Quantitative Language Automata

Thomas A. Henzinger, Pavol Kebis, Nicolas Mazzocchi, N. Ege Saraç

RP'25

published in CONCUR'25

Institute of Science and Technology Austria

STU
SLOVAK UNIVERSITY OF TECHNOLOGY IN BRATISLAVA

TL;DR

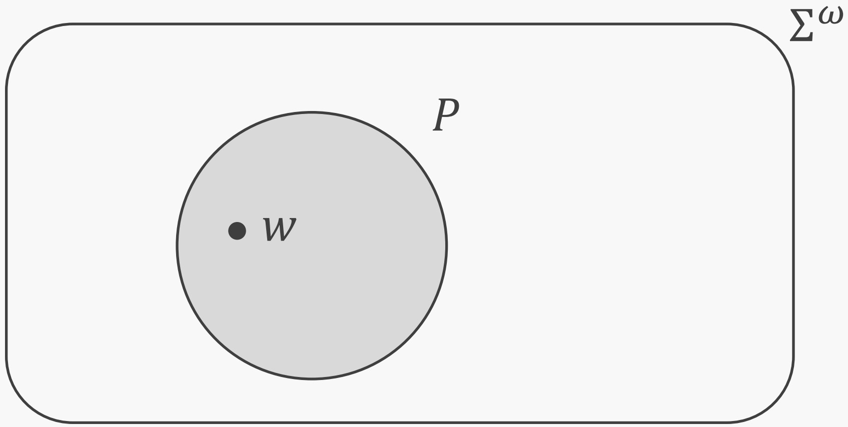
- Quantitative *word* automata (QWAs)
  - $\mathcal{A} : \Sigma^\omega \to \mathbb{D}$
  - $\mathcal{A}(w) = g_{\rho \in Runs(w)} f(\rho)$
- Quantitative *language* automata (QLAs)
  - $\mathbb{A} : 2^{\Sigma^\omega} \to \mathbb{D}$
  - $\mathbb{A}(L) = h_{w \in L}\, g_{\rho \in Runs(w)} f(\rho)$
- QLAs define *quantitative hyperproperties*
  - $\forall/\exists \rightarrow \sup/\inf/\cdots$
- No quantifier alternation
  - QLA problems reduce to QWA problems

Context and Motivation
Boolean Trace Properties

$$P \subseteq \Sigma^\omega$$

For every *execution* of…

- a server, *is it true* that each request is eventually granted?
- a drone, *is it true* that the designated path is never left?
- …



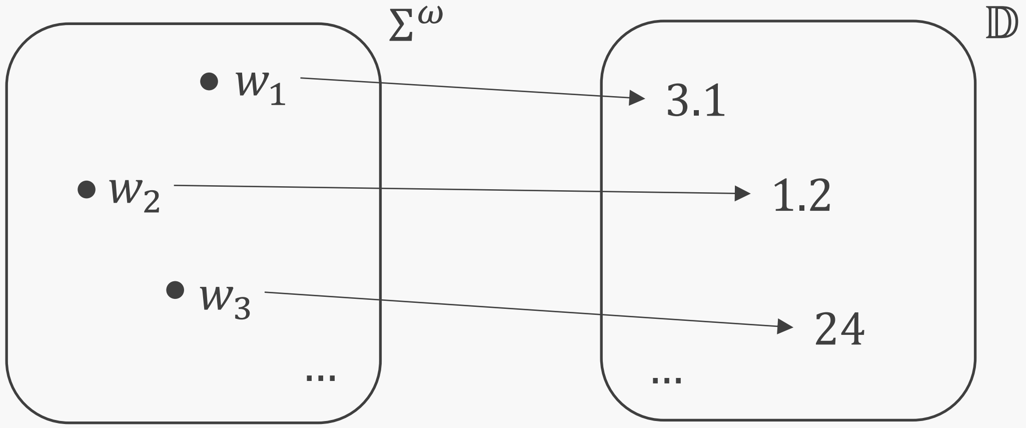
Context and Motivation

Quantitative Trace Properties [CDH08]

$$\Phi : \Sigma^\omega \to \mathbb{D}$$

Given an *execution* of…

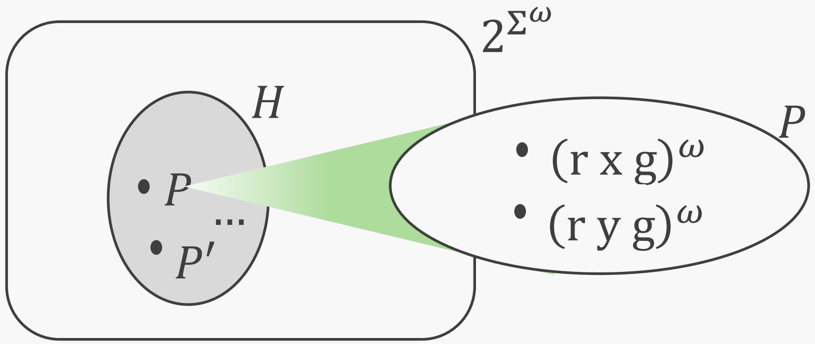
- a server, *what is* its average response time?
- a drone, *what is* the worst-case deviation from its designated path?
- …



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

Context and Motivation

Boolean Hyperproperties [CS08]



$$H \subseteq 2^{\Sigma^\omega}$$

For every *implementation* of…

- a server, *is it true* that every pair of executions with the same request pattern has the same grant pattern?

$$\forall \pi, \pi' \colon G(\mathrm{r}_\pi \leftrightarrow \mathrm{r}_{\pi'}) \rightarrow G(\mathrm{g}_\pi \leftrightarrow \mathrm{g}_{\pi'})$$

- a drone, *is it true* that for every high-wind execution there is a matching low-wind execution whose paths are ε-close?

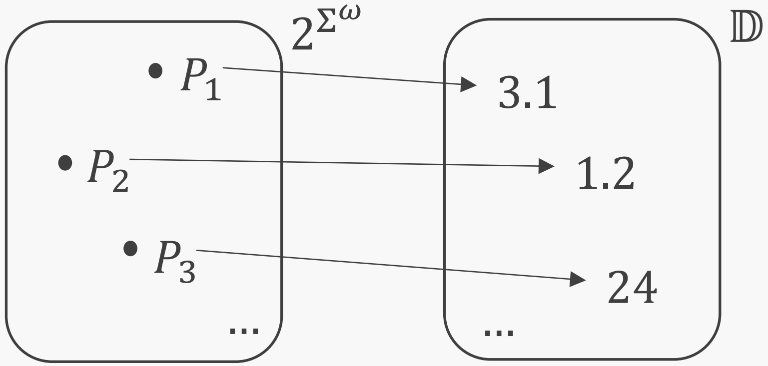
$$\forall \pi \colon G(\mathrm{hiWind}_\pi) \rightarrow \left(\exists \pi' \colon G(\mathrm{loWind}_{\pi'}) \wedge (\mathrm{tgt}_\pi \leftrightarrow \mathrm{tgt}_{\pi'}) \wedge G(\mathrm{close}_\varepsilon(\pi, \pi'))\right)$$

- …

Clarkson and Schneider, "Hyperproperties", CSF 2008.

Context and Motivation

Quantitative Hyperproperties



$$\Theta : 2^{\Sigma^\omega} \to \mathbb{D}$$

Given an *implementation* of…

- a server, *what is* its worst-case average response time?

$$P \mapsto \sup_{w \in P} AvgRespTime(w)$$

- a drone, *what is* the maximal distance between its high-wind runs and their low-wind equivalents?

$$P \mapsto \sup_{w \in P} \inf_{w' \in P} WindDist(w, w')$$

- …

Our Contribution

Quantitative Language Automata (QLAs):
the first specification framework for QHPs of reactive systems

(a)	Evaluation					Nonemptiness		
	$h = g$	$h \neq g$	$h = \mathbb{E}$	$h \in \{\mathsf{Inf}, \mathsf{Sup}\}$	$h = \mathbb{E}$	$h \in \{\mathsf{Inf}, \mathsf{Sup}, \mathbb{E}\}$		
	$\in \{\mathsf{Inf}, \mathsf{Sup}\}$	$\in \{\mathsf{Inf}, \mathsf{Sup}\}$	$g \in \{\mathsf{Inf}, \mathsf{Sup}\}$	$g = \mathbb{E}$	$g = \mathbb{E}$	$g = \mathsf{Sup}$	$g = \mathsf{Inf}$	$g = \mathbb{E}$
$f \in \{\mathsf{Inf}, \mathsf{Sup}, \mathsf{LimInf}, \mathsf{LimSup}\}$	PTIME	PSPACE	EXPTIME	Undecidable	PTIME	PTIME	PSPACE	Undecidable
$f \in \{\mathsf{LimInfAvg}, \mathsf{LimSupAvg}\}$	PTIME	Undecidable	Undecidable	Undecidable	PTIME	PTIME	Undecidable	Undecidable
$f = \mathsf{DSum}$	PTIME	Open-hard	Open-hard	Undecidable	PTIME	PTIME	Open-hard	Undecidable

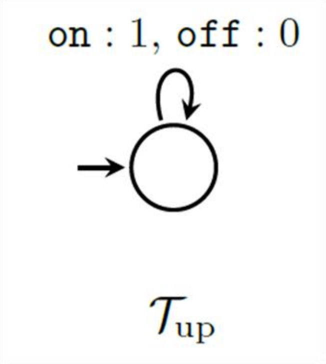
(b)	Evaluation	Nonemptiness	Universality
$h, g, f \in \{\mathsf{Inf}, \mathsf{Sup}, \mathsf{LimInf}, \mathsf{LimSup}\}$ and at least one of h or g is in $\{\mathsf{LimInf}, \mathsf{LimSup}\}$	PSPACE	PSPACE	PSPACE

Quantitative Word Automata (QWAs) [CDH08]

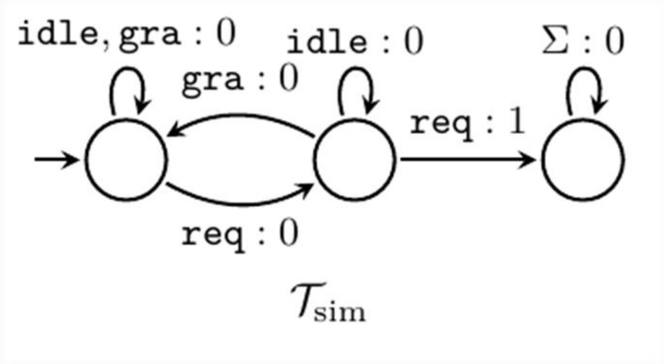
$\mathcal{A} = (g, f\ \mathcal{T})$ $\qquad \mathcal{A}(w) = g_{\rho \in Runs(w,\mathcal{T})} f(\rho)$

- $\mathcal{T}$: weighted labeled finite transition system
- f: run aggregator (a.k.a. value function) in {Inf, Sup, LimInf, LimSup, LimInfAvg, LimSupAvg, DSum}
- g: word aggregator (a.k.a. resolver) in {Inf, Sup, LimInf, LimSup, $\mathbb{E}$}

Example. $\mathcal{A}_1 = (g, \text{LimInfAvg}, \mathcal{T}_{\text{up}})$



Example. $\mathcal{A}_2 = (g, \text{DSum}_2, \mathcal{T}_{\text{sim}})$



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

Quantitative Language Automata (QLAs)

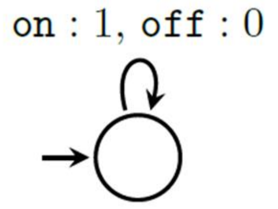
$\mathbb{A} = (h, \mathcal{A})$ $\qquad$ $\mathbb{A}(L) = h_{w \in L} \mathcal{A}(w)$

$\mathcal{A}$ → QWA

h → language aggregator in $\{\mathrm{Inf}, \mathrm{Sup}, \mathrm{LimInf}, \mathrm{LimSup}, \mathbb{E}\}$

Example (worst-case avg. uptime).

$\mathbb{A}_1 = (\mathrm{Inf}, \mathcal{A}_1)$



$\mathcal{A}_1$
(LimInfAvg)

$$\mathbb{A}_1(L) = \inf_{w \in L} \mathcal{A}_1(w)$$

Quantitative Language Automata (QLAs)

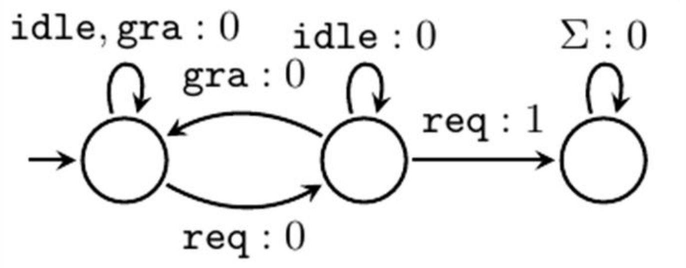
$\mathbb{A} = (h, \mathcal{A})$ $\qquad \mathbb{A}(L) = h_{w \in L} \mathcal{A}(w)$

QWA

language aggregator in $\{\mathrm{Inf}, \mathrm{Sup}, \mathrm{LimInf}, \mathrm{LimSup}, \mathbb{E}\}$

Example (model measuring).

$\mathbb{A}_2 = (\mathrm{Sup}, \mathcal{A}_2)$



$\mathcal{A}_2$
(DSum_2)

$$\mathbb{A}_2(L) = \sup_{w \in L} \mathcal{A}_2(w)$$
$$= \sup_{w \in L} \inf_{w' \in P} d_{Cantor}(w, w')$$

where $P =$ "no two pending req"

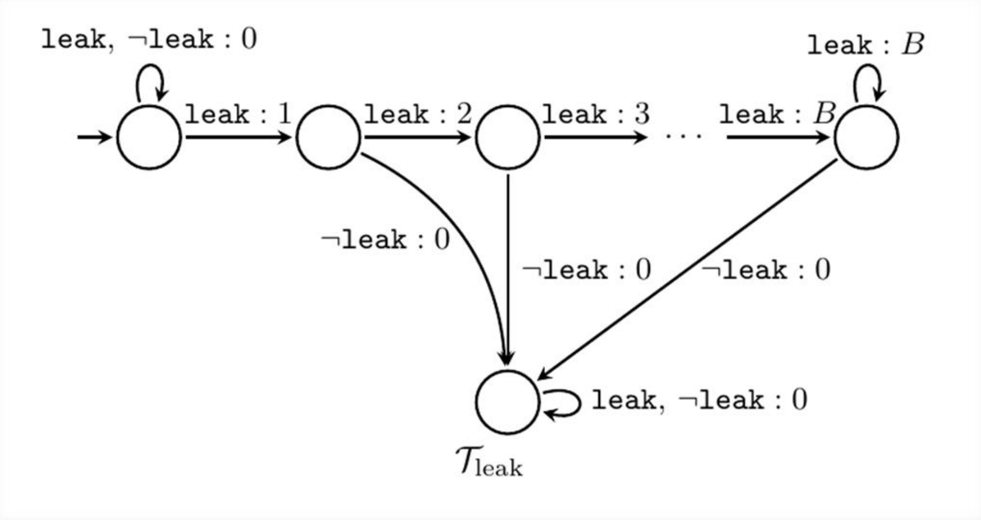
Quantitative Language Automata (QLAs)

Example (longest leaking block).

$$\mathbb{A}_3 = (\mathrm{Sup}, \mathcal{A}_3) \quad \mathcal{A}_3 = (\mathrm{Sup}, \mathrm{Sup}, \mathcal{T}_{\mathrm{leak}})$$

$$\Sigma = 2^{\{lo,hi,out,other\}} \qquad \Sigma' = \Sigma \times \Sigma$$

$$\mathrm{leak}(\sigma, \sigma') \coloneqq (\sigma_{lo} \leftrightarrow \sigma'_{lo}) \land (\sigma_{hi} \not\leftrightarrow \sigma'_{hi}) \land (\sigma_{out} \not\leftrightarrow \sigma'_{out})$$



$\mathcal{A}_3(w)$ = length of the longest leaking block in w (up to B)

$$L \subseteq \Sigma^\omega \to L' \subseteq {\Sigma'}^\omega$$

$$\mathbb{A}_3(L') = \sup_{w \in L'} \mathcal{A}(w) = \sup_{w \in L} \sup_{w' \in L} \mathcal{A}(w, w')$$

Core Problems

Given a QLA $\mathbb{A} = (h, \mathcal{A})$, a threshold $k \in \mathbb{Q}$, and $\sim \in \{>, \geq\}$.

1. **Evaluation**
   Given a nondeterministic Büchi automaton $\mathcal{B}$, compute $\mathbb{A}(L_{\mathcal{B}})$.
2. **Nonemptiness**
   Does $\mathbb{A}(L) \sim k$ hold for some nonempty $L \subseteq \Sigma^\omega$?
3. **Universality**
   Does $\mathbb{A}(L) \sim k$ hold for every nonempty $L \subseteq \Sigma^\omega$?

Evaluation

Given a QLA $\mathbb{A} = (h, \mathcal{A})$ and a nondeterministic Büchi automaton $\mathcal{B}$.

Compute $\mathbb{A}(L_{\mathcal{B}})$.

What happens when the value of an ω-regular language may not be realizable by a lasso word or any word?

Assume $g, h \in \{\mathrm{Inf}, \mathrm{Sup}\}$.

$f \in \cdots$	$\{\mathrm{Inf}, \mathrm{Sup}, \mathrm{LimInf}, \mathrm{LimSup}\}$	$\{\mathrm{LimInfAvg}, \mathrm{LimSupAvg}\}$	$\{\mathrm{DSum}\}$
Evaluation	PTime when $g = h$ PSpace when $g \neq h$	PTime when $g = h$ Incomputable when $g \neq h$	PTime when $g = h$ Open-hard when $g \neq h$

Nonemptiness and Universality

Given a QLA $\mathbb{A} = (h, \mathcal{A})$, a threshold $k \in \mathbb{Q}$, and $\sim \in \{>, \geq\}$.

Does $\mathbb{A}(L) \sim k$ hold for some (resp. every) nonempty $L \subseteq \Sigma^\omega$?

Assume $g = \mathrm{Sup}$ and $h \in \{\mathrm{Inf}, \mathrm{Sup}\}$.

$f \in \cdots$	$\{\mathrm{Inf}, \mathrm{Sup}, \mathrm{LimInf}, \mathrm{LimSup}\}$	$\{\mathrm{LimInfAvg}, \mathrm{LimSupAvg}\}$	$\{\mathrm{DSum}\}$
Nonemptiness	PTime	PTime	PTime
Universality	PSpace	Undecidable	Open-hard

Finite-state Universality

Are extreme values realizable or approximable by lasso words?

$\inf_{w \in \Sigma^\omega} \mathcal{A}(w)$

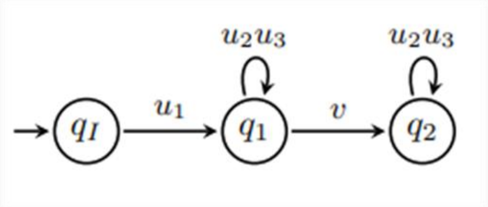
- Consider a QLA $\mathbb{A} = (h, \mathcal{A})$ and a threshold $k \in \mathbb{Q}$.
  If for every $\varepsilon > 0$ there is lasso word w such that $\mathcal{A}(w) < \perp_{\mathcal{A}} + \varepsilon$,
  then $\mathbb{A}(L) \geq k$ for all L iff $\mathbb{A}(L) \geq k$ for all ω-regular L.

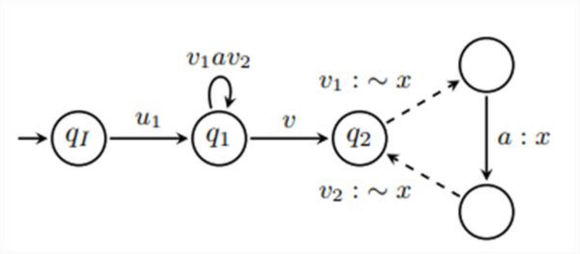
- For every $\varepsilon > 0$ there is lasso word w such that $\mathcal{A}(w) < \perp_{\mathcal{A}} + \varepsilon$.
  - $\mathcal{A} = (\mathrm{Sup}, \mathrm{LimInfAvg}, \mathcal{T})$ False
  - $\mathcal{A} = (\mathrm{Sup}, \mathrm{LimSupAvg}, \mathcal{T})$ True

Limit Aggregators

How to decide if
- a word w has infinitely many runs of value v?
- a language L has infinitely many words of value v?

LimInf and LimSup as word and language aggregators.





Solution: Characterize the patterns in quantitative automata that capture when a value is infinitely realizable (similar to characterizing ambiguity in boolean word automata [WS91, LP18]).

Weber and Seidl, "On the degree of ambiguity of finite automata", TCS, 1991.
Löding and Pirogov, "On finitely ambiguous Büchi automata", DLT 2018.

Conclusion

Quantitative Language Automata (QLAs):
the first specification framework for QHPs of reactive systems

(a)	Evaluation					Nonemptiness		
						$h \in \{\mathsf{Inf}, \mathsf{Sup}, \mathbb{E}\}$		
	$h = g \in \{\mathsf{Inf}, \mathsf{Sup}\}$	$h \neq g \in \{\mathsf{Inf}, \mathsf{Sup}\}$	$h = \mathbb{E}$, $g \in \{\mathsf{Inf}, \mathsf{Sup}\}$	$h \in \{\mathsf{Inf}, \mathsf{Sup}\}$, $g = \mathbb{E}$	$h = \mathbb{E}$, $g = \mathbb{E}$	$g = \mathsf{Sup}$	$g = \mathsf{Inf}$	$g = \mathbb{E}$
$f \in \{\mathsf{Inf}, \mathsf{Sup}, \mathsf{LimInf}, \mathsf{LimSup}\}$	PTime	PSpace	ExpTime	Undecidable	PTime	PTime	PSpace	Undecidable
$f \in \{\mathsf{LimInfAvg}, \mathsf{LimSupAvg}\}$	PTime	Undecidable	Undecidable	Undecidable	PTime	PTime	Undecidable	Undecidable
$f = \mathsf{DSum}$	PTime	Open-hard	Open-hard	Undecidable	PTime	PTime	Open-hard	Undecidable

(b)	Evaluation	Nonemptiness	Universality
$h, g, f \in \{\mathsf{Inf}, \mathsf{Sup}, \mathsf{LimInf}, \mathsf{LimSup}\}$ and at least one of h or g is in $\{\mathsf{LimInf}, \mathsf{LimSup}\}$	PSpace	PSpace	PSpace

Future Work

- Quantifier alternation
- Alternative run aggregators

Thank you!

Related Work

- Robustness semantics of HyperSTL [NKJ+17]
  - $\forall v\colon \exists v'\colon G_{[0,2]}(v > 1) \rightarrow F_{[1,2]}(v' > 2)$
  - Only robustness
- HyperLTL with counting [FHT19]
  - $\forall \pi\colon \#\sigma.\, O\colon G(\pi =_I \sigma) \leq 2^c$
  - Expressively equivalent to HyperLTL
- Quantitative reasoning with predicate transformers [ZZK+24]
  - $\mathrm{whp}\, [C_{qif}](\mathbb{f}_{\ell=x}(h))$
  - Only for finite executions

Nguyen, Kapinski, Jin, Deshmukh, and Johnson, "Hyperproperties of real-valued signals", MEMOCODE 2017.
Finkbeiner, Hahn, and Torfah, "Model checking quantitative hyperproperties", CAV 2019.
Zhang, Zilberstein, Kaminski, and Silva, "Quantitative weakest hyper pre", OOPSLA 2024.

Core Challenges

1. **Evaluation**
   What happens when the value of an ω-regular language may not be realizable by a lasso word or any word?
2. **Finite-state nonemptiness/universality**
   Are extreme values realizable or approximable by lasso word?
3. **Limit word and language aggregators** $\mathrm{g}, \mathrm{h} \in \{\mathrm{LimInf}, \mathrm{LimSup}\}$
   How to decide if a word w has infinitely many runs of value v or a language L has infinitely many words of value v?

Core Problems

▸ **Proposition 4.2.** *Consider a QLA* $\mathbb{A} = (h, \mathcal{A})$ *with* $h \in \{\mathsf{Inf}, \mathsf{Sup}, \mathbb{E}\}$*, a rational* $k \in \mathbb{Q}$*, and* $\triangleright \in \{>, \geq\}$*.*

(a) *Unrestricted variant*

(i) *If* $h \neq \mathsf{Sup}$ *or* $\triangleright = >$*, then* $\mathbb{A}$ *is* $\triangleright$*-nonempty for* k *iff* $\mathcal{A}$ *is* $\triangleright$*-nonempty for* k*.*

(ii) *If* $h = \mathsf{Sup}$*, then* $\mathbb{A}$ *is* $\geq$*-nonempty for* k *iff* $\mathcal{A}$ *is approximate-nonempty for* k*.*

(b) *Finite-state variant*

(i) *If* $h = \mathsf{Sup}$*, then* $\mathbb{A}$ *is finite-state* $\triangleright$*-nonempty for* k *iff* $\mathbb{A}$ *is* $\triangleright$*-nonempty for* k*.*

(ii) *If* $h = \mathsf{Inf}$*, then* $\mathbb{A}$ *is finite-state* $\triangleright$*-nonempty for* k *iff* $\mathcal{A}$ *is lasso-word* $\triangleright$*-nonempty for* k*.*

(iii) *If* $\top_{\mathcal{A}}$ *is achievable by a lasso word, then* $\mathbb{A}$ *is finite-state* $\triangleright$*-nonempty for* k *iff* $\mathbb{A}$ *is* $\triangleright$*-nonempty for* k *iff* $\mathcal{A}$ *is lasso-word* $\triangleright$*-nonempty for* k*.*

For universality, we have the duals where we exchange Inf *with* Sup*,* $>$ *with* $\geq$ *, nonempty with universal, approximate-nonempty with approximate-universal, and* $\top_{\mathcal{A}}$ *with* $\bot_{\mathcal{A}}$*.*

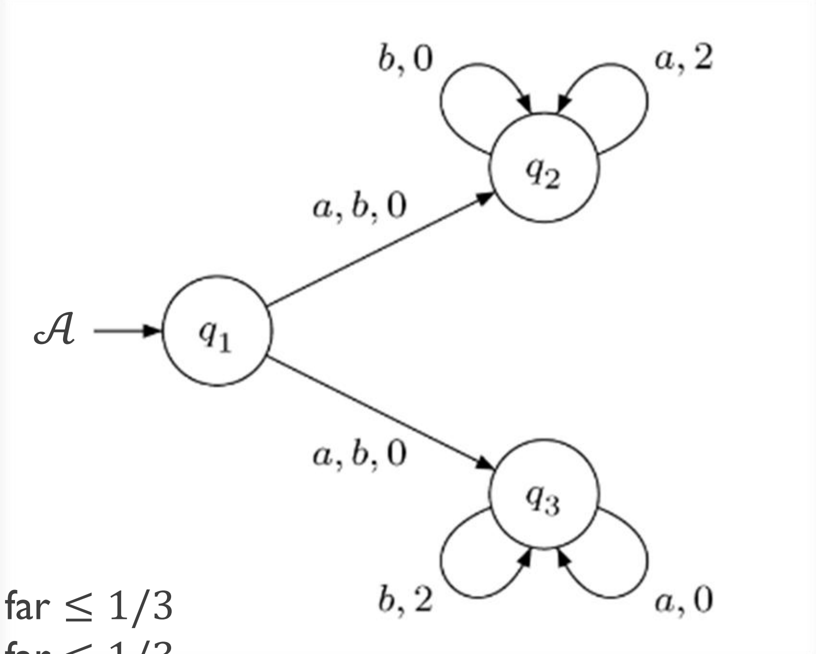
Approximating $\perp_{\mathcal{A}}$ by Lasso Words

Why it fails for LimInfAvg [CDH08]

- $\mathcal{A}(w) \geq 1$ for all lasso w

- $\mathcal{A}(w') < 1$ for some non-lasso w'

$$w' = u_0 u_1 u_2 \dots$$
$$u_0 = \epsilon$$
$$u_i = \alpha_i \beta_i$$



α_i: sufficiently long block of a's s.t. the b-density so far $\leq 1/3$

β_i: sufficiently long block of b's s.t. the a-density so far $\leq 1/3$

$$\Rightarrow \mathcal{A}(w') \leq 2/3$$

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

Approximating $\bot_{\mathcal{A}}$ by Lasso Words

Why it works for $\mathrm{LimSupAvg}$

- Given a word w with value $< \bot_{\mathcal{A}} + \frac{\varepsilon}{4}$,
  all sufficiently long prefixes have every run's average $< \bot_{\mathcal{A}} + \frac{\varepsilon}{2}$.
  (Otherwise, contradiction to word's value)
- Pick two prefixes $u_1 \prec u_2 \prec w$ reaching the same state set,
  and pump the middle.
- Any run on the pumped block stays low average,
  so the lasso's $\mathrm{LimSupAvg}$ stays $<\bot_{\mathcal{A}} + \varepsilon$.
- $\Rightarrow$ For QLAs with nondeterministic $\mathrm{LimSupAvg}$-automata,
  unrestricted $\geq$-universality = finite-state $\geq$-universality

Approximating $\perp_{\mathcal{A}}$ by Lasso Words

Corollary.

Let $f \in \{\text{LimSupAvg}, \text{LimInfAvg}\}$.

Given $\mathcal{A} = (\text{Sup}, f, \mathcal{T})$ and $k \in \mathbb{Q}$,
checking whether $\mathcal{A}(w) \geq k$ for every lasso word w is undecidable.

$\{\text{LimSupAvg}, \text{LimInfAvg}\} \times \{\text{All words}, \text{Lasso words}\} \times \{>, \geq\}$

- Every other combination here was proved undecidable [DDG+10, HPP+18]

Degorre, Doyen, Gentilini, Raskin, and Toruńczyk, "Energy and mean-payoff games with imperfect information", CSL 2010.
Hunter, Pauly, Pérez, and Raskin, "Mean-payoff games with partial observation", TCS, 2018.

Evaluation

Given a QLA $\mathbb{A} = (h, \mathcal{A})$ and an NBA $\mathcal{B}$.

Compute $\mathbb{A}(L_\mathcal{B})$.

Is there a word w such that $\mathbb{A}(L_\mathcal{B}) = \mathcal{A}(w)$?

$f \in \cdots$	$\{\mathrm{Inf}, \mathrm{Sup}, \mathrm{LimInf}, \mathrm{LimSup}\}$	$\{\mathrm{LimInfAvg}, \mathrm{LimSupAvg}\}$	$\{\mathrm{DSum}\}$
	$w \in L_\mathcal{B}$ and lasso	$w \in L_\mathcal{B}$ when $g = h$	$w \in \mathrm{Safe}(L_\mathcal{B})$ when $g = h$
	PTime when $g = h$ PSpace when $g \neq h$	PTime when $g = h$ Incomputable when $g \neq h$	PTime when $g = h$ Open-hard when $g \neq h$