HIGHLIGHTS 2024 – BORDEAUX FRANCE

Udi Boker [1]
Marek Chalupa [2]
Thomas A. Henzinger [2]
Nicolas Mazzocchi [2 3]
N. Ege Saraç [2]

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

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

Safety and Liveness but Quantitative

Boolean Setting

Definition

A Boolean property $\varPhi \subseteq \Sigma^\omega$ or equivalently $\varPhi \colon \Sigma^\omega \to \{0, 1\}$, 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

Requests Not Duplicated

Liveness

All Requests Granted

Theorem: Decomposition[1]

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

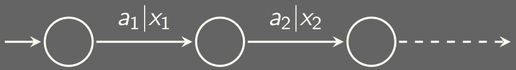
Φ_{safe} is safe *Φ_{live} is live*

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

Quantitative Automata

Quantitative Automata Kit

Runs



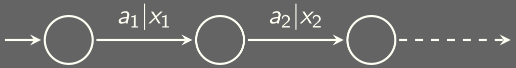
Input: $w = a_1 a_2 \dots$ Output: $x = \mathrm{Val}(x_1 x_2 \dots)$

Value function Val

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

Quantitative Automata

Runs

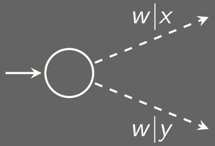


Input: $w = a_1 a_2 \ldots$ Output: $x = \mathsf{Val}(x_1 x_2 \ldots)$

Value function Val

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

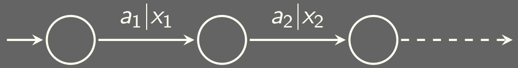
Non-determinism



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

Quantitative Automata

Runs



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

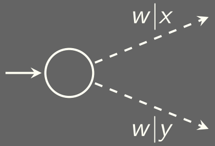
Subset of quantitative properties[2]

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

Value function Val

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

Non-determinism



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

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

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

- $\Sigma = \{\mathtt{r}, \mathtt{g}, \mathtt{t}, \mathtt{o}\}$ $\quad$ $\mathtt{r}$: 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

$$w = \mathtt{t\,r\,t\,o\,t\,t\,o\,g\,t\,o\,o\,r\,t\,t\,o\,r\,t\,t\,o\,g\,t\,r} \cdots$$
$$\Phi(w) \geq 3: \quad \mathtt{T\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,F\,.\,.} \cdots$$

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

$$\forall x \in \mathbb{D} : \forall w \in \Sigma^\omega : \Phi(w) \ngeq x \implies \exists u \sqsubseteq w : \sup_{v \in \Sigma^\omega} \Phi(uv) \ngeq x$$

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

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[3]: 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[3]: Φ is safe $\iff$ $\Phi = \Phi^\star$ where $\Phi^\star$ is the safety closure of Φ

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

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

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

Quantitative Liveness

Intuition

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

Example: Average Response Time

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

Definition[4]: A quantitative property $\Phi : \Sigma^\omega \to \mathbb{D}$ is live when

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

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

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

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

Theorem[4]: Φ is live $\iff \forall w : \Phi^\star(w) = \top$ where Φ is supremum closed

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

Decision Procedures

implementation right there

Classes Inf, Sup, LimInf, LimSup

Safety: $A = A^\star$

Liveness: $A^\star = \top$

- Equivalence is decidable

Decision Procedures

implementation right there

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)

Decision Procedures

implementation right there →

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

- $A = B \iff [A - B] = 0$ holds if all runs of B are **eventually constant** as for $A^\star$ and $\top$

$C \leq 0$ is PTime[5] $C \geq 0$ is undecidable[6] $C = 0$ is PSpace[7]

Decision Procedures

implementation right there

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

- $A = B \iff [A - B] = 0$ holds if all runs of B are **eventually constant** as for $A^\star$ and $\top$

$C \leq 0$ is PTime[5]

$C \geq 0$ is undecidable[6]

$C = 0$ is PSpace[7]

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

Decision Procedures

implementation right there

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

- $A = B \iff [A - B] = 0$ holds if all runs of B are **eventually constant** as for $A^\star$ and $\top$

$C \leq 0$ is $\textsc{PTime}$[5] $C \geq 0$ is undecidable[6] $C = 0$ is $\textsc{PSpace}$[7]

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

Decision Procedures

implementation right there

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

- $A = B \iff [A - B] = 0$ holds if all runs of B are **eventually constant** as for $A^\star$ and $\top$

$C \leq 0$ is PTime[5] $C \geq 0$ is undecidable[6] $C = 0$ is PSpace[7]

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

In a nutshell

	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	EXPSPACE \ PSPACE-hard	$O(1)$
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

In a nutshell

Quantitative Automata Kit

	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	EXPSPACE \ PSPACE-hard	$O(1)$
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**	$O(1)$

Thank you

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