# THE SAFETY FRAGMENT OF LTL


**Alessandro Cimatti**
Fondazione Bruno Kessler, Italy

**Luca Geatti**
Free University of Bozen-Bolzano, Italy

**Nicola Gigante**
Free University of Bozen-Bolzano, Italy

**Angelo Montanari**
University of Udine, Italy

**Stefano Tonetta**
Fondazione Bruno Kessler, Italy



VardiFest 22
August 1, 2022
Haifa, Israel

# INTRODUCTION

Moshe Vardi's research has deeply investigated **Linear Temporal Logic** (LTL) and its **safety fragment**.

Some papers on these topics:

- *Model checking of safety properties*
  with O. Kupferman
- *SAT-based induction for temporal safety properties*,
  with R. Armoni, L. Fix, R .Fraer, S. Huddleston, N. Piterman
- *Falsification of LTL safety properties in hybrid systems*,
  with E. Plaku, L. E. Kavraki
- *A Symbolic Approach to Safety-LTL Synthesis*,
  with S. Zhu, L. M. Tabajara, J. Li, G. Pu
- ... and many other papers ...

# INTRODUCTION

Moshe Vardi's research has deeply investigated **Linear Temporal Logic** (LTL) and its **safety fragment**.

Some papers on these topics:

- *Model checking of safety properties*, 1999 $\leftarrow$ *I was given my first computer as a kid*
  with O. Kupferman
- *SAT-based induction for temporal safety properties*,
  with R. Armoni, L. Fix, R .Fraer, S. Huddleston, N. Piterman
- *Falsification of LTL safety properties in hybrid systems*,
  with E. Plaku, L. E. Kavraki
- *A Symbolic Approach to Safety-LTL Synthesis*,
  with S. Zhu, L. M. Tabajara, J. Li, G. Pu
- ... and many other papers ...

# SAFETY AND CO-SAFETY LANGUAGES

In formal verification, **safety languages** are an important class of formal languages that codify the very common class of properties, *i.e.*, those of the kind:

*Something* **bad** *never happens.*
*Any violation is* **irremediable**.

**Importance of safety languages**

The identification of a property as safety can considerably help verification algorithms, while being able to capture a variety of real-world requirements.

# SAFETY AND CO-SAFETY LANGUAGES

Let $\Sigma$ be an alphabet.

**Definition (Safety language)**

Let $\mathcal{L} \subseteq \Sigma^\omega$. We say that $\mathcal{L}$ is a **safety language** if and only if for all the words $\sigma \in \Sigma^\omega$ it holds that, if $\sigma \notin \mathcal{L}$, then there exists an $i \in \mathbb{N}$ such that, for all $\sigma' \in \Sigma^\omega$, $\sigma_{[0,i]} \cdot \sigma' \notin \mathcal{L}$.

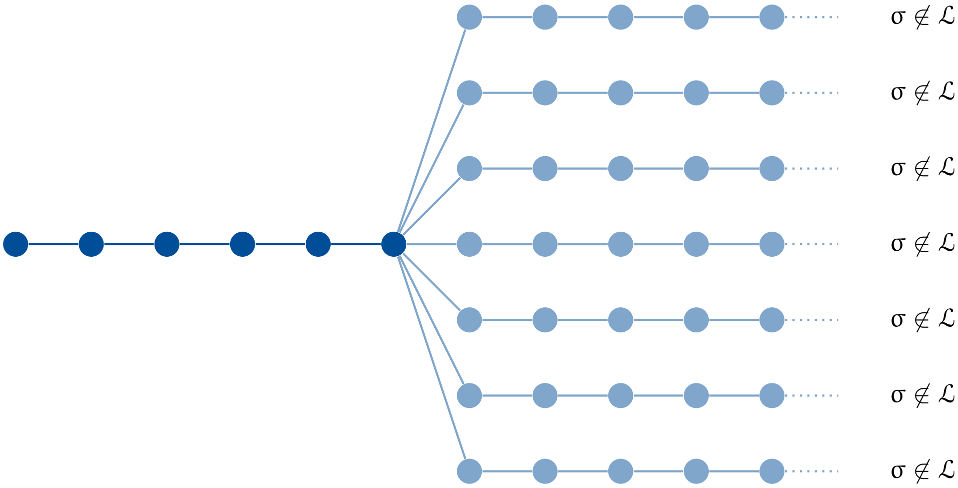
# SAFETY AND CO-SAFETY LANGUAGES

$\sigma \notin \mathcal{L}$

# SAFETY AND CO-SAFETY LANGUAGES

$\sigma \notin \mathcal{L}$

# SAFETY AND CO-SAFETY LANGUAGES



# SAFETY AND CO-SAFETY LANGUAGES

By duality, **coSafety languages** express the property that:

*Something* **good** *will eventually happen.*

Let $\Sigma$ be an alphabet.

**Definition (Co-safety language)**

Let $\mathcal{L} \subseteq \Sigma^\omega$. We say that $\mathcal{L}$ is a **co-safety language** if and only if for all the words $\sigma \in \Sigma^\omega$ it holds that, if $\sigma \in \mathcal{L}$, then there exists an $i \in \mathbb{N}$ such that, for all $\sigma' \in \Sigma^\omega$, $\sigma_{[0,i]} \cdot \sigma' \in \mathcal{L}$.

# LINEAR TEMPORAL LOGIC

Linear Temporal Logic (**LTL**) is a very common specification language in formal verification, artificial intelligence and other fields.

$$
\begin{aligned}
\phi \coloneqq p \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi \qquad & \text{Boolean connectives} \\
\mid \mathsf{X}\phi \mid \widetilde{\mathsf{X}}\phi \mid \phi \,\mathsf{U}\, \phi \mid \phi \,\mathsf{R}\, \phi \qquad & \text{Future temporal operators}
\end{aligned}
$$

# FINITE- AND INFINITE-TRACES

LTL is usually interpreted over **infinite** traces.

Recently, the community payed attention to the **finite** trace semantics.

# KAMP'S THEOREM

$$
\begin{tikzcd}
{[\![\mathsf{LTL}]\!]^{<\omega}} \arrow[r, leftrightarrow] \arrow[d, leftrightarrow] \arrow[dr, phantom, "\textbf{finite words}"] & {[\![\mathsf{S1S\text{-}FO}]\!]^{<\omega}} \arrow[d, leftrightarrow] \\
\text{star-free R.E.} \arrow[r, leftrightarrow] & \text{counter-free NFAs}
\end{tikzcd}
$$

$$[\![\mathbb{L}]\!]^{<\omega} = \{\mathcal{L}^{<\omega}(\phi) \mid \phi \in \mathbb{L}\}$$

# KAMP'S THEOREM

$$
\begin{tikzcd}
\llbracket \mathsf{LTL} \rrbracket \arrow[r, leftrightarrow] \arrow[d, leftrightarrow] & \llbracket \mathsf{S1S\text{-}FO} \rrbracket \arrow[d, leftrightarrow] \\
\text{star-free omega-R.E.} \arrow[r, leftrightarrow] & \text{counter-free NBAs}
\end{tikzcd}
$$

**infinite words**

$$\llbracket \mathbb{L} \rrbracket = \{\mathcal{L}(\phi) \mid \phi \in \mathbb{L}\}$$

Four characterizations of the **safety fragment of** LTL:

$$\begin{tikzcd}[column sep=large, row sep=huge]
\text{Temporal Modal Logics} \arrow[r, leftrightarrow] \arrow[d, leftrightarrow] \arrow[dr, phantom, "\textbf{infinite words}"] & \text{First-order Logics} \arrow[d, leftrightarrow] \\
\text{Formal Languages Theory} \arrow[r, leftrightarrow] & \text{Automata Theory}
\end{tikzcd}$$

# SAFETY - TEMPORAL MODAL LOGICS

Four characterizations of the **safety fragment of** LTL:

$$
\begin{tikzcd}
\text{Temporal Modal Logics} \arrow[r, leftrightarrow] \arrow[d, leftrightarrow] & \text{First-order Logics} \arrow[d, leftrightarrow] \\
\text{Formal Languages Theory} \arrow[r, leftrightarrow] & \text{Automata Theory}
\end{tikzcd}
$$

**infinite words**

# SAFETY - TEMPORAL MODAL LOGICS

Three main **equivalent** characterizations in terms of temporal modal logic:

- Safety-LTL: (Chang, Manna, Pnueli - 1995)

$$\phi \coloneqq p \mid \neg p \mid \phi \wedge \phi \mid \phi \vee \phi \mid X\phi \mid \phi \, R \, \phi \mid G\phi$$

# SAFETY - TEMPORAL MODAL LOGICS

Three main **equivalent** characterizations in terms of temporal modal logic:

- Safety-LTL: (Chang, Manna, Pnueli - 1995)

$$\phi \coloneqq p \mid \neg p \mid \phi \wedge \phi \mid \phi \vee \phi \mid X\phi \mid \phi \mathrel{R} \phi \mid G\phi$$

- $G(\alpha)$ such that $\alpha$ belongs to pure-past LTL+P
  (Lichtenstein, Pnueli, Zuck - 1985)

Three main **equivalent** characterizations in terms of temporal modal logic:

- Safety-LTL: (Chang, Manna, Pnueli - 1995)

$$\phi \coloneqq p \mid \neg p \mid \phi \wedge \phi \mid \phi \vee \phi \mid X\phi \mid \phi \, R \, \phi \mid G\phi$$

- $G(\alpha)$ such that $\alpha$ belongs to pure-past LTL+P
  (Lichtenstein, Pnueli, Zuck - 1985)

- $\neg\phi$ such that $\mathcal{L}(\phi) \in [\![\text{coSafety-LTL}(-\widetilde{X})]\!]^{<\omega} \cdot (2^{\Sigma})^{\omega}$
  (Cimatti, Geatti, Gigante, Montanari, Tonetta - 2022)

# SAFETY - FIRST-ORDER LOGIC

$$\begin{tikzcd}
\text{Temporal Modal Logics} \arrow[r, leftrightarrow] \arrow[d, leftrightarrow] \arrow[dr, phantom, "\textbf{infinite words}"] & \text{First-order Logics} \arrow[d, leftrightarrow] \\
\text{Formal Languages Theory} \arrow[r, leftrightarrow] & \text{Automata Theory}
\end{tikzcd}$$

# SAFETY - FIRST-ORDER LOGIC

Two main **equivalent** characterizations in terms of first-order logic:

- **Bounded-FO**: (Thomas - 1988)
  - a formula $\phi(x)$ with one free variable $x$ is *bounded* iff all quantifiers in $\phi(x)$ are of the form $\exists y(y \leqslant x \wedge \ldots)$ or $\forall y(y \leqslant x \rightarrow \ldots)$.
  - Bounded-FO is defined as the set of formulas of type $\forall x \,.\, \phi(x)$ where $\phi(x)$ is bounded.

# SAFETY - FIRST-ORDER LOGIC

Two main **equivalent** characterizations in terms of first-order logic:

- **Bounded-FO**: (Thomas - 1988)
  - a formula $\phi(x)$ with one free variable $x$ is *bounded* iff all quantifiers in $\phi(x)$ are of the form $\exists y(y \leqslant x \wedge \ldots)$ or $\forall y(y \leqslant x \rightarrow \ldots)$.
  - Bounded-FO is defined as the set of formulas of type $\forall x \,.\, \phi(x)$ where $\phi(x)$ is bounded.
- **Safety-FO**: (Cimatti, Geatti, Gigante, Montanari, Tonetta - 2022)

$$atomic := x < y \mid x = y \mid x \neq y \mid P(x) \mid \neg P(x)$$
$$\phi := atomic \mid \phi_1 \vee \phi_2 \mid \phi_1 \wedge \phi_2 \mid \exists y(x < y < z \wedge \phi_1) \mid \forall y(x < y \Rightarrow \phi_1)$$

where $x$, $y$, and $z$ are first-order variables, $P$ is a unary predicate, and $\phi_1$ and $\phi_2$ are Safety-FO formulas.

# SAFETY - AUTOMATA THEORY

$$
\begin{tikzcd}
\text{Temporal Modal Logics} \arrow[r, leftrightarrow] \arrow[d, leftrightarrow] & \text{First-order Logics} \arrow[d, leftrightarrow] \\
\text{Formal Languages Theory} \arrow[r, leftrightarrow] & \text{Automata Theory}
\end{tikzcd}
$$

**infinite words**

# SAFETY - AUTOMATA THEORY

- Safety Automata: (Manna, Pnueli - 1990)
  - They are deterministic counter-free Streett automata whose set of states $Q$ is partitioned into the set of *good* ($G$) and *bad* ($B$) states.
  - There is *no* transition from a bad state ($q \in B$) to a good state ($q' \in G$).

Safety Automata = counter-free + no transition from B to G

- Occurrence co-Büchi Counter-free Automata: (Cerna, Pelanek - 2003)
  - a run is accepting iff it never visits a final state of the automaton.

- (complement of a) Terminal Büchi Counter-free Automata: (Cerna, Pelanek - 2003 , only one inclusion of the equivalence)
  - any final state of the automaton has at least a successor, and all its successors are final states as well.

## SAFETY - FORMAL LANGUAGES THEORY

$$
\begin{tikzcd}
\text{Temporal Modal Logics} \arrow[r, leftrightarrow] \arrow[d, leftrightarrow] & \text{First-order Logics} \arrow[d, leftrightarrow] \\
\text{Formal Languages Theory} \arrow[r, leftrightarrow] & \text{Automata Theory}
\end{tikzcd}
$$

**infinite words**

- $\omega$-regular expressions of this type: (Thomas - 1988)

$$L \text{ is an LTL-definable safety language}$$
$$\Leftrightarrow$$
$$\overline{L} = S \cdot \Sigma^{\omega}$$

where $S$ is a **star-free** regular expression.

# CONCLUSIONS

**Safety languages** are an interesting and useful topic:

- many different characterizations
- many interesting properties
- just touched the surface here

# THANK YOU