Università di Genova | DIPARTIMENTO INFORMATICA, BIOINGEGNERIA, ROBOTICA E INGEGNERIA DEI SISTEMI

**Computer Science Workshop**
*PhD program in Computer Science and Systems Engineering*

# Ain't No Stoppin' Us Monitoring Now

Luca Ciccone[1], Francesco Dagnino[2], Angelo Ferrando[2]

Università di Torino[1], Università di Genova[2]

## Introduction

Not all properties are monitorable. This is a well-known fact which means that there exist properties that cannot be fully verified at runtime. However, given a non-monitorable property, a monitor can still be synthesized, but it could end up in a state where no verdict will ever be concluded on the satisfaction/violation of the property. For this reason, such properties are usually discarded. We carry out an in-depth analysis on monitorability and we show how non-monitorable properties can still be partially monitored.

## Main Contributions

- Monitoring *safety* properties is enough by considering (co)safety approximations
- We present Linear Time $\nu$-Calculus (LT$\nu$) for expressing *safety* properties
- We show how to obtain the approximations by encoding Büchi Automata to LT$\nu$ terms

## A Semantic Approach To Monitorability

- Assume a set $\mathcal{E}$ of *events* and denote by $\mathcal{E}^\star$, $\mathcal{E}^\omega$, $\mathcal{E}^\infty$ the sets of finite $u$, infinite $w$ and possibly infinite $\sigma$ traces over $\mathcal{E}$
- A universe of traces is a non-empty $\mathcal{T} \subseteq \mathcal{E}^\infty$ satisfying $\mathcal{E}^\star\mathcal{T} \subseteq \mathcal{T}$. **Properties** $P, Q$ on $\mathcal{T}$ are subsets of $\mathcal{T}$
- Informally, *safety*/*cosafety* properties (denoted $\mathbb{S}$/co$\mathbb{S}$) are those that are always finitely *refutable*/*satisfiable*

### Monitorability

- A property is **monitorable** when it is possible to synthesize a monitor that can always eventually determine the satisfaction/violation of the property
- (Co)Safety properties are monitorable

- **Abstract Monitor** $\mathcal{M}_P : \mathcal{E}^\star \to \{\text{yes}, \text{no}, ?\}$

$$\mathcal{M}_P(u) = \begin{cases} \text{yes} & u\mathcal{T} \subseteq P \\ \text{no} & u\mathcal{T} \cap P = \emptyset \\ ? & \text{otherwise} \end{cases}$$

- **(Co)Safety Approximations**

$$\Gamma_{\mathbb{S}}(P) = \bigcap\{Q \in \mathbb{S} \mid P \subseteq Q\} \qquad \Delta_{\text{co}\mathbb{S}}(P) = \bigcup\{Q \in \text{co}\mathbb{S} \mid Q \subseteq P\}$$

### Theorems

- Let $P$ be a property on $\mathcal{T}$ and $u \in \mathcal{E}^\star$. Then, $\mathcal{M}_P(u) = \text{no}$ iff $\mathcal{M}_{\Gamma_{\mathbb{S}}(P)}(u) = \text{no}$
- Let $P$ be a property on $\mathcal{T}$ and $u \in \mathcal{E}^\star$. Then, $\mathcal{M}_P(u) = \text{yes}$ iff $\mathcal{M}_{\Delta_{\text{co}\mathbb{S}}(P)}(u) = \text{yes}$
- If $P$ is a cosafety property then $\mathcal{T} \setminus P$ is a safety property (*Safety Is Enough*)

- **Generalized Abstract Monitor** $\widehat{\mathcal{M}}_P : \mathcal{E}^\star \to \{\text{yes}, \text{no}, \chi, ?_{\text{yes}}, ?_{\text{no}}, ?\}$

$$\widehat{\mathcal{M}}_P(u) = \begin{cases} \text{yes} & \mathcal{M}_{\Delta_{\text{co}\mathbb{S}}(P)}(u) = \text{yes} \\ \text{no} & \mathcal{M}_{\Gamma_{\mathbb{S}}(P)}(u) = \text{no} \\ \chi & \mathcal{M}_{\Gamma_{\mathbb{S}}(P)}(u) = \text{yes and } \mathcal{M}_{\Delta_{\text{co}\mathbb{S}}(P)}(u) = \text{no} \\ ?_{\text{yes}} & \mathcal{M}_{\Gamma_{\mathbb{S}}(P)}(u) = \text{yes and } \mathcal{M}_{\Delta_{\text{co}\mathbb{S}}(P)}(u) = ? \\ ?_{\text{no}} & \mathcal{M}_{\Gamma_{\mathbb{S}}(P)}(u) = ? \text{ and } \mathcal{M}_{\Delta_{\text{co}\mathbb{S}}(P)}(u) = \text{no} \\ ? & \mathcal{M}_{\Gamma_{\mathbb{S}}(P)}(u) = ? \text{ and } \mathcal{M}_{\Delta_{\text{co}\mathbb{S}}(P)}(u) = ? \end{cases}$$

- $\chi$ means that no verdict at all can be reached

## Linear Time $\nu$-Calculus

The Linear Time $\nu$-Calculus is a purely coinductive fragment of the Linear Time $\mu$-Calculus which is obtained by enriching Linear Temporal Logic with fixed points. Let $AP$ be a set of *atomic propositions* $p$ and $\langle\!\langle - \rangle\!\rangle : AP \to \wp(\mathcal{E})$ an interpretation function.

- The terms of LT$\nu$ are inductively generated by the grammar

$$\mathsf{t}, \mathsf{s} ::= \top \mid \bot \mid p \mid p^\perp \mid \mathsf{t} \wedge \mathsf{s} \mid \mathsf{t} \vee \mathsf{s} \mid \circ\mathsf{t} \mid X \mid \nu X.\mathsf{t}$$

### Linear Time $\nu$-Calculus Semantics

- $w \models_C$ t: $w$ *satisfies* t, **coinductively** defined. We denote $[\![\, \mathsf{t} \,]\!]_C = \{w \in \mathcal{E}^\omega \mid w \models_C \mathsf{t}\}$
- t $\xrightarrow{e}$ s: t *reduces to* s *with* $e$, **inductively** defined. We write t $\overset{u}{\Rightarrow}_*$ s and t $\overset{w}{\Rightarrow}_\omega$ for finite and infinite reductions respectively.

### Theorems

- For all t there exists s *contractive* (*i.e.* vars guarded by $\circ$) such that $[\![\, \mathsf{t} \,]\!]_C = [\![\, \mathsf{s} \,]\!]_C$
- Let t be a LT$\nu$ term. Then $[\![\, \mathsf{t} \,]\!]_C$ is a **safety** property
- Let $w \in \mathcal{E}^\omega$ and t a LT$\nu$ term. Then $w \models_C$ t if and only if t $\overset{w}{\Rightarrow}_\omega$

- **Proof System** (We use $\Gamma, \Delta$ to range over sets of LT$\nu$ terms)

$$\frac{}{\vdash p_1, \dots, p_n, p_{n+1}^\perp, \dots, p_m^\perp, \Gamma}\ \bigcup_{i=1}^{n}\langle\!\langle p_i \rangle\!\rangle \cup \bigcup_{i=n+1}^{m}(\mathcal{E}^\omega \setminus \langle\!\langle p_i \rangle\!\rangle) = \mathcal{E}^\omega \qquad \frac{}{\vdash \top, \Gamma} \qquad \frac{\vdash \mathsf{t}, \Gamma \quad \vdash \mathsf{s}, \Gamma}{\vdash \mathsf{t} \wedge \mathsf{s}, \Gamma}$$

$$\frac{\vdash \mathsf{t}, \mathsf{s}, \Gamma}{\vdash \mathsf{t} \vee \mathsf{s}, \Gamma} \qquad \frac{\vdash \mathsf{t}\{\nu X.\mathsf{t}/X\}, \Gamma}{\vdash \nu X.\mathsf{t}, \Gamma} \qquad \frac{\vdash \Gamma}{\vdash \circ\Gamma, \Delta}$$

### Theorem

- Let t be a LT$\nu$ term. Then $[\![\, \mathsf{t} \,]\!]_C = \mathcal{E}^\omega$ if and only if $\vdash$ t

Given a LT$\nu$ term t we can build a monitor $M[\![\, \mathsf{t} \,]\!]_C : \mathcal{E}^\star \to \{\text{yes}, \text{no}, ?\}$ such that

$$M_{\mathsf{t}}(u) = \begin{cases} \text{yes} & \mathsf{t} \overset{u}{\Rightarrow}_* \mathsf{s} \text{ and } \vdash \mathsf{s} \\ \text{no} & \mathsf{t} \overset{u}{\Rightarrow}_* \mathsf{s} \not\to \text{ or } \mathsf{t} \overset{u}{\not\Rightarrow} \\ ? & otherwise \end{cases}$$

In order to monitor any property $P$ we have to write $\mathsf{t}_{\mathbb{S}}, \mathsf{t}_{\text{co}\mathbb{S}}$ that are the *safety approximation* and the complement of the *cosafety approximation* of $P$ respectively.

### Example

1. *Property* (written in the usual LTL syntax) $\phi = (a \wedge \Diamond b) \vee (c \wedge \Box \Diamond d)$
2. *(Co)Safety Completions* $\Gamma_{\mathbb{S}}(\phi) = a \vee c, \Delta_{\text{co}\mathbb{S}}(\phi) = a \wedge \Diamond b$
3. *LT$\nu$ Terms* $\mathsf{t}_{\mathbb{S}} = a \vee c, \mathsf{t}_{\text{co}\mathbb{S}} = a^\perp \vee (\nu X.b^\perp \wedge \circ X)$

## Encoding From Büchi Automata

Let $\mathcal{A} =< \mathcal{Q}, \Sigma, \delta, \mathcal{Q}_0, \mathcal{F} >$ be a Büchi automaton such that $\Sigma = \wp_F^*(AP)$ (we denote $\alpha$ an element of $\Sigma$). We make the following assumptions:

### Assumptions

- For each $q \in \mathcal{F}$, $q$ lies in a cycle
- For all $q \in \mathcal{Q}$, $q$ can always eventually reach a final state

```
Assume a variable X_q for each q ∈ Q

procedure T(q, S)
    if q ∈ S then X_q
    else
        νX_q. ∨ {T(α)∧∘T(q′, S ∪ {q})| α ∈ Σ, q′ ∈ δ(q, α)}

T(α) = ∧{p | p ∈ α} ∧ {p^⊥ | p ∉ α}
T(A) = ∨{T(q, ∅)| q ∈ Q_0}
```

### Theorem

- Let $\mathcal{A}$ be a Büchi automaton. Then $\Gamma_{\mathbb{S}}(\mathcal{L}(\mathcal{A})) = [\![\, T(\mathcal{A}) \,]\!]_C$

- The algorithm can be applied to those automata obtained from properties written in some formalism, *e.g.* Linear Temporal Logic

## Acknowledgements

I am grateful to my colleagues and friends Francesco Dagnino and Angelo Ferrando for having worked on a topic which is not strictly correlated to our research. This work is the result of meetings in which we tried to merge our experience in different research areas.

**SUPPLEMENTARY MATERIAL**

**CONTACTS**

**Luca Ciccone**
luca.ciccone@unito.it

**Angelo Ferrando**
angelo.ferrando@unige.it

**Francesco Dagnino**
francesco.dagnino@dibris.unige.it

CSW