GT Vérif – Université Paris-Est

Safety and Liveness of Quantitative Properties and Automata

Udi Boker [1]

Marek Chalupa [2]

Thomas A. Henzinger [2]

Nicolas Mazzocchi [3]

N. Ege Saraç [2]

(1) Reichman University, Israel
(2) Institute of Science and Technology, Austria
(3) Slovak University of Technology in Bratislava, Slovakia

Supported by ERC-2020-AdG 101020093 (VAMOS)

Boolean Setting

Definition

A Boolean property $\Phi \subseteq \Sigma^\omega$ or equivalently $\Phi \colon \Sigma^\omega \to \{0,1\}$, is a language

Safety

Requests Not Duplicated

Liveness

All Requests Granted

Boolean Setting

Definition

A Boolean property $\Phi \subseteq \Sigma^\omega$ or equivalently $\Phi \colon \Sigma^\omega \to \{0,1\}$, is a language

Safety	Liveness
Requests Not Duplicated	All Requests Granted

Theorem: Decomposition[1]

All Boolean property Φ can be expressed by $\Phi = \Phi_{safe} \cap \Phi_{live}$

Φ_{safe} *is safe* Φ_{live} *is live*

[1] Alpern, Schneider. *Defining liveness.* 1985

Quantitative Setting

Definition

A quantitative property[2] $\Phi\colon \Sigma^\omega \to \mathbb{D}$ is a quantitative language where $\mathbb{D}$ is a complete lattice

[2] Chatterjee, Doyen, Henzinger. *Quantitative Languages*. 2010

Quantitative Setting

Definition

A quantitative property $\Phi\colon \Sigma^\omega \to \mathbb{D}$ is a quantitative language where $\mathbb{D}$ is a complete lattice

Safety[3]

Minimal Response Time

Liveness[3]

Average Response Time

Theorem: Decomposition[3]

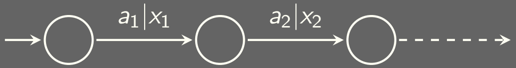
All quantitative property Φ can be expressed by $\Phi(w) = \min\{\Phi_{safe}(w), \Phi_{live}(w)\}$ for all $w \in \Sigma^\omega$

Φ_{safe} is quantitative safe — *Φ_{live} is quantitative live*

[3] Henzinger, Mazzocchi, Saraç. *Quantitative Safety and Liveness.* 2023

Quantitative Automata

Runs



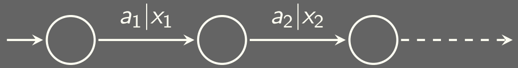
Input: $w = a_1 a_2 \dots$ Output: $x = \mathrm{Val}(x_1 x_2 \dots)$

Value function Val

Inf, Sup, LimInf, LimSup
LimInfAvg, LimSupAvg, DSum

Quantitative Automata

Runs

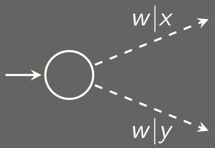


Input: $w = a_1 a_2 \ldots$ Output: $x = \mathsf{Val}(x_1 x_2 \ldots)$

Value function Val

Inf, Sup, LimInf, LimSup
LimInfAvg, LimSupAvg, DSum

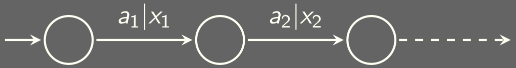
Non-determinism



$A(w) = \sup\{\text{values of } w\text{'s runs}\}$

Quantitative Automata

Runs



Input: $w = a_1 a_2 \ldots$ Output: $x = \mathsf{Val}(x_1 x_2 \ldots)$

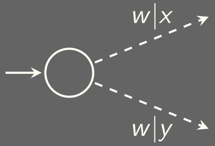
Value function Val

Inf, Sup, LimInf, LimSup
LimInfAvg, LimSupAvg, DSum

Subset of quantitative properties

- totally ordered domain
- finitely many weights
- realistically-optimistic
  $\forall u \in \Sigma^* : \sup_{v \in \Sigma^\omega} A(uv) \in \{A(uv') : v' \in \Sigma^\omega\}$

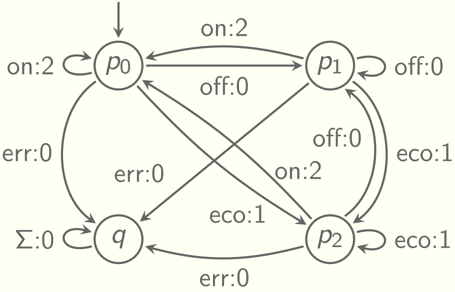
Non-determinism



$A(w) = \sup\{\text{values of } w\text{'s runs}\}$

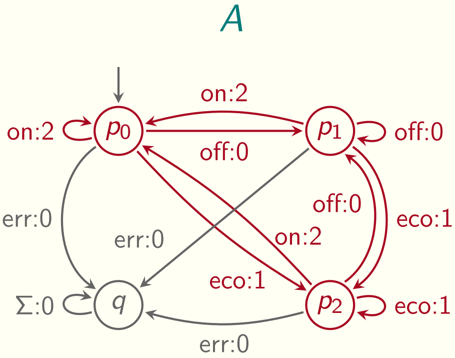
Example of LimSup Automaton

A



$w =$ off on eco off eco off eco ... off eco ... $A(w) = \text{LimSup } 0210101 \ldots 01 \cdots = 1$

Example of LimSup Automaton

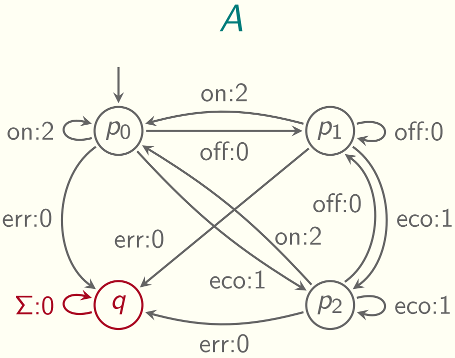


No Error

$$\forall u \in (\Sigma \setminus \{\text{err}\})^* : A(u\ \text{on}^\omega) = 2$$
$$\forall u \in (\Sigma \setminus \{\text{err}\})^* : A(u\ \text{eco}^\omega) = 1$$
$$\forall u \in (\Sigma \setminus \{\text{err}\})^* : A(u\ \text{off}^\omega) = 0$$

$w = \text{off on eco off eco off eco} \ldots \text{off eco} \ldots \qquad A(w) = \text{LimSup } 0210101 \ldots 01 \cdots = 1$

Example of LimSup Automaton



No Error

$$\forall u \in (\Sigma \setminus \{\mathrm{err}\})^* : A(u\ \mathrm{on}^\omega) = 2$$
$$\forall u \in (\Sigma \setminus \{\mathrm{err}\})^* : A(u\ \mathrm{eco}^\omega) = 1$$
$$\forall u \in (\Sigma \setminus \{\mathrm{err}\})^* : A(u\ \mathrm{off}^\omega) = 0$$

After Error

$$\forall v \in \Sigma^\omega : A(\mathrm{err}\ v) = 0$$

$w = \mathrm{off\ on\ eco\ off\ eco\ off\ eco} \dots \mathrm{off\ eco} \dots \qquad A(w) = \mathrm{LimSup}\ 0210101 \dots 01 \dots = 1$

Safety

Boolean Safety

Intuition

Every **wrong** hypothesis $w \in \Phi$ can always be rejected after a finite number of observations

Boolean Safety

Intuition

Every **wrong** hypothesis $w \in \Phi$ can always be rejected after a finite number of observations

Example: Requests Not Duplicated

- $\Sigma = \{\mathtt{r}, \mathtt{g}, \mathtt{t}, \mathtt{o}\}$ $\qquad$ $\mathtt{r}$: request, $\mathtt{g}$: grant, $\mathtt{t}$: clock-tick, $\mathtt{o}$: other
- Φ = no $\mathtt{r}$ is followed by another $\mathtt{r}$ without some $\mathtt{g}$ in between

$$
\begin{array}{rl}
w = & \mathtt{t\,r\,t\,o\,t\,t\,o\,g\,t\,o\,o\,r\,t\,t\,o\,r\,t\,t\,o\,g\,t\,r}\cdots \\
w \in \Phi\colon & \mathtt{T\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,F\,.\,.\,.\,.\,.\,.}\cdots
\end{array}
$$

Boolean Safety

Intuition

Every **wrong** hypothesis $w \in \Phi$ can always be rejected after a finite number of observations

Example: Requests Not Duplicated

- $\Sigma = \{\mathtt{r}, \mathtt{g}, \mathtt{t}, \mathtt{o}\}$ $\mathtt{r}$: request, $\mathtt{g}$: grant, $\mathtt{t}$: clock-tick, $\mathtt{o}$: other
- $\Phi =$ no $\mathtt{r}$ is followed by another $\mathtt{r}$ without some $\mathtt{g}$ in between

Definition: Safety of $\Phi \subseteq \Sigma^\omega$

$$\forall w \in \Sigma^\omega : w \notin \Phi \implies \exists u \sqsubseteq w : \forall v \in \Sigma^\omega : uv \notin \Phi$$

Quantitative Safety

Intuition

Every **wrong** hypothesis $\Phi(w) \geq x$, can always be rejected after a finite number of observations

Quantitative Safety

Intuition

Every **wrong** hypothesis $\Phi(w) \geq x$, can always be rejected after a finite number of observations

Example: Minimal Response Time

- $\Sigma = \{\mathtt{r}, \mathtt{g}, \mathtt{t}, \mathtt{o}\}$ $\mathtt{r}$: request, $\mathtt{g}$: grant, $\mathtt{t}$: clock-tick, $\mathtt{o}$: other
- $\Phi_{\mathsf{min}}(w) =$ greatest lower bound on the occurrences of $\mathtt{t}$ between all matching $\mathtt{r}/\mathtt{g}$ in w

$$
\begin{array}{rl}
w = & \mathtt{t\,r\,t\,o\,t\,t\,o\,g\,t\,o\,o\,r\,t\,t\,o\,r\,t\,t\,o\,g\,t\,r} \cdots \\
\Phi(w) \geq 3\colon & \mathtt{T\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,F\,.\,.} \cdots
\end{array}
$$

Quantitative Safety

Intuition

Every **wrong** hypothesis $\Phi(w) \geq x$, can always be rejected after a finite number of observations

Example: Minimal Response Time

- $\Sigma = \{\mathtt{r}, \mathtt{g}, \mathtt{t}, \mathtt{o}\}$ $\mathtt{r}$: request, $\mathtt{g}$: grant, $\mathtt{t}$: clock-tick, $\mathtt{o}$: other
- $\Phi_{\mathsf{min}}(w) =$ greatest lower bound on the occurrences of $\mathtt{t}$ between all matching $\mathtt{r}/\mathtt{g}$ in w

Definition[4]: Safety of $\Phi : \Sigma^\omega \to \mathbb{D}$

$$\forall x \in \mathbb{D} : \forall w \in \Sigma^\omega : \Phi(w) \not\geq x \implies \exists u \sqsubseteq w : \sup_{v \in \Sigma^\omega} \Phi(uv) \not\geq x$$

[4] Henzinger, Mazzocchi, Saraç. *Quantitative Safety and Liveness*. 2023

Boolean Safety

$$\forall w \in \Sigma^\omega : w \notin \Phi \implies \exists u \sqsubseteq w : \forall v \in \Sigma^\omega : uv \notin \Phi$$

Quantitative Safety

$$\forall x \in \mathbb{D} : \forall w \in \Sigma^\omega : \Phi(w) \not\geq x \implies \exists u \sqsubseteq w : \sup_{v \in \Sigma^\omega} \Phi(uv) \not\geq x$$

Safety of Quantitative Automata

Boolean Safety

$$\forall w \in \Sigma^\omega : w \notin \Phi \implies \exists u \sqsubseteq w : \forall v \in \Sigma^\omega : uv \notin \Phi$$

Quantitative Safety

$$\forall x \in \mathbb{D} : \forall w \in \Sigma^\omega : \Phi(w) \not\geq x \implies \exists u \sqsubseteq w : \sup_{v \in \Sigma^\omega} \Phi(uv) \not\geq x$$

Definition: Threshold Safety of $\Phi : \Sigma^\omega \to \mathbb{D}$

$$\forall x \in \mathbb{D} : \Phi_{\geq x} = \{w \in \Sigma^\omega \mid \Phi(w) \geq x\} \textit{ is safe}$$

Safety of Quantitative Automata

Quantitative Automata Kit

Boolean Safety

$$\forall w \in \Sigma^\omega : w \notin \Phi \implies \exists u \sqsubseteq w : \forall v \in \Sigma^\omega : uv \notin \Phi$$

Quantitative Safety

$$\forall x \in \mathbb{D} : \forall w \in \Sigma^\omega : \Phi(w) \not\geq x \implies \exists u \sqsubseteq w : \sup_{v \in \Sigma^\omega} \Phi(uv) \not\geq x$$

Definition: Threshold Safety of $\Phi : \Sigma^\omega \to \mathbb{D}$

$$\forall x \in \mathbb{D} : \Phi_{\geq x} = \{w \in \Sigma^\omega \mid \Phi(w) \geq x\} \textit{ is safe}$$

Theorem: For totally ordered domain, threshold-safety = quantitative safety

Quantitative Safety Closure

Intuition

The safety closure $\Phi^\star$ is the least safety property that bound Φ from above

Quantitative Safety Closure

Intuition

The safety closure $\Phi^\star$ is the least safety property that bound Φ from above

Example: Minimal Response Time

- $\Sigma = \{\mathtt{r}, \mathtt{g}, \mathtt{t}, \mathtt{o}\}$
- $\Phi_{\text{min}}(w) =$ greatest lower bound on the occurrences of $\mathtt{t}$ between all matching $\mathtt{r}/\mathtt{g}$ in w

$$
\begin{array}{rl}
w = & \mathtt{t\,r\,t\,o\,t\,t\,o\,g\,t\,o\,o\,r\,t\,t\,o\,r\,t\,t\,o\,g\,t\,r} \cdots \\
\text{least upper bound}: & \infty\,.\,.\,.\,.\,.\,3\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,2\,.\,.\,\cdots
\end{array}
$$

Quantitative Safety Closure

Intuition

The safety closure $\Phi^\star$ is the least safety property that bound Φ from above

Example: Minimal Response Time

- $\Sigma = \{\mathtt{r}, \mathtt{g}, \mathtt{t}, \mathtt{o}\}$
- $\Phi_{\mathsf{min}}(w)$ = greatest lower bound on the occurrences of $\mathtt{t}$ between all matching $\mathtt{r}/\mathtt{g}$ in w

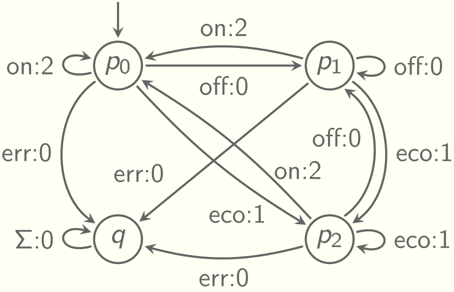
Definition[5]: Safety closure of $\Phi : \Sigma^\omega \to \mathbb{D}$

$$w \mapsto \Phi^\star(w) := \inf_{u \sqsubseteq w} \sup_{v \in \Sigma^\omega} \Phi(uv)$$

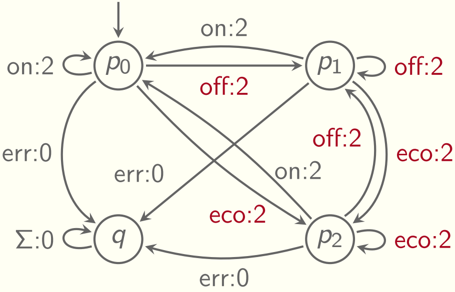
[5] Henzinger, Mazzocchi, Saraç. *Quantitative Safety and Liveness*. 2023

Example of Safety Closure

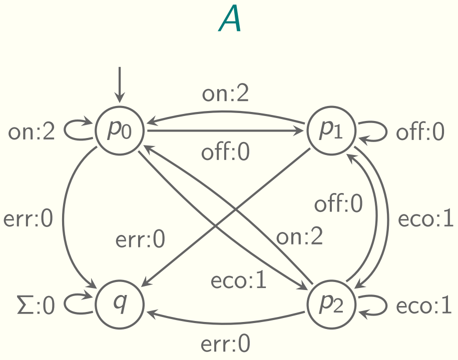
A

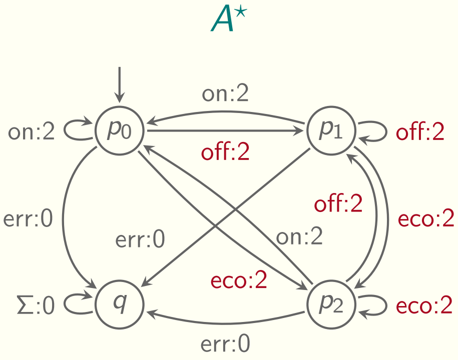


$A^\star$



Example of Safety Closure





A is not safe since $A \neq A^\star$ as witnessed by $A(\text{eco}^\omega) = 1$, $A^\star(\text{eco}^\omega) = 2$

Characterizations of Safety

Theorem: Properties of the Safety Closure

- Φ is safe $\iff$ $\Phi = \Phi^\star$

Characterizations of Safety

Theorem: Properties of the Safety Closure

- $\varPhi$ is safe $\iff$ $\varPhi = \varPhi^{\star}$

Theorem: Properties of Inf-automata

- Inf automata are always safe (as well as DSum automata)
- Sup, LimInf, LimSup, LimInfAvg, LimSupAvg automata safe $\iff$ Inf-expressible

Characterizations of Safety

Theorem: Properties of the Safety Closure

- Φ is safe $\iff$ $\Phi = \Phi^\star$

Theorem: Properties of Inf-automata

- Inf automata are always safe (as well as DSum automata)
- Sup, LimInf, LimSup, LimInfAvg, LimSupAvg automata safe $\iff$ Inf-expressible

Proposition[6]: Inf-automata are determinizable in exponential time.

[6] Chatterjee, Doyen, Henzinger. *Quantitative Languages*. 2010

Characterizations of Safety

Theorem: Properties of the Safety Closure

- Φ is safe $\iff \Phi = \Phi^\star$

Theorem: Properties of Inf-automata

- Inf automata are always safe (as well as DSum automata)
- Sup, LimInf, LimSup, LimInfAvg, LimSupAvg automata safe $\iff$ Inf-expressible

Proposition[6]: Inf-automata are determinizable in exponential time.

Corollary: LimInf, LimSup, LimInfAvg, LimSupAvg automata are determinizable if safe

[6] Chatterjee, Doyen, Henzinger. *Quantitative Languages*. 2010

Application to Monitoring

Let $\mathcal{A}$ be a Val-automaton where $\mathsf{Val} \in \{\mathsf{Inf}, \mathsf{Sup}, \mathsf{LimInf}, \mathsf{LimSup}\}$

$$\mathcal{A}^\star(w) := \inf_{u \sqsubseteq w} \sup_{v \in \Sigma^\omega} \Phi(uv)$$

$$\mathcal{A}_\star(w) := \sup_{u \sqsubseteq w} \inf_{v \in \Sigma^\omega} \Phi(uv)$$

- $\mathcal{A}^\star$ is determinizable
- $\mathcal{A}_\star$ is determinizable

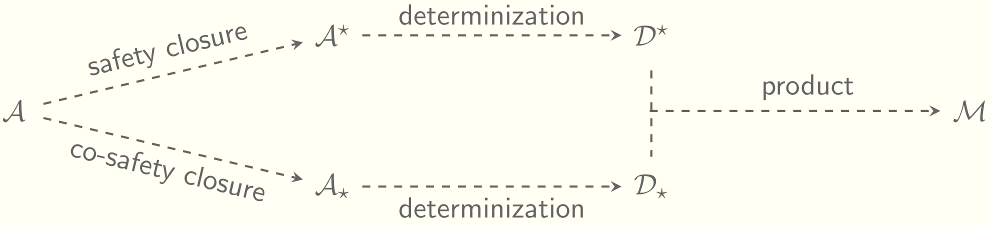
Application to Monitoring

Let $\mathcal{A}$ be a Val-automaton where $\mathsf{Val} \in \{\mathsf{Inf}, \mathsf{Sup}, \mathsf{LimInf}, \mathsf{LimSup}\}$

$$\mathcal{A}^\star(w) \coloneqq \inf_{u \sqsubseteq w} \sup_{v \in \Sigma^\omega} \Phi(uv)$$

$$\mathcal{A}_\star(w) \coloneqq \sup_{u \sqsubseteq w} \inf_{v \in \Sigma^\omega} \Phi(uv)$$

- $\mathcal{A}^\star$ is determinizable
- $\mathcal{A}_\star$ is determinizable



Liveness

Boolean Liveness

Intuition

Some **wrong** hypothesis $w \in \Phi$ can never be rejected after any finite number of observations

Boolean Liveness

Intuition

Some **wrong** hypothesis $w \in \Phi$ can never be rejected after any finite number of observations

Example: All Requests Granted

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

$$
\begin{array}{rl}
w = & \mathtt{t\,r\,t\,o\,t\,t\,o\,g\,t\,o\,o\,r\,t\,t\,o\,r\,t\,t\,o\,g\,t\,\color{red}{r}} \cdots \\
w \in \Phi\text{:} & \mathtt{T\,.\,?} \cdots
\end{array}
$$

Boolean Liveness

Intuition

Some **wrong** hypothesis $w \in \Phi$ can never be rejected after any finite number of observations

Example: All Requests Granted

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

Definition: Liveness of $\Phi \subseteq \Sigma^\omega$

$$\forall u \in \Sigma^* : \exists v \in \Sigma^\omega : uv \in \Phi$$

Quantitative Liveness

Intuition

Some **wrong** hypothesis $\Phi(w) \geq x$ can never be rejected after any finite number of observations

Quantitative Liveness

Intuition

Some **wrong** hypothesis $\Phi(w) \geq x$ can never be rejected after any finite number of observations

Example: Average Response Time

- $\Sigma = \{\mathtt{r}, \mathtt{g}, \mathtt{t}, \mathtt{o}\}$
- $\Phi_{\text{avg}}(w) =$ average on the occurrences of $\mathtt{t}$ between all matching $\mathtt{r}/\mathtt{g}$ in w

$$\begin{array}{rl} w = & \mathtt{t\,r\,t\,o\,t\,t\,o\,g\,t\,o\,o\,r\,t\,t\,o\,r\,t\,t\,o\,g\,t\,r} \cdots \\ \Phi(w) \geq 3: & \mathtt{T\,.\,?} \cdots \end{array}$$

Quantitative Liveness

Intuition

Some **wrong** hypothesis $\Phi(w) \geq x$ can never be rejected after any finite number of observations

Example: Average Response Time

- $\Sigma = \{\mathtt{r}, \mathtt{g}, \mathtt{t}, \mathtt{o}\}$
- $\Phi_{\text{avg}}(w) =$ average on the occurrences of $\mathtt{t}$ between all matching $\mathtt{r}/\mathtt{g}$ in w

Definition[7]: Lineness of $\Phi : \Sigma^\omega \to \mathbb{D}$

$$\forall w \in \Sigma^\omega : \Phi(w) < \top \implies \exists x \in \mathbb{D} : \Phi(w) \not\geq x \wedge \forall u \sqsubseteq w : \sup_{v \in \Sigma^\omega} \Phi(uv) \geq x$$

[7] Henzinger, Mazzocchi, Saraç. *Quantitative Safety and Liveness*. 2023

Definition: Threshold Liveness of $\Phi : \Sigma^\omega \to \mathbb{D}$

$$\forall x \in \mathbb{D} : \Phi_{\geq x} = \{w \in \Sigma^\omega \mid \Phi(w) \geq x\} \textit{ is live}$$

Liveness of Quantitative Automata

Definition: Threshold Liveness of $\Phi : \Sigma^\omega \to \mathbb{D}$

$$\forall x \in \mathbb{D} : \Phi_{\geq x} = \{w \in \Sigma^\omega \mid \Phi(w) \geq x\} \textit{ is live}$$

Theorem: A property Φ is threshold live iff the set $\{w \in \Sigma^\omega \mid \Phi(w) = \top\}$ is dense

Liveness of Quantitative Automata

Definition: Threshold Liveness of $\Phi : \Sigma^\omega \to \mathbb{D}$

$$\forall x \in \mathbb{D} : \Phi_{\geq x} = \{w \in \Sigma^\omega \mid \Phi(w) \geq x\} \textit{ is live}$$

Theorem: A property Φ is threshold live iff the set $\{w \in \Sigma^\omega \mid \Phi(w) = \top\}$ is dense

Definition: Top Liveness of $\Phi : \Sigma^\omega \to \mathbb{D}$

$$w \mapsto \Phi^\star(w) = \top$$

Liveness of Quantitative Automata

Definition: Threshold Liveness of $\Phi : \Sigma^\omega \to \mathbb{D}$

$$\forall x \in \mathbb{D} : \Phi_{\geq x} = \{w \in \Sigma^\omega \mid \Phi(w) \geq x\} \textit{ is live}$$

Theorem: A property Φ is threshold live iff the set $\{w \in \Sigma^\omega \mid \Phi(w) = \top\}$ is dense

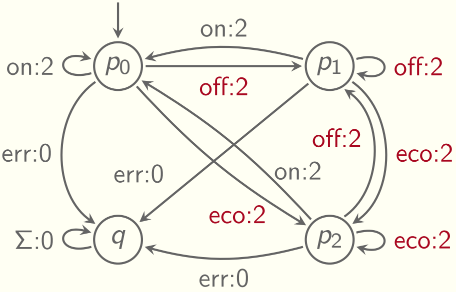
Definition: Top Liveness of $\Phi : \Sigma^\omega \to \mathbb{D}$

$$w \mapsto \Phi^\star(w) = \top$$

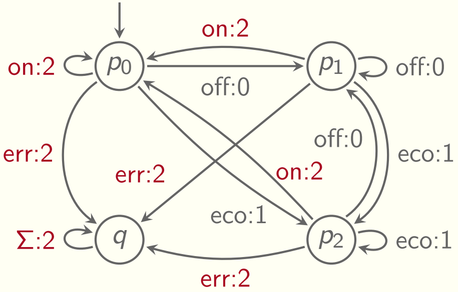
Theorem: For realistically-optimistic properties, top-liveness = threshold-liveness = liveness

Safety-Liveness Decomposition

$A_{\text{safe}} = A^\star$



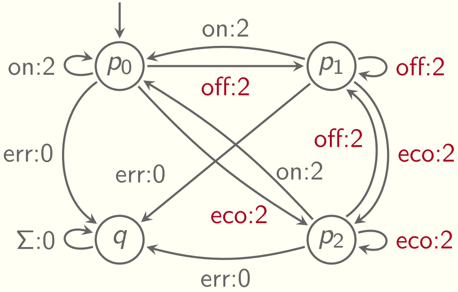
A_{live}



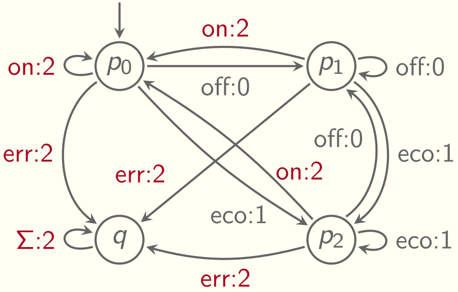
$$A(w) = \min\{A_{\text{safe}}(w), A_{\text{live}}(w)\}$$

Safety-Liveness Decomposition

$A_{\text{safe}} = A^{\star}$



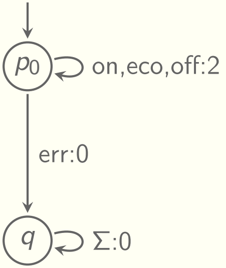
A_{live}



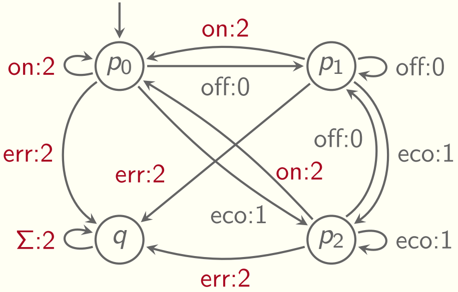
construction for **deterministic** for Sup, LimInf, and LimSup automata

Safety-Liveness Decomposition

$A_{\text{safe}} = A^\star$



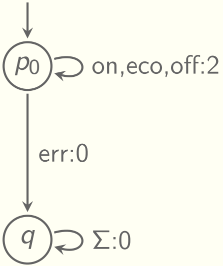
A_{live}



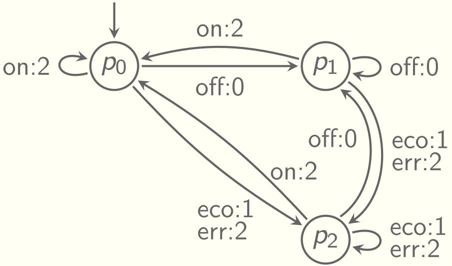
construction for **deterministic** for Sup, LimInf, and LimSup automata

Safety-Liveness Decomposition

$A_{\text{safe}} = A^{\star}$



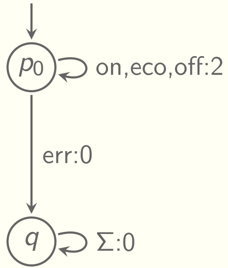
A_{live}



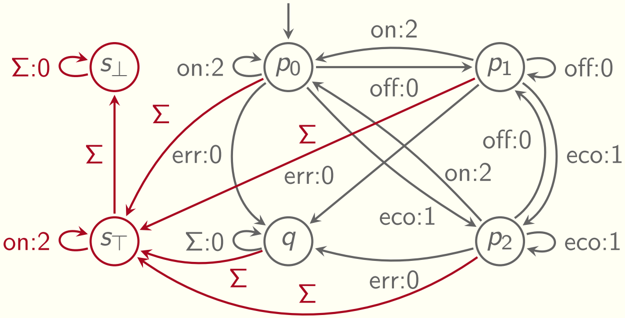
construction for **deterministic** for Sup, LimInf, and LimSup automata

Safety-Liveness Decomposition

$A_{\text{safe}} = A^{\star}$



A_{live}



construction for LimInf, LimSup, LimInfAvg, and LimSupAvg automata

Decision Procedures

Deciding Safety and Liveness

Classes Inf, Sup, LimInf, LimSup

Safety: $A = A^\star$

- Equivalence is decidable

Liveness: $A^\star = \top$

Deciding Safety and Liveness

Classes Inf, Sup, LimInf, LimSup

Safety: $A = A^\star$ **Liveness**: $A^\star = \top$

- Equivalence is decidable

Class DSum

Safety: alway true **Liveness**: $A = \top$

- For each state, determine the transition leading to highest achievable value
- Decide universality of the underlying finite state automaton (all state accepting)

Deciding Safety and Liveness

Classes Inf, Sup, LimInf, LimSup

Safety: $A = A^\star$ **Liveness**: $A^\star = \top$

- Equivalence is decidable

Class DSum

Safety: alway true **Liveness**: $A = \top$

- For each state, determine the transition leading to highest achievable value
- Decide universality of the underlying finite state automaton (all state accepting)

Classes LimInfAvg and LimSupAvg

$C \leq 0$ is PTIME[8] $C \geq 0$ is undecidable[9] $C = 0$ is PSPACE[10]

Deciding Safety and Liveness

Classes Inf, Sup, LimInf, LimSup

Safety: $A = A^\star$ — **Liveness**: $A^\star = \top$

- Equivalence is decidable

Class DSum

Safety: alway true — **Liveness**: $A = \top$

- For each state, determine the transition leading to highest achievable value
- Decide universality of the underlying finite state automaton (all state accepting)

Classes LimInfAvg and LimSupAvg

$C \leq 0$ is $\textsc{PTime}$[8] — $C \geq 0$ is undecidable[9] — $C = 0$ is $\textsc{PSpace}$[10]

[8] Chatterjee, Doyen, Henzinger. *Quantitative Languages*. 2010

Deciding Safety and Liveness

Classes Inf, Sup, LimInf, LimSup

Safety: $A = A^\star$ **Liveness**: $A^\star = \top$

- Equivalence is decidable

Class DSum

Safety: alway true **Liveness**: $A = \top$

- For each state, determine the transition leading to highest achievable value
- Decide universality of the underlying finite state automaton (all state accepting)

Classes LimInfAvg and LimSupAvg

$C \leq 0$ is PTIME[8] $C \geq 0$ is undecidable[9] $C = 0$ is PSPACE[10]

[9] Degorre, Doyen, Gentilini, Raskin, Torunczyk. *Energy and MP Games with Imperfect Information*. 2010

Deciding Safety and Liveness

Classes Inf, Sup, LimInf, LimSup

Safety: $A = A^\star$ **Liveness**: $A^\star = \top$

- Equivalence is decidable

Class DSum

Safety: alway true **Liveness**: $A = \top$

- For each state, determine the transition leading to highest achievable value
- Decide universality of the underlying finite state automaton (all state accepting)

Classes LimInfAvg and LimSupAvg

$C \leq 0$ is PTIME[8] $C \geq 0$ is undecidable[9] $C = 0$ is PSPACE[10]

[10] Boker, Henzinger, Mazzocchi, Saraç. *Safety and Liveness of Quantitative Automata*. 2023

Taming Constant Average

Deciding constancy[11] $C = x = \top$

(1) Reduce to Zeroness, i.e., $C - \top = 0$

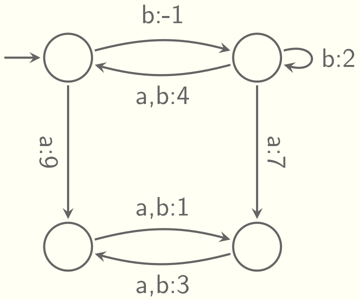
- Subtract $\top$ computed by Karps's algorithm

(2) All edges non-positive

- Johnson's algorithm

(3) From Avg **to** LimInf

- $\forall w_1 : \exists w_2 : A_{\text{LimInf}}(w_1) \neq 0 \Rightarrow A_{\text{Avg}}(w_2) \neq 0$



[11] Chalupa, Henzinger, Mazzocchi, Saraç. *QuAK: Quantitative Automata Kit*. 2024

Taming Constant Average

Deciding constancy[11] $C = x = \top$

(1) Reduce to Zeroness, i.e., $C - \top = 0$

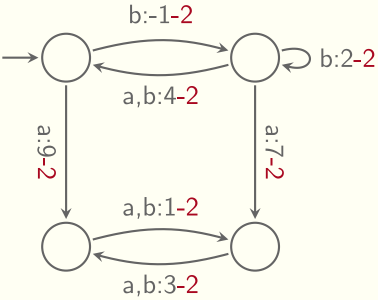
- Subtract $\top$ computed by Karps's algorithm

(2) All edges non-positive

- Johnson's algorithm

(3) From Avg **to** LimInf

- $\forall w_1 : \exists w_2 : A_{\mathrm{LimInf}}(w_1) \neq 0 \Rightarrow A_{\mathrm{Avg}}(w_2) \neq 0$



[11] Chalupa, Henzinger, Mazzocchi, Saraç. *QuAK: Quantitative Automata Kit*. 2024

Taming Constant Average

Deciding constancy[11] $C = x = \top$

(1) Reduce to Zeroness, i.e., $C - \top = 0$

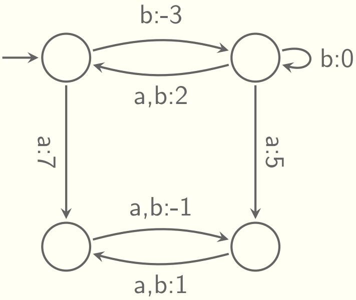
- Subtract $\top$ computed by Karps's algorithm

(2) All edges non-positive

- Johnson's algorithm

(3) From Avg **to** LimInf

- $\forall w_1 : \exists w_2 : A_{\text{LimInf}}(w_1) \neq 0 \Rightarrow A_{\text{Avg}}(w_2) \neq 0$



[11] Chalupa, Henzinger, Mazzocchi, Saraç. *QuAK: Quantitative Automata Kit*. 2024

Taming Constant Average

Deciding constancy[11] $C = x = \top$

(1) Reduce to Zeroness, i.e., $C - \top = 0$

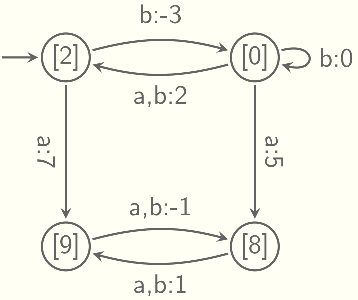
- Subtract $\top$ computed by Karps's algorithm

(2) All edges non-positive

- Johnson's algorithm

(3) From Avg **to** LimInf

- $\forall w_1 : \exists w_2 : A_{\mathrm{LimInf}}(w_1) \neq 0 \Rightarrow A_{\mathrm{Avg}}(w_2) \neq 0$



[11] Chalupa, Henzinger, Mazzocchi, Saraç. *QuAK: Quantitative Automata Kit*. 2024

Taming Constant Average

Deciding constancy[11] $C = x = \top$

(1) Reduce to Zeroness, i.e., $C - \top = 0$

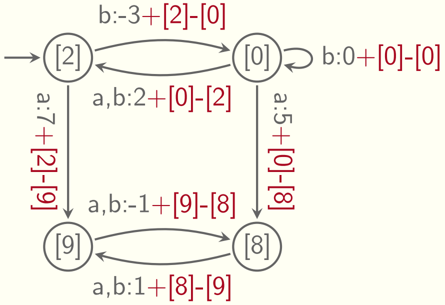
- Subtract $\top$ computed by Karps's algorithm

(2) All edges non-positive

- Johnson's algorithm

(3) From Avg **to** LimInf

- $\forall w_1 : \exists w_2 : A_{\mathrm{LimInf}}(w_1) \neq 0 \Rightarrow A_{\mathrm{Avg}}(w_2) \neq 0$



[11] Chalupa, Henzinger, Mazzocchi, Saraç. *QuAK: Quantitative Automata Kit*. 2024

Taming Constant Average

Deciding constancy[11] $C = x = \top$

(1) Reduce to Zeroness, i.e., $C - \top = 0$

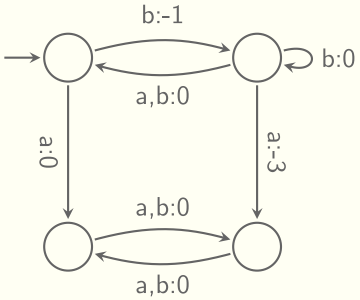
- Subtract $\top$ computed by Karps's algorithm

(2) All edges non-positive

- Johnson's algorithm

(3) From Avg **to** LimInf

- $\forall w_1 : \exists w_2 : A_{\text{LimInf}}(w_1) \neq 0 \Rightarrow A_{\text{Avg}}(w_2) \neq 0$



[11] Chalupa, Henzinger, Mazzocchi, Saraç. *QuAK: Quantitative Automata Kit*. 2024

Taming Constant Average

Quantitative Automata Kit

Deciding constancy[11] $C = x = \top$

(1) Reduce to Zeroness, i.e., $C - \top = 0$

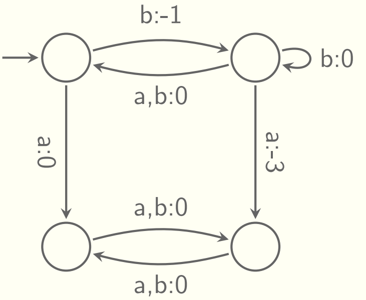
- Subtract $\top$ computed by Karps's algorithm

(2) All edges non-positive

- Johnson's algorithm

(3) From Avg **to** LimInf

- $\forall w_1 : \exists w_2 : A_{\text{LimInf}}(w_1) \neq 0 \Rightarrow A_{\text{Avg}}(w_2) \neq 0$



Deciding safety $C = C^\star$

- $C = C^\star \iff C - C^\star = 0 \iff [C - C^\star] = 0$ where $C^\star$ is determinized

[11] Chalupa, Henzinger, Mazzocchi, Saraç. *QuAK: Quantitative Automata Kit*. 2024

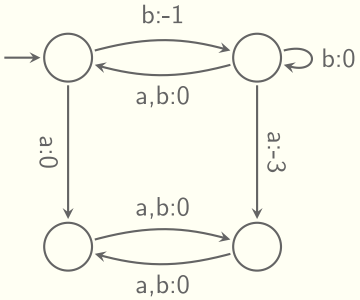
Taming Constant Average

Deciding constancy[11] $\quad C = x = \top$

(1) Reduce to Zeroness, i.e., $C - \top = 0$
- Subtract $\top$ computed by Karps's algorithm

(2) All edges non-positive
- Johnson's algorithm

(3) From Avg **to** LimInf
- $\forall w_1 : \exists w_2 : A_{\mathrm{LimInf}}(w_1) \neq 0 \Rightarrow A_{\mathrm{Avg}}(w_2) \neq 0$



Deciding safety $\quad C = C^\star$

- $C = C^\star \iff C - C^\star = 0 \iff [C - C^\star] = 0$ where $C^\star$ is determinized
- $\mathrm{Avg}(x_1 x_2 \ldots) - \mathrm{Avg}(y_1 y_2 \ldots) \neq \mathrm{Avg}((x_1 - y_1)(x_2 - y_2) \ldots)$

[11] Chalupa, Henzinger, Mazzocchi, Saraç. *QuAK: Quantitative Automata Kit*. 2024

Taming Constant Average

Deciding constancy[11] $C = x = \top$

(1) Reduce to Zeroness, i.e., $C - \top = 0$

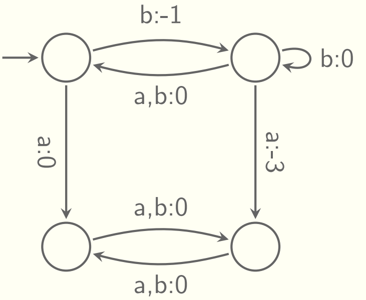
- Subtract $\top$ computed by Karps's algorithm

(2) All edges non-positive

- Johnson's algorithm

(3) From Avg **to** LimInf

- $\forall w_1 : \exists w_2 : A_{\mathrm{LimInf}}(w_1) \neq 0 \Rightarrow A_{\mathrm{Avg}}(w_2) \neq 0$



Deciding safety $C = C^\star$

- $C = C^\star \iff C - C^\star = 0 \iff [C - C^\star] = 0$ where $C^\star$ is determinized
- $\mathrm{Avg}(x_1 x_2 \dots) - \mathrm{Avg}(y_1 y_2 \dots) \neq \mathrm{Avg}((x_1 - y_1)(x_2 - y_2) \dots)$
- $\mathrm{Avg}(x_1 x_2 \dots) - \mathrm{Avg}(y_1 y_2 \dots y_n (z)^\omega) = \mathrm{Avg}((x_1 - z)(x_2 - z) \dots)$

[11] Chalupa, Henzinger, Mazzocchi, Saraç. *QuAK: Quantitative Automata Kit*. 2024

Complexity results

	Inf	**Sup***, LimInf, LimSup	LimInfAvg, LimSupAvg	DSum
Safety Closure construct $A^\star$	$O(1)$	PTIME		$O(1)$
Is A constant? e.g., $A = 0$	PSPACE-complete			
Is A safe? i.e., $A^\star = A$	$O(1)$	PSPACE-complete	PSPACE-complete	$O(1)$
Is A live? i.e., $A^\star = \top$	PSPACE-complete			
Decomposition $A = \min A_{\text{safe}} \ A_{\text{live}}$	$O(1)$	PTIME **keeps determinism**	PTIME **losses determinism**	$O(1)$

* For **Sup** we provide a Inf-Sup decomposition since Sup-Sup is infeasible in general

QuAK's Library

	Input	Problem	Val
Top value $\top$	A	$\top = \sup\{A(w) : w \in \Sigma^\omega\}$	-
Bottom value $\bot$	A	$\bot = \inf\{A(w) : w \in \Sigma^\omega\}$	$\neq$ Avg
Safety closure $A^\star$	A	Least safe over approximation of A	-
Non-emptiness	$A,\ x$	$\exists w \in \Sigma^\omega : A(w) \geq x \iff \top \geq x$	-
Universality	$A,\ x$	$\forall w \in \Sigma^\omega : A(w) \geq x \iff \bot \geq x$	$\neq$ Avg
Inclusion	$A,\ B$	$\forall w \in \Sigma^\omega : A(w) \geq B(w)$	$\neq$ Avg
Constant	A	$\forall w \in \Sigma^\omega : A(w_1) = \top$	-
Safety	A	$\forall w \in \Sigma^\omega : A^\star(w) = A(w)$	-
Liveness	A	$\forall w \in \Sigma^\omega : A^\star(w) = \top$	-
Decomposition	A	$\forall w \in \Sigma^\omega : A(w) = \min\{A_{\text{safe}}(w), A_{\text{live}}(w)\}$	-

QuAK's Library

	Input	Problem	Val
Top value $\top$	A	$\top = \sup\{A(w) : w \in \Sigma^\omega\}$	-
Bottom value $\bot$	A	$\bot = \inf\{A(w) : w \in \Sigma^\omega\}$	$\neq$ Avg
Safety closure $A^\star$	A	Least safe over approximation of A	-
Non-emptiness	$A,\ x$	$\exists w \in \Sigma^\omega : A(w) \geq x \iff \top \geq x$	-
Universality	$A,\ x$	$\forall w \in \Sigma^\omega : A(w) \geq x \iff \bot \geq x$	$\neq$ Avg
Inclusion	$A,\ B$	$\forall w \in \Sigma^\omega : A(w) \geq B(w)$	$\neq$ Avg
Constant	A	$\forall w \in \Sigma^\omega : A(w_1) = \top$	-
Safety	A	$\forall w \in \Sigma^\omega : A^\star(w) = A(w)$	-
Liveness	A	$\forall w \in \Sigma^\omega : A^\star(w) = \top$	-
Decomposition	A	$\forall w \in \Sigma^\omega : A(w) = \min\{A_{\text{safe}}(w), A_{\text{live}}(w)\}$	-

Ongoing work: Extension to nested automata

Thank you