Assertions and Measurements for Mixed-Signal Simulation

PhD Thesis

Thomas Ferrère

VERIMAG, University of Grenoble (directeur: Oded Maler)
Mentor Graphics Corporation (co-encadrant: Ernst Christen)

October 28, 2016

Cyber-Physical Systems

- Both discrete and continuous modes of operation
- Example: a cell phone
  - A design
  - A bug
- Verification is needed

Cyber-Physical Systems

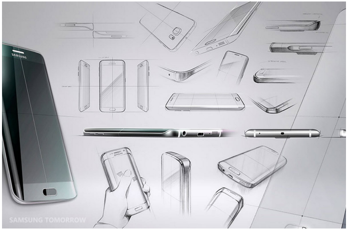
- Both discrete and continuous modes of operation
- Example: a cell phone
  - A design:
  - A bug:

(courtesy of Samsung and AppleInsider)

- Verification is needed

Cyber-Physical Systems

- Both discrete and continuous modes of operation
- Example: a cell phone
  - A design:



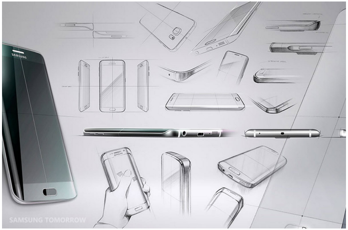
  - A bug:

(courtesy of Samsung and AppleInsider)

- Verification is needed

Cyber-Physical Systems

- Both discrete and continuous modes of operation
- Example: a cell phone
  - A design:



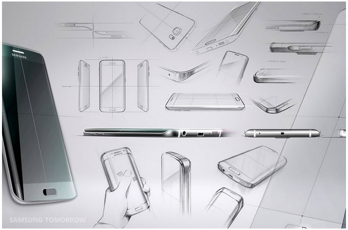
  - A bug:

(courtesy of Samsung and AppleInsider)

- Verification is needed

Cyber-Physical Systems

- Both discrete and continuous modes of operation
- Example: a cell phone
  - A design:



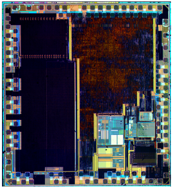
  - A bug:

(courtesy of Samsung and AppleInsider)

- Verification is needed

Mixed-Signal Simulation

Integrated Circuits



(courtesy of ST Microelectronics)

- Implement both analog and digital electronics
- Design uses HDL and net lists at several stages

Modeling

- Digital: event-driven

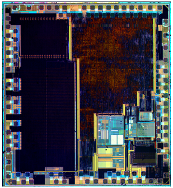
- Analog: algebraic differential equations

$$f_p\left(x, \frac{\mathrm{d}x}{\mathrm{d}t}\right) = 0$$

- Mixed-Signal: analog events $\uparrow(x > 2.0)$ and digital control f_q

Mixed-Signal Simulation

Integrated Circuits

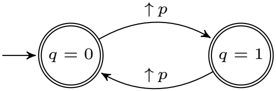


(courtesy of ST Microelectronics)

- Implement both analog and digital electronics
- Design uses HDL and net lists at several stages

Modeling

- Digital: event-driven



- Analog: algebraic differential equations

$$f_p\left(x, \frac{\mathrm{d}x}{\mathrm{d}t}\right) = 0$$

- Mixed-Signal: analog events $\uparrow(x > 2.0)$ and digital control f_q

Simulation-Based Verification

- During the design stage run multiple simulations
- Each simulation produces a trace
  - Records evolution of quantities over time
  - Real-valued and Boolean signals
- Monitoring: each traced need to be analysed
  - Evaluate requirements: correctness, robusteness, diagnostics
  - In general measuring some performance
- Automation of the monitoring activity:
  - Additional observer blocks
  - Declarative property or measurement languages

Declarative Languages in Industry

Assertions

- Digital domain
- Languages PSL and SVA built using two layers:
  - regular expression
  - temporal logic
- Discrete time interpretation

Measurements

- Analog domain
- EXTRACT commands: signal processing, offline
- MEAS commands: event-driven, online

Research on Realtime Properties

Problem: mixed-signal characterized by a synchronous interaction
Solution: use continous-time representation

- Metric Temporal Logic (Koymans, 1990)
  - Signal Temporal Logic for real-valued signals (Maler and Nickovic, 2004)
  - Quantitative semantics for robustness estimate (Fainekos and Pappas, 2009)
- Timed Regular Expressions (Asarin, Caspi and Maler, 1998)

Limitations of Existing Tools and Techniques

- Digital assertions bound to precision of sampling clock
- Realtime properties monitoring not implemented
- Robustness computation is not efficient
- No easy diagnostic of temporal logic properties failure
- Measurements not controllable by sequential conditions
- No analog measures in a digital context

Outline

1. Preliminaries
2. Robustness Computation
3. Diagnostics
4. Regular Expressions Monitoring
5. Pattern-Based Measurements
6. Analog Measures in Digital Environment
7. Conclusion

Outline

Signal Temporal Logic

- Propositions p: Boolean variables q, conditions $x \leq c$, and events $\uparrow p$
- Temporal operators:
  - Until: $\varphi \, \mathrm{U}_I \, \psi$
  - Eventually: $\Diamond_I \, \psi = \top \, \mathrm{U}_I \, \psi$
  - Always: $\Box_I \, \psi = \neg \, \Diamond_I \, \neg\psi$

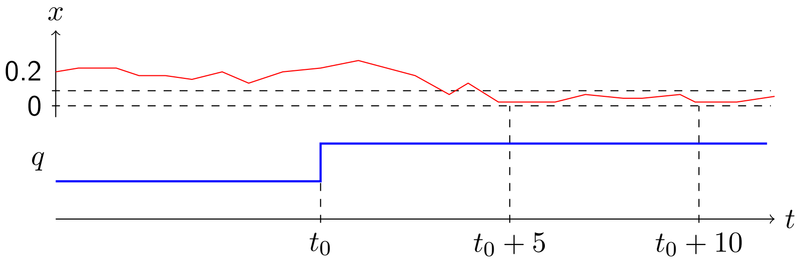
  Formulas can be written with $\Diamond_{[a,b]}$ and U only

- Example: stabilization property $\varphi = \Box(\uparrow q \rightarrow \Diamond_{[0,5]} \Box_{[0,5]} \, x \leq 0.2)$

Signal Temporal Logic

- Propositions p: Boolean variables q, conditions $x \leq c$, and events $\uparrow p$
- Temporal operators:
  - Until: $\varphi \, \mathrm{U}_I \, \psi$
  - Eventually: $\Diamond_I \, \psi = \top \, \mathrm{U}_I \, \psi$
  - Always: $\Box_I \, \psi = \neg \Diamond_I \neg \psi$

  Formulas can be written with $\Diamond_{[a,b]}$ and U only
- Example: stabilization property $\varphi = \Box(\uparrow q \rightarrow \Diamond_{[0,5]} \Box_{[0,5]} \, x \leq 0.2)$



Monitoring

Offline approach (Maler and Nickovic, 2004): for each subformula φ compute set of times $[\varphi]_{\boldsymbol{w}}$ where φ holds according to $\boldsymbol{w}$

Definition (Satisfaction Set)

$$[p]_{\boldsymbol{w}} = \{t : p_{\boldsymbol{w}}(t) = 1\} \qquad [\neg\varphi]_{\boldsymbol{w}} = \overline{[\varphi]_{\boldsymbol{w}}}$$

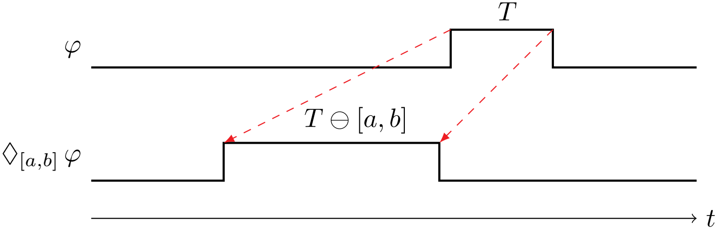
$$\left[\Diamond_{[a,b]}\, \varphi\right]_{\boldsymbol{w}} = [\varphi]_{\boldsymbol{w}} \ominus [a,b] \qquad [\varphi \vee \psi]_{\boldsymbol{w}} = [\varphi]_{\boldsymbol{w}} \cup [\psi]_{\boldsymbol{w}}$$

Computation

Theorem

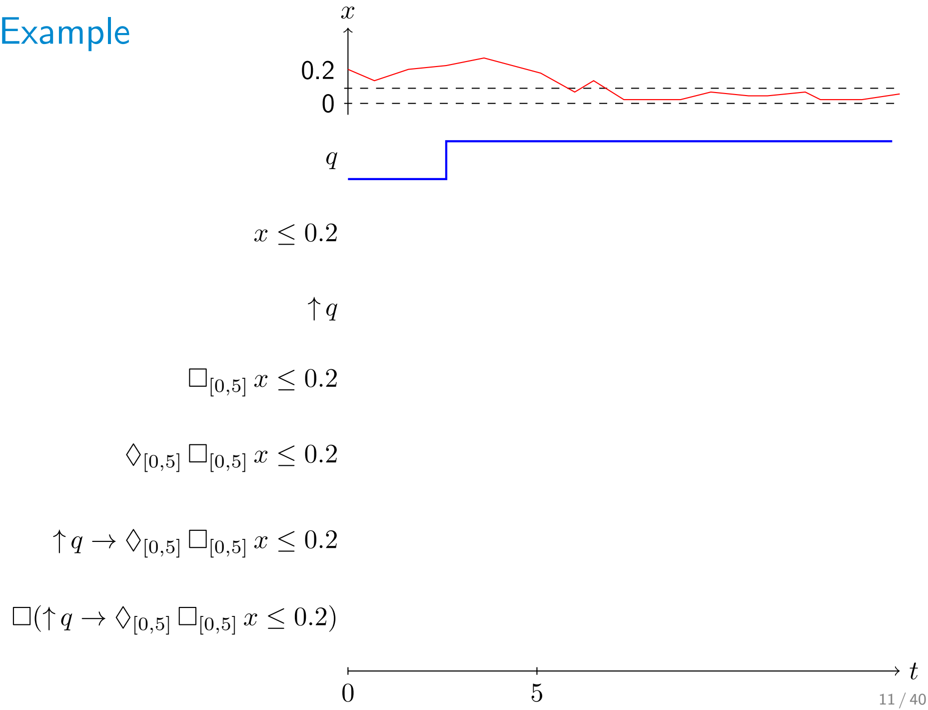
For any φ and $\boldsymbol{w}$ with finite variability, $[\varphi]_{\boldsymbol{w}}$ is finite union of intervals

- Eventually operator:

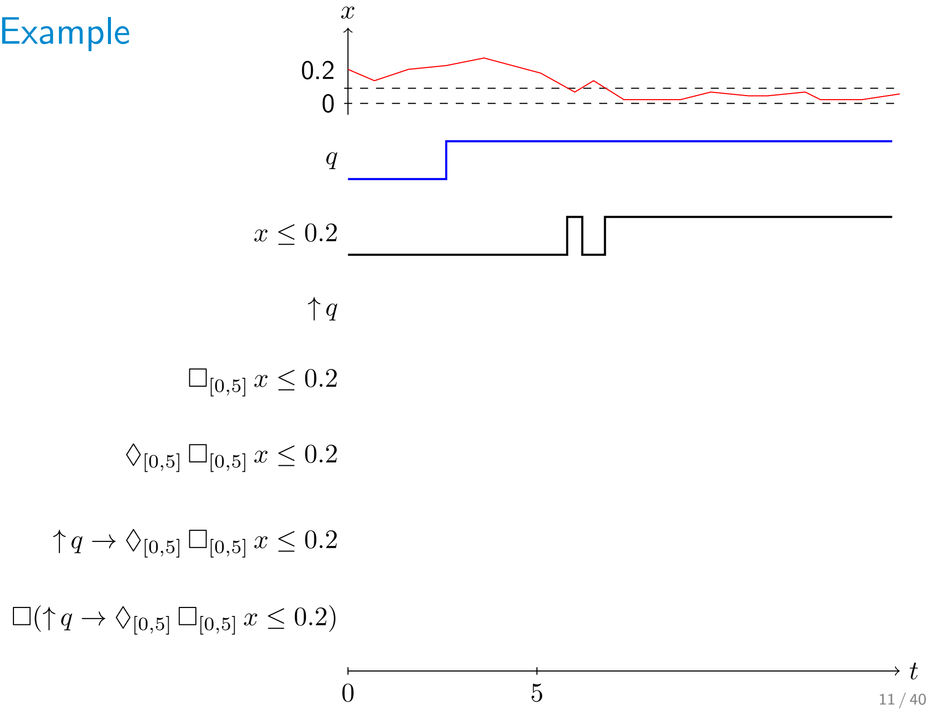


- Worst-case complexity $O(|\varphi|)^2 \cdot |\boldsymbol{w}|$

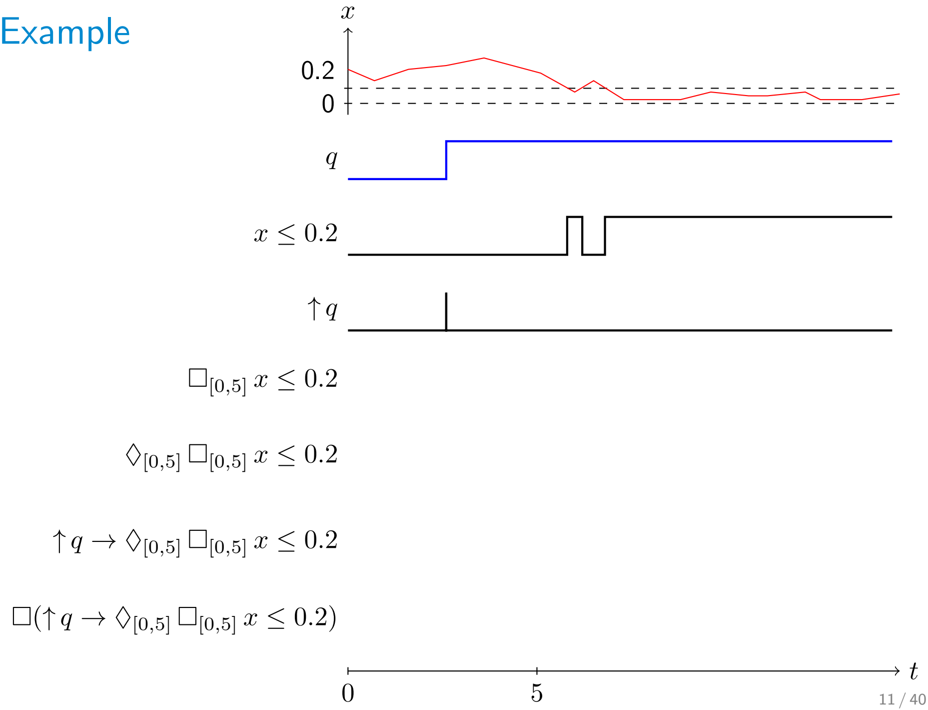
Example


x
0.2
0
q
$x \leq 0.2$
$\uparrow q$
$\Box_{[0,5]}\, x \leq 0.2$
$\Diamond_{[0,5]}\, \Box_{[0,5]}\, x \leq 0.2$
$\uparrow q \rightarrow \Diamond_{[0,5]}\, \Box_{[0,5]}\, x \leq 0.2$
$\Box(\uparrow q \rightarrow \Diamond_{[0,5]}\, \Box_{[0,5]}\, x \leq 0.2)$
0
5
t

Example

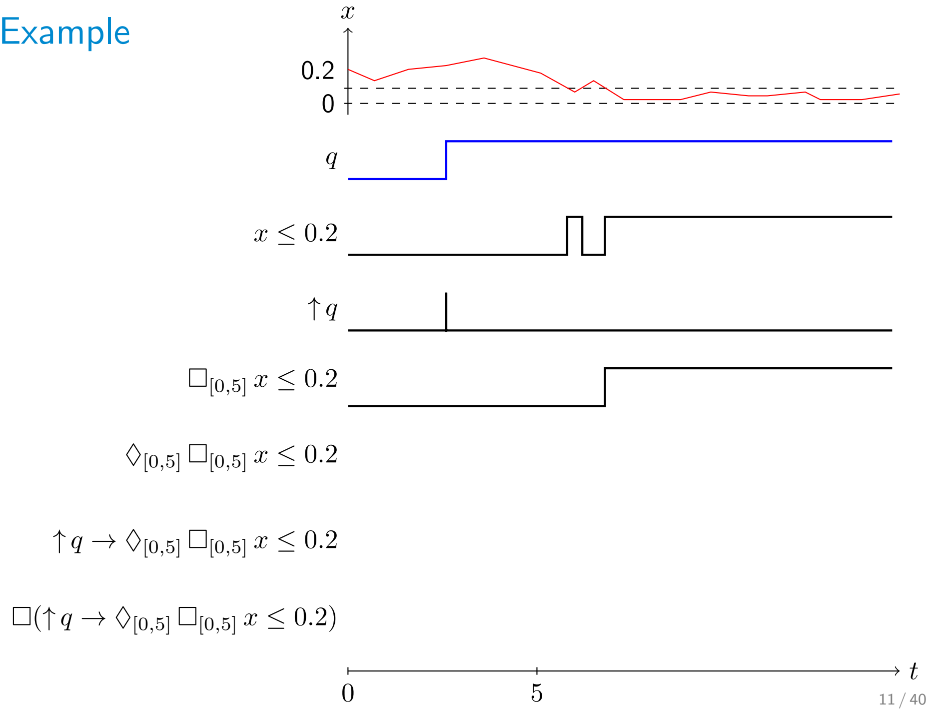

x
0.2
0
q
$x \leq 0.2$
$\uparrow q$
$\Box_{[0,5]}\, x \leq 0.2$
$\Diamond_{[0,5]}\, \Box_{[0,5]}\, x \leq 0.2$
$\uparrow q \rightarrow \Diamond_{[0,5]}\, \Box_{[0,5]}\, x \leq 0.2$
$\Box(\uparrow q \rightarrow \Diamond_{[0,5]}\, \Box_{[0,5]}\, x \leq 0.2)$
t
0
5

Example



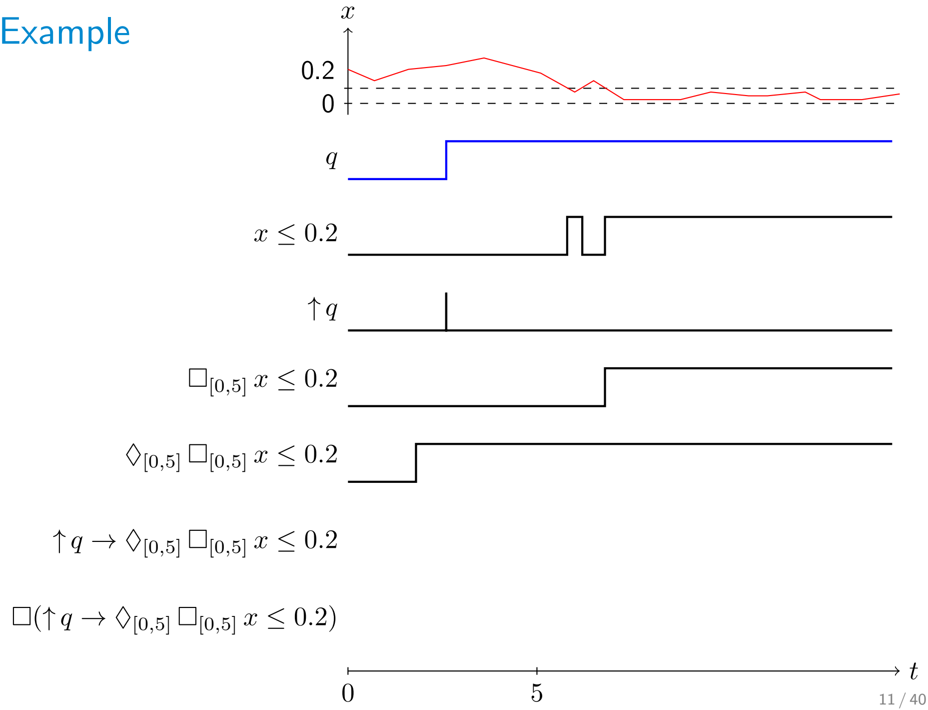
x
0.2
0
q
$x \leq 0.2$
$\uparrow q$
$\Box_{[0,5]}\, x \leq 0.2$
$\Diamond_{[0,5]}\, \Box_{[0,5]}\, x \leq 0.2$
$\uparrow q \rightarrow \Diamond_{[0,5]}\, \Box_{[0,5]}\, x \leq 0.2$
$\Box(\uparrow q \rightarrow \Diamond_{[0,5]}\, \Box_{[0,5]}\, x \leq 0.2)$
0
5
t

Example

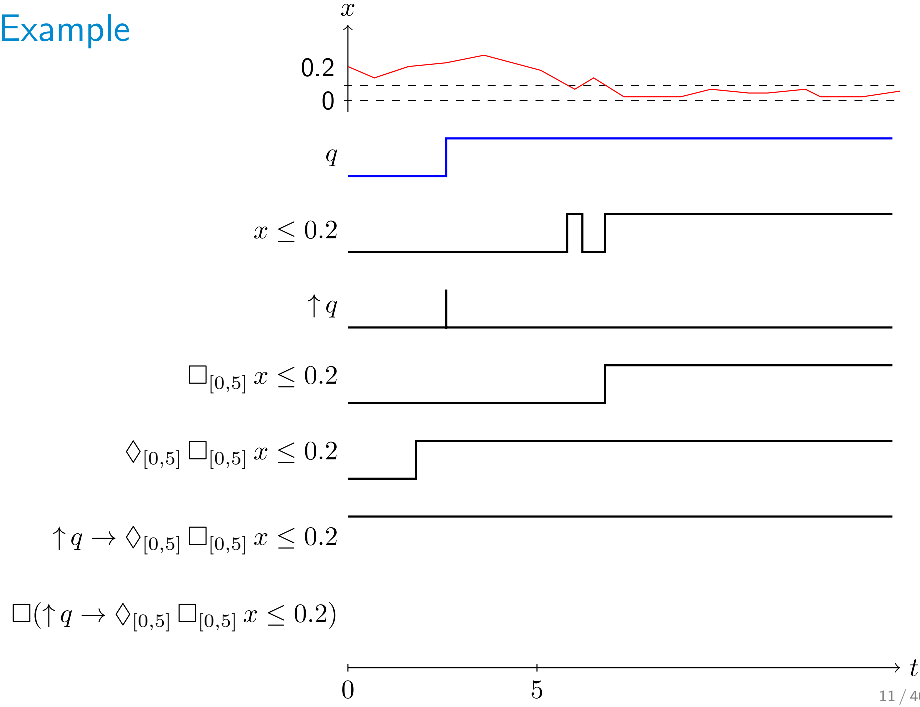


x
0.2
0
q
$x \leq 0.2$
$\uparrow q$
$\Box_{[0,5]}\, x \leq 0.2$
$\Diamond_{[0,5]}\, \Box_{[0,5]}\, x \leq 0.2$
$\uparrow q \rightarrow \Diamond_{[0,5]}\, \Box_{[0,5]}\, x \leq 0.2$
$\Box(\uparrow q \rightarrow \Diamond_{[0,5]}\, \Box_{[0,5]}\, x \leq 0.2)$
0
5
t

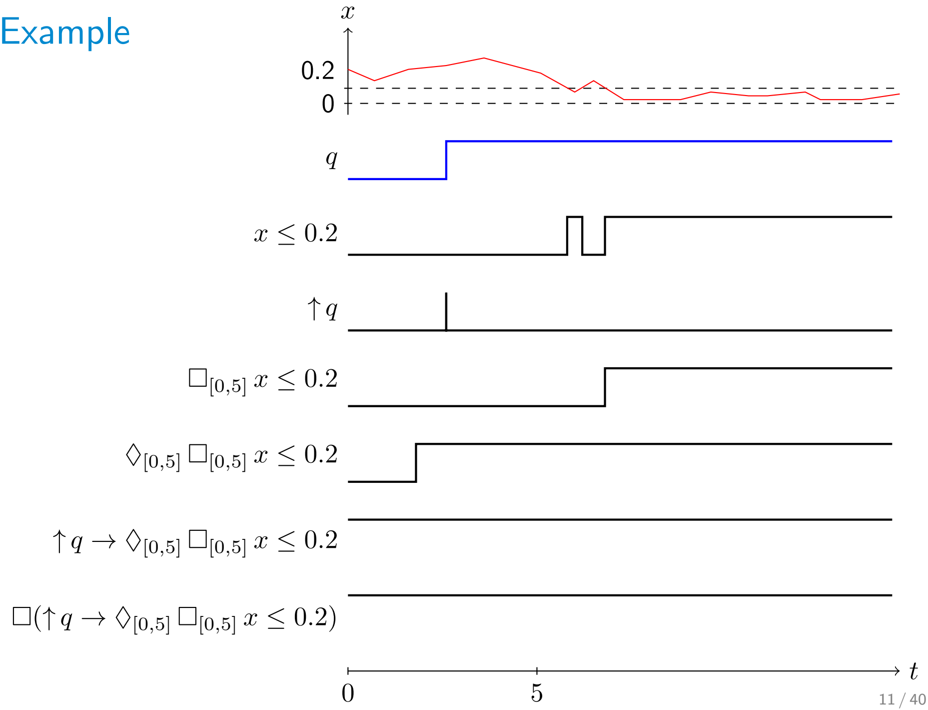
Example


x
0.2
0
q
$x \leq 0.2$
$\uparrow q$
$\Box_{[0,5]}\, x \leq 0.2$
$\Diamond_{[0,5]}\, \Box_{[0,5]}\, x \leq 0.2$
$\uparrow q \rightarrow \Diamond_{[0,5]}\, \Box_{[0,5]}\, x \leq 0.2$
$\Box(\uparrow q \rightarrow \Diamond_{[0,5]}\, \Box_{[0,5]}\, x \leq 0.2)$
0
5
t

Example


x
0.2
0
q
$x \leq 0.2$
$\uparrow q$
$\Box_{[0,5]}\, x \leq 0.2$
$\Diamond_{[0,5]}\, \Box_{[0,5]}\, x \leq 0.2$
$\uparrow q \rightarrow \Diamond_{[0,5]}\, \Box_{[0,5]}\, x \leq 0.2$
$\Box(\uparrow q \rightarrow \Diamond_{[0,5]}\, \Box_{[0,5]}\, x \leq 0.2)$
0
5
t

Example



x
0.2
0
q
$x \leq 0.2$
$\uparrow q$
$\Box_{[0,5]}\, x \leq 0.2$
$\Diamond_{[0,5]}\, \Box_{[0,5]}\, x \leq 0.2$
$\uparrow q \rightarrow \Diamond_{[0,5]}\, \Box_{[0,5]}\, x \leq 0.2$
$\Box(\uparrow q \rightarrow \Diamond_{[0,5]}\, \Box_{[0,5]}\, x \leq 0.2)$
t
0
5

Quantitative Semantics

Robustness value $[\![\varphi]\!]_{\boldsymbol{w}}$ indicates how strongly φ is satisfied / violated by $\boldsymbol{w}$

- Positive if satisfied / negative if violated
- Magnitude $=$ conservative estimate of distance to satisfaction / violation boundary

Definition (Robustness Signal)

$$[\![x \leq c]\!]_{\boldsymbol{w}} = c - x_{\boldsymbol{w}} \qquad [\![\neg\varphi]\!]_{\boldsymbol{w}} = -[\![\varphi]\!]_{\boldsymbol{w}}$$

$$\left[\!\left[\Diamond_{[a,b]}\,\varphi\right]\!\right]_{\boldsymbol{w}} = t \mapsto \sup_{t' \in [t+a, t+b]} [\![\varphi]\!]_{\boldsymbol{w}}(t') \qquad [\![\varphi \vee \psi]\!]_{\boldsymbol{w}} = \max\{[\![\varphi]\!]_{\boldsymbol{w}}, [\![\psi]\!]_{\boldsymbol{w}}\}$$

Outline

Principle

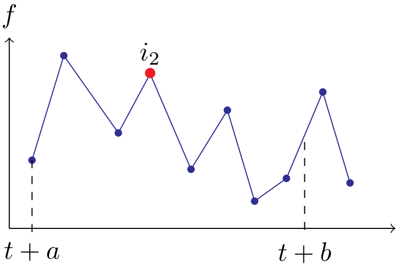
Theorem

For any φ and $\boldsymbol{w}$ piecewise linear, $[\![\varphi]\!]_{\boldsymbol{w}}$ is piecewise linear

- Until rewrite rules preserve the robustness value
- Timed eventually computed using optimal streaming algorithm of (Lemire, 2006) adapted to variable-step sampling

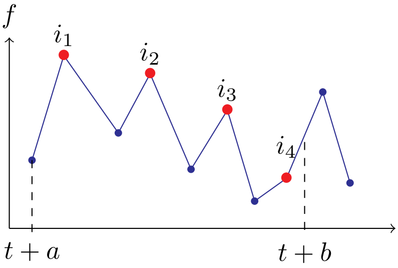
Eventually Computation

- Problem: compute $g(t) = \sup_{t' \in [t+a, t+b]} f(t')$
- Solution: take maximum of f at $t+a, t+b$ and sampling points inside (a, b)



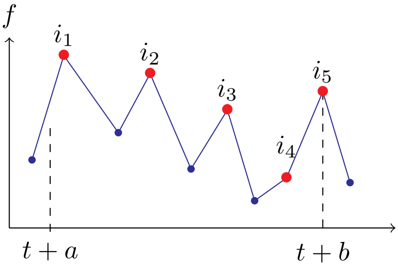
Eventually Computation

- Problem: compute $g(t) = \sup_{t' \in [t+a, t+b]} f(t')$
- Solution: take maximum of f at $t + a, t + b$ and sampling points inside (a, b)



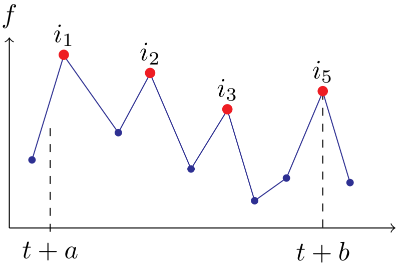
Eventually Computation

- Problem: compute $g(t) = \sup_{t' \in [t+a, t+b]} f(t')$
- Solution: take maximum of f at $t + a, t + b$ and sampling points inside (a, b)



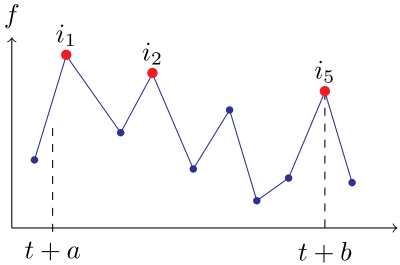
Eventually Computation

- Problem: compute $g(t) = \sup_{t' \in [t+a, t+b]} f(t')$
- Solution: take maximum of f at $t + a, t + b$ and sampling points inside (a, b)



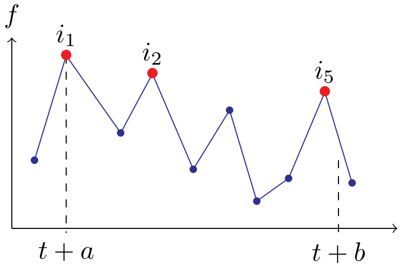
Eventually Computation

- Problem: compute $g(t) = \sup_{t' \in [t+a, t+b]} f(t')$
- Solution: take maximum of f at $t+a, t+b$ and sampling points inside (a, b)



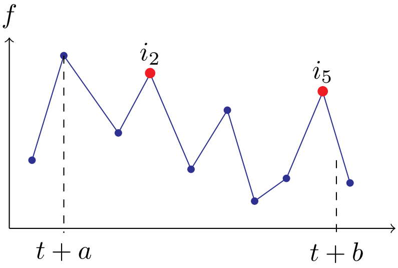
Eventually Computation

- Problem: compute $g(t) = \sup_{t' \in [t+a, t+b]} f(t')$
- Solution: take maximum of f at $t+a, t+b$ and sampling points inside (a, b)

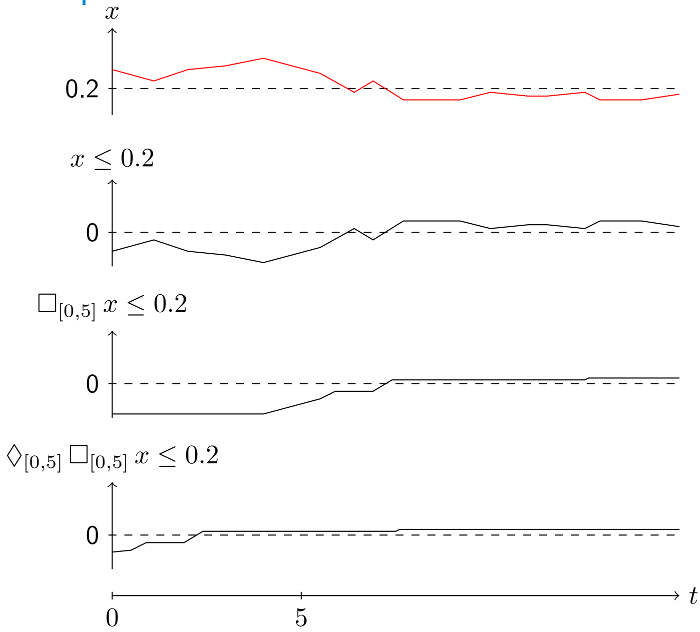


Eventually Computation

- Problem: compute $g(t) = \sup_{t' \in [t+a, t+b]} f(t')$
- Solution: take maximum of f at $t+a, t+b$ and sampling points inside (a, b)



Example



x
0.2
$x \leq 0.2$
0
$\square_{[0,5]}\, x \leq 0.2$
0
$\lozenge_{[0,5]}\, \square_{[0,5]}\, x \leq 0.2$
0
t
0
5

Evaluation

- Worst-case complexity in $2^{O(|\varphi|)} \cdot |\boldsymbol{w}|$
- Implementation benchmarked with random signals:

$\|\boldsymbol{w}\|$	10^2	10^3	10^4	10^5
$\Diamond_{[1,2]}$	0.0031	0.0030	0.0040	0.019
$\Diamond_{[1,11]}$	0.0029	0.0026	0.0039	0.017
$\Diamond_{[1,21]}$	0.0027	0.0026	0.0041	0.018
$\Diamond_{[1,31]}$	0.0030	0.0028	0.0041	0.021

- Cost of computing $\Diamond_{[a,b]}$ independent from $b - a$
- Improves on related works by several orders of magnitude

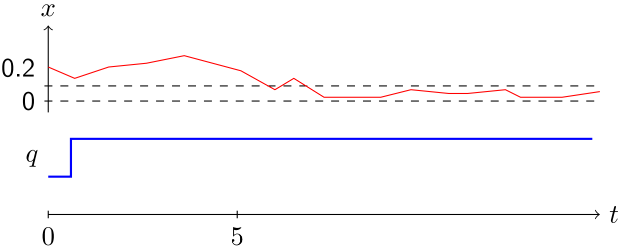
Publications

- Donzé, Ferrère, and Maler. Efficient robust monitoring for STL. In *Computer Aided Verification (CAV)*, 2013.

Outline

Motivation

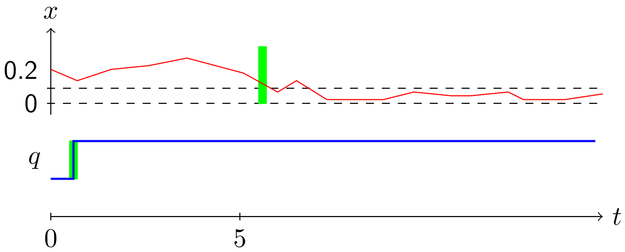
- Find small segment of $\boldsymbol{w}$ sufficient to cause violation of φ
- Example: violation of $\Box(\uparrow q \rightarrow \Diamond_{[0,5]} \Box_{[0,5]}\, x \leq 0.2)$



- Sub-traces = temporal **implicants**

Motivation

- Find small segment of $\boldsymbol{w}$ sufficient to cause violation of φ
- Example: violation of $\Box(\uparrow q \rightarrow \Diamond_{[0,5]} \Box_{[0,5]} x \leq 0.2)$



- Sub-traces = temporal **implicants**

Propositional Implicants

- Implicant of φ $\approx$ partial valuation whose extensions satisfy φ

Definition

Implicant of φ = term γ such that $\gamma \Rightarrow \varphi$
Prime implicant of φ = implicant of φ maximal relative to $\Rightarrow$

- For diagnostic: implicant compatible with observed values $\boldsymbol{v}$

Problem (Diagnostic)

For given φ and $\boldsymbol{v}$, find $\gamma \Rightarrow \neg\varphi$ such that $\boldsymbol{v} \models \gamma$

Propositional Implicants

- Implicant of $\varphi \quad \approx \quad$ partial valuation whose extensions satisfy φ

Definition

Implicant of φ = term γ such that $\gamma \Rightarrow \varphi$
Prime implicant of φ = implicant of φ maximal relative to $\Rightarrow$

- For diagnostic: implicant compatible with observed values $\boldsymbol{v}$

Problem (Diagnostic)

For given φ and $\boldsymbol{v}$, find $\gamma \Rightarrow \neg\varphi$ such that $\boldsymbol{v} \models \gamma$

Temporal Implicants

- Temporal implicant of $\varphi \;\approx\;$ partial trace whose extensions satisfy φ
- Syntactical considerations:
  - Terms with conjunctions $\bigwedge_{t \in T} \theta(t)$ over intervals
  - Limit values handled by non-standard reals t^+, t^-
- Example:

$$\bigwedge_{t \in [0.5, 3.0]} \neg p(t) \quad \Rightarrow \quad \neg \Diamond_{[1,2]}\, p$$

Theorem

Every realtime property φ has a prime implicant

Relies on boundedness of the time domain and non-standard extension

Computation for Signal Temporal Logic

Diagnostic operators E, F such that:

- Explanation $E(\varphi) \Rightarrow \varphi$
- Falsification $F(\varphi) \Rightarrow \neg\varphi$

Definition (Diagnostic Signal)

$$E(p) = p \qquad E(\neg\varphi) = F(\varphi)$$

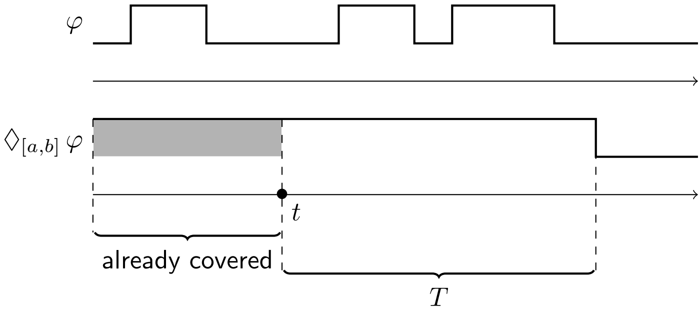
$$E(\Diamond_{[a,b]}\,\varphi) = t \mapsto E(\varphi)(\xi(t)) \qquad F(\Diamond_{[a,b]}\,\varphi) = t \mapsto \bigwedge_{t' \in [t+a, t+b]} F(\varphi)(t')$$

with **selection function** ξ such that $\xi(t) \in [t+a, t+b]$

Selection Function

Compute ξ over some interval T where $\Diamond_{[a,b]}\,\varphi$ holds:

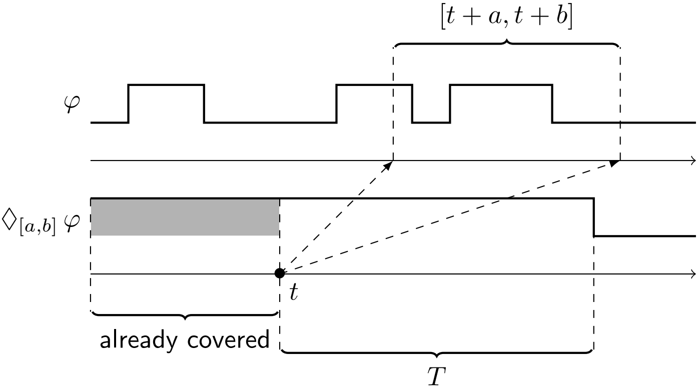
- Current time t is at start of T
- Select last witness s of φ to account for $\Diamond_{[a,b]}\,\varphi$ at t
- Remove from T the part R that has been accounted for



Selection Function

Compute ξ over some interval T where $\Diamond_{[a,b]}\,\varphi$ holds:

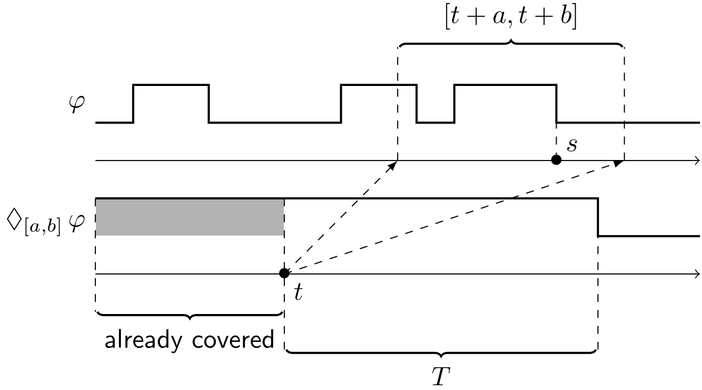
- Current time t is at start of T
- Select last witness s of φ to account for $\Diamond_{[a,b]}\,\varphi$ at t
- Remove from T the part R that has been accounted for



Selection Function

Compute ξ over some interval T where $\Diamond_{[a,b]}\,\varphi$ holds:

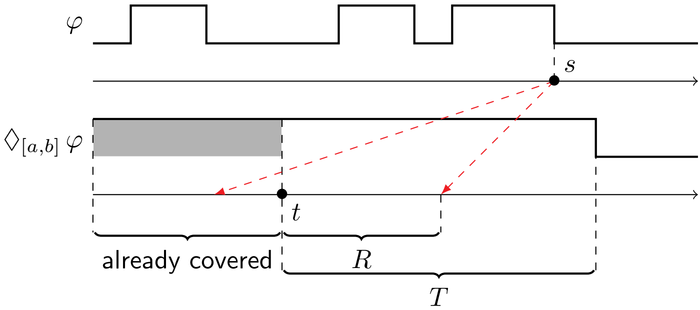
- Current time t is at start of T
- Select last witness s of φ to account for $\Diamond_{[a,b]}\,\varphi$ at t
- Remove from T the part R that has been accounted for



Selection Function

Compute ξ over some interval T where $\Diamond_{[a,b]}\,\varphi$ holds:

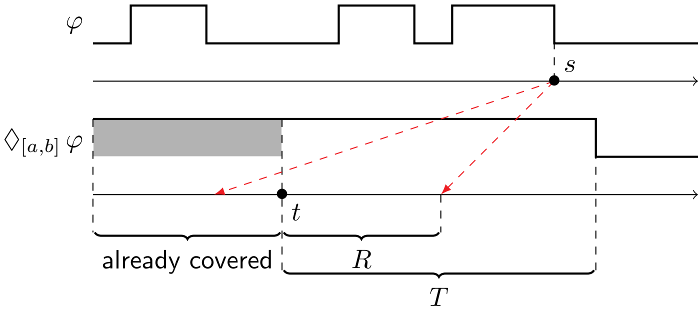
- Current time t is at start of T
- Select last witness s of φ to account for $\Diamond_{[a,b]}\,\varphi$ at t
- Remove from T the part R that has been accounted for



Selection Function

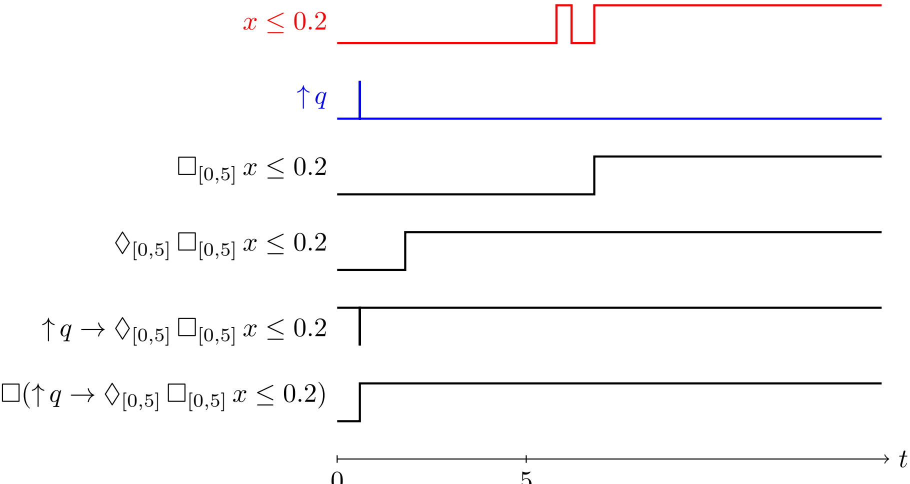
Compute ξ over some interval T where $\Diamond_{[a,b]}\,\varphi$ holds:

- Current time t is at start of T
- Select last witness s of φ to account for $\Diamond_{[a,b]}\,\varphi$ at t
- Remove from T the part R that has been accounted for



Overview

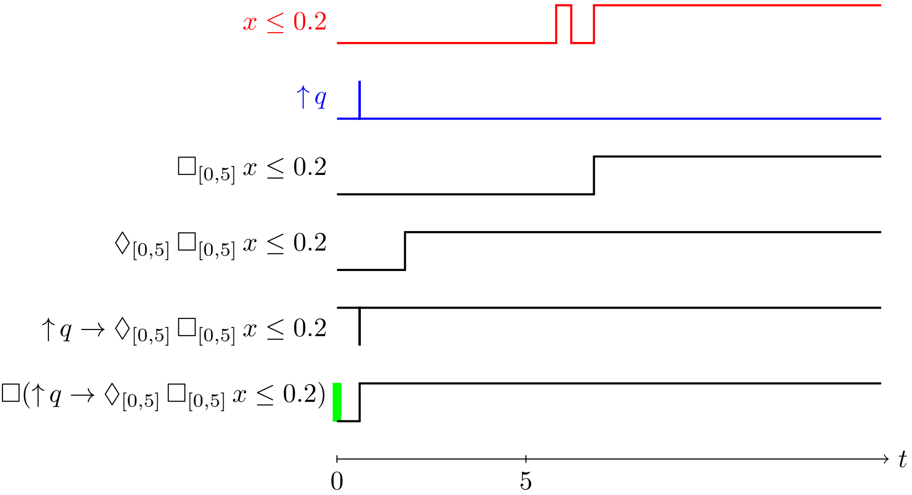
- Example:



- Worst-case complexity $O(|\varphi|)^2 \cdot |\boldsymbol{w}|$

Overview

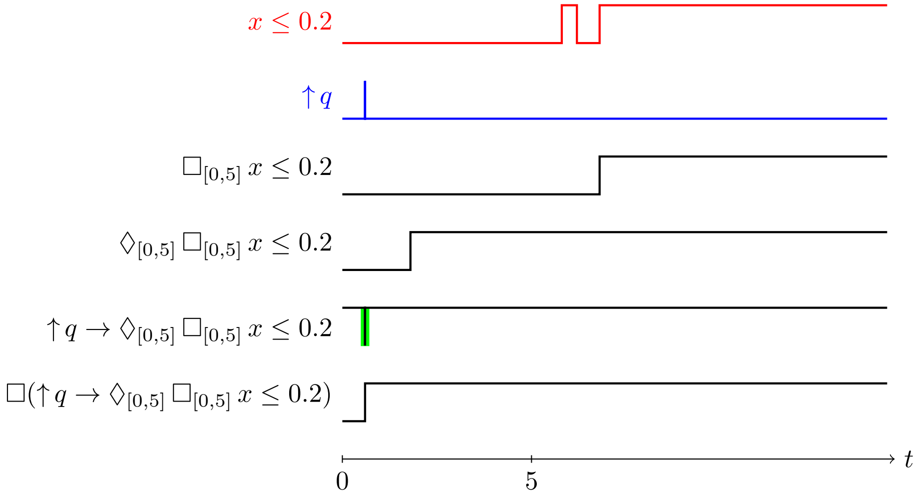
- Example:



- Worst-case complexity $O(|\varphi|)^2 \cdot |\boldsymbol{w}|$

Overview

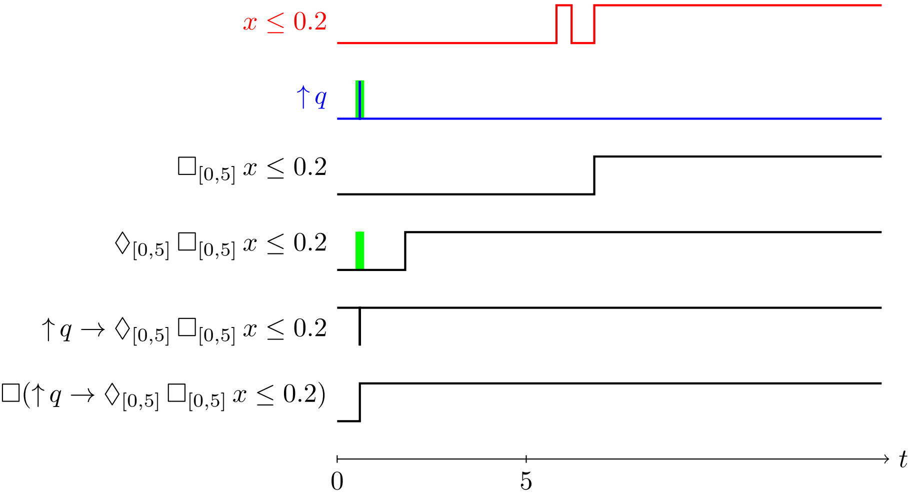
- Example:



- Worst-case complexity $O(|\varphi|)^2 \cdot |\boldsymbol{w}|$

Overview

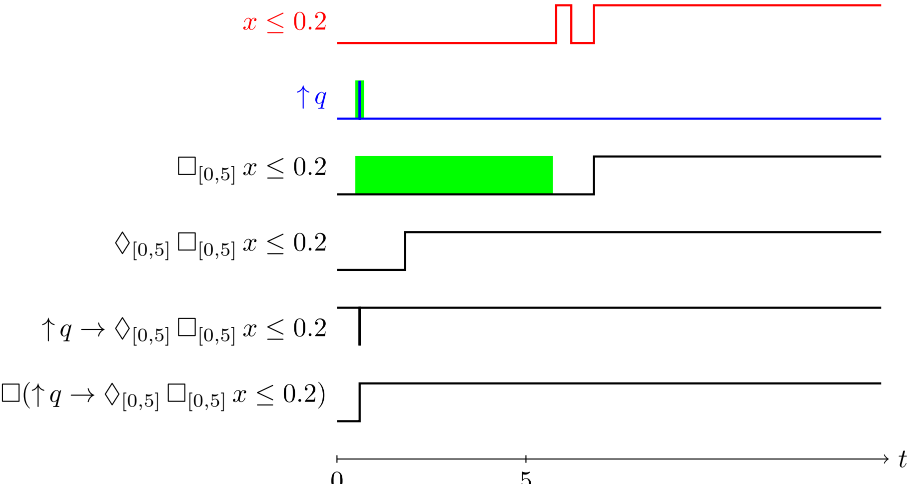
- Example:



- Worst-case complexity $O(|\varphi|)^2 \cdot |\boldsymbol{w}|$

Overview

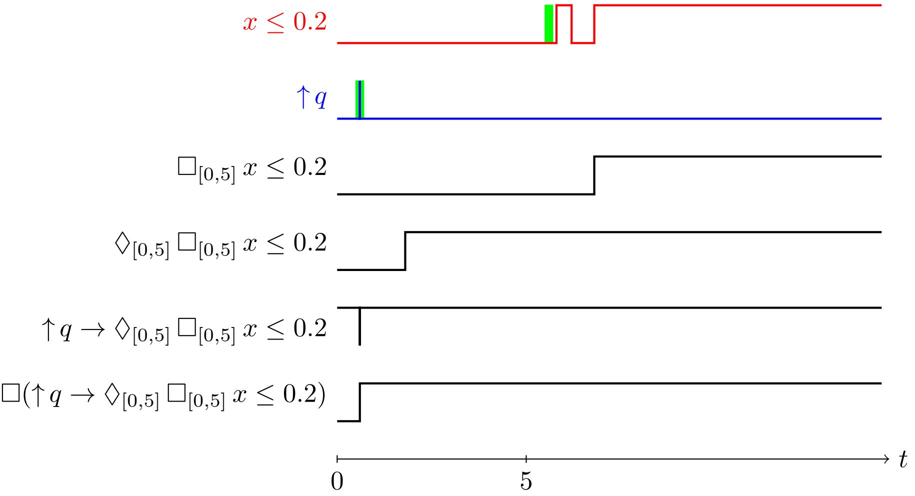
- Example:



- Worst-case complexity $O(|\varphi|)^2 \cdot |\boldsymbol{w}|$

Overview

- Example:



- Worst-case complexity $O(|\varphi|)^2 \cdot |\boldsymbol{w}|$

Publications

- Ferrère, Maler, and Nickovic. Trace diagnostics using temporal implicants. In *Automated Technology for Verification and Analysis (ATVA)*, 2015.

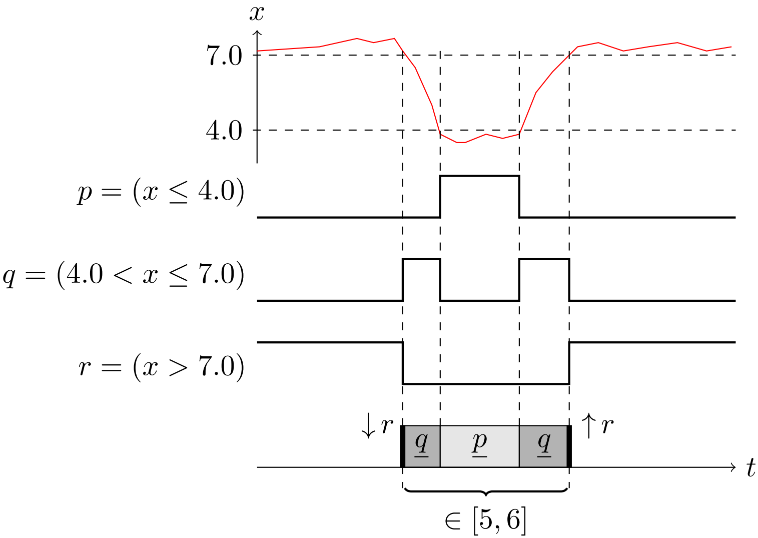
Outline

Signal Regular Expressions

- Propositions p: Boolean variables q, threshold conditions $x \leq c$
- Atomic expressions: holding $\underline{p}$, events $\uparrow p$
- Concatenation: $\varphi \cdot \psi$
- Kleene star: φ^*
- Duration restriction: $\langle \varphi \rangle_I$

Example

Pulse pattern: $\psi = \downarrow r \cdot \langle \underline{q} \cdot \underline{p} \cdot \underline{q} \rangle_{[5,6]} \cdot \uparrow r$



Monitoring

- For any $\boldsymbol{w}$ expression φ defines a set of segments (t, t') such that $\boldsymbol{w}[t, t']$ matches φ
- Offline approach: for all subexpressions φ compute the complete set of matches $[\varphi]_{\boldsymbol{w}}$ of φ relative to $\boldsymbol{w}$

Definition (Match Set)

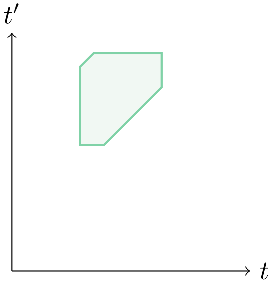
$$[\underline{p}]_{\boldsymbol{w}} = \{(t, t') : t < t'' < t' \rightarrow p_{\boldsymbol{w}}(t'') = 1\} \qquad [\varphi \vee \psi]_{\boldsymbol{w}} = [\varphi]_{\boldsymbol{w}} \cup [\psi]_{\boldsymbol{w}}$$

$$[\langle\varphi\rangle_I]_{\boldsymbol{w}} = \{(t, t') : t' - t \in I\} \cap [\varphi]_{\boldsymbol{w}} \qquad [\varphi \wedge \psi]_{\boldsymbol{w}} = [\varphi]_{\boldsymbol{w}} \cap [\psi]_{\boldsymbol{w}}$$

$$[\varphi \cdot \psi]_{\boldsymbol{w}} = [\varphi]_{\boldsymbol{w}} \fatsemi [\psi]_{\boldsymbol{w}} \qquad [\varphi^*]_{\boldsymbol{w}} = \bigcup_{i \geq 0} [\varphi^i]_{\boldsymbol{w}}$$

Match Set Representation

- A zone = convex set with horizontal, vertical and diagonal boundaries
- Represents a set of signal segments

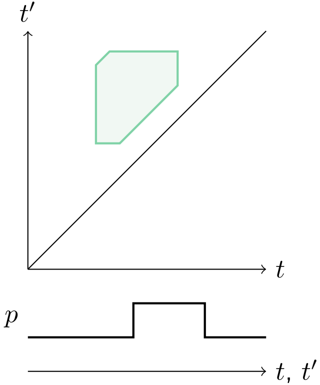


Theorem

For any φ and w with finite variability, $[\varphi]_w$ is a finite union of **zones**

Match Set Representation

- A zone = convex set with horizontal, vertical and diagonal boundaries
- Represents a set of signal segments

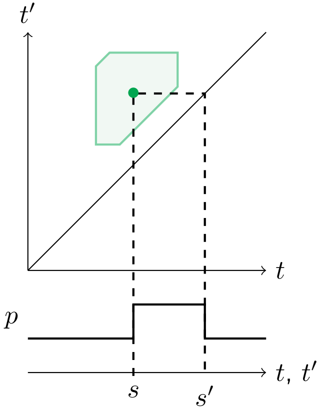


Theorem

For any φ and w with finite variability, $[\varphi]_w$ is a finite union of **zones**

Match Set Representation

- A zone = convex set with horizontal, vertical and diagonal boundaries
- Represents a set of signal segments

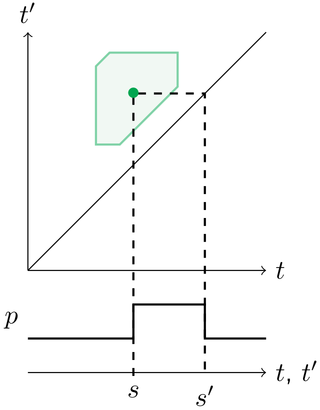


Theorem

For any φ and w with finite variability, $[\varphi]_w$ is a finite union of **zones**

Match Set Representation

- A zone = convex set with horizontal, vertical and diagonal boundaries
- Represents a set of signal segments



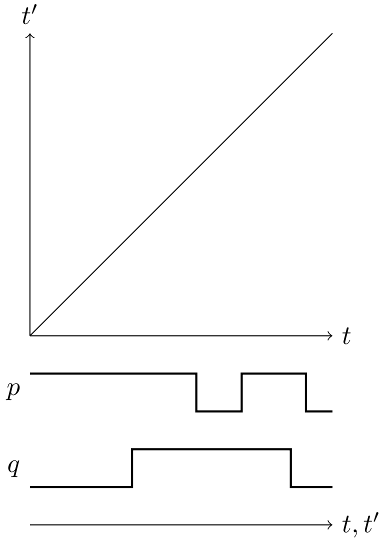
Theorem

For any φ and $\boldsymbol{w}$ with finite variability, $[\varphi]_{\boldsymbol{w}}$ is a finite union of **zones**

Example

$$\langle \underline{p} \rangle_{[2,4]} \cdot \langle \underline{q} \rangle_{[1,2]}$$

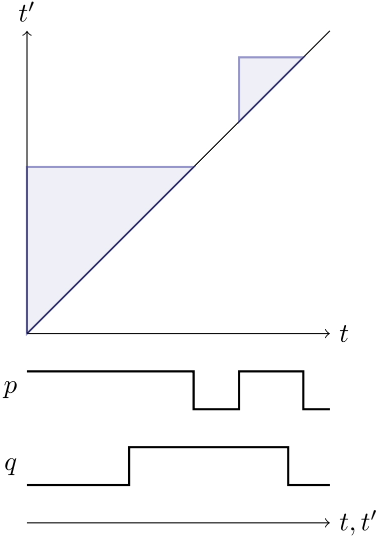
- Match set of $\underline{p}$
- Match set of $\langle \underline{p} \rangle_{[2,4]}$
- Match set of $\langle \underline{q} \rangle_{[1,2]}$
- Match set of $\langle \underline{p} \rangle_{[2,4]} \cdot \langle \underline{q} \rangle_{[1,2]}$



Example

$$\langle \underline{p} \rangle_{[2,4]} \cdot \langle \underline{q} \rangle_{[1,2]}$$

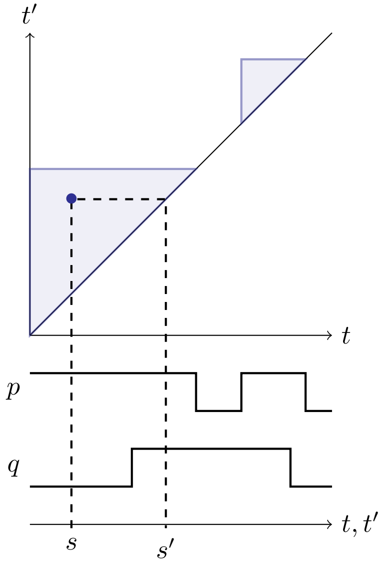
- Match set of $\underline{p}$
- Match set of $\langle \underline{p} \rangle_{[2,4]}$
- Match set of $\langle \underline{q} \rangle_{[1,2]}$
- Match set of $\langle \underline{p} \rangle_{[2,4]} \cdot \langle \underline{q} \rangle_{[1,2]}$



Example

$$\langle \underline{p} \rangle_{[2,4]} \cdot \langle \underline{q} \rangle_{[1,2]}$$

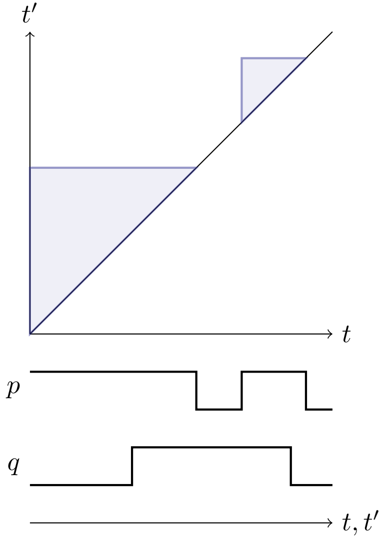
- Match set of $\underline{p}$
- Match set of $\langle \underline{p} \rangle_{[2,4]}$
- Match set of $\langle \underline{q} \rangle_{[1,2]}$
- Match set of $\langle \underline{p} \rangle_{[2,4]} \cdot \langle \underline{q} \rangle_{[1,2]}$



Example

$$\langle \underline{p} \rangle_{[2,4]} \cdot \langle \underline{q} \rangle_{[1,2]}$$

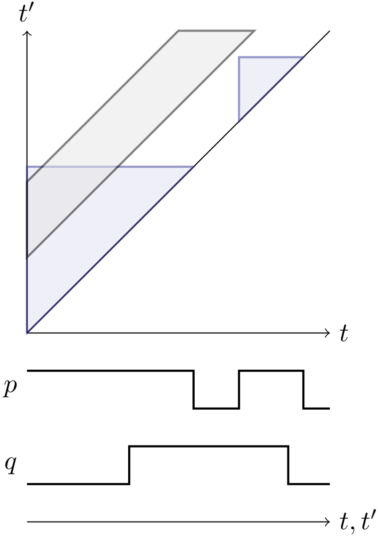
- Match set of $\underline{p}$
- Match set of $\langle \underline{p} \rangle_{[2,4]}$
- Match set of $\langle \underline{q} \rangle_{[1,2]}$
- Match set of $\langle \underline{p} \rangle_{[2,4]} \cdot \langle \underline{q} \rangle_{[1,2]}$



Example

$$\langle \underline{p} \rangle_{[2,4]} \cdot \langle \underline{q} \rangle_{[1,2]}$$

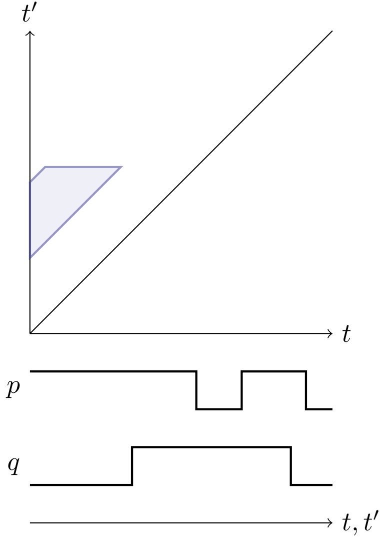
- Match set of $\underline{p}$
- Match set of $\langle \underline{p} \rangle_{[2,4]}$
- Match set of $\langle \underline{q} \rangle_{[1,2]}$
- Match set of $\langle \underline{p} \rangle_{[2,4]} \cdot \langle \underline{q} \rangle_{[1,2]}$



Example

$$\langle \underline{p} \rangle_{[2,4]} \cdot \langle \underline{q} \rangle_{[1,2]}$$

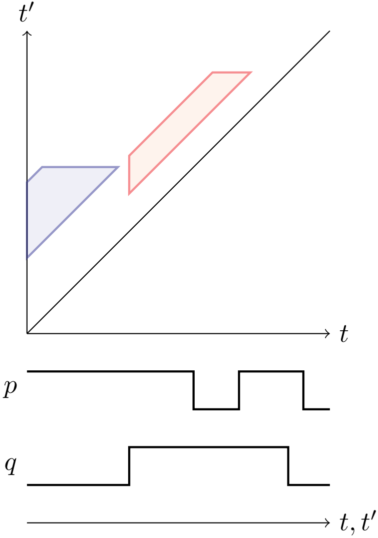
- Match set of $\underline{p}$
- Match set of $\langle \underline{p} \rangle_{[2,4]}$
- Match set of $\langle \underline{q} \rangle_{[1,2]}$
- Match set of $\langle \underline{p} \rangle_{[2,4]} \cdot \langle \underline{q} \rangle_{[1,2]}$



Example

$$\langle \underline{p} \rangle_{[2,4]} \cdot \langle \underline{q} \rangle_{[1,2]}$$

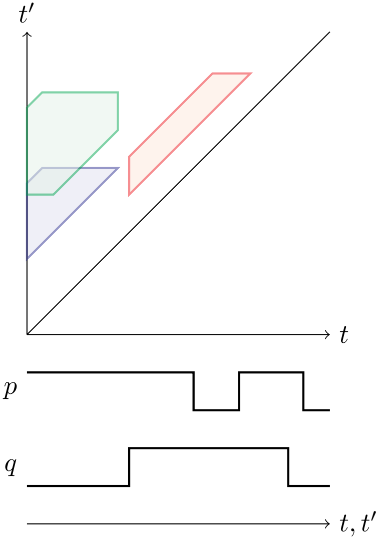
- Match set of $\underline{p}$
- Match set of $\langle \underline{p} \rangle_{[2,4]}$
- Match set of $\langle \underline{q} \rangle_{[1,2]}$
- Match set of $\langle \underline{p} \rangle_{[2,4]} \cdot \langle \underline{q} \rangle_{[1,2]}$



Example

$$\langle \underline{p} \rangle_{[2,4]} \cdot \langle \underline{q} \rangle_{[1,2]}$$

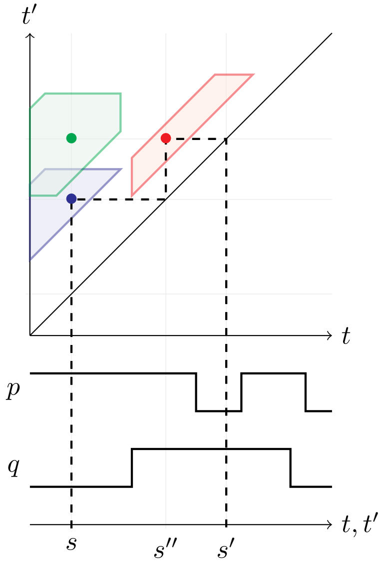
- Match set of $\underline{p}$
- Match set of $\langle \underline{p} \rangle_{[2,4]}$
- Match set of $\langle \underline{q} \rangle_{[1,2]}$
- Match set of $\langle \underline{p} \rangle_{[2,4]} \cdot \langle \underline{q} \rangle_{[1,2]}$



Example

$$\langle \underline{p} \rangle_{[2,4]} \cdot \langle \underline{q} \rangle_{[1,2]}$$

- Match set of $\underline{p}$
- Match set of $\langle \underline{p} \rangle_{[2,4]}$
- Match set of $\langle \underline{q} \rangle_{[1,2]}$
- Match set of $\langle \underline{p} \rangle_{[2,4]} \cdot \langle \underline{q} \rangle_{[1,2]}$



Kleene Star

On bounded traces $\boldsymbol{w}$ the sequence $\bigvee_{i=0}^{n} \varphi^i$ converges to a fix-point in finitely many steps

- Assume $\boldsymbol{w}$ can be split in m constant segments $\boldsymbol{v}$ of length less that 1
- Over each segment either $[\varphi]_{\boldsymbol{v}} = [\top]_{\boldsymbol{v}}$ or $[\varphi]_{\boldsymbol{v}} = [\bot]_{\boldsymbol{v}}$

Lemma

$[\varphi^n]_{\boldsymbol{w}} \subseteq \left[\varphi^{n-1}\right]_{\boldsymbol{w}}$ *for any* $n > 2m + 1$

Compute $\bigvee_{i=0}^{n} \varphi^i$ by squaring: ϵ, φ, φ^2, φ^4, $\ldots$, φ^{2^k} up to $k > \log(2m + 1)$

Evaluation

- Worst-case complexity: $|\boldsymbol{w}|^{O(|\varphi|)}$ without star
- Implementation using DBM for efficient zones computation
- Benchmarked for

$$\varphi = \langle ((\langle \underline{p} \cdot \underline{\neg p} \rangle_{[0,10]})^* \wedge (\langle \underline{q} \cdot \underline{\neg q} \rangle_{[0,10]})^* \rangle_{[80,\infty]}$$

with randomized traces:

$\|\boldsymbol{w}\|$	$\|[\varphi]_{\boldsymbol{w}}\|$	time
3654	0	0.27
6715	10	1.35
13306	23	2.73
26652	47	5.83

- Observed performance linear in $|\boldsymbol{w}|$

Publications

- Ulus, Ferrère, Asarin, and Maler. Timed pattern matching. In *Formal Modeling and Analysis of Timed Systems (FORMATS)*, 2014.
- Ulus, Ferrère, Asarin, and Maler. Online timed pattern matching using derivatives In *Tools and Algorithms for the Construction and Analysis of Systems (TACAS)*, 2016.

Outline

Measurement Language

- Motivation: automate the extraction of mixed-signal measures
- Signal Regular Expressions control when the measure takes place
- Measure: aggregating operator $\mathrm{duration}$, min, max, and $\mathrm{average}$
- Example:

$$\mathrm{average}(\uparrow(x > 1.0) \cdot (x > 1.0) \cdot \downarrow(x > 1.0))$$

measures average value of x on high portions

Conditionals and Events

Construct expressions delimited by events

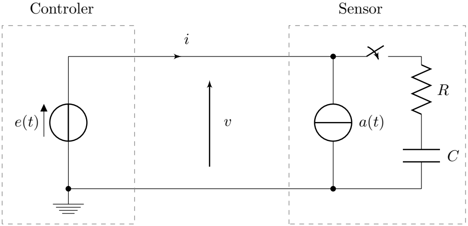
- **conditional operators**:
  - $?\varphi$ begins a match of φ
  - $!\varphi$ ends a match of φ
- **event-bounded** expressions ψ:
  - event $\uparrow p$, $\downarrow p$
  - conditional event $\psi?$, $\psi!$
  - sequence $\psi \cdot \varphi \cdot \psi$

Theorem

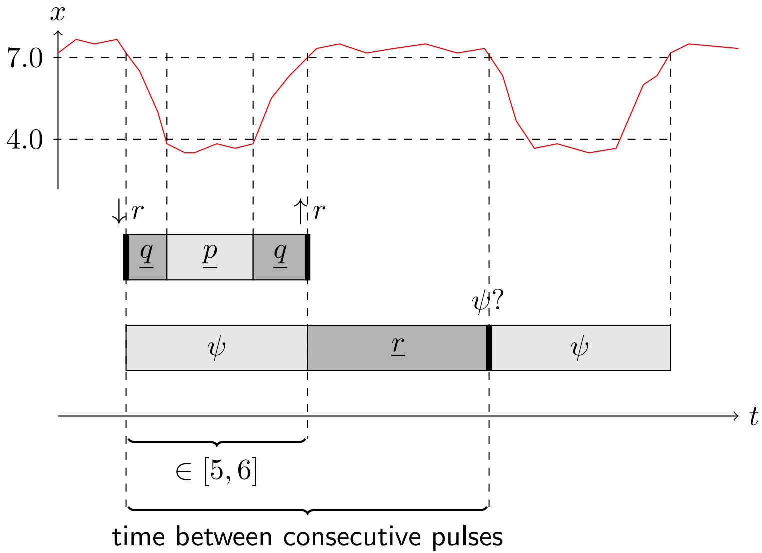
For any $\boldsymbol{w}$ and ψ event-bounded, $[\varphi]_\psi$ is finite

Case Study: Distributed System Interface

- DSI3 is a protocol for electronics in automotive industry
- Based on pulse communication
- Requirements about magnitude of signals and timing of events
- Implementation: behavioral model



Timing Requirement



Results

- Pulse description:

$$\psi = \downarrow r \cdot \langle \underline{q} \cdot \underline{p} \cdot \underline{q} \rangle_{[5,6]} \cdot \uparrow r$$

- Measure expression:

$$\varphi = \mathrm{duration}(\psi \cdot \underline{r} \cdot \psi?)$$

- Computation time cost:

$\lvert \boldsymbol{w} \rvert$	quantize	match	extract	total
$1 \cdot 10^6$	0.047	0.617	0.000	0.664
$5 \cdot 10^6$	0.197	0.612	0.000	0.809
$1 \cdot 10^7$	0.386	0.606	0.000	0.992
$2 \cdot 10^7$	0.759	0.609	0.000	1.368

Publications

- Ferrère, Maler, Nickovic, and Ulus. Measuring with timed patterns. In *Computer Aided Verification (CAV)*, 2015.

Outline

Analog Measurements and Digital Testbench

- Simulator-implemented measures provide guarantees:
  - accuracy
  - reproducible
- Unfortunately only accessible in analog environment
- Digital testbench enables structured verification
  - assertion tracking
  - coverage indicators
  - ...
- Mixed-signal verification often done with user-defined monitors

Measurement Tasks

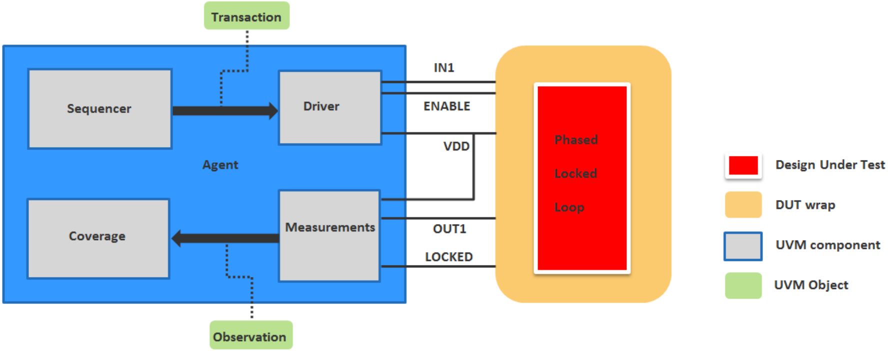
- We propose new measurements functions as **system tasks**

$$\texttt{task}_\mu(x, p, y, q, e, r)$$

- Input: (x, p), output: (y, q)
- Control: enable event e and reset event r
- Accessed in a variety of context: module, class, etc.
- Prototype implementation using VPI with functions: $\texttt{initialize}_\mu$, $\texttt{update}_\mu$, $\texttt{status}_\mu$, and $\texttt{evaluate}_\mu$

Phase Locked Loop

- Digital testbench using the Universal Verification Methodology:



- Measure relative jitter online, locking time and enforce safe operating area of current through VDD
- Computation time < 1s for measurements, ≈ 300s for simulation

Outline

Contributions

- Diagnostic procedure for realtime assertions
- Efficient algorithms for robustness computation
- Monitoring of regular expressions
- Pattern-based measurements
- Bring practice of analog and digital verification closer

Publications

1. Donzé, Ferrère, and Maler. Efficient robust monitoring for STL. In *Computer Aided Verification (CAV)*, 2013.
2. Ulus, Ferrère, Asarin, and Maler. Timed pattern matching. In *Formal Modeling and Analysis of Timed Systems (FORMATS)*, 2014.
3. Ferrère, Maler, Nickovic, and Ulus. Measuring with timed patterns. In *Computer Aided Verification (CAV)*, 2015.
4. Ferrère, Maler, and Nickovic. Trace diagnostics using temporal implicants. In *Automated Technology for Verification and Analysis (ATVA)*, 2015.
5. Ulus, Ferrère, Asarin, and Maler. Online timed pattern matching using derivatives In *Tools and Algorithms for the Construction and Analysis of Systems (TACAS)*, 2016.

Future Works

- Robustness of Signal Regular Expressions
- New monitoring algorithms for SRE
- Integrate SRE with STL
- Formal verification using regular expressions