Trace Diagnostics for MTL Specifications

MT CPS

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

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

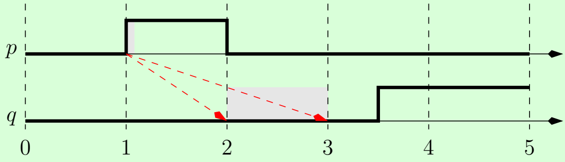
11 April, 2016

Motivation

- Practical question: understand **why** a simulation violates an MTL property.
- Problem: **long** simulation trace with **large** alphabet.
- Solution: isolate **segments** of the trace sufficient to cause violation.

Example

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



Formalization

Problem (Diagnostics)

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

- 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.

- Temporal case: syntactic representation? existence of prime implicants?

Metric Temporal Logic

- Syntax:

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

- Derived operators: $\Box_I \varphi \equiv \neg \Diamond_I \neg \varphi$
- Semantics:

$$\begin{array}{lll}
(w,t) \models p & \leftrightarrow & w_p[t] = 1 \\
(w,t) \models \neg\varphi & \leftrightarrow & \ldots \\
(w,t) \models \varphi \vee \psi & \leftrightarrow & \ldots \\
(w,t) \models \Diamond_I \varphi & \text{iff} & \exists t' \in t \oplus I,\ (w,t') \models \varphi \\
(w,t) \models \varphi \,\mathcal{U}\, \psi & \text{iff} & \exists t' > t,\ (w,t') \models \psi \text{ and } \forall t'' \in (t,t'),\ (w,t'') \models \varphi
\end{array}$$

- Models: $w \models \varphi$ iff $(w,0) \models \varphi$

Partial signals and refinements

Definition

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

Problem reformulation

Definition

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

Semantic view

- Prime implicant of φ $=$ minimal sub-model of φ
- Diagnostic of φ relative to w $=$ sub-model v of φ s.t. $v \sqsubseteq w$

Dense-time issues

- Unbounded variability sub-models

Example

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

- Absence of 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:

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

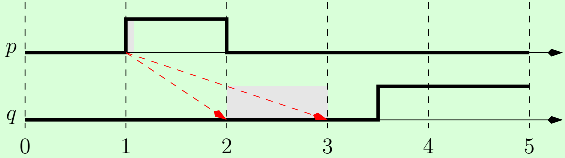
for T subset of time domain, Θ function from time to terms.

- Semantics:

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

Example

Shaded sub-signal corresponds to term $p[1] \wedge \bigwedge_{t \in [2,3]} \neg q[t]$



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.

Sub-signals with finitely many switching points can be represented as normal form terms.

Minimality

- introduce **non-standard reals** t^+, t^- for all times 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.
- The maximum $\theta_* \equiv \bigwedge_{i \geq 0} \theta_i$ has a simple normal form
- Show $\theta_* \Rightarrow \varphi$: take $w \models \theta_*$ and assume $w \not\models \theta_n$ for all n
  - there exists ℓ and (t_i) such that $\theta_i \Rightarrow \ell[t_i]$ and $w_\ell[t_i] = 0$
  - Bolzano-Weierstrass Theorem: 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_*
  - $w_\ell[t_*] = 1$, by finite variability $\exists j, w_\ell[t_j] = 1$. Contradiction!
- Thus $\theta_* \Rightarrow \theta_n$ for some n, and $\theta_n \Rightarrow \varphi$ by hypothesis, so the partial order of implicants has a maximal element

□

MTL extended semantics

Arithmetic on non-standard reals

- $t < t'$ iff $\Re(t) < \Re(t')$ or $t = t' \neq \Re(t) = \Re(t')$
- $t^+ + c = (t+c)^+$ and $t^- + c = (t+c)^-$

Definition (extended semantics)

For t non-standard real:

- $(w,t) \models \Diamond_I \varphi$ iff $\exists t' \in t \oplus I$, $(w,t') \models \varphi$
- $(w,t) \models \varphi \mathcal{U} \psi$ iff $\exists t' > t$, $(w,t') \models \psi$ and $\forall t < t'' < t'$, $(w,t'') \models \varphi$

Lemma

For t non-standard real: $(w,t) \models \varphi$ *iff* $\lim_{s \to t} w_\varphi[t] = 1$

Selection functions

- Used to select a **witnesses** of a formula.
- A function ξ labeled by a formula, such that $\xi_{\varphi \vee \psi}[t] \in \{\varphi, \psi\}$, $\xi_{\Diamond_I \psi}[t] \in t \oplus I$, and $\xi_{\varphi \mathcal{U} \psi}[t] > t$.
- 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 $(w, t') \models \varphi$ for all $t' \in (t, \xi[t])$
- 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:

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

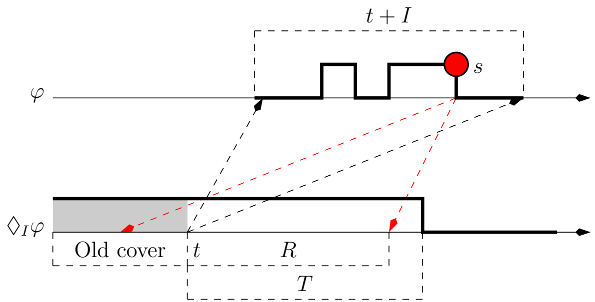
$$E(\neg\varphi)[t] = F(\varphi)[t] \qquad F(\neg\varphi)[t] = \dots$$

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

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

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

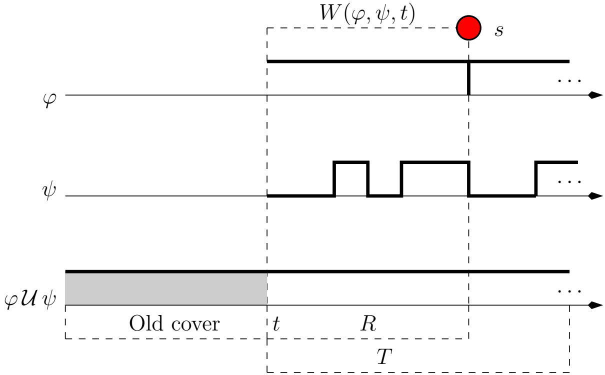
Selection of eventually witnesses



Algorithm

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

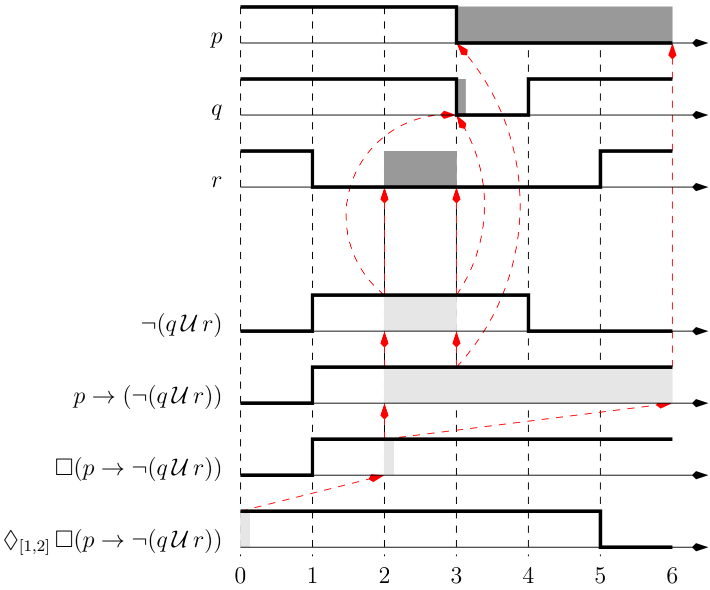
Selection of until witnesses



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



Results

Correctness and Completeness

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

Complexity Issues

Proposition

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

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

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**