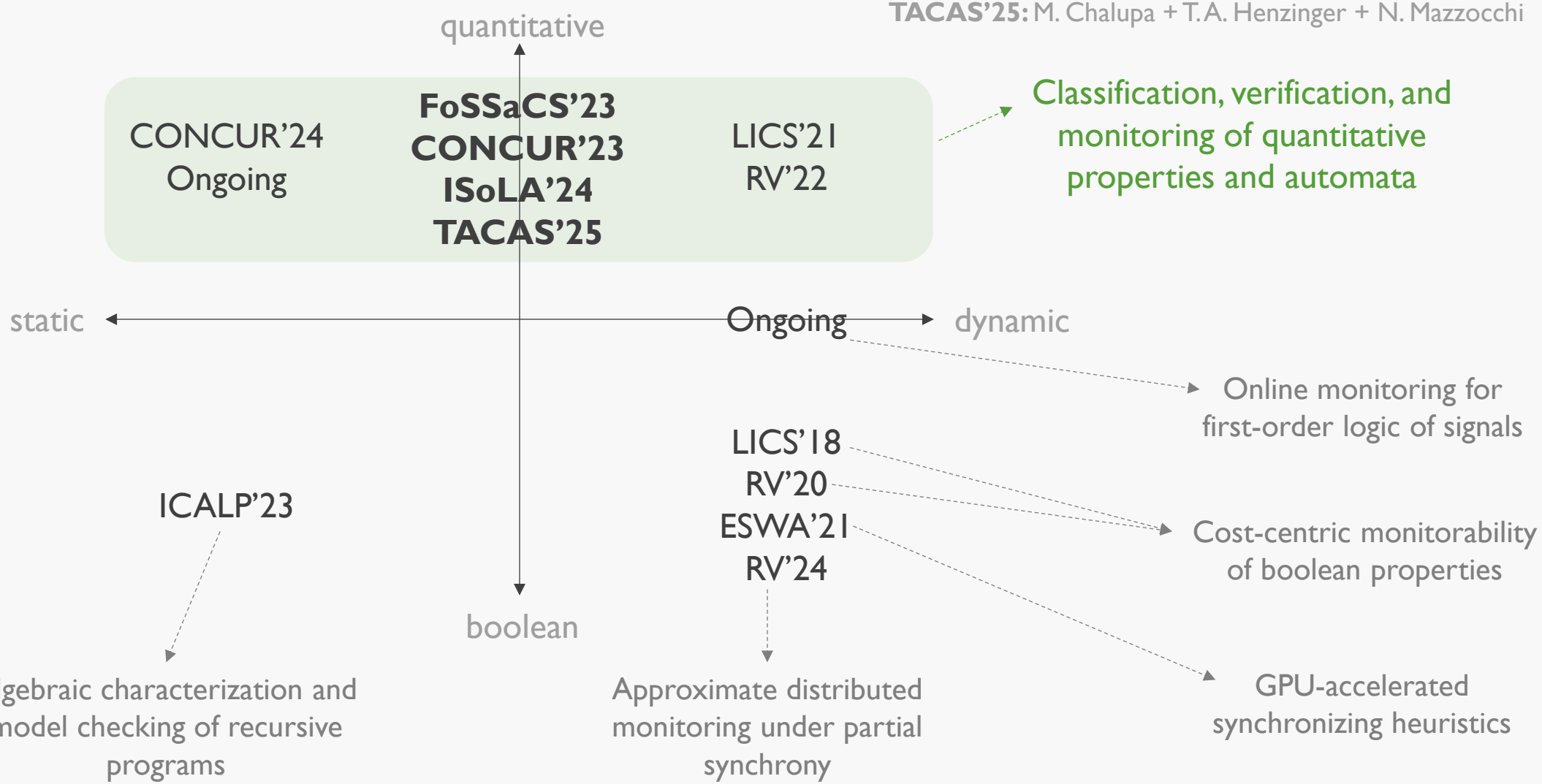
Safety and Liveness of Quantitative Properties and Automata

N. Ege Saraç

Institute of Science and Technology Austria

My Research

Joint work with
FoSSaCS'23: T.A. Henzinger + N. Mazzocchi
CONCUR'23: U. Boker + T.A. Henzinger + N. Mazzocchi
ISoLA'24: M. Chalupa + T.A. Henzinger + N. Mazzocchi
TACAS'25: M. Chalupa + T.A. Henzinger + N. Mazzocchi



Motivation

Quantitative properties.

- Map traces to *richer value domains* (e.g., real numbers)
- Reasoning about *robustness* and *performance* (e.g., response time)
- *Approximate* and *dynamic* methods (e.g., runtime monitoring)

Safety and liveness.

- Specification: *all we need*
- Verification: *easy for safety*, difficult for liveness

Contribution and Overview

1. Quantitative generalizations of *safety and liveness*

2. *Decision procedures and constructions* for safety and liveness of quantitative automata

3. *First tool* to automate the analysis of quantitative automata

Quantitative Properties

Quantitative property.

$\Phi : \Sigma^{\omega} \to D$ where Σ is a finite alphabet of observations

D is a value domain (complete lattice)

Boolean Safety

Example (no double request).

- $\Sigma = \{r, g, t, o\}$
- $P =$ no r is followed by another r without some g in between

$$w = t\ r\ t\ o\ t\ t\ o\ g\ t\ o\ o\ r\ t\ t\ o\ r\ t\ t\ o\ g\ t\ t\ \ldots$$

A boolean property $P : \Sigma^\omega \to \{0,1\}$ is *safe* iff

$$\forall w \in \Sigma^\omega : P(w) \not\geq 1 \;\Rightarrow\; \exists\, u \prec w : \forall w' \in \Sigma^\omega : P(uw') \not\geq 1$$

For every word, wrong membership hypotheses have a finite witness.

Lamport, "Proving the correctness of multiprocess programs", 1977.
Alpern and Schneider, "Defining liveness", 1985.

Boolean Safety

Example (no double request).

- $\Sigma = \{r, g, t, o\}$
- $P =$ no r is followed by another r without some g in between

$$w = t\ r\ t\ o\ t\ t\ o\ g\ t\ o\ o\ r\ t\ t\ o\ r\ t\ t\ o\ g\ t\ t \ldots$$

$$M_P : 1 \ldots\ldots\ldots\ldots\ldots\ldots\ldots 0 \ldots\ldots\ldots\ldots$$

A boolean property $P : \Sigma^\omega \to \{0,1\}$ is *safe* iff

$$\forall w \in \Sigma^\omega : P(w) \not\geq 1 \;\Rightarrow\; \exists\, u \prec w : \forall w' \in \Sigma^\omega : P(uw') \not\geq 1$$

For every word, wrong membership hypotheses have a finite witness.

Lamport, "Proving the correctness of multiprocess programs", 1977.
Alpern and Schneider, "Defining liveness", 1985.

Quantitative Safety

Example (minimal response time).

- $\Sigma = \{r, g, t, o\}$
- $\Phi(w) =$ greatest lower bound on the occurrences of t between each r and the matching g in w

$$w = t\ r\ t\ o\ t\ t\ o\ g\ t\ o\ o\ r\ t\ t\ o\ r\ t\ t\ o\ g\ t\ t\ \ldots$$

$$M_{\Phi \geq 3} : T \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots F \ldots\ldots$$

A quantitative property $\Phi : \Sigma^\omega \to D$ is *safe* iff

$$\forall w \in \Sigma^\omega : \forall v \in D : \Phi(w) \not\geq v \Rightarrow \exists\, u \prec w : \sup_{w' \in \Sigma^\omega} \Phi(uw') \not\geq v$$

For every word, **every** wrong membership hypothesis has a finite witness.

Quantitative Safety Closure

Example (minimal response time).

- $\Sigma = \{r, g, t, o\}$
- $\Phi(w) =$ greatest lower bound on the occurrences of t between each r and the matching g in w

$$w = t\ r\ t\ o\ t\ t\ o\ g\ t\ o\ o\ r\ t\ t\ o\ r\ t\ t\ o\ g\ t\ t \ldots$$

$$\sup : \infty \ldots\ldots\ldots 3 \ldots\ldots\ldots\ldots\ldots\ldots 2 \ldots\ldots$$

$$\Phi^*(w) = \inf_{u \prec w} \sup_{w' \in \Sigma^\omega} \Phi(uw')$$

Make Φ safe by increasing each word's value as little as possible.

Quantitative Safety & Safety Closure

Theorem.

- Φ^* is the least safety property that bounds Φ from above.
- Φ is safe iff $\Phi = \Phi^*$
- Φ is safe iff Φ is upper semicontinuous (when D is a total order)

$$\Phi^*(w) = \inf_{u \prec w} \sup_{w' \in \Sigma^\omega} \Phi(uw')$$

Make Φ safe by increasing each word's value as little as possible.

Quantitative Co-safety

Example (maximal response time).

- $\Sigma = \{r, g, t, o\}$
- $\Phi(w) =$ least upper bound on the occurrences of t between each r and the matching g in w

$$w = t\ r\ t\ o\ t\ t\ o\ g\ t\ o\ o\ r\ t\ t\ o\ r\ t\ t\ o\ g\ t\ t \ldots$$

$$M_{\Phi \leq 3} : T \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots F \ldots\ldots\ldots$$

$$\inf : 0 \ldots 1 \ldots 2\,3 \ldots\ldots\ldots\ldots\ldots\ldots\ldots 4 \ldots\ldots\ldots$$

A quantitative property $\Phi : \Sigma^\omega \to D$ is *co-safe* iff

$$\forall w \in \Sigma^\omega : \forall v \in D : \Phi(w) \not\leq v \Rightarrow \exists\, u \prec w : \inf_{w' \in \Sigma^\omega} \Phi(uw') \not\leq v$$

Boolean Liveness

Example (response).

- $\Sigma = \{r, g, t, o\}$
- P = every r is eventually followed by some g

$$w = t\ r\ t\ o\ t\ t\ o\ g\ t\ o\ o\ r\ t\ t\ o\ r\ t\ t\ o\ g\ t\ t \ldots$$

$$M_P : T \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

A boolean property $P: \Sigma^\omega \to \{0,1\}$ is *live* iff

$$\forall w \in \Sigma^\omega : P(w) \not\geq 1 \Rightarrow\ \forall u \prec w : \exists w' \in \Sigma^\omega : P(uw') \geq 1$$

For every word, wrong membership hypotheses have no finite witness.

Lamport, "Proving the correctness of multiprocess programs", 1977.
Alpern and Schneider, "Defining liveness", 1985.

Quantitative Liveness

Example (average response time).

- $\Sigma = \{r, g, t, o\}$
- $\Phi(w)$ = lower limit of the running avg. of the occurrences of t between each r and the matching g in w

$$w = t\ r\ t\ o\ t\ t\ o\ g\ t\ o\ o\ r\ t\ t\ o\ r\ t\ t\ o\ g\ t\ t\ \ldots$$

$$M_{\Phi \geq 3} : T \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

A quantitative property $\Phi : \Sigma^\omega \to D$ is *live* iff

$$\forall w \in \Sigma^\omega : \Phi(w) < \top \Rightarrow \exists v \in D : \Phi(w) \not\geq v \ \wedge\ \forall\, u \prec w : \sup_{w' \in \Sigma^\omega} \Phi(uw') \geq v$$

For every word (with value $< \top$), **some** wrong membership hypothesis has no finite witness.

Quantitative Liveness

Theorem.
Φ is live
iff
$\Phi(w) < \Phi^*(w)$ whenever $\Phi(w) < \top$

Example (average response time).

- $\Sigma = \{r, g, t, o\}$
- $\Phi(w)$ = lower limit of the running avg. of the occurrences of t between each r and the matching g in w

$$w = t\ r\ t\ o\ t\ t\ o\ g\ t\ o\ o\ r\ t\ t\ o\ r\ t\ t\ o\ g\ t\ t\ \ldots$$

$$M_{\Phi \geq 3} : T \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

A quantitative property $\Phi : \Sigma^\omega \to D$ is *live* iff

$$\forall w \in \Sigma^\omega : \Phi(w) < \top \Rightarrow \exists v \in D : \Phi(w) \not\geq v \ \wedge\ \forall\, u \prec w : \sup_{w' \in \Sigma^\omega} \Phi(uw') \geq v$$

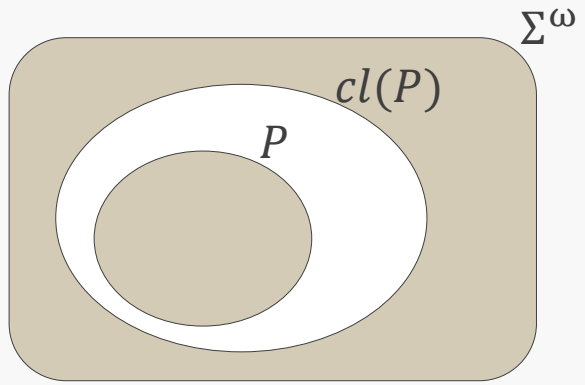
For every word (with value $< \top$), **some** wrong membership hypothesis has no finite witness.

Safety-Liveness Decomposition

In the boolean setting.

- $P = \underbrace{cl(P)}_{\text{safe}} \cap \underbrace{\left(P \cup \left(\Sigma^\omega \setminus cl(P)\right)\right)}_{\text{live}}$

Alpern and Schneider, "Defining liveness", 1985.



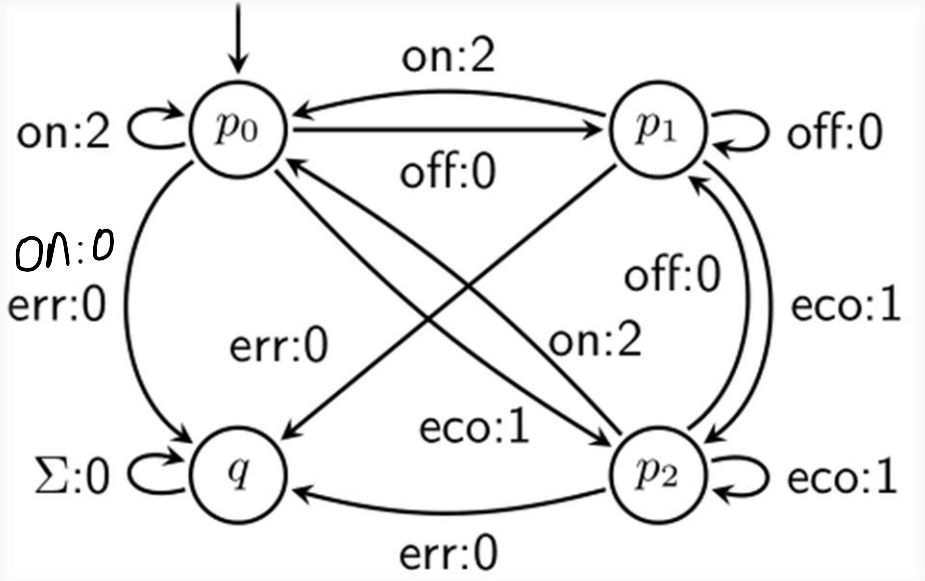
In the quantitative setting.

Theorem.

$$\Phi = \min(\underbrace{\Phi^*}_{\text{safe}}, \underbrace{\Psi}_{\text{live}})$$

$$\Psi(w) = \begin{cases} \Phi(w) & \text{if } \Phi(w) < \Phi^*(w) \\ \top & \text{if } \Phi(w) = \Phi^*(w) \end{cases}$$

Quantitative Automata



$A(w) = \sup\{v \mid v \text{ is the value of a run of } A \text{ on } w\}$

$w = \text{on} \,.\, \text{off} \,.\, (\text{eco} \,.\, \text{off})^{\omega}$

$s_w = 2 \,.\, 0 \,.\, (1 \,.\, 0)^{\omega}$

- $\text{Sup}(s_w) = 2$
- $\text{LimSup}(s_w) = 1$
- $\text{LimInfAvg}(s_w) = \text{LimSupAvg}(s_w) = \frac{1}{2}$
- $\text{DSum}_2(s_w) = 2^0 \cdot 2 + 2^{-1} \cdot 0 + \cdots = \frac{7}{3}$

- Acceptance condition → Value function
- Val ∈ {Inf, Sup, LimInf, LimSup, LimInfAvg, LimSupAvg, DSum}

Safety Reachability Co-Büchi Büchi Games with quantitative objectives

Chatterjee, Doyen, and Henzinger, "Quantitative languages", 2008.

What's Decidable About These Automata?

	Inf	Sup	LimInf	LimSup	LimInfAvg	LimSupAvg	DSum
Emptiness (w.r.t v) $\exists w: A(w) \geq v$	PTime						
Universality (w.r.t v) $\forall w: A(w) \geq v$	PSpace-complete				Undecidable		Open
Inclusion $\forall w: A(w) \leq B(w)$	PSpace-complete				Undecidable		Open
Equivalence $\forall w: A(w) = B(w)$	PSpace-complete				Undecidable		Open

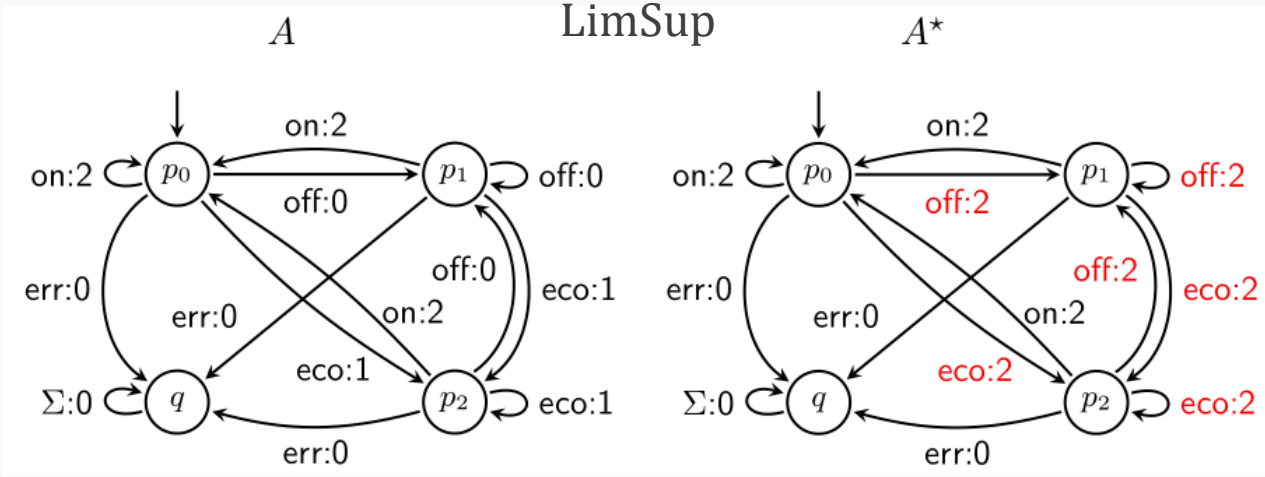
Kupferman and Lustig, "Lattice automata", 2007.
Chatterjee, Doyen, and Henzinger, "Quantitative languages", 2008.
Degorre, Doyen, Gentilini, Raskin, and Torunczyk, "Energy and mean-payoff games with imperfect information", 2010.
Chatterjee, Doyen, Edelsbrunner, Henzinger, and Rannou, "Mean-payoff automaton expressions", 2010.
Hunter, Pérez, and Raskin, "Mean-payoff games with partial observation", 2014.

Safety Closure of Quantitative Automata

- For each state q of A
  - Compute $\top_q$ = largest value A can achieve starting from q
  - Replace the weights of all incoming transitions of q with $\top_q$

- A is not safe

$$A(\text{eco}^\omega) = 1$$
$$A^*(\text{eco}^\omega) = 2$$



Safety of Quantitative Automata

	Inf	**Sup**	**LimInf**	**LimSup**	**LimInfAvg**	**LimSupAvg**	**DSum**
Equivalence $\forall w: A(w) = B(w)$	PSpace-complete				Undecidable		Open
Deciding safety	PSpace				???		???

A is safe $\Leftrightarrow A = A^*$

Safety of Quantitative Automata

	Inf	Sup	LimInf	LimSup	LimInfAvg	LimSupAvg	DSum
Equivalence $\forall w: A(w) = B(w)$	PSpace-complete				Undecidable		Open
Deciding safety	$O(1)$	PSpace-complete			???		$O(1)$

Theorem.

- Every DSum and Inf automaton is safe.

Liveness of Quantitative Automata

Recall.

Φ is live
iff
$\Phi(w) < \Phi^*(w)$ whenever $\Phi(w) < \top$

Theorem.
A is live $\Leftrightarrow A^* \geq \top$

Liveness of Quantitative Automata

	Inf	Sup	LimInf	LimSup	LimInfAvg	LimSupAvg	DSum
Universality (w.r.t v) $\forall w: A(w) \geq v$	PSpace-complete				Undecidable		Open
Deciding safety	$O(1)$	PSpace-complete			???		$O(1)$
Deciding liveness	PSpace-complete				???		???

Theorem.

A is live $\Leftrightarrow A^* \geq \top$

Liveness of Quantitative Automata

	Inf	Sup	LimInf	LimSup	LimInfAvg	LimSupAvg	DSum
Universality (w.r.t v) $\forall w: A(w) \geq v$	PSpace-complete				Undecidable		Open
Deciding safety	$O(1)$	PSpace-complete			???		$O(1)$
Deciding liveness	PSpace-complete				???		???

Theorem.

A is live $\Leftrightarrow A^* = \top$

A is safe $\Leftrightarrow A - A^* = 0$

Given A and $k \in \mathbb{Q}$

$\forall w : A(w) < k$	PTime
$\forall w : A(w) = k$	???
$\forall w : A(w) \geq k$	Undecidable / Open (limit-average) (disc. sum)

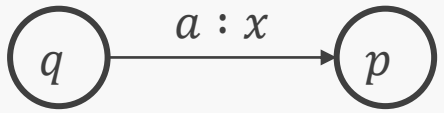
Constant-Function Check

	Inf	Sup	LimInf	LimSup	LimInfAvg	LimSupAvg	DSum
Constant-function check	PSpace-complete				PSpace-h.		PSpace-h.

Constant-Function Check

	Inf	Sup	LimInf	LimSup	LimInfAvg	LimSupAvg	DSum
Constant-function check	PSpace-complete				PSpace-h.		PSpace-c.

Theorem.
Discounted-sum constant-function check reduces to NFA universality.



Remove if $x + \lambda \mathsf{T}_p < \mathsf{T}_q$

$\Rightarrow$ DSum constant T iff NFA universal

Constant-Function Check

	Inf	Sup	LimInf	LimSup	LimInfAvg	LimSupAvg	DSum
Constant-function check	PSpace-complete				PSpace-c.		PSpace-c.

Theorem.
Limit-average constant-function check reduces to distance automata limitedness.

- Distance automata = Min-plus automata with weights in $\{0, 1\}$
- A distance automaton D is *limited* iff $\exists m \in \mathbb{N} : \forall u \in \Sigma^* : D(u) \leq m$

Constant-Function Check: Limit-Average

Let A be a limit-average automaton with the top value $\top$

- Construct a limit-average automaton B
  - only weights in $\{0, 1\}$
  - resolves nondeterminism with $\inf$
  - A is constant $\top$ iff B is constant 0

- Construct a distance automaton D from B by taking all states as accepting
  - Claim: B is constant 0 iff D is limited

Constant-Function Check: Limit-Average

Show: limited ⇒ constant

- Assume D is limited by some $b \in \mathbb{N}$.
- Let $w \in \Sigma^{\omega}$ be a word and consider the run tree T over its prefixes.
- There is an infinite path ρ where the sum of weights is bounded by b. (Otherwise, there exists a finite prefix u of w with $D(u) > b$).
- Limit-average of such runs is 0.
- B maps all words to 0.

Constant-Function Check: Limit-Average

Show: not limited ⇒ not constant

(D^S = the copy of D where the initial states are set to S)

- Assume D is not limited.
- $(\star)$: There is $u \in \Sigma^*$ such that $D(u) = 1$ and the runs of D on u lead to a set of states U such that D^U is also not limited.
- Repeatedly apply $(\star)$ until reaching a set U_ℓ that was seen at jth iter.
- Take $w = u_1 \dots u_j \left(u_{j+1} \dots u_\ell\right)^\omega$ and let $m = \max_{1 \le i \le \ell} |u_i|$.
- For any run over w and for each i, the average after reading u_i is $\geq \frac{1}{m}$.
- B maps w to > 0.

Deciding Safety and Liveness

	Inf	Sup	LimInf	LimSup	LimInfAvg	LimSupAvg	DSum
Deciding safety	$O(1)$	PSpace-complete			ExpSpace; PSpace-hard		$O(1)$
Deciding liveness	PSpace-complete						
Constant-function check	PSpace-complete						

Theorem.

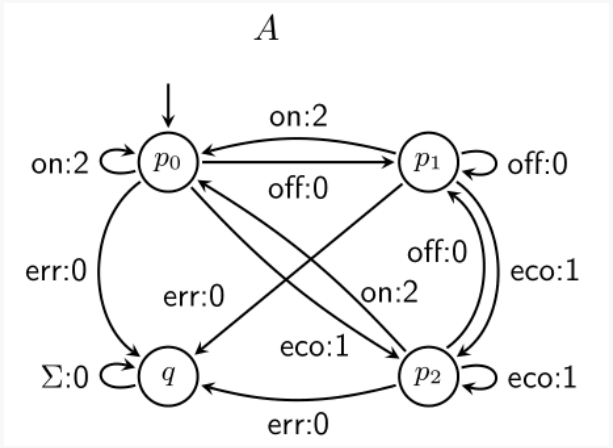
A is safe $\Leftrightarrow A - A^* = 0$

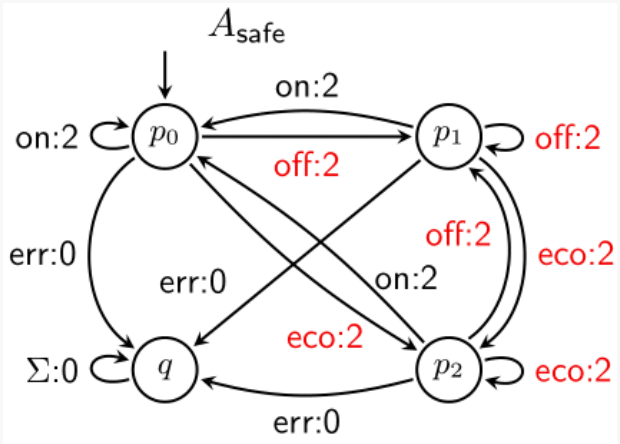
needs to be determinized

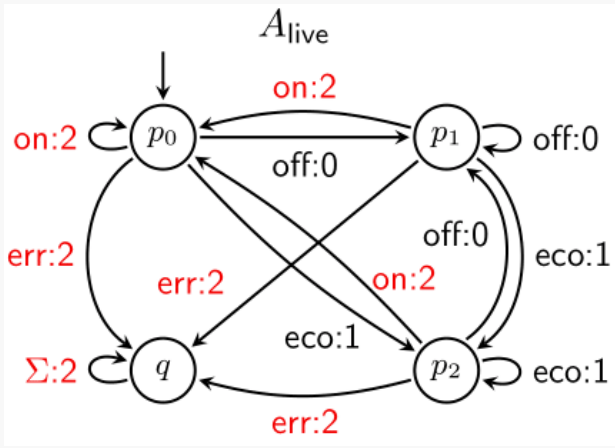
Safety-Liveness Decompositions

Deterministic

- Given a deterministic Val-automaton A where $\mathrm{Val} \in \{\mathrm{Sup}, \mathrm{LimInf}, \mathbf{LimSup}\}$
  - $A_{\mathrm{safe}} = A^*$
  - A_{live} is a copy of A where for every transition t
    - if A and A_{safe} agree on the weight of t, then A_{live} takes $\top$ as its weight
    - otherwise, A_{live} takes the weight in A





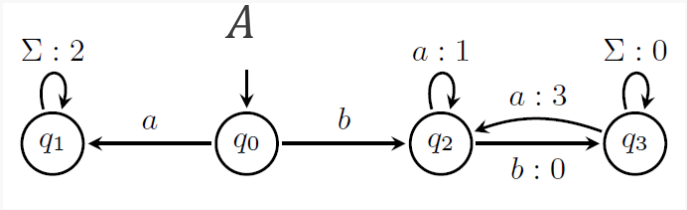


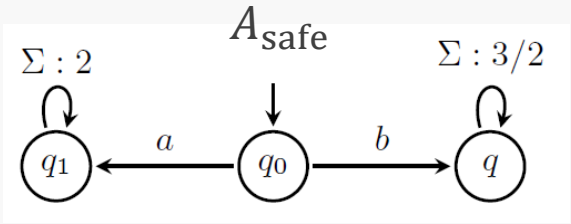
Safety-Liveness Decompositions

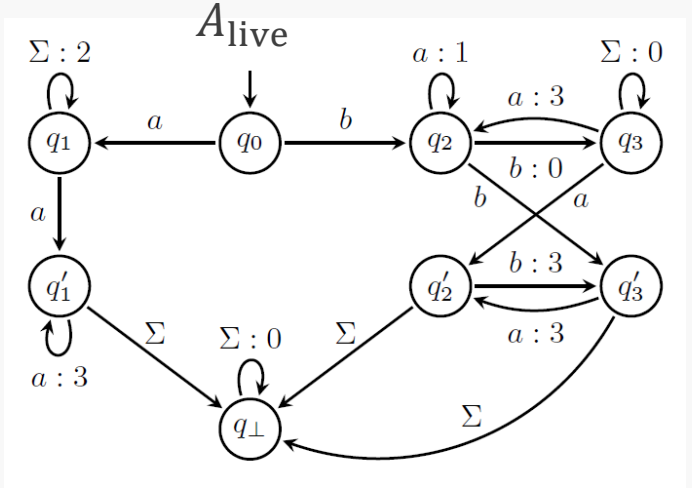
Non-deterministic

- Given a Val-automaton A where

$\mathrm{Val} \in \{\mathrm{LimInf}, \mathrm{LimSup}, \mathbf{LimInfAvg}, \mathbf{LimSupAvg}\}$







In a Nutshell

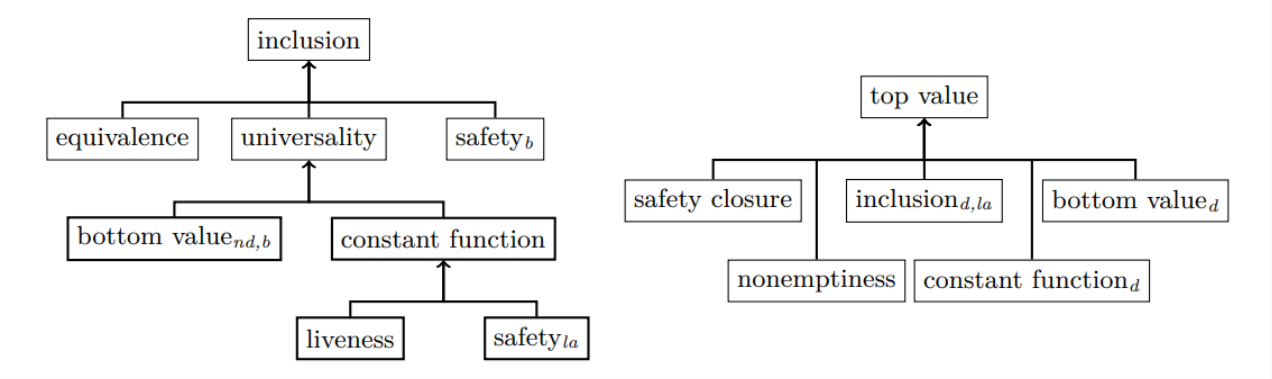
Safe: For every word, *every* wrong membership hypothesis has a finite witness.

Live: For every word (with value $< \top$), *some* wrong membership hypothesis has no finite witness.

	Inf	**Sup**	**LimInf**	**LimSup**	**LimInfAvg**	**LimSupAvg**	**DSum**
Constructing the safety closure	$O(1)$	PTime					$O(1)$
Safety-liveness decomposition	$O(1)$	PTime					$O(1)$
Constant-function check	PSpace-complete						
Deciding safety	$O(1)$	PSpace-complete			ExpSpace; PSpace-hard		$O(1)$
Deciding liveness	PSpace-complete						

QuAK: Quantitative Automata Kit

- *First tool* for the analysis of quantitative automata
  - Currently supports $\mathrm{Val} \in \{\mathrm{Inf}, \mathrm{Sup}, \mathrm{LimInf}, \mathrm{LimSup}, \mathrm{LimInfAvg}, \mathrm{LimSupAvg}\}$
  - Open-source, no dependencies beyond the C++ standard library
- Implements both the *standard* and the *novel* algorithms
  - Emptiness, universality, (antichain-based) inclusion, …
  - Constant-check, safety closure, deciding safety/liveness, …
  - Monitoring
- Available at **github.com/ista-vamos/QuAK**



Future Work

- *Topological characterization* of liveness
- Safety and liveness of quantitative properties *beyond finite-state*
- *Efficient verification* methods for quantitative safety
- *Approximate monitoring* through (approximate) safety
- Safety and liveness of *probabilistic properties*
- *Quantitative hyperproperties* and their safety and liveness

Future Work

- *Topological characterization* of liveness
- Safety and liveness of quantitative properties *beyond finite-state*
- *Efficient verification* methods for quantitative safety
- *Approximate monitoring* through (approximate) safety
- Safety and liveness of *probabilistic properties*
- *Quantitative hyperproperties* and their safety and liveness
- Your idea?

Thanks!