Trace Diagnostics using Temporal Implicants

ATVA'15

Thomas Ferrère[1] Dejan Nickovic[2] Oded Maler[1]

[1] VERIMAG, University of Grenoble / CNRS
[2] Austrian Institute of Technology

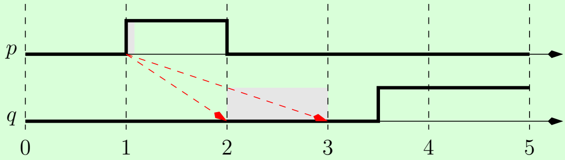
October 14, 2015

Motivation

- Practical question: understand **why** a simulation / formal verification violates MTL / LTL property.
- Problem: **long** simulation / counter-example trace with **large** (product) alphabet.
- Solution: isolate **segments** of the trace sufficient to cause violation.

Example

Diagnostics of $\Box(p \to \Diamond_{[1,2]}\, q)$ violation on sample trace



Implicant: $p[1] \wedge \bigwedge_{t \in [2,3]} \neg q[t]$.

Outline

Problem Formulation

Dense-time Issues

MTL Diagnostics

Outline

Diagnostics

Problem (Diagnostics)

Given specification φ and behavior w with $w \models \varphi$, find small implicant θ of φ with $w \models \theta$.

Applications

- Monitoring: find small subset of a **finite variability**, bounded counter-example of some MTL property.
- Model-checking: find small subset of an **ultimately-periodic** counter-example of some LTL property.

Implicants

- Propositional case

Example

$$\varphi = (p \wedge q) \vee (p \wedge \neg q) \vee \neg r, \qquad w = \{p \mapsto 1, q \mapsto 1, r \mapsto 0\}$$

Formula $\theta = p$ is a minimal diagnostic of φ relative to w.
Semantically: any valuation that contains $p \mapsto 1$ satisfies φ.

Proposition

For every φ, w such that $w \models \varphi$ there exists a minimal diagnostic: a **prime implicant** *θ such that $w \models \theta$.*

- Temporal case
  - syntactic representation of implicants?
  - infinite valuation domain: are there prime temporal implicants?

Temporal Logic

Signals

- A function $w : (\mathbb{T} \times \mathbb{P}) \to \{0,1\}$ with $\mathbb{T} = [0,d]$ time domain and $\mathbb{P}$ finite set of propositions.

- Projection $w_p : \mathbb{T} \to \{0,1\}$ of signal w onto variable p, and also **satisfaction signal** $w_\varphi : \mathbb{T} \to \{0,1\}$ for any formula φ.

Metric Temporal Logic

- syntax:

$$\varphi := p \mid \neg\varphi \mid \varphi_1 \vee \varphi_1 \mid \Diamond_I \varphi \mid \varphi_1 \,\mathcal{U}\, \varphi_2$$

- semantics:

$$\begin{array}{lll} (w,t) \models \Diamond_I \varphi & \text{iff} & \exists t' \in t \oplus I,\ (w,t') \models \varphi \\ (w,t) \models \varphi \,\mathcal{U}\, \psi & \text{iff} & \exists t' > t,\ (w,t') \models \psi \text{ and } \forall t < t'' < t',\ (w,t'') \models \varphi \end{array}$$

- derived operators: $\Box_I \varphi \equiv \neg\Diamond_I \neg\varphi, \quad \varphi \mathcal{R} \psi \equiv \neg(\neg\varphi \,\mathcal{U}\, \neg\psi)$
- models: $w \models \varphi$ iff $(w,0) \models \varphi$

Partial signals and refinements

Definition

- **sub-signal**: partial function from $\mathbb{T} \times \mathbb{P}$ to $\{0, 1\}$
- **refinement relation**: sub-signals $u \sqsubseteq v$ iff $u^{-1} \subseteq v^{-1}$ and $u_p[t] = v_p[t]$ where u is defined.

Proposition

Relation $\sqsubseteq$ defines a **semi-lattice**. *Meet operation $\sqcap$ such that $(u \sqcap v)^{-1} \subseteq u^{-1} \cap v^{-1}$, and minimal element $\perp : \emptyset \to \{0, 1\}$.*

Diagnostics (semantic reformulation)

Definition

Sub-signal u is **sub-model** of φ iff $w \models \varphi$ for all signals $w \sqsupseteq v$.

Reformulation

- prime implicants of φ $\sim$ minimal sub-models of φ
- diagnostics of φ resp. w $\sim$ sub-model v of φ s.t. $v \sqsubseteq w$

Outline

Problem Formulation

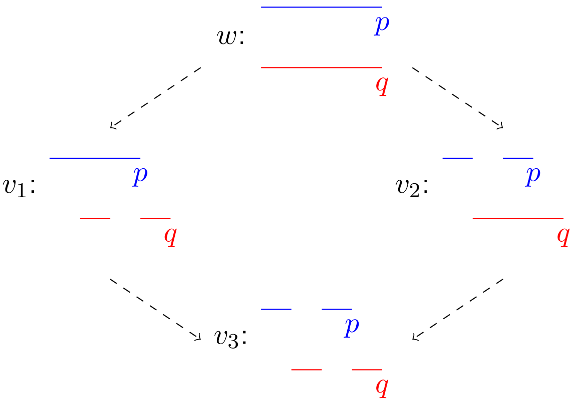
Dense-time Issues

MTL Diagnostics

Unbounded variability sub-models

Example

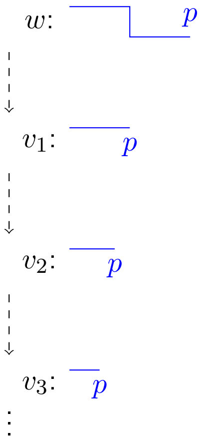
$\varphi := \Box(p \vee q)$ has minimal sub-models $I \times \{p\} \mapsto 1$, $J \times \{q\} \mapsto 1$ for arbitrary I, J partition of $\mathbb{T}$.



No minimal sub-model

Example

$\varphi = p\,\mathcal{U}\,\top$ has sub-models $(0,t) \times \{p\} \mapsto 1$ for arbitrary $t > 0$.



Temporal terms

- Syntax:

$$\theta := p[t] \mid \neg p[t] \mid \theta_1 \wedge \theta_2 \mid \bigwedge_{t \in T} \Theta[t]$$

  T subset of time domain, Θ function from time to terms.

- Semantics:

$$w \models \bigwedge_{t \in T} \Theta[t] \;\leftrightarrow\; \forall t \in T,\, w \models \Theta[t]$$

Example

Temporal term $\bigwedge_{t \in [0,1]} \neg p[t]$ represents sub-signal $[0,1] \times \{p\} \mapsto 0$.

Solving dense-time issues

Bounded variability

Definition

normal form terms: $\bigwedge_{i=1}^{m} \bigwedge_{t \in T_i} \ell_i[t]$ with T_i intervals and ℓ_i literals.

Bounded variability terms can be put in normal form.

Minimality

- introduce **non-standard reals** t^+, t^- for all t in the time domain with $t^- < t < t^+$
- terms over the extended time domain.

Existence of prime implicants

Theorem

Any satisfiable property φ admits prime implicants.

Proof.

- Zorn's Lemma: show that any chain of implicants $\theta_0 \Rightarrow \theta_1 \Rightarrow \theta_2 \Rightarrow \ldots$ of φ has a maximum.
- Take $\theta_* \equiv \bigwedge_{i \geq 0} \theta_i$ and show that $\theta_* \Rightarrow \varphi$.
- Given $w \models \theta_*$ there exists n such that $w \models \theta_n$.
  - if not there exists ℓ and (t_i) such that $\theta_i \Rightarrow \ell[t_i]$ and $w_\ell[t_i] = 0$
  - Bolzano Weierstrass: we may assume (t_i) monotonic and converging to t_*
  - for arbitrary $\delta > 0$ there exists i such that t_i is δ-close to t_*
  - $w_\ell[t_*] = 1$ and by finite variability $\exists j, w_\ell[t_j] = 1$. Contradiction

$\square$

Outline

Problem Formulation

Dense-time Issues

MTL Diagnostics

MTL semantics (non-standard extension)

Definition

$(w, t^+) \models \varphi$ iff $\lim_{t' \to t^+} w_\varphi[t'] = 1$

Arithmetic on non-standard reals

- $t \ll t'$ iff $t < t'$ or $t = t' \notin \mathbb{R}$.
- $t + I$ = closure $t \oplus I$ in the non-standard reals.

Proposition

- $(w, t) \models \Diamond_I \varphi$ *iff* $\exists t' \in t + I$, $(w, t') \models \varphi$
- $(w, t) \models \varphi \,\mathcal{U}\, \psi$ *iff* $\exists t' \gg t$, $(w, t') \models \psi$ *and* $\forall t \ll t'' \ll t'$, $(w, t'') \models \varphi$

Selection functions

- Used to select a **witnesses** of a formula.
- A function ξ labeled by a formula, such that $\xi_{\varphi \vee \psi}[t] \in \{\varphi, \psi\}$, $\xi_{\Diamond_I \psi}[t] \in t + I$, and $\xi_{\varphi \mathcal{U} \psi}[t] \gg t$.
- A **correct** selection function ξ when $(w, t) \models \varphi$ verifies
  - disjunction: $(w, t) \models \xi[t]$
  - eventually: $(w, \xi[t]) \models \psi$
  - until: $(w, \xi[t]) \models \psi$ and $\forall t \ll t' \ll \xi[t]$, $(w, t') \models \varphi$
- Bounded variability: ξ piecewise constant / linear with slope 1.

Generating implicants

The **diagnostics** of a formula φ:

$$D(\varphi) = \begin{cases} E(\varphi)[0] & \text{if } (w,0) \models \varphi \\ F(\varphi)[0] & \text{otherwise} \end{cases}$$

Dual **explanation** and **falsification** operators:

$$E(p)[t] = p[t] \qquad F(p)[t] = \dots$$

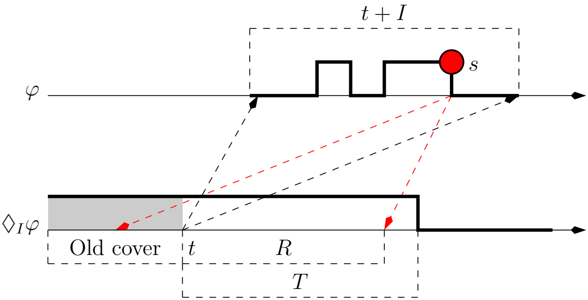
$$E(\neg\varphi)[t] = F(\varphi)[t] \qquad F(\neg\varphi)[t] = \dots$$

$$E(\varphi \vee \psi)[t] = E(\xi_{\varphi\vee\psi}[t])[t] \qquad F(\varphi \vee \psi)[t] = F(\varphi)[t] \wedge F(\psi)[t]$$

$$E(\Diamond_I \varphi)[t] = E(\varphi)[\xi_{\Diamond_I\varphi}[t]] \qquad F(\Diamond_I \varphi)[t] = \bigwedge_{t' \in t+I} F(\varphi)[t']$$

$$E(\varphi\,\mathcal{U}\,\psi)[t] = E(\psi)[\xi_{\varphi\mathcal{U}\psi}[t]] \wedge \dots \qquad F(\varphi\,\mathcal{U}\,\psi)[t] = E(\varphi\,\mathcal{R}\,\psi)[t]$$

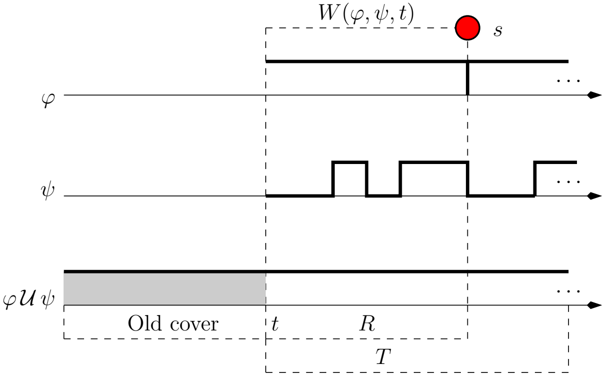
Selection of eventually witnesses



Algorithm

- pick the **latest** witness s of φ in $t + I$ with t start of domain to cover
- witness accounts for $\Diamond_I \varphi$ throughout $s - I$
- remove $s - I$ from the domain to cover

Selection of until witnesses

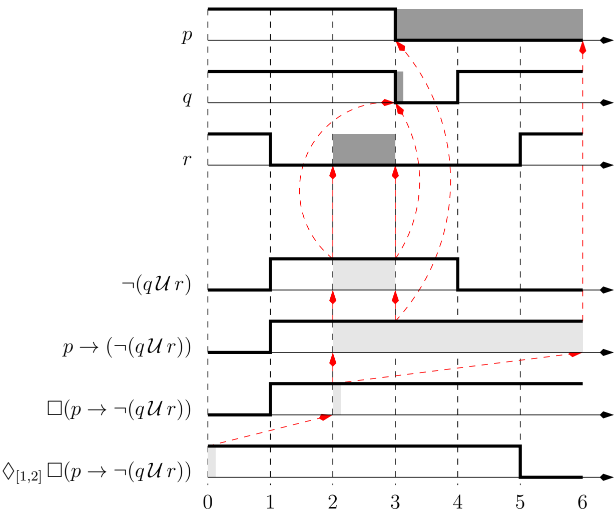


Algorithm

- pick the **latest** witness s of ψ such that φ holds throughout $[t, s)$ with t start of domain to cover
- witness accounts for $\varphi\,\mathcal{U}\,\psi$ throughout $[t, s)$
- remove $[t, s)$ from the domain to cover

Example solution

"Between 1 to 2 time units from now,
always if p holds then q does not hold until r"



Results

Correctness

- term $D(\varphi)$ is solution to the diagnostics of φ and w;
- **small** implicant, not necessarily a **prime** implicant.

Complexity

Proposition

The computation of $D(\varphi)$ takes time in $\mathcal{O}(|\varphi|^2 \cdot |w|)$.

Minimal diagnostics: EXPSPACE-hard in $|\varphi| + |w|$.

Perspectives

- Advantages of **minimal** versus **inductive** diagnostic:
  - minimal diagnostic $\rightsquigarrow$ localize fault "in the execution"
  - inductive diagnostic $\rightsquigarrow$ localize fault "in the specification"

- Same technique applies to analysis of LTL model-checking counter-examples for ultimately-periodic signals

- Theory of implicants: possible extension from trace diagnostics to **system diagnostics**

Thank you.

Normalization of terms

- Inductive procedure yields normal form terms.
- Reductions:
  - elimination of symbolic terms

Example (explanation of disjunction)

$$\bigwedge_{t \in T} E(\xi[t])[t] \Leftrightarrow \bigwedge_{i=1}^{m} \bigwedge_{t \in T_i} E(\varphi)[t] \wedge \bigwedge_{i=1}^{n} \bigwedge_{t \in T'_i} E(\psi)[t]$$

  - elimination of nesting

Example (falsification of eventually)

$$\bigwedge_{t \in T} \bigwedge_{t' \in t+I} F(\varphi)[t'] \Leftrightarrow \bigwedge_{t' \in T+I} F(\varphi)[t']$$

MTL semantics

Definition

For signal $w : (\mathbb{T} \times \mathbb{P}) \to \{0,1\}$ and time $t \in \mathbb{T}$:

$$
\begin{aligned}
(w,t) \models p &\quad\leftrightarrow\quad & w_p[t] = 1 \\
(w,t) \models \neg\varphi &\quad\leftrightarrow\quad & (w,t) \not\models \varphi \\
(w,t) \models \varphi \vee \psi &\quad\leftrightarrow\quad & (w,t) \models \varphi_1 \text{ or } (w,t) \models \varphi_2 \\
(w,t) \models \Diamond_I \varphi &\quad\leftrightarrow\quad & \exists t' \in t \oplus I,\ (w,t') \models \varphi \\
(w,t) \models \varphi\, \mathcal{U}\, \psi &\quad\leftrightarrow\quad & \exists t' > t,\ (w,t') \models \psi \text{ and} \\
& & \forall t'' \in (t,t'),\ (w,t'') \models \varphi
\end{aligned}
$$

Model of a formula

$$w \models \varphi \quad \text{if and only if} \quad (w,0) \models \varphi$$