (DSI3) – Discovery Mode

![Diagram showing Power Ramp, Discovery Pulse, and End Discovery Pulse with corresponding voltage and current waveforms.](image-url)
Outline

- Specification Languages
  - Signal Temporal Logic
  - Timed Regular Expressions

- Monitoring and Measuring Algorithms
  - STL with qualitative and quantitative semantics
  - STL with Quantitative semantics
  - Pattern matching TRE

- Beyond Signal Temporal Logic and Timed Regular Expressions

- Tools and Applications

- Future Perspectives
Specification Languages
Signal Temporal Logic

- High-level specification language
  - Continuous interpretation of time
  - Predicates over real-valued variables

\[
\alpha := p \mid x < c \mid x \leq c \\
\varphi := \alpha \mid \neg \varphi \mid \varphi_1 \lor \varphi_2 \mid \varphi_1 U I \varphi_2 \mid \varphi_1 S I \varphi_2
\]

- [MN04,MN13]
Signal Temporal Logic

Semantics

\[
\begin{align*}
\varphi_2 & \quad \varphi_1 & \quad \varphi_1 \mathcal{S}_{[a,b]} \varphi_2 \\
\downarrow & \quad \downarrow & \\
t' & \quad t & \\
t - b & \quad t - a & \\
\end{align*}
\]

\[
\begin{align*}
\varphi_1 \mathcal{U}_{[a,b]} \varphi_2 & \quad \varphi_1 & \quad \varphi_2 \\
\downarrow & \quad \downarrow & \\
t & \quad t' & \\
t & \quad t' & \\
\end{align*}
\]

22.09.2015
Signal Temporal Logic

Satisfaction Signals

- For every STL formula $\varphi$ and behavior $w$, we associate a satisfaction signal $u$ that has the following property.

$$u(t) = 1 \iff (w, t) \models \varphi$$

- Satisfaction signal $u$ for the formula $\Diamond_I p$
Signal Temporal Logic

Derived Operators

- Timed always, eventually, historically and once

\[
\begin{align*}
\Diamond I \varphi & \equiv True \; U_I \varphi \\
\square I \varphi & \equiv \neg \Diamond I \neg \varphi \\
\Diamond I \varphi & \equiv True \; S_I \varphi \\
\square I \varphi & \equiv \neg \Diamond I \neg \varphi
\end{align*}
\]

- Events – rising and falling edges

\[
\begin{align*}
\uparrow \varphi & \equiv (\varphi \land (\neg \varphi \; S \; True)) \lor (\neg \varphi \land (\varphi \; U \; True)) \\
\downarrow \varphi & \equiv (\neg \varphi \land (\varphi \; S \; True)) \lor (\varphi \land (\neg \varphi \; U \; True))
\end{align*}
\]
Signal Temporal Logic

Formalization of DSI3 Requirements

- Discovery pulse
  \[ \varphi_{shape} \equiv \downarrow v_h \land (v_b \cup v_l \cup v_b \cup v_h) \]
  \[ \varphi_{dur} \equiv \downarrow v_h \land (\neg v_h \cup I_{Disc-Pulse} \uparrow v_h) \]
  \[ \varphi_{pulse} \equiv \varphi_{shape} \land \varphi_{dur} \]

- Distance between consecutive discovery pulses
  \[ \Box (\varphi_{pulse} \rightarrow ((\neg \varphi_{pulse} \cup I_{Disc-per} \varphi_{pulse}) \lor \Box (\neg \varphi_{pulse}))) \]

\( V_{high} \)
\( V_{low} \)
\( v_l \equiv v \leq V_{low} \)
\( v_b \equiv V_{low} \leq v \leq V_{high} \)
\( v_h \equiv v \geq V_{high} \)
Signal Temporal Logic

Quantitative Semantics - Motivation

Domain of reals

$x > 5$
Signal Temporal Logic

Quantitative Semantics

- From satisfaction relation to **robustness degree**
  \[ (w, t) \models \varphi_1 \lor \varphi_2 \iff (w, t) \models \varphi_1 \text{ or } (w, t) \models \varphi_2 \]
  \[ \rho(\varphi_1 \lor \varphi_2, w, t) = \max\{\rho(\varphi_1, w, t), \rho(\varphi_2, w, t)\} \]

- **Spatial** quantitative semantics

- [FP09]
Timed Regular Expressions

Syntax and Semantics

- Extension of regular expressions with real-time constraints [ACM97]
- Syntax

\[ \alpha ::= \epsilon | \theta | \alpha_1 \cdot \alpha_2 | \alpha_1 \cup \alpha_2 | \alpha_1 \cap \alpha_2 | \alpha^* | \langle \alpha \rangle_I \]

- Semantics

\[
\begin{align*}
(w, t, t') & \models \epsilon \quad \iff \quad t = t' \\
(w, t, t') & \models \theta \quad \iff \quad t < t' \text{ and } \forall t < t'' < t', \pi_\theta(w)[t''] = 1 \\
(w, t, t') & \models \alpha_1 \cdot \alpha_2 \quad \iff \quad \exists t \leq t'' \leq t', (w, t, t'') \models \alpha_1 \text{ and } (w, t'', t') \models \alpha_2 \\
(w, t, t') & \models \langle \alpha \rangle_I \quad \iff \quad t' - t \in I \text{ and } (w, t, t') \models \alpha
\end{align*}
\]

- Match set

\[ \mathcal{M}(\alpha, w) = \{(t, t') \in \mathbb{R}^2 \mid (w, t, t') \models \alpha\} \]
Timed Regular Expressions

Conditional Expressions and Events

- Conditional Expressions
  \[(w, t, t') \models \alpha_1 ? \alpha_2 \iff (w, t, t') \models \alpha_2 \text{ and } \exists t'' \leq t, (w, t'', t) \models \alpha_1\]
  \[(w, t, t') \models \alpha_1 ! \alpha_2 \iff (w, t, t') \models \alpha_1 \text{ and } \exists t'' \geq t', (w, t', t'') \models \alpha_2\]

\[p \quad \overline{p} \quad p \quad \overline{p}\]

- Events
  \[\uparrow \theta \equiv \neg \theta ? \epsilon ! \theta\]
  \[\downarrow \theta \equiv \uparrow \neg \theta\]
Timed Regular Expressions

Measurement Specification Language

- Event-bounded timed regular expressions

\[ \psi := \uparrow p \mid \psi_1 \cdot \alpha \cdot \psi_2 \mid \psi_1 \cup \psi_2 \mid \psi_1 \cap \alpha \]

- Measurement language

\[
\begin{align*}
\llbracket \text{time}(\uparrow p) \rrbracket_w &= \set{t \mid (t, t) \in M(\uparrow p, w)} \\
\llbracket \text{value}_x(\uparrow p) \rrbracket_w &= \set{\pi_x(w)[t] \mid (t, t) \in M(\uparrow p, w)} \\
\llbracket \text{duration}(\alpha) \rrbracket_w &= \set{t' - t \mid (t, t') \in M(\alpha, w)} \\
\llbracket \text{inf}_x(\alpha) \rrbracket_w &= \set{\min_{t \leq \tau \leq t'} \pi_x(w)(\tau) \mid (t, t') \in M(\alpha, w)} \\
\llbracket \text{sup}_x(\alpha) \rrbracket_w &= \set{\max_{t \leq \tau \leq t'} \pi_x(w)(\tau) \mid (t, t') \in M(\alpha, w)} \\
\llbracket \text{integral}_x(\alpha) \rrbracket_w &= \set{\int_t^{t'} \pi_x(w)(\tau) d\tau \mid (t, t') \in M(\alpha, w)} \\
\llbracket \text{average}_x(\alpha) \rrbracket_w &= \set{\frac{1}{t' - t} \int_t^{t'} \pi_x(w)(\tau) d\tau \mid (t, t') \in M(\alpha, w)}
\end{align*}
\]

- [FMN+15]
Timed Regular Expressions

Formalization of DSI3 Requirements

- Discovery pulse
  \[ \alpha_{\text{pulse}} \equiv \downarrow (v_h) \cdot \langle v_b \cdot v_l \cdot v_b \rangle I_{\text{Disc_Pulse}} \cdot \uparrow (v_h) \]

- Distance between consecutive discovery pulses
  - Cannot be expressed
    - No negation
    - No universal quantification over time

\[ v_l \equiv v \leq V_{\text{low}} \]
\[ v_b \equiv V_{\text{low}} \leq v \leq V_{\text{high}} \]
\[ v_h \equiv v \geq V_{\text{high}} \]
Timed Regular Expressions

Formalization of DSI3 Requirements - Measurements

- Segment between two consecutive discovery pulses
  \[ \alpha_1 \equiv \epsilon \]
  \[ \psi \equiv \alpha_{\text{pulse}} \cdot v_h \cdot \downarrow (v_h) \]
  \[ \alpha_2 \equiv \alpha_{\text{pulse}} \]
  \[ \alpha \equiv \alpha_1 ? \psi ! \alpha_2 \]

- Average duration between consecutive discovery pulses
  \[ D = \text{duration}(\alpha) \]
  \[ \text{avg} = \frac{\Sigma_{\delta \in D} \delta}{|D|} \]
Summary

- Signal temporal logic
  - Patterns could be formalized
    - Difficult
  - Temporal relations could be formalized
    - Easy
  - No measurement specifications

- Timed regular expressions
  - Patterns could be formalized
    - Easy
  - Temporal properties could not be formalized
    - No negation
  - Measurement specifications

22.09.2015
Monitoring and Measuring Algorithms
Handling Numerical Predicates

- Specification formalisms defined with respect to ideal mathematical behaviors
  - Function from continuous-time to real valued domain

- Simulator provide imperfect approximation of behaviors
  - Collection of timestamp-value pairs

- Interpolation
  - Step, linear, etc.
Monitoring Signal Temporal Logic

- **Marking:** a procedure that computes the satisfaction signal or the robustness degree of each sub-formula of an STL specification
  - Doubly-recursive procedure, on time and the structure of the formula
  - Procedure directly applied on signals, no automata

- Algorithms for monitoring STL properties
  - **Offline marking:** input is fully available
  - **Incremental marking:** input is dynamically observed
  - **Quantitative marking:** computation of robustness degree
Monitoring Signal Temporal Logic

Offline Qualitative

\[ x \geq 5 \]
Monitoring Signal Temporal Logic

Incremental Qualitative

\[ \varphi_{1,3}(x \geq 5) \]

\[ \Box \varphi_{1,3}(x \geq 5) \]
Monitoring Signal Temporal Logic

Quantitative

\[ 0 \leq x \leq 5 \]

\[ 0 \rightarrow [1,3] (x \geq 5) \]

\[ x \geq 5 \]

\[ 0 \rightarrow [1,3] (x \geq 5) \]

\[ \square [1,3] (x \geq 5) \]
Pattern Matching Timed Regular Expressions

- Computing the match set of an expression
  - Finite union of 2-dimensional zones

- Timed regular expression operators
  - Operations on zones

- [UFA+14]
Pattern Matching Timed Regular Expressions

\[
\langle p \rangle_{[1,2]} \quad p \\
\begin{array}{cccccccc}
0 & 2 & 4 & 6 & 8 & 10 & 12 \\
\end{array}
\]

\[
\begin{array}{cccccccc}
0 & 2 & 4 & 6 & 8 & 10 & 12 \\
\end{array}
\]

\[
\begin{array}{cccccccc}
0 & 2 & 4 & 6 & 8 & 10 & 12 \\
\end{array}
\]

\[
\begin{array}{cccccccc}
0 & 2 & 4 & 6 & 8 & 10 & 12 \\
\end{array}
\]

\[
\begin{array}{cccccccc}
0 & 2 & 4 & 6 & 8 & 10 & 12 \\
\end{array}
\]

\[
\begin{array}{cccccccc}
0 & 2 & 4 & 6 & 8 & 10 & 12 \\
\end{array}
\]
Beyond Signal Temporal Logic and Timed Regular Expressions
Time-Frequency Logic

- Specification language that captures
  - Time-domain
  - Frequency-domain properties

- Extends STL with frequency domain predicates
  - Short-time Fourier transform

- [DMB+12]
Signal Temporal Logic with Freeze Quantifiers

- STL with freezing operator
  - Freeze a value in the behavior when a sub-property evaluates to true
  - Use it for comparison in another sub-property

- Powerful mechanism
  - Similar to local variables in PSL and SVA
  - Similar to TPTL

- Qualitative and quantitative semantics

- [BDS+14]
Parametric Signal Temporal Logic

- Signal Temporal Logic with **magnitude** and **time parameters**
  \[ \square_{[0,s_1]} \Diamond_{[0,s_2]} (x < p) \]

- \( s_1, s_2 \) and \( p \) are parameters

- Given an STL formula with timing and magnitude parameters and a behavior of a system, find the range of parameters that makes the formula satisfied with respect to the behavior

- Two algorithms
  - Quantifier elimination
  - Approximation of Pareto fronts

- [ADM+11]
Spatio Temporal Logic

- SpaTeL – unification of
  - Signal Temporal Logic
  - Tree Spatial Superposition Logic

- Specification of spatial patterns that evolve over time

- Distributed and networked systems

- Quantitative semantics + statistical model checking

- [HJK+15]
Tools and Applications
Analog Monitoring Tool

http://www-verimag.imag.fr/DIST-TOOLS/TEMPO/AMT/content.html

- STL with qualitative semantics
  - Correctness
- Offline monitoring
- Incremental monitoring

[NM07]
Breach

http://www.eecs.berkeley.edu/~donze/breach_page.html

- MATLAB toolbox for
  - Simulation
  - Verification of temporal properties
  - Reachability
- STL with qualitative and quantitative semantics
  - Correctness
  - Robustness
- [Don10]
S-TaLiRo

https://sites.google.com/a/asu.edu/s-taliro/s-taliro

- MATLAB toolbox for searching trajectories with minimal robustness
  - Randomized testing
    - Monte-Carlo simulation
    - Ant-colony optimization
    - Simulated annealing
    - Genetic algorithms
    - Cross entropy

- MTL with quantitative semantics
  - Robustness

- [FSU+12]
CPSGrader

http://cpsgrader.org/

- Auto grader for laboratory courses
  - STL-based *test benches*
  - Monitor simulation traces of student solutions for faults

- STL with quantitative semantics
  - Robustness

- [JDJ+14]
U-Check

- Model checking and parameter synthesis for STL against stochastic dynamical systems
  - Machine learning techniques
  - Tutorial this afternoon

- [BMS15]
Applications

- **Automotive**
  - Correctness of DSI3 protocol implementation
  - Measuring DSI3 quantitative properties
  - Directed testing of powertrain control system
  - Robustness checking (S-TaLiRo) of
    - automatic transmission
    - powertrain control system
    - port fuel injected spark ignition systems

- **Analog and mixed signal circuits**
  - Correctness of DDR3 and Flash memory interfaces

- **Music**
  - Time-frequency domain properties

- **Biology**
  - Design of synthetic biological circuits
  - Logical characterization of an oscillator of the circadian clock in Ostreococcus Tauri
  - Qualitative properties of the behavior of cellular mechanisms with STL
  - Robust STL semantics for biological systems
    - Schlögl system
    - Incoherent type 1 feed-forward loops
    - Repressilator – synthetical biology clock

- **Medical**
  - Insuline pump usage parameter synthesis
  - Assisted ventilation
  - Discrimination of cardiac malfunction in ECG
Future Perspectives
Specification Languages

- Gap between informal requirements and formal languages

\[ v_l \equiv v \leq V_{low} \]
\[ v_b \equiv V_{low} \leq v \leq V_{high} \]
\[ v_h \equiv v \geq V_{high} \]
\[ \varphi_{shape} \equiv \downarrow v_h \land (v_b \mathcal{U} v_l \mathcal{U} v_b \mathcal{U} v_h) \]
\[ \varphi_{dur} \equiv \downarrow v_h \land (\neg v_h \mathcal{U} I_{Disc, Pulse} \uparrow v_h) \]
\[ \varphi_{pulse} \equiv \varphi_{shape} \land \varphi_{dur} \]
\[ \square (\varphi_{pulse} \rightarrow ((\neg \varphi_{pulse} \mathcal{U} I_{Disc, pulse} \varphi_{pulse}) \lor \square (\neg \varphi_{pulse}))) \]

- Steep learning curve for non-experts
- ViSpec

[DHF15]
Specification Languages

- Specification libraries
  - Reuse
    - Same design, different phases
    - Same design, different context
  - Parameterization

- Expressiveness
  - Slew rates
  - Data integrity
  - Etc.
Fault Explanation and Localization

- Violation found!
  - How to help debugging?

- Automatic explanation and localization of faults

- Recent work [FMN15]
  - Idea of implicants
  - Computation of small implicants
Monitors Implemented on Hardware

- Monitoring + simulation is very scalable
  - Not always true!!!

- Mixed-signal simulation at SPICE level
  - Several ms of real time = hours to days of simulation time
  - A simulation trace size = hundreds of MB to tens of GB

- Solution:
  - Design emulation on FPGA HW
    • Precision vs. Efficiency

- Need for monitors implemented on FPGA hardware
HARMONIA Project

- Asserion-based Hardware Monitoring for Automotive Applications

- National Austrian project
  - 2014 - 2017
  - AIT, Infineon Technologies AG, TU Wien
  - 2 PhD students

- STL monitors implemented on FPGA hardware
  - Qualitative and quantitative semantics

- Diagnosis

- Large automotive case study
HARMONIA Project

- Preliminary results

![Image of measurement results]

[JBG+15]

22.09.2015
References

References