CONCUR 2024 – Calgary Canada

Strategic Dominance: A New Preorder for Nondeterministic Processes

Thomas A. Henzinger ‡

Nicolas Mazzocchi † ‡

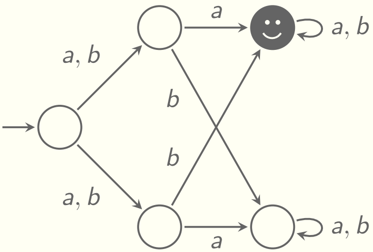
N. Ege Saraç ‡

† Slovak University of Technology, Slovakia

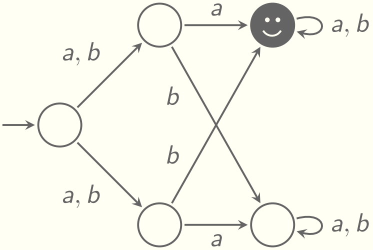
‡ Institute of Science and Technology, Austria

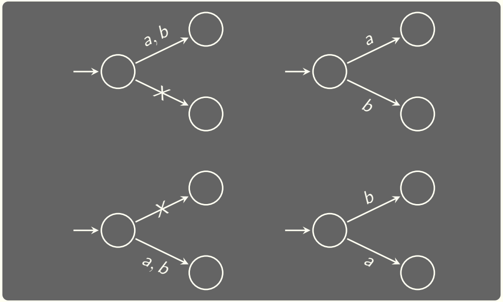
This talk is supported by the ERC-2020-AdG 101020093

Resolving non-determinism

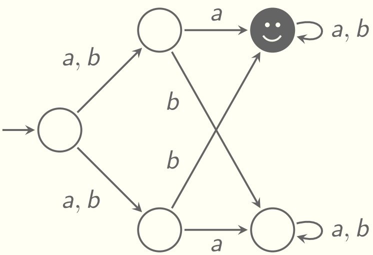


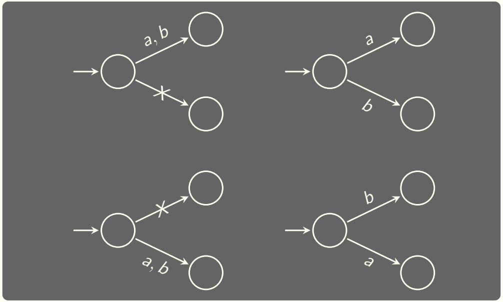
Resolving non-determinism





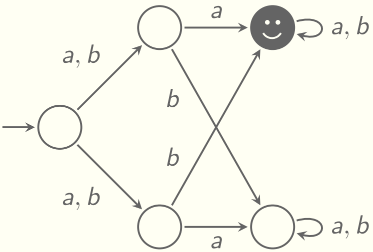
Resolving non-determinism

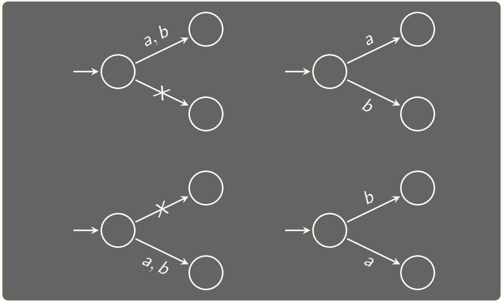




- $\forall w \in \Sigma^\omega : \exists f \in R(\mathcal{A}) :$ ☺ True
- $\exists f \in R(\mathcal{A}) : \forall w \in \Sigma^\omega :$ ☺ False

Resolving non-determinism





- $\forall w \in \Sigma^\omega : \exists f \in R(\mathcal{A}) :$ ☺ True
- $\exists f \in R(\mathcal{A}) : \forall w \in \Sigma^\omega :$ ☺ False

$\exists f : \forall w :$ ☺ $\implies \forall w : \exists f :$ ☺

Motivating Problems

Trace Inclusion and Simulation

Inclusion of linear-time properties and branching-time properties respectively

History Determinism

Can the non-determinism of a given automaton be expressed by a single resolver?

Inclusion of Hyperproperties

For two set of properties given by non-deterministic automata, is one subset of the another?

Safety

Is the properties given by an automaton safe?

Motivating Problems

Trace Inclusion and Simulation

Inclusion of linear-time properties and branching-time properties respectively

History Determinism

Can the non-determinism of a given automaton be expressed by a single resolver?

Inclusion of Hyperproperties

For two set of properties given by non-deterministic automata, is one subset of the another?

Safety

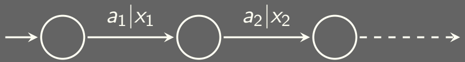
Is the properties given by an automaton safe?

Contribution

One algorithm that solves them all

Automata and Resolvers

Runs



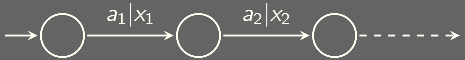
Input: $w = a_1 a_2 \dots$ Output: $x = \mathrm{Val}(x_1 x_2 \dots)$

Value function Val

- Inf (safety)
- Sup (reachability)
- LimInf (co-Büchi)
- LimSup (Büchi)

Automata and Resolvers

Runs

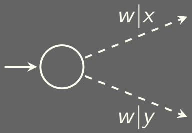


Input: $w = a_1 a_2 \ldots$ Output: $x = \mathsf{Val}(x_1 x_2 \ldots)$

Value function Val

- Inf (safety)
- Sup (reachability)
- LimInf (co-Büchi)
- LimSup (Büchi)

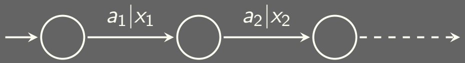
Non-determinism



sup $\{$values of runs over $w\}$

Automata and Resolvers

Runs



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

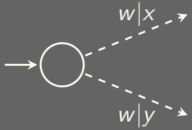
Resolvers

- $f\colon \mathsf{Edges}^*(\mathcal{A}) \times \Sigma \to \mathsf{State}(\mathcal{A})$
- $\forall w \in \Sigma^\omega\colon \forall f \in R(\mathcal{A})\colon \mathcal{A}^f(w) \in \mathsf{Edges}^\omega(\mathcal{A})$

Value function Val

- Inf (safety)
- Sup (reachability)
- LimInf (co-Büchi)
- LimSup (Büchi)

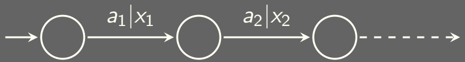
Non-determinism



sup $\{$values of runs over $w\}$

Automata and Resolvers

Runs



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

Resolvers

- $f : \mathsf{Edges}^*(\mathcal{A}) \times \Sigma \to \mathsf{State}(\mathcal{A})$
- $\forall w \in \Sigma^\omega : \forall f \in R(\mathcal{A}) : \mathcal{A}^f(w) \in \mathsf{Edges}^\omega(\mathcal{A})$

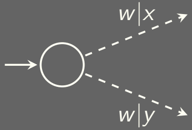
Trace Inclusion

$$\forall w \in \Sigma^\omega : \mathcal{A}^{\mathsf{sup}}(w) \leq \mathcal{B}^{\mathsf{sup}}(w)$$

Value function Val

- Inf (safety)
- Sup (reachability)
- LimInf (co-Büchi)
- LimSup (Büchi)

Non-determinism



sup {values of runs over w}

Trace Inclusion

Resolver Expressiblity

- $\forall w \in \Sigma^\omega : \mathcal{A}^{\mathsf{sup}}(w) \leq \mathcal{B}^{\mathsf{sup}}(w)$ $\qquad \mathcal{A} \subseteq \mathcal{B}$
- $\forall w \in \Sigma^\omega \quad \begin{matrix} \exists f \in R(\mathcal{A}) \colon \forall f' \in R(\mathcal{A}) \colon \mathcal{A}^f(w) \geq \mathcal{A}^{f'}(w) \\ \exists g \in R(\mathcal{B}) \colon \forall g' \in R(\mathcal{B}) \colon \mathcal{B}^g(w) \geq \mathcal{B}^{g'}(w) \end{matrix} \quad \mathcal{A}^f(w) \leq \mathcal{B}^g(w)$

Trace Inclusion

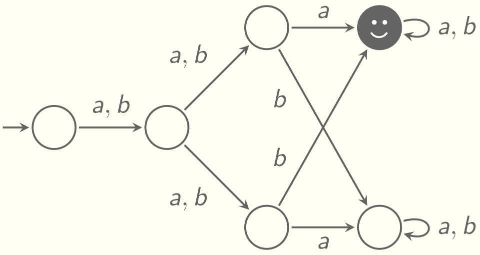
Resolver Expressiblity

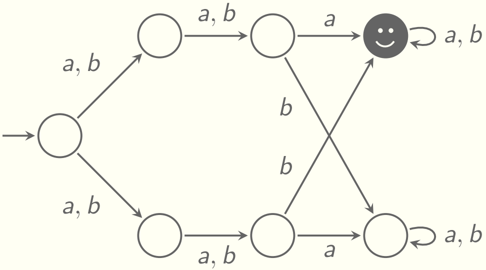
- $\forall w \in \Sigma^\omega : \mathcal{A}^{\mathsf{sup}}(w) \leq \mathcal{B}^{\mathsf{sup}}(w)$ $\qquad \mathcal{A} \subseteq \mathcal{B}$
- $\forall w \in \Sigma^\omega \quad \begin{matrix} \exists f \in R(\mathcal{A}) : \forall f' \in R(\mathcal{A}) : \mathcal{A}^f(w) \geq \mathcal{A}^{f'}(w) \\ \exists g \in R(\mathcal{B}) : \forall g' \in R(\mathcal{B}) : \mathcal{B}^g(w) \geq \mathcal{B}^{g'}(w) \end{matrix} \quad \mathcal{A}^f(w) \leq \mathcal{B}^g(w)$

Thm: Deciding Trace Inclusion

$$\begin{aligned} \mathcal{A} \subseteq \mathcal{B} \iff & \forall w \in \Sigma^\omega : \forall f \in R(\mathcal{A}) : \exists g \in R(\mathcal{B}) : \mathcal{A}^f(w) \leq \mathcal{B}^g(w) \\ \iff & \forall w \in \Sigma^\omega : \exists g \in R(\mathcal{B}) : \forall f \in R(\mathcal{A}) : \mathcal{A}^f(w) \leq \mathcal{B}^g(w) \end{aligned}$$

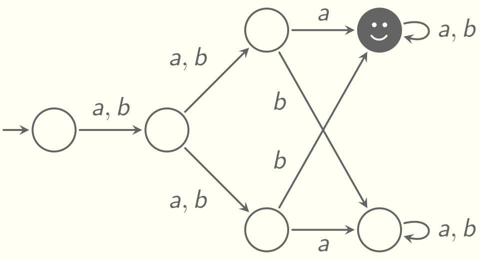
Word Blindness

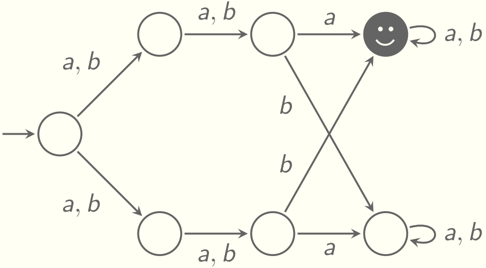




- $\forall f \in R(\mathcal{A}) : \exists g \in R(\mathcal{B}) : \forall w \in \Sigma^\omega : \mathcal{A}^f(w) \leq \mathcal{B}^g(w)$ $\iff$ $\mathcal{A} \trianglelefteq \mathcal{B}$ True
- $\exists g \in R(\mathcal{B}) : \forall f \in R(\mathcal{A}) : \forall w \in \Sigma^\omega : \mathcal{A}^f(w) \leq \mathcal{B}^g(w)$ $\iff$ $\mathcal{A} \underline{\blacktriangleleft} \mathcal{B}$ False

Word Blindness

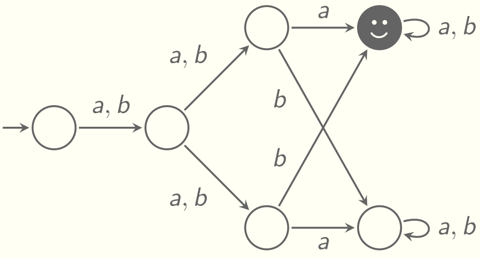


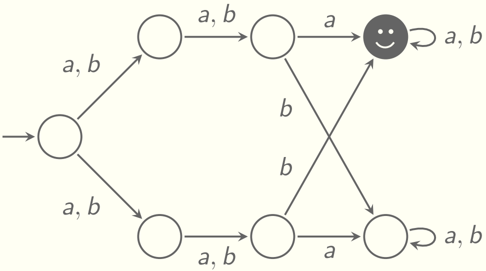


- $\forall f \in R(\mathcal{A}) \colon \exists g \in R(\mathcal{B}) \colon \forall w \in \Sigma^\omega \colon \mathcal{A}^f(w) \leq \mathcal{B}^g(w) \iff \mathcal{A} \trianglelefteq \mathcal{B}$ True
- $\exists g \in R(\mathcal{B}) \colon \forall f \in R(\mathcal{A}) \colon \forall w \in \Sigma^\omega \colon \mathcal{A}^f(w) \leq \mathcal{B}^g(w) \iff \mathcal{A} \blacktriangleleft\!\!\underline{\ } \mathcal{B}$ False

$\blacktriangleleft\!\!\underline{\ } \implies \trianglelefteq \implies \subseteq$

Word Blindness





- $\forall f \in R(\mathcal{A}) : \exists g \in R(\mathcal{B}) : \forall w \in \Sigma^\omega : \mathcal{A}^f(w) \leq \mathcal{B}^g(w) \iff \mathcal{A} \trianglelefteq \mathcal{B}$ True
- $\exists g \in R(\mathcal{B}) : \forall f \in R(\mathcal{A}) : \forall w \in \Sigma^\omega : \mathcal{A}^f(w) \leq \mathcal{B}^g(w) \iff \mathcal{A} \,\underline{\blacktriangleleft}\, \mathcal{B}$ False

Thm: $\mathcal{A} \,\underline{\blacktriangleleft}\, \mathcal{A} \iff \mathcal{A}$ is history deterministic

$\underline{\blacktriangleleft} \implies \trianglelefteq \implies \subseteq$

Simulation

Definition: Quantitative simulation turn-based game $\preceq$

1. a configuration is $(p, q) \in \mathsf{State}(\mathcal{A}) \times \mathsf{State}(\mathcal{B})$, the game starts with initial states
2. the antagonist chooses a transition $(p, a, p') \in \mathsf{Edge}(\mathcal{A})$
3. the protagonist chooses a transition $(q, a, q') \in \mathsf{Edge}(\mathcal{B})$
4. the new configuration is $(p', q') \in \mathsf{State}(\mathcal{A}) \times \mathsf{State}(\mathcal{B})$

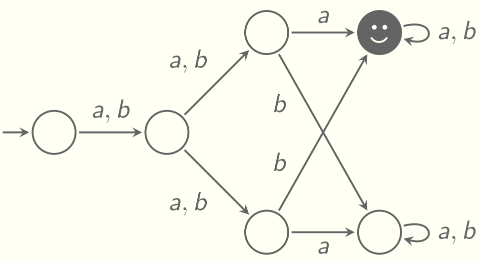
- The winner is the player with highest run value

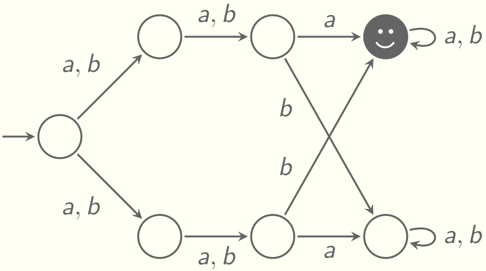
Simulation

Definition: Quantitative simulation turn-based game $\preceq$

1. a configuration is $(p, q) \in \mathrm{State}(\mathcal{A}) \times \mathrm{State}(\mathcal{B})$, the game starts with initial states
2. the antagonist chooses a transition $(p, a, p') \in \mathrm{Edge}(\mathcal{A})$
3. the protagonist chooses a transition $(q, a, q') \in \mathrm{Edge}(\mathcal{B})$
4. the new configuration is $(p', q') \in \mathrm{State}(\mathcal{A}) \times \mathrm{State}(\mathcal{B})$

- The winner is the player with highest run value



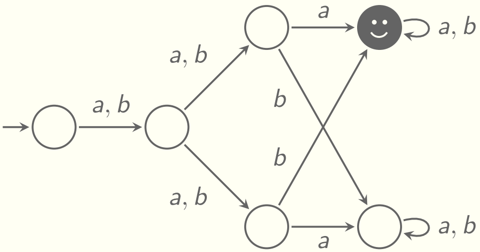


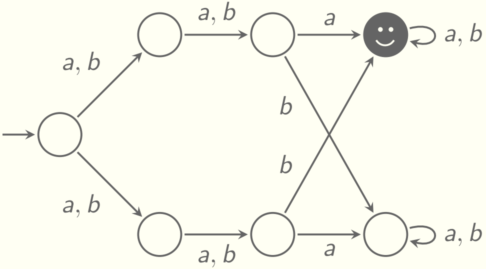
Simulation

Definition: Quantitative simulation turn-based game $\preceq \neq \trianglelefteq$

1. a configuration is $(p, q) \in \text{State}(\mathcal{A}) \times \text{State}(\mathcal{B})$, the game starts with initial states
2. the antagonist chooses a transition $(p, a, p') \in \text{Edge}(\mathcal{A})$
3. the protagonist chooses a transition $(q, a, q') \in \text{Edge}(\mathcal{B})$
4. the new configuration is $(p', q') \in \text{State}(\mathcal{A}) \times \text{State}(\mathcal{B})$

- The winner is the player with highest run value



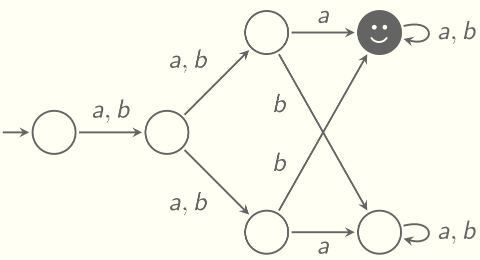


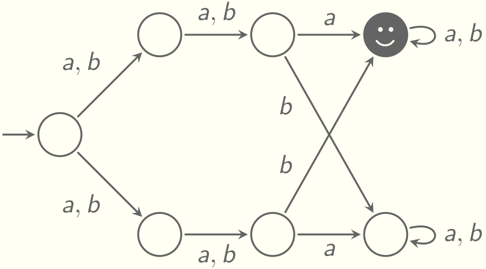
Simulation

Definition: Quantitative simulation turn-based game $\blacktriangleleft \neq \preceq \neq \trianglelefteq$

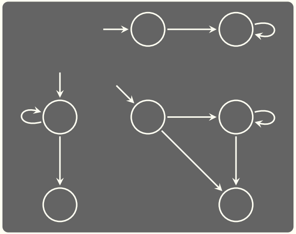
1. a configuration is $(p, q) \in \text{State}(\mathcal{A}) \times \text{State}(\mathcal{B})$, the game starts with initial states
2. the antagonist chooses a transition $(p, a, p') \in \text{Edge}(\mathcal{A})$
3. the protagonist chooses a transition $(q, a, q') \in \text{Edge}(\mathcal{B})$
4. the new configuration is $(p', q') \in \text{State}(\mathcal{A}) \times \text{State}(\mathcal{B})$

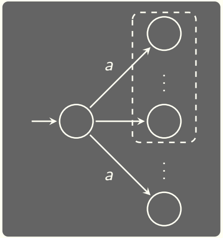
- The winner is the player with highest run value



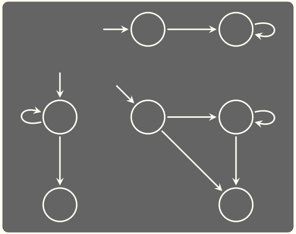


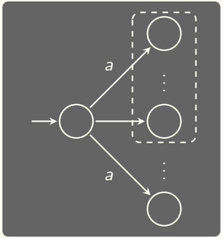
Partial Resolvers and Products





Partial Resolvers and Products

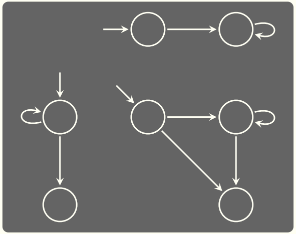


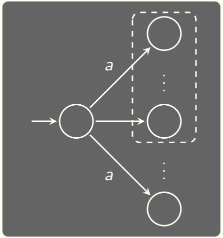


Combining Partial Resolvers

- $f : \text{Edges}^*(\mathcal{A} \times \mathcal{B}) \times \Sigma \to \text{State}(\mathcal{A})$
- $g : \text{Edges}^*(\mathcal{A} \times \mathcal{B}) \times \Sigma \to \text{State}(\mathcal{B})$
- $[\mathcal{A} \times_1 \mathcal{B}]^{\{f,g\}}$ has weights of $\mathcal{A}$
- $[\mathcal{A} \times_2 \mathcal{B}]^{\{f,g\}}$ has weights of $\mathcal{B}$

Partial Resolvers and Products



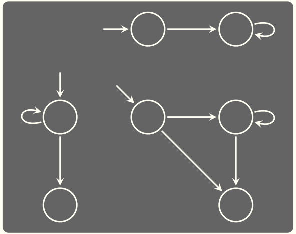


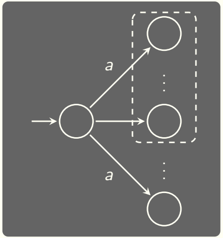
Combining Partial Resolvers

- $f : \text{Edges}^*(\mathcal{A} \times \mathcal{B}) \times \Sigma \to \text{State}(\mathcal{A})$
- $g : \text{Edges}^*(\mathcal{A} \times \mathcal{B}) \times \Sigma \to \text{State}(\mathcal{B})$
- $[\mathcal{A} \times_1 \mathcal{B}]^{\{f,g\}}$ has weights of $\mathcal{A}$
- $[\mathcal{A} \times_2 \mathcal{B}]^{\{f,g\}}$ has weights of $\mathcal{B}$

- $\forall f \in R_1(\mathcal{A}, \mathcal{B})$: $\exists g \in R_2(\mathcal{A}, \mathcal{B})$: $\forall w \in \Sigma^\omega$: $[\mathcal{A} \times_1 \mathcal{B}]^{\{f,g\}}(w) \leq [\mathcal{A} \times_2 \mathcal{B}]^{\{f,g\}}(w)$ $\trianglelefteq_\times$
- $\exists g \in R_2(\mathcal{A}, \mathcal{B})$: $\forall f \in R_1(\mathcal{A}, \mathcal{B})$: $\forall w \in \Sigma^\omega$: $[\mathcal{A} \times_1 \mathcal{B}]^{\{f,g\}}(w) \leq [\mathcal{A} \times_2 \mathcal{B}]^{\{f,g\}}(w)$ $\blacktriangleleft_\times$

Partial Resolvers and Products





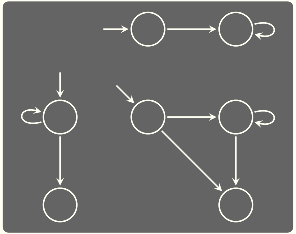
Combining Partial Resolvers

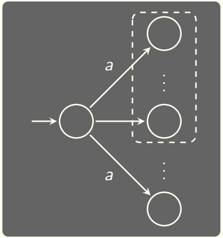
- $f\colon \text{Edges}^*(\mathcal{A}\times\mathcal{B})\times\Sigma\to\text{State}(\mathcal{A})$
- $g\colon \text{Edges}^*(\mathcal{A}\times\mathcal{B})\times\Sigma\to\text{State}(\mathcal{B})$
- $[\mathcal{A}\times_1\mathcal{B}]^{\{f,g\}}$ has weights of $\mathcal{A}$
- $[\mathcal{A}\times_2\mathcal{B}]^{\{f,g\}}$ has weights of $\mathcal{B}$

- $\forall f\in R_1(\mathcal{A},\mathcal{B})\colon \exists g\in R_2(\mathcal{A},\mathcal{B})\colon \forall w\in\Sigma^\omega\colon [\mathcal{A}\times_1\mathcal{B}]^{\{f,g\}}(w)\le[\mathcal{A}\times_2\mathcal{B}]^{\{f,g\}}(w)$ $\trianglelefteq_\times$
- $\exists g\in R_2(\mathcal{A},\mathcal{B})\colon \forall f\in R_1(\mathcal{A},\mathcal{B})\colon \forall w\in\Sigma^\omega\colon [\mathcal{A}\times_1\mathcal{B}]^{\{f,g\}}(w)\le[\mathcal{A}\times_2\mathcal{B}]^{\{f,g\}}(w)$ $\blacktriangleleft_\times$

Thm: $\preceq \iff \trianglelefteq_\times$

Partial Resolvers and Products





Combining Partial Resolvers

- $f : \text{Edges}^*(\mathcal{A} \times \mathcal{B}) \times \Sigma \to \text{State}(\mathcal{A})$
- $g : \text{Edges}^*(\mathcal{A} \times \mathcal{B}) \times \Sigma \to \text{State}(\mathcal{B})$
- $[\mathcal{A} \times_1 \mathcal{B}]^{\{f,g\}}$ has weights of $\mathcal{A}$
- $[\mathcal{A} \times_2 \mathcal{B}]^{\{f,g\}}$ has weights of $\mathcal{B}$

- $\forall f \in R_1(\mathcal{A},\mathcal{B})\colon \exists g \in R_2(\mathcal{A},\mathcal{B})\colon \forall w \in \Sigma^\omega\colon [\mathcal{A} \times_1 \mathcal{B}]^{\{f,g\}}(w) \leq [\mathcal{A} \times_2 \mathcal{B}]^{\{f,g\}}(w)$ $\quad \trianglelefteq_\times$
- $\exists g \in R_2(\mathcal{A},\mathcal{B})\colon \forall f \in R_1(\mathcal{A},\mathcal{B})\colon \forall w \in \Sigma^\omega\colon [\mathcal{A} \times_1 \mathcal{B}]^{\{f,g\}}(w) \leq [\mathcal{A} \times_2 \mathcal{B}]^{\{f,g\}}(w)$ $\quad \underline{\blacktriangleleft}_\times$

Thm: $\preceq \iff \trianglelefteq_\times$

$\underline{\blacktriangleleft} \implies \underline{\blacktriangleleft}_\times \implies \preceq \Leftrightarrow \trianglelefteq_\times \implies \trianglelefteq \implies \subseteq$

Hyperproperties and Safety

Definition

- Hyperproperty = Set of properties
- $H_{\mathcal{A}} = \{\mathcal{A}^f \mid f \in R(\mathcal{A})\}$
- Incomparable with HyperLTL

Hyperproperties and Safety

Definition

- Hyperproperty = Set of properties
- $H_{\mathcal{A}} = \{\mathcal{A}^f \mid f \in R(\mathcal{A})\}$
- Incomparable with HyperLTL

Thm: Deciding Hyper-Inclusion

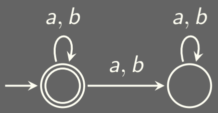
$$H_{\mathcal{A}} \subseteq H_{\mathcal{B}} \iff \forall f \in R(\mathcal{A}) \colon \exists g \in R(\mathcal{B}) \colon \forall w \in \Sigma^{\omega} \colon \mathcal{A}^f(w) = \mathcal{B}^g(w)$$

Hyperproperties and Safety

Definition

- Hyperproperty = Set of properties
- $H_\mathcal{A} = \{\mathcal{A}^f \mid f \in R(\mathcal{A})\}$
- Incomparable with HyperLTL

Automaton $\mathcal{S}$



Thm: Deciding Hyper-Inclusion

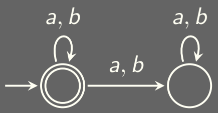
$$H_\mathcal{A} \subseteq H_\mathcal{B} \iff \forall f \in R(\mathcal{A}) \colon \exists g \in R(\mathcal{B}) \colon \forall w \in \Sigma^\omega \colon \mathcal{A}^f(w) = \mathcal{B}^g(w)$$

Hyperproperties and Safety

Definition

- Hyperproperty = Set of properties
- $H_{\mathcal{A}} = \{\mathcal{A}^f \mid f \in R(\mathcal{A})\}$
- Incomparable with HyperLTL

Automaton $\mathcal{S}$



Thm: Deciding Hyper-Inclusion

$$H_{\mathcal{A}} \subseteq H_{\mathcal{B}} \iff \forall f \in R(\mathcal{A}) \colon \exists g \in R(\mathcal{B}) \colon \forall w \in \Sigma^\omega \colon \mathcal{A}^f(w) = \mathcal{B}^g(w)$$

Thm: Deciding Safety

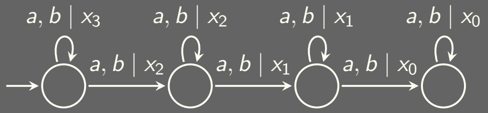
$$\mathcal{A} \text{ safe} \Leftrightarrow \exists g \in R(\mathcal{S}) \colon \forall w \in \Sigma^\omega \colon \exists f \in R(\mathcal{A}) \colon \forall f' \in R(\mathcal{A}) \colon \mathcal{A}^f(w) \geq \mathcal{A}^{f'}(w) \wedge \mathcal{A}^f(w) = \mathcal{S}^g(w)$$

Hyperproperties and Safety

Definition

- Hyperproperty = Set of properties
- $H_{\mathcal{A}} = \{\mathcal{A}^f \mid f \in R(\mathcal{A})\}$
- Incomparable with HyperLTL

Automaton $\mathcal{S}$



Thm: Deciding Hyper-Inclusion

$$H_{\mathcal{A}} \subseteq H_{\mathcal{B}} \iff \forall f \in R(\mathcal{A}) \colon \exists g \in R(\mathcal{B}) \colon \forall w \in \Sigma^\omega \colon \mathcal{A}^f(w) = \mathcal{B}^g(w)$$

Thm: Deciding Safety

$$\mathcal{A} \text{ safe} \Leftrightarrow \exists g \in R(\mathcal{S}) \colon \forall w \in \Sigma^\omega \colon \exists f \in R(\mathcal{A}) \colon \forall f' \in R(\mathcal{A}) \colon \mathcal{A}^f(w) \geq \mathcal{A}^{f'}(w) \wedge \mathcal{A}^f(w) = \mathcal{S}^g(w)$$

Resolver Logic

Definition

$$\Psi = \exists w \in \Sigma^\omega : \Psi' \mid \forall w \in \Sigma^\omega : \Psi' \mid \exists f \in R(\mathcal{A}) : \Psi' \mid \forall f \in R(\mathcal{A}) : \Psi' \mid \varphi$$

Word variables	$w \in W$ is interpreted over Σ^ω
Resolver variables	$f \in F_i$ is interpreted over $R(\mathcal{A}_i)$
Integer variables	$x \in X$ is interpreted over $\{\mathcal{A}_i^f(w) \mid f \in F_i, w \in W\}$

- $\mathcal{A}$ range over non-deterministic automata of a finite domain $\{\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_n\}$
- φ range over existential Presburger formulas, i.e., $\exists FO(\mathbb{Z}, \leq, +, 1)$

Resolver Logic

Definition

$$\Psi = \exists w \in \Sigma^\omega : \Psi' \mid \forall w \in \Sigma^\omega : \Psi' \mid \exists f \in R(\mathcal{A}) : \Psi' \mid \forall f \in R(\mathcal{A}) : \Psi' \mid \varphi$$

Word variables	$w \in W$ is interpreted over Σ^ω
Resolver variables	$f \in F_i$ is interpreted over $R(\mathcal{A}_i)$
Integer variables	$x \in X$ is interpreted over $\{\mathcal{A}_i^f(w) \mid f \in F_i, w \in W\}$

- $\mathcal{A}$ range over non-deterministic automata of a finite domain $\{\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_n\}$
- φ range over existential Presburger formulas, i.e., $\exists FO(\mathbb{Z}, \leq, +, 1)$

Thm: Model-checking a fixed formula Ψ over $\{\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_n\}$ is

- d-EXPTIME with $d > 0$ quantifier alternations,
- PTIME with no quantifier alternation

Summary

$$\underline{\blacktriangleleft} \implies \underline{\blacktriangleleft}_{\times} \implies \preceq \iff \trianglelefteq_{\times} \implies \trianglelefteq \implies \subseteq$$

Summary

$$\underline{\blacktriangleleft} \implies \underline{\blacktriangleleft}_\times \implies \underline{\prec} \Leftrightarrow \trianglelefteq_\times \implies \trianglelefteq \implies \subseteq$$

Motivating Problems

- Trace Inclusion
- Strategic Dominance
- Simulation
- History Determinism
- Hyperproperty Inclusion
- Safety
- Emptiness
- Universality

Provided Complexity

- 2 – EXPTIME
- 2 – EXPTIME
- 2 – EXPTIME
- EXPTIME
- 2 – EXPTIME
- 3 – EXPTIME
- PTIME
- 2 – EXPTIME

Best Known

- PSPACE
- PSPACE
- PTIME
- EXPTIME (for LimInf)
- PSPACE
- PSPACE
- PTIME
- PSPACE

Summary

$$\underline{\blacktriangleleft} \implies \underline{\blacktriangleleft}_{\times} \implies \preceq \Leftrightarrow \trianglelefteq_{\times} \implies \trianglelefteq \implies \subseteq$$

Motivating Problems	Provided Complexity	Best Known
Trace Inclusion	2 – ExpTime	PSpace
Strategic Dominance	2 – ExpTime	PSpace
Simulation	2 – ExpTime	PTime
History Determinism	ExpTime	ExpTime (for LimInf)
Hyperproperty Inclusion	2 – ExpTime	PSpace
Safety	3 – ExpTime	PSpace
Emptiness	PTime	PTime
Universality	2 – ExpTime	PSpace

Thank You