Automating the Analysis of Quantitative Automata with QuAK

TACAS 2025 – Hamilton Canada

Marek Chalupa [1]
Thomas A. Henzinger [1]
Nicolas Mazzocchi [1 2]
N. Ege Saraç [1]

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

This talk is supported by the ERC-2020-AdG 101020093

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

funding: ERC-2020-AdG 101020093

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

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

Nicolas Mazzocchi

funding: ERC-2020-AdG 101020093

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

funding: ERC-2020-AdG 101020093

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

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 $w \in \Sigma^\omega$

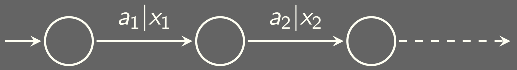
Φ_{safe} is quantitative safe — *Φ_{live} is quantitative live*

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

funding: ERC-2020-AdG 101020093

Quantitative Automata

Runs



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

Value function Val

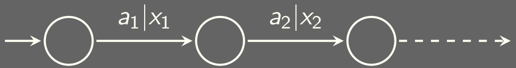
Inf, Sup, LimInf, LimSup
LimInfAvg, LimSupAvg

Nicolas Mazzocchi

funding: ERC-2020-AdG 101020093

Quantitative Automata

Runs

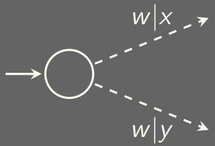


Input: $w = a_1 a_2 \dots$ Output: $x = \mathsf{Val}(x_1 x_2 \dots)$

Value function Val

Inf, Sup, LimInf, LimSup
LimInfAvg, LimSupAvg

Non-determinism



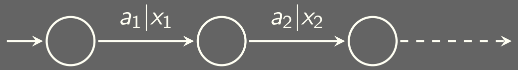
$A(w) = \sup\{\text{values of } w\text{'s runs}\}$

Nicolas Mazzocchi

funding: ERC-2020-AdG 101020093

Quantitative Automata

Runs



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

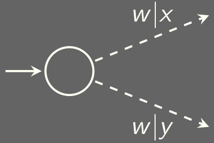
Subset of quantitative properties[4]

- $\Phi \colon \Sigma^\omega \to \mathbb{D}$ where $\mathbb{D}$ is a complete lattice
- totally ordered domain
- finitely many weights
- supremum-closed

Value function Val

Inf, Sup, LimInf, LimSup
LimInfAvg, LimSupAvg

Non-determinism



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

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

funding: ERC-2020-AdG 101020093

Quantitative Safety

Intuition

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

funding: ERC-2020-AdG 101020093

Quantitative Safety

Intuition

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

Example: Minimal Response Time

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

$$w = \mathtt{t\,r\,t\,o\,t\,t\,o\,g\,t\,o\,o\,r\,t\,t\,o\,r\,t\,t\,o\,g\,t\,r} \cdots$$

$$\Phi(w) \geq 3: \quad \mathtt{T\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,F\,.\,.} \cdots$$

Nicolas Mazzocchi

funding: ERC-2020-AdG 101020093

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

Definition[5]: A quantitative property $\Phi : \Sigma^\omega \to \mathbb{D}$ is safe when

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

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

funding: ERC-2020-AdG 101020093

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[5]: A quantitative property $\Phi : \Sigma^\omega \to \mathbb{D}$ is safe when

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

Theorem[5]: Φ is safe $\iff$ $\Phi = \Phi^\star$ where $\Phi^\star$ is the safety closure of Φ

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

funding: ERC-2020-AdG 101020093

Quantitative Liveness

Intuition

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

funding: ERC-2020-AdG 101020093

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

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

funding: ERC-2020-AdG 101020093

Quantitative Liveness

Intuition

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

Example: Average Response Time

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

Definition[6]: A quantitative property $\Phi : \Sigma^\omega \to \mathbb{D}$ is live when

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

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

funding: ERC-2020-AdG 101020093

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[6]: A quantitative property $\Phi : \Sigma^\omega \to \mathbb{D}$ is live when

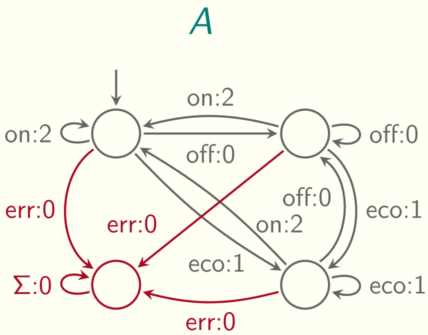
$$\forall w \in \Sigma^\omega : \Phi(w) < \top \implies \exists x \in \mathbb{D} : \Phi(w) \not\geq x \land \forall u \sqsubseteq w : \sup_{v \in \Sigma^\omega} \Phi(uv) \geq x$$

Theorem[6]: Φ is live $\iff \forall w : \Phi^\star(w) = \top$ where Φ is supremum closed

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

funding: ERC-2020-AdG 101020093

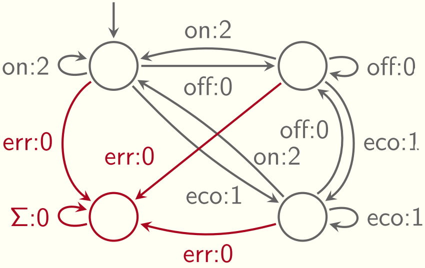
Safety-Liveness Decomposition



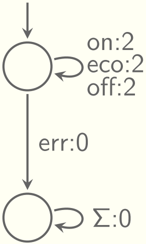
funding: ERC-2020-AdG 101020093

Safety-Liveness Decomposition

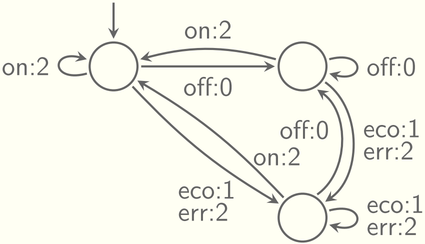
A



A_{safe}



A_{live}



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

Nicolas Mazzocchi

funding: ERC-2020-AdG 101020093

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	$\forall w \in \Sigma^\omega : A(w) = \min\{A_{\text{safe}}(w), A_{\text{live}}(w)\}$	-

funding: ERC-2020-AdG 101020093

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	$\forall w \in \Sigma^\omega : A(w) = \min\{A_{\text{safe}}(w), A_{\text{live}}(w)\}$	-

funding: ERC-2020-AdG 101020093

Complexities

	Inf	Sup, LimInf, LimSup	LimInfAvg, LimSupAvg
Is A non-empty? i.e., $\top \geq x$	PTime		
Is A universal? i.e., $\bot \geq x$	PSpace-complete		Undecidable
Is A constant?[7] i.e., $\top = A = \bot$	PSpace-complete		
Is A safe?[7] i.e., $A^\star = A$	$O(1)$	PSpace-complete	ExpSpace \ PSpace-hard
Is A live?[7] i.e., $A^\star = \top$	PSpace-complete		

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

funding: ERC-2020-AdG 101020093

Challenges overcome

Efficient constant testing

- Constant check without relying on the limitedness of distance automata[8]

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

funding: ERC-2020-AdG 101020093

Challenges overcome

Efficient constant testing

- Constant check without relying on the limitedness of distance automata[8]

Efficient inclusion testing

- Generalization of the antichain based inclusion of FORKLIFT[9]

[9] Doveri, Ganty, Mazzocchi. *FORQ-Based Language Inclusion Formal Testing*. 2022

funding: ERC-2020-AdG 101020093

Challenges overcome

Efficient constant testing

- Constant check without relying on the limitedness of distance automata[8]

Efficient inclusion testing

- Generalization of the antichain based inclusion of FORKLIFT[9]

Exhaustive decomposition framework

- PTIME safety-liveness decomposition for all quantitative automata (including LimSup, LimInfAvg and LimSupAvg automata previously left open[10])

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

funding: ERC-2020-AdG 101020093

Challenges overcome

Efficient constant testing

- Constant check without relying on the limitedness of distance automata[8]

Efficient inclusion testing

- Generalization of the antichain based inclusion of FORKLIFT[9]

Exhaustive decomposition framework

- PTIME safety-liveness decomposition for all quantitative automata (including LimSup, LimInfAvg and LimSupAvg automata previously left open[10])

Thank you

funding: ERC-2020-AdG 101020093