Regular Separability of WSTS

Wojciech Czerwiński[1], Sławomir Lasota[1], Roland Meyer[2],
Sebastian Muskalla[2], K Narayan Kumar[3], and Prakash Saivasan[2]

September 6, CONCUR 2018, Beijing

1 University of Warsaw, Poland
`{wczerwin,sl}@mimuw.edu.pl`

2 TU Braunschweig, Germany
`{roland.meyer,s.muskalla,p.saivasan}@tu-bs.de`

3 Chennai Mathematical Institute and UMI RELAX, India
`kumar@cmi.ac.in`

Separability

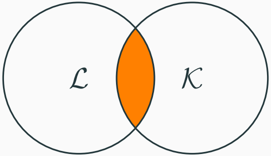
Separability

Given $\mathcal{L}, \mathcal{K} \subseteq \Sigma^*$ from class $\mathcal{F}$.
What is their relationship?

Separability

Given $\mathcal{L}, \mathcal{K} \subseteq \Sigma^*$ from class $\mathcal{F}$.
What is their relationship?

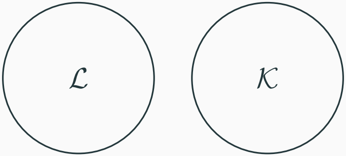
Case 1: $\mathcal{L} \cap \mathcal{K} \neq \varnothing$



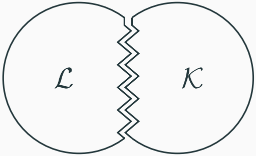
↳ study $\mathcal{L} \cap \mathcal{K}$

Separability

Case 2: $\mathcal{L} \cap \mathcal{K} = \varnothing$



vs.



Separability

Consider separability

<u>Separability of $\mathcal{F}$ by $\mathcal{S}$</u>

Given: Languages $\mathcal{L}, \mathcal{K} \subseteq \Sigma^*$ from $\mathcal{F}$

Decide: Is there $\mathcal{R} \subseteq \Sigma^*$ from $\mathcal{S}$ such that

$$\mathcal{L} \subseteq \mathcal{R}, \quad \mathcal{K} \cap \mathcal{R} = \emptyset?$$

Separability

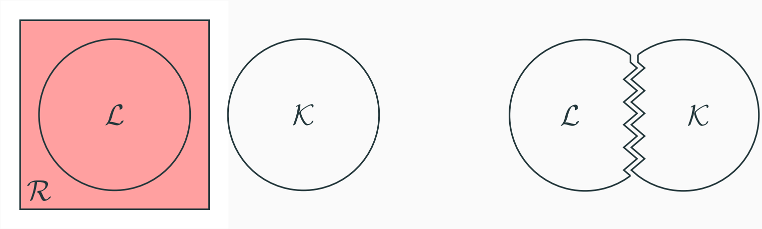
Consider separability

Separability of $\mathcal{F}$ by $\mathcal{S}$

Given: Languages $\mathcal{L}, \mathcal{K} \subseteq \Sigma^*$ from $\mathcal{F}$

Decide: Is there $\mathcal{R} \subseteq \Sigma^*$ from $\mathcal{S}$ such that

$$\mathcal{L} \subseteq \mathcal{R}, \quad \mathcal{K} \cap \mathcal{R} = \varnothing?$$



Consider separability

Separability of $\mathcal{F}$ by $\mathcal{S}$

Given: Languages $\mathcal{L}, \mathcal{K} \subseteq \Sigma^*$ from $\mathcal{F}$

Decide: Is there $\mathcal{R} \subseteq \Sigma^*$ from $\mathcal{S}$ such that

$$\mathcal{L} \subseteq \mathcal{R}, \quad \mathcal{K} \cap \mathcal{R} = \varnothing?$$

Commonly studied:

- $\mathcal{S} \subset \mathcal{F} = REG$

  e.g. $\mathcal{S}$ = star-free languages

  ↳ Separability is decidable [PZ16]

Separability

Consider separability

Separability of $\mathcal{F}$ by $\mathcal{S}$

Given: Languages $\mathcal{L}, \mathcal{K} \subseteq \Sigma^*$ from $\mathcal{F}$

Decide: Is there $\mathcal{R} \subseteq \Sigma^*$ from $\mathcal{S}$ such that

$$\mathcal{L} \subseteq \mathcal{R}, \quad \mathcal{K} \cap \mathcal{R} = \varnothing?$$

Commonly studied:

- $\mathcal{S} \subset \mathcal{F} = REG$
  e.g. $\mathcal{S}$ = star-free languages
  ↳ Separability is decidable [PZ16]
- $\mathcal{S} = REG \subset \mathcal{F}$
  Regular separability
  (related work in a second)

Regular separability

Regular separability of $\mathcal{F}$

Given: Languages $\mathcal{L}, \mathcal{K} \subseteq \Sigma^*$ from $\mathcal{F}$

Decide: Is there $\mathcal{R} \subseteq \Sigma^*$ regular such that

$$\mathcal{L} \subseteq \mathcal{R}, \quad \mathcal{K} \cap \mathcal{R} = \varnothing?$$

Observation:

Problem is symmetric in the input:

If $\quad \mathcal{L} \subseteq \mathcal{R}, \quad \mathcal{K} \cap \mathcal{R} = \varnothing,$

then $\quad \mathcal{K} \subseteq \overline{\mathcal{R}}, \quad \mathcal{L} \cap \overline{\mathcal{R}} = \varnothing.$

↳ Call $\mathcal{L}, \mathcal{K}$ regularly separable if separator $\mathcal{R}$ exists.

Regular separability of $\mathcal{F}$

Given: Languages $\mathcal{L}, \mathcal{K} \subseteq \Sigma^*$ from $\mathcal{F}$

Decide: Is there $\mathcal{R} \subseteq \Sigma^*$ regular such that

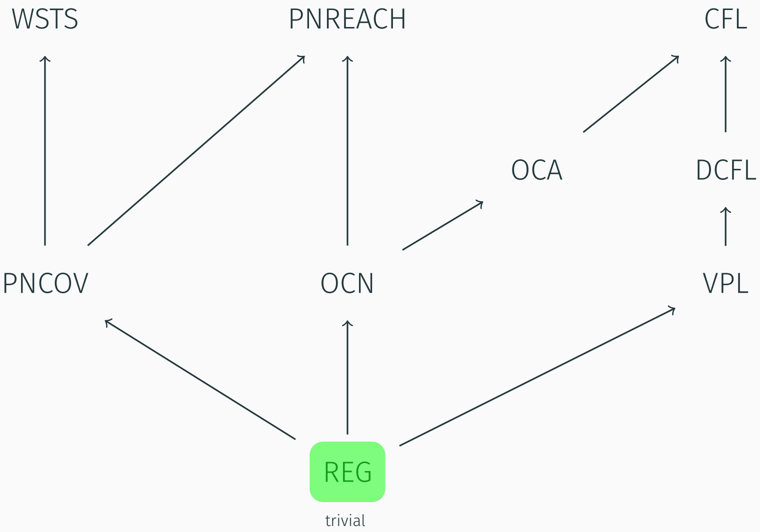
$$\mathcal{L} \subseteq \mathcal{R}, \quad \mathcal{K} \cap \mathcal{R} = \varnothing?$$

Disjointness is always a necessary condition for any kind of separability.

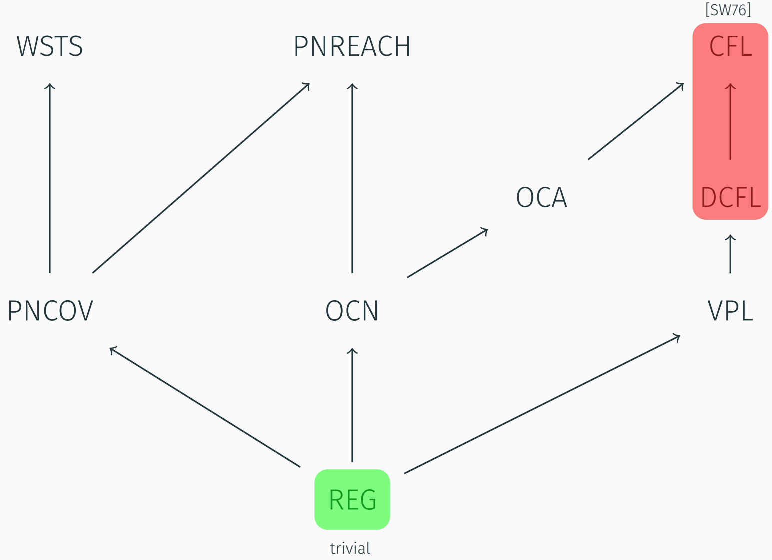
It is not always sufficient, consider

$$\mathcal{L} = a^n b^n, \quad \mathcal{K} = \overline{\mathcal{L}}\ .$$

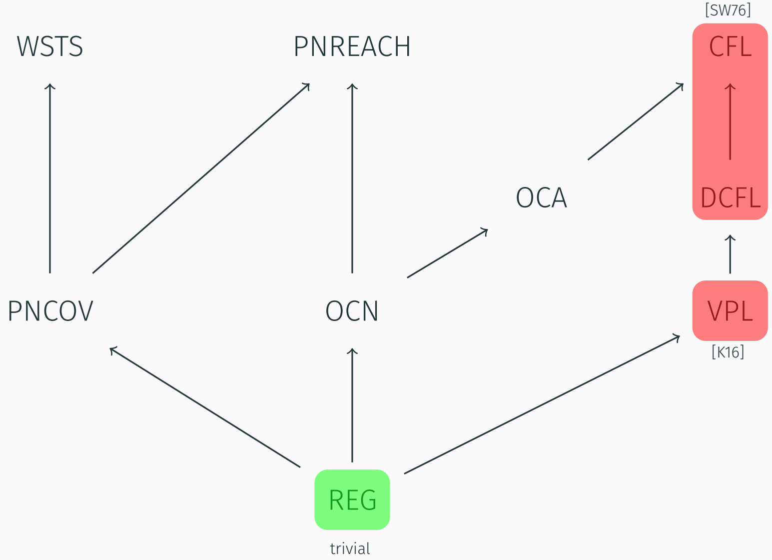
Regular separability - A map



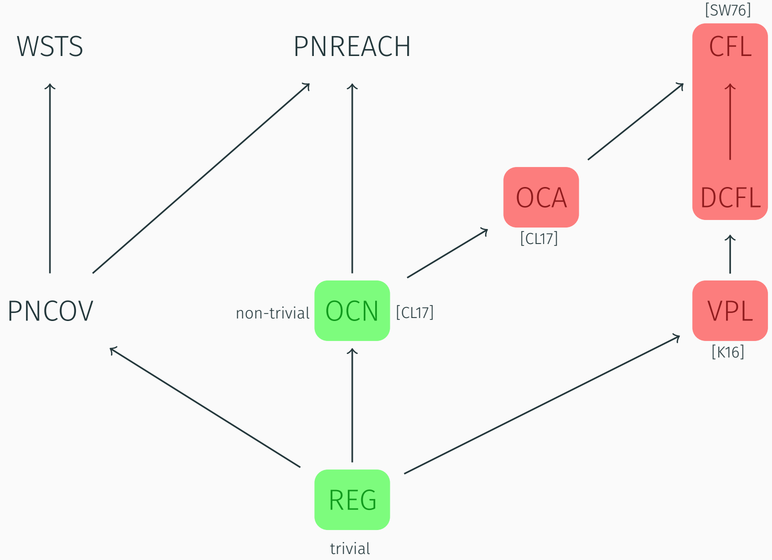
Regular separability - A map



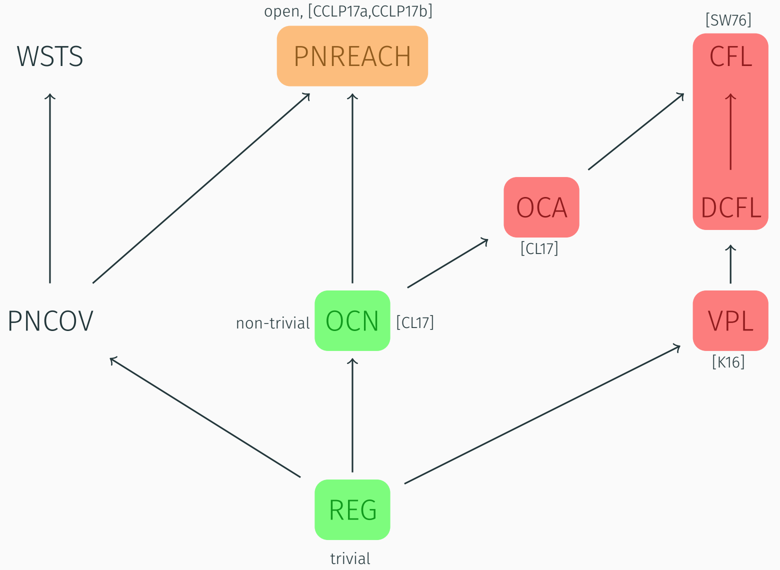
Regular separability - A map



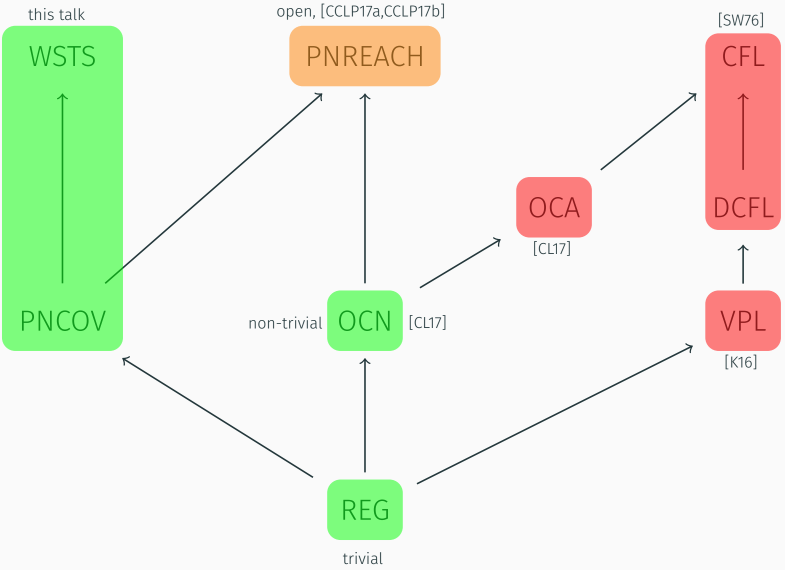
Regular separability - A map



Regular separability - A map



Regular separability - A map



Well-structured transition systems

Well quasi orders

Consider $(X, \leqslant)$ quasi order (reflexive, transitive)

Well quasi orders

Consider $(X, \leqslant)$ quasi order (reflexive, transitive)

$(S, \leqslant)$ well quasi order (wqo)

iff upward-closed sets have finitely many minimal elements

iff all antichains and descending chains are finite

Consider $(X, \leqslant)$ quasi order (reflexive, transitive)

	$(S, \leqslant)$ well quasi order (wqo)
iff	upward-closed sets have finitely many minimal elements
iff	all antichains and descending chains are finite

Lemma (Dickson's lemma)

$(\mathbb{N}^k, \leqslant^k)$ *is a well quasi order*

$$(1,2) \not\leqslant^2 (2,1) \leqslant^2 (2,2)$$

Well quasi orders

Consider $(X, \leqslant)$ quasi order (reflexive, transitive)

	$(S, \leqslant)$ well quasi order (wqo)
iff	upward-closed sets have finitely many minimal elements
iff	all antichains and descending chains are finite

Lemma (Dickson's lemma)

$(\mathbb{N}^k, \leqslant^k)$ *is a well quasi order*

$$(1,2) \not\leqslant^2 (2,1) \leqslant^2 (2,2)$$

Lemma (Higman's lemma)

$(\Sigma^*, \leqslant^*)$ *is a well quasi order*

RADAR $\leqslant^*$ ABRACADABRA

Well structured transiton systems

Consider a labeled version of well-structured transition systems (WSTS) [F87,ACJT96,FS01].

Well structured transiton systems

Consider a labeled version of well-structured transition systems (WSTS) [F87,ACJT96,FS01].

$$\mathcal{W} = (S, \leqslant, T, I, F)$$

$(S, \leqslant)$ states wqo

$T \subseteq S \times \Sigma \times S$ labeled transitions

$I \subseteq S$ initial states

$F \subseteq S$ final states, upward-closed

Well structured transiton systems

Consider a labeled version of well-structured transition systems (WSTS) [F87,ACJT96,FS01].

$$\mathcal{W} = (S, \leqslant, T, I, F)$$

- $(S, \leqslant)$ states wqo
- $T \subseteq S \times \Sigma \times S$ labeled transitions
- $I \subseteq S$ initial states
- $F \subseteq S$ final states, upward-closed
- Monotonicity / Simulation property:

$$\begin{array}{ccc} s' & \overset{a}{\dashrightarrow} & r' \ (\exists) \\ \rotatebox{90}{$\leqslant$} & & \rotatebox{90}{$\leqslant$} \\ s & \xrightarrow{a} & r \end{array}$$

Well structured transiton systems

Consider a labeled version of well-structured transition systems (WSTS) [F87,ACJT96,FS01].

$$\mathcal{W} = (S, \leqslant, T, I, F)$$

- $(S, \leqslant)$ states wqo
- $T \subseteq S \times \Sigma \times S$ labeled transitions
- $I \subseteq S$ initial states
- $F \subseteq S$ final states, upward-closed

Coverability language

$$\mathcal{L}(\mathcal{W}) = \left\{ w \in \Sigma^* \;\middle|\; c_i \xrightarrow{w} c_f \text{ for some } c_i \in I, c_f \in F \right\}$$

Consider a labeled version of well-structured transition systems (WSTS) [F87,ACJT96,FS01].

$$\mathcal{W} = (S, \leqslant, T, I, F)$$

Example 1:

Labeled Petri net with covering M_f as acceptance condition induces WSTS

$$(\mathbb{N}^P, \leqslant^P, T, M_0, M_f\!\uparrow) \ .$$

Well structured transiton systems

Consider a labeled version of well-structured transition systems (WSTS) [F87,ACJT96,FS01].

$$\mathcal{W} = (S, \leqslant, T, I, F)$$

Example 1:

Labeled Petri net with covering M_f as acceptance condition induces WSTS

$$(\mathbb{N}^P, \leqslant^P, T, M_0, M_f\!\uparrow)\ .$$

Example 2:

Labeled lossy channel system (LCS) [AJ93] induces a WSTS.

The result & and its consequences

The result & its consequences

Theorem

If two WSTS languages, one of them finitely branching, are disjoint, then they are regularly separable.

The result & its consequences

Theorem

If two WSTS languages, one of them finitely branching, are disjoint, then they are regularly separable.

Corollary

If a language and its complement are finitely-branching WSTS languages, they are necessarily regular.

The result & its consequences

Theorem

If two WSTS languages, one of them finitely branching, are disjoint, then they are regularly separable.

Corollary

If a language and its complement are finitely-branching WSTS languages, they are necessarily regular.

This generalizes earlier results for Petri net coverability languages. [MKR98a,MKR98b]

The result & its consequences

Theorem

If two WSTS languages, one of them finitely branching, are disjoint, then they are regularly separable.

Corollary

If a language and its complement are finitely-branching WSTS languages, they are necessarily regular.

This generalizes earlier results for Petri net coverability languages. [MKR98a,MKR98b]

Corollary

No subclass of finitely-branching WSTS beyond REG is closed under complement.

Expressibility results

Our result - Recall

Theorem

If two WSTS languages, one of them finitely branching, are disjoint, then they are regularly separable.

$\mathcal{W}$ finitely branching: I finite, $\text{Post}_\Sigma(c)$ finite for all c

Our result - Recall

Theorem

If two WSTS languages, one of them finitely branching, are disjoint, then they are regularly separable.

$\mathcal{W}$ finitely branching: I finite, $\mathrm{Post}_\Sigma(c)$ finite for all c

How much of a restriction is it to assume finite branching?

What do we gain by assuming finite branching?

Expressibility I

Proposition

Languages of ω^2-WSTS

$\subseteq$ Languages of finitely branching WSTS.

$$\begin{array}{ll} & (S, \leqslant)\ \omega^2 \text{ wqo} \\ \text{iff} & (\mathcal{P}^{\downarrow}(S), \subseteq) \text{ wqo} \\ \text{iff} & (S, \leqslant) \text{ does not embed the Rado order} \end{array}$$

Our result applies to all WSTS of practical interest!

Expressibility II

Proposition

Languages of finitely branching WSTS

= Languages of deterministic WSTS.

Sufficient to show:

Theorem

If two WSTS languages, one of them deterministic, are disjoint, then they are regularly separable.

Proof sketch

Proof approach

Theorem

If two WSTS languages, one of them deterministic, are disjoint, then they are regularly separable.

Proof approach:

Relate separability to the existence of certain invariants:

> Separability talks about the languages,
>
> Invariants talk about the state space!

Inductive invariant

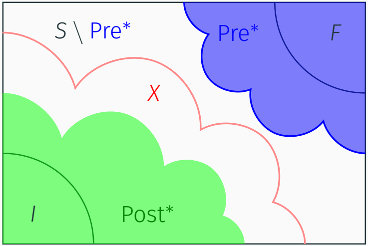
Inductive invariant [MP95] X for WSTS $\mathcal{W}$:

(1) $X \subseteq S$ downward-closed

(2) $I \subseteq X$

(3) $F \cap X = \varnothing$

(4) $\mathrm{Post}_{\Sigma}(X) \subseteq X$



Inductive invariant

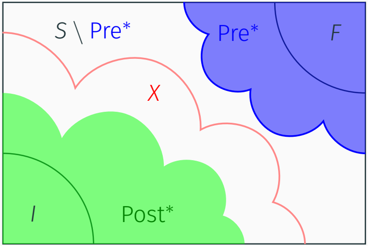
Inductive invariant [MP95] X for WSTS $\mathcal{W}$:

(1) $X \subseteq S$ downward-closed

(2) $I \subseteq X$

(3) $F \cap X = \varnothing$

(4) $\mathrm{Post}_\Sigma(X) \subseteq X$



Lemma

$\mathcal{L}(\mathcal{W}) = \varnothing$ iff inductive invariant for $\mathcal{W}$ exists.

Proof approach

$$\mathcal{L}(\mathcal{W}_1), \mathcal{L}(\mathcal{W}_2) \text{ reg. sep} \overset{!}{\iff} \mathcal{L}(\mathcal{W}_1) \cap \mathcal{L}(\mathcal{W}_2) = \mathcal{L}(\mathcal{W}_1 \times \mathcal{W}_2) = \varnothing$$

Proof approach

$$\mathcal{L}(\mathcal{W}_1), \mathcal{L}(\mathcal{W}_2) \text{ reg. sep} \overset{!}{\iff} \mathcal{L}(\mathcal{W}_1) \cap \mathcal{L}(\mathcal{W}_2) = \mathcal{L}(\mathcal{W}_1 \times \mathcal{W}_2) = \varnothing$$

$$\Updownarrow$$

$\mathcal{W}_1 \times \mathcal{W}_2$ has inductive invariant

Proof approach

$$\begin{tikzcd}
\mathcal{L}(\mathcal{W}_1), \mathcal{L}(\mathcal{W}_2) \text{ reg. sep} \arrow[rr, Leftrightarrow, "!"] & & \mathcal{L}(\mathcal{W}_1) \cap \mathcal{L}(\mathcal{W}_2) = \mathcal{L}(\mathcal{W}_1 \times \mathcal{W}_2) = \varnothing \\
& \mathcal{W}_1 \times \mathcal{W}_2 \text{ has inductive invariant} \arrow[ul, Rightarrow, "?"] \arrow[ur, Leftrightarrow] &
\end{tikzcd}$$

Finitely represented invariants

The desired implication does not hold.

Call an invariant X finitely represented if $X = Q\downarrow$ for Q finite

Finitely represented invariants

The desired implication does not hold.

Call an invariant X finitely represented if $X = Q\downarrow$ for Q finite

Recall:

$(S, \leqslant)$ well quasi order (wqo)
iff upward-closed sets have finitely many minimal elements.

No such statement for downward-closed sets and maximal elements!

Finitely represented invariants

The desired implication does not hold.

Call an invariant X finitely represented if $X = Q\downarrow$ for Q finite

We can show:

Theorem

Let $\mathcal{W}_1, \mathcal{W}_2$ WSTS, $\mathcal{W}_2$ deterministic.

If $\mathcal{W}_1 \times \mathcal{W}_2$ admits a finitely-represented inductive invariant, then $\mathcal{L}(\mathcal{W}_1)$ and $\mathcal{L}(\mathcal{W}_2)$ are regularly separable.

Proof approach II

$$
\begin{tikzcd}
\mathcal{L}(\mathcal{W}_1), \mathcal{L}(\mathcal{W}_2) \text{ reg. sep} \arrow[rr, Leftrightarrow, "!"] & & \mathcal{L}(\mathcal{W}_1) \cap \mathcal{L}(\mathcal{W}_2) = \mathcal{L}(\mathcal{W}_1 \times \mathcal{W}_2) = \varnothing \arrow[dl, Rightarrow, dashed] \\
& \mathcal{W}_1 \times \mathcal{W}_2 \text{ has fin.-rep. invariant} \arrow[ul, Rightarrow, "\checkmark"'] &
\end{tikzcd}
$$

Proof approach II

$$\mathcal{L}(\mathcal{W}_1), \mathcal{L}(\mathcal{W}_2) \text{ reg. sep} \overset{!}{\iff} \mathcal{L}(\mathcal{W}_1) \cap \mathcal{L}(\mathcal{W}_2) = \mathcal{L}(\mathcal{W}_1 \times \mathcal{W}_2) = \varnothing$$

✓ ✗

$\mathcal{W}_1 \times \mathcal{W}_2$ has fin.-rep. invariant

Ideals

Finitely represented invariants do not necessarily exist.

Solution: Ideals

Definition

For WSTS $\mathcal{W}$, let $\widehat{\mathcal{W}}$ be its ideal completion. [KP92][BFM14,FG12]

Lemma

$\mathcal{L}(\mathcal{W}) = \mathcal{L}(\widehat{\mathcal{W}})$.

Ideals

Finitely represented invariants do not necessarily exist.

Solution: Ideals

Definition

For WSTS $\mathcal{W}$, let $\widehat{\mathcal{W}}$ be its ideal completion. [KP92][BFM14,FG12]

Lemma

$\mathcal{L}(\mathcal{W}) = \mathcal{L}(\widehat{\mathcal{W}})$.

Proposition

If X is an inductive invariant for $\mathcal{W}$,
then its ideal decomposition $\textsc{Idec}(X)\downarrow$
is a finitely-represented inductive invariant for $\widehat{\mathcal{W}}$.

Proof

Putting everything together:

If $\mathcal{W}_1, \mathcal{W}_2$ are disjoint, $\mathcal{W}_1 \times \mathcal{W}_2$ admits an invariant X.

Then $\textsc{Idec}(X)\downarrow$ is a finitely-represented invariant for $\widehat{\mathcal{W}_1 \times \mathcal{W}_2} \cong \widehat{\mathcal{W}_1} \times \widehat{\mathcal{W}_2}$.

This finitely-represented invariant gives rise to a regular separator.

Proof

Putting everything together:

If $\mathcal{W}_1, \mathcal{W}_2$ are disjoint, $\mathcal{W}_1 \times \mathcal{W}_2$ admits an invariant X.

Then $\textsc{Idec}(X){\downarrow}$ is a finitely-represented invariant for $\widehat{\mathcal{W}_1 \times \mathcal{W}_2} \cong \widehat{\mathcal{W}_1} \times \widehat{\mathcal{W}_2}$.

This finitely-represented invariant gives rise to a regular separator.

We have shown:

Theorem

If two WSTS languages are disjoint,
one of them finitely branching or deterministic or ω^2,
then they are regularly separable.

Proof details:

From fin.-rep. invariants to regular separators

From invariants to separability

Theorem

Let $\mathcal{W}_1, \mathcal{W}_2$ WSTS, $\mathcal{W}_2$ deterministic.

If $\mathcal{W}_1 \times \mathcal{W}_2$ admits a finitely-represented inductive invariant, then $\mathcal{L}(\mathcal{W}_1)$ and $\mathcal{L}(\mathcal{W}_2)$ are regularly separable.

From invariants to separability

Theorem

Let $\mathcal{W}_1, \mathcal{W}_2$ WSTS, $\mathcal{W}_2$ deterministic.

If $\mathcal{W}_1 \times \mathcal{W}_2$ admits a finitely-represented inductive invariant, then $\mathcal{L}(\mathcal{W}_1)$ and $\mathcal{L}(\mathcal{W}_2)$ are regularly separable.

Assume $Q{\downarrow}$ is invariant.

Idea: Construct separating NFA with Q as states

From invariants to separability

Theorem

Let $\mathcal{W}_1, \mathcal{W}_2$ WSTS, $\mathcal{W}_2$ deterministic.

If $\mathcal{W}_1 \times \mathcal{W}_2$ admits a finitely-represented inductive invariant, then $\mathcal{L}(\mathcal{W}_1)$ and $\mathcal{L}(\mathcal{W}_2)$ are regularly separable.

Definition

$\mathcal{A} = (Q, \rightarrow, Q_I, Q_F)$ where

From invariants to separability

Theorem

Let $\mathcal{W}_1, \mathcal{W}_2$ WSTS, $\mathcal{W}_2$ deterministic.

If $\mathcal{W}_1 \times \mathcal{W}_2$ admits a finitely-represented inductive invariant, then $\mathcal{L}(\mathcal{W}_1)$ and $\mathcal{L}(\mathcal{W}_2)$ are regularly separable.

Definition

$\mathcal{A} = (Q, \rightarrow, Q_I, Q_F)$ where

$$Q_I = \{(s, s') \in Q \mid (c, c') \leqslant (s, s') \text{ for some } (c, c') \text{ initial}\}$$

From invariants to separability

Theorem

Let $\mathcal{W}_1, \mathcal{W}_2$ WSTS, $\mathcal{W}_2$ deterministic.

If $\mathcal{W}_1 \times \mathcal{W}_2$ admits a finitely-represented inductive invariant, then $\mathcal{L}(\mathcal{W}_1)$ and $\mathcal{L}(\mathcal{W}_2)$ are regularly separable.

Definition

$\mathcal{A} = (Q, \rightarrow, Q_I, Q_F)$ where

$$Q_I = \{(s, s') \in Q \mid (c, c') \leqslant (s, s') \text{ for some } (c, c') \text{ initial}\}$$

$$Q_F = \{(s, s') \in Q \mid s \in F_1\}$$

Theorem

Let $\mathcal{W}_1, \mathcal{W}_2$ WSTS, $\mathcal{W}_2$ deterministic.

If $\mathcal{W}_1 \times \mathcal{W}_2$ admits a finitely-represented inductive invariant, then $\mathcal{L}(\mathcal{W}_1)$ and $\mathcal{L}(\mathcal{W}_2)$ are regularly separable.

Definition

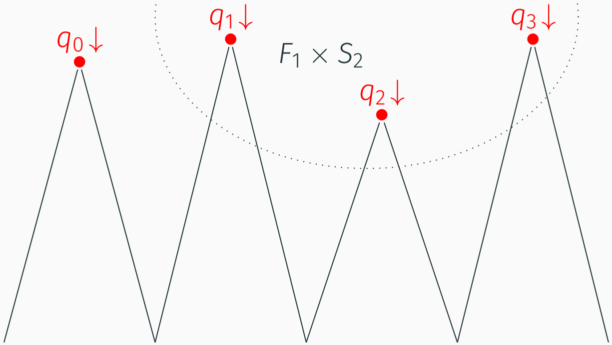
$\mathcal{A} = (Q, \rightarrow, Q_I, Q_F)$ where

$$Q_I = \{(s, s') \in Q \mid (c, c') \leqslant (s, s') \text{ for some } (c, c') \text{ initial}\}$$

$$Q_F = \{(s, s') \in Q \mid s \in F_1\}$$

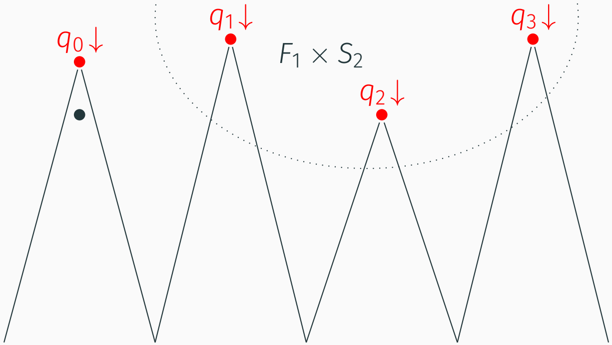
$$\begin{tikzcd}
 & (r, r') \in Q \arrow[d, phantom, "\rotatebox[origin=c]{-90}{$\leqslant$}"] \\
Q \ni (s, s') \arrow[ur, bend left, "a", "\text{in } \mathcal{A}"'] \arrow[r, "a", "\text{in } \mathcal{W}_1 \times \mathcal{W}_2"'] & (t, t') \in S_1 \times S_2
\end{tikzcd}$$

Behavior of $\mathcal{A}$



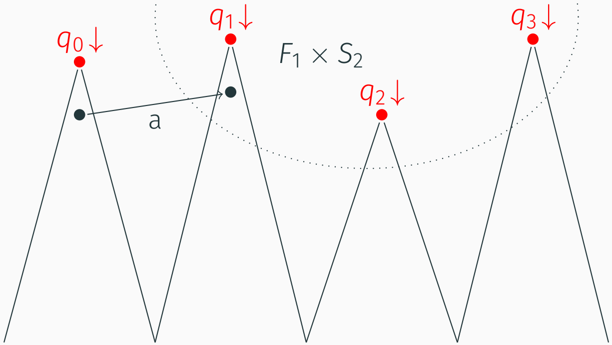
$\mathcal{A}$ over-approximates the behavior of the product system using the configurations from Q.

Behavior of $\mathcal{A}$



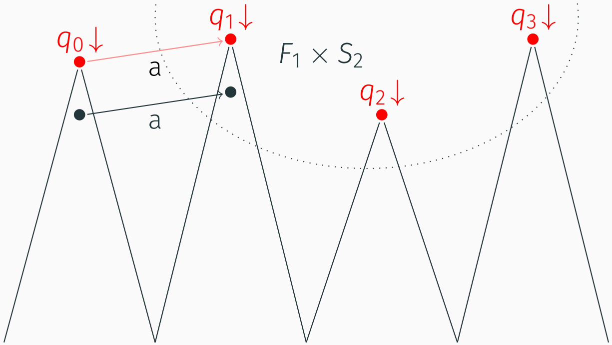
$\mathcal{A}$ over-approximates the behavior of the product system using the configurations from Q.

Behavior of $\mathcal{A}$



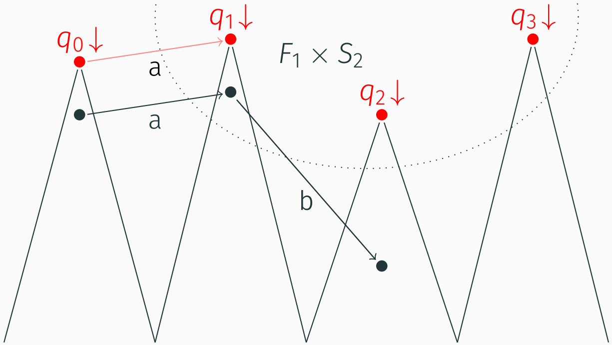
$\mathcal{A}$ over-approximates the behavior of the product system using the configurations from Q.

Behavior of $\mathcal{A}$



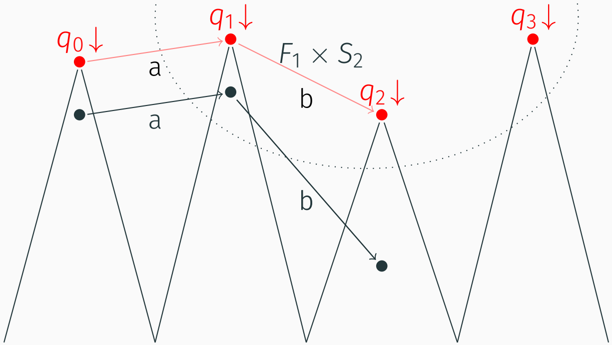
$\mathcal{A}$ over-approximates the behavior of the product system using the configurations from Q.

Behavior of $\mathcal{A}$



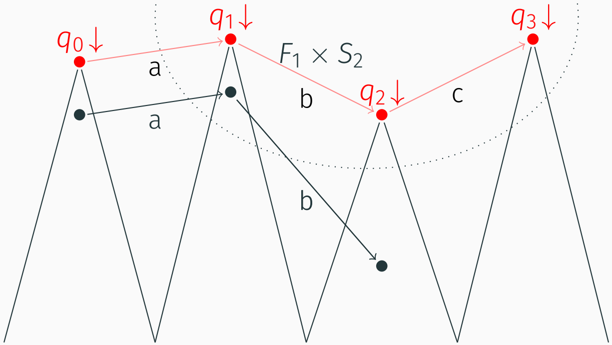
$\mathcal{A}$ over-approximates the behavior of the product system using the configurations from Q.

Behavior of $\mathcal{A}$

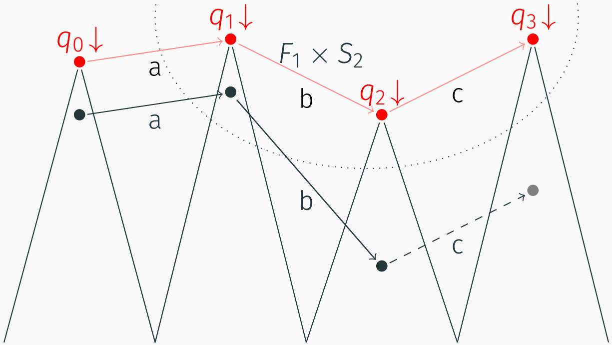


$\mathcal{A}$ over-approximates the behavior of the product system using the configurations from Q.

Behavior of $\mathcal{A}$



$\mathcal{A}$ over-approximates the behavior of the product system using the configurations from Q.



$\mathcal{A}$ over-approximates the behavior of the product system using the configurations from Q.

Proving separability: Inclusion

Lemma

$\mathcal{L}(\mathcal{W}_1) \subseteq \mathcal{L}(\mathcal{A})$.

Proving separability: Inclusion

Lemma

$\mathcal{L}(\mathcal{W}_1) \subseteq \mathcal{L}(\mathcal{A})$.

Proof.

Any run $c \xrightarrow{w} d$ of $\mathcal{W}_1$

synchronizes with **the** run of $\mathcal{W}_2$ for w

in the run $(c, c') \xrightarrow{w} (d, d')$ of $\mathcal{W}_1 \times \mathcal{W}_2$.

$\square$

Proving separability: Inclusion

Lemma

$\mathcal{L}(\mathcal{W}_1) \subseteq \mathcal{L}(\mathcal{A})$.

Proof.

Any run $c \xrightarrow{w} d$ of $\mathcal{W}_1$

synchronizes with **the** run of $\mathcal{W}_2$ for w

in the run $(c, c') \xrightarrow{w} (d, d')$ of $\mathcal{W}_1 \times \mathcal{W}_2$.

This run can be over-approximated in $\mathcal{A}$.

$\square$

Lemma

$\mathcal{L}(\mathcal{W}_1) \subseteq \mathcal{L}(\mathcal{A})$.

Proof.

Any run $c \xrightarrow{w} d$ of $\mathcal{W}_1$

synchronizes with **the** run of $\mathcal{W}_2$ for w

in the run $(c, c') \xrightarrow{w} (d, d')$ of $\mathcal{W}_1 \times \mathcal{W}_2$.

This run can be over-approximated in $\mathcal{A}$.

If d is final in $\mathcal{W}_1$,

the over-approximation of (d, d') is final in $\mathcal{A}$. $\square$

Proving separability: Disjointness

Lemma

$\mathcal{L}(\mathcal{W}_2) \cap \mathcal{L}(\mathcal{A}) = \varnothing$.

Proving separability: Disjointness

Lemma

$\mathcal{L}(\mathcal{W}_2) \cap \mathcal{L}(\mathcal{A}) = \varnothing$.

Proof.

Any run of $\mathcal{A}$ for w over-approximates

in the second component the unique run of $\mathcal{W}_2$ for w.

$\square$

Proving separability: Disjointness

Lemma

$\mathcal{L}(\mathcal{W}_2) \cap \mathcal{L}(\mathcal{A}) = \varnothing$.

Proof.

Any run of $\mathcal{A}$ for w over-approximates

in the second component the unique run of $\mathcal{W}_2$ for w.

If $w \in \mathcal{L}(\mathcal{W}_2) \cap \mathcal{L}(\mathcal{A})$

then some run of $\mathcal{A}$ reaches a state (q, q') with

- q final in $\mathcal{W}_1$ (def. of Q_I)
- q' final in $\mathcal{W}_2$ ($w \in \mathcal{L}(\mathcal{W}_2)$ + argument above)

$\square$

Proving separability: Disjointness

Lemma

$\mathcal{L}(\mathcal{W}_2) \cap \mathcal{L}(\mathcal{A}) = \varnothing$.

Proof.

Any run of $\mathcal{A}$ for w over-approximates

in the second component the unique run of $\mathcal{W}_2$ for w.

If $w \in \mathcal{L}(\mathcal{W}_2) \cap \mathcal{L}(\mathcal{A})$

then some run of $\mathcal{A}$ reaches a state (q, q') with

- q final in $\mathcal{W}_1$ (def. of Q_I)
- q' final in $\mathcal{W}_2$ ($w \in \mathcal{L}(\mathcal{W}_2)$ + argument above)

Contradiction to $F_1 \times F_2 \cap Q\downarrow = \varnothing$! $\square$

Proof details:
The ideal completion and fin.-rep. invariants

Finitely represented invariants

Lemma

Let $U \subseteq S$ be an upward-closed set in a wqo.

There is a finite set U_{min} such that $U = U_{min}\uparrow$.

A similar result for downward-closed subsets and maximal elements does not hold.

Finitely represented invariants

Lemma

Let $U \subseteq S$ be an upward-closed set in a wqo.

There is a finite set U_{min} such that $U = U_{min}\uparrow$.

A similar result for downward-closed subsets and maximal elements does not hold.

Example:

Consider $\mathbb{N}$ in $(\mathbb{N}, \leqslant)$

Intuitively, $\mathbb{N} = \omega\downarrow$

Finitely represented invariants

Lemma

Let $U \subseteq S$ be an upward-closed set in a wqo.

There is a finite set U_{min} such that $U = U_{min}\uparrow$.

A similar result for downward-closed subsets and maximal elements does not hold.

Consequence:
Finitely represented invariants may not exist!

Solution:
Move to a language-equivalent system for which they always exist.

Ideals

Let $(S, \leqslant)$ be a wqo
An ideal $\mathcal{I} \subseteq S$ is a set that is

- non-empty
- downward-closed

Ideals

Let $(S, \leqslant)$ be a wqo

An ideal $\mathcal{I} \subseteq S$ is a set that is

- non-empty
- downward-closed
- directed: $\forall x, y \in \mathcal{I}\, \exists z \in \mathcal{I} \colon x \leqslant z, y \leqslant z$

Ideals

Let $(S, \leqslant)$ be a wqo

An ideal $\mathcal{I} \subseteq S$ is a set that is

- non-empty
- downward-closed
- directed: $\forall x, y \in \mathcal{I}\, \exists z \in \mathcal{I} : x \leqslant z, y \leqslant z$

Example 1:

For each $c \in S$, $c\!\downarrow$ is an ideal

Ideals

Let $(S, \leqslant)$ be a wqo
An ideal $\mathcal{I} \subseteq S$ is a set that is

- non-empty
- downward-closed
- directed: $\forall x, y \in \mathcal{I}\, \exists z \in \mathcal{I} : x \leqslant z, y \leqslant z$

Example 2:
Consider $(\mathbb{N}^k, \leqslant)$
The ideals are the sets $u{\downarrow}$ for $u \in (\mathbb{N} \cup \{\omega\})^k$

Ideal decomposition

Lemma ([KP92])

Let $(S, \leqslant)$ be a wqo

For $D \subseteq S$ downward closed, let $\textsc{Idec}(D)$ be the set of inclusion-maximal ideals in D

$\textsc{Idec}(D)$ is unique, finite and we have

$$D = \bigcup \textsc{Idec}(D)$$

Ideal completion

Definition ([BFM14,FG12])

Let $\mathcal{W} = (S, \leqslant, T, I, F)$ WSTS

Its ideal completion is
$\widehat{\mathcal{W}} = (\{\mathcal{I} \subseteq S \mid \mathcal{I} \text{ ideal}\}, \subseteq, \widehat{T}, \textsc{Idec}(I{\downarrow}), \widehat{F})$ with

Ideal completion

Definition ([BFM14,FG12])

Let $\mathcal{W} = (S, \leqslant, T, I, F)$ WSTS

Its ideal completion is
$\widehat{\mathcal{W}} = (\{\mathcal{I} \subseteq S \mid \mathcal{I} \text{ ideal}\}, \subseteq, \widehat{T}, \textsc{Idec}(I{\downarrow}), \widehat{F})$ with

$$\widehat{F} = \{\mathcal{I} \mid \mathcal{I} \cap F \neq \varnothing\}$$

Ideal completion

Definition ([BFM14,FG12])

Let $\mathcal{W} = (S, \leqslant, T, I, F)$ WSTS

Its ideal completion is
$\widehat{\mathcal{W}} = (\{\mathcal{I} \subseteq S \mid \mathcal{I} \text{ ideal}\}, \subseteq, \widehat{T}, \textsc{Idec}(I{\downarrow}), \widehat{F})$ with

$$\widehat{F} = \{\mathcal{I} \mid \mathcal{I} \cap F \neq \varnothing\}$$

$\widehat{T}$ defined by $\mathrm{Post}_a^{\widehat{\mathcal{W}}}(\mathcal{I}) = \textsc{Idec}\big(\mathrm{Post}_a^{\mathcal{W}}(\mathcal{I}){\downarrow}\big)$

Ideal completion

Definition ([BFM14,FG12])

Let $\mathcal{W} = (S, \leqslant, T, I, F)$ WSTS

Its ideal completion is
$\widehat{\mathcal{W}} = (\{\mathcal{I} \subseteq S \mid \mathcal{I} \text{ ideal}\}, \subseteq, \widehat{T}, \textsc{Idec}(I{\downarrow}), \widehat{F})$ with

$$\widehat{F} = \{\mathcal{I} \mid \mathcal{I} \cap F \neq \varnothing\}$$
$$\widehat{T} \text{ defined by } \mathrm{Post}_a^{\widehat{\mathcal{W}}}(\mathcal{I}) = \textsc{Idec}\big(\mathrm{Post}_a^{\mathcal{W}}(\mathcal{I}){\downarrow}\big)$$

Lemma

- $\widehat{\mathcal{W}}$ *finitely branching*

Ideal completion

Definition ([BFM14,FG12])

Let $\mathcal{W} = (S, \leqslant, T, I, F)$ WSTS

Its ideal completion is
$\widehat{\mathcal{W}} = (\{\mathcal{I} \subseteq S \mid \mathcal{I} \text{ ideal}\}, \subseteq, \widehat{T}, \textsc{Idec}(I{\downarrow}), \widehat{F})$ with

$$\widehat{F} = \{\mathcal{I} \mid \mathcal{I} \cap F \neq \varnothing\}$$
$$\widehat{T} \text{ defined by } \mathrm{Post}_a^{\widehat{\mathcal{W}}}(\mathcal{I}) = \textsc{Idec}\big(\mathrm{Post}_a^{\mathcal{W}}(\mathcal{I}){\downarrow}\big)$$

Lemma

- $\widehat{\mathcal{W}}$ *finitely branching*
- $\mathcal{W}$ *deterministic* $\implies$ $\widehat{\mathcal{W}}$ *deterministic*

Ideal completion

Definition ([BFM14,FG12])

Let $\mathcal{W} = (S, \leqslant, T, I, F)$ WSTS

Its ideal completion is
$\widehat{\mathcal{W}} = (\{\mathcal{I} \subseteq S \mid \mathcal{I} \text{ ideal}\}, \subseteq, \widehat{T}, \textsc{Idec}(I{\downarrow}), \widehat{F})$ with

$$\widehat{F} = \{\mathcal{I} \mid \mathcal{I} \cap F \neq \varnothing\}$$

$\widehat{T}$ defined by $\mathrm{Post}_a^{\widehat{\mathcal{W}}}(\mathcal{I}) = \textsc{Idec}\big(\mathrm{Post}_a^{\mathcal{W}}(\mathcal{I}){\downarrow}\big)$

Lemma

- $\widehat{\mathcal{W}}$ *finitely branching*
- $\mathcal{W}$ *deterministic* $\implies$ $\widehat{\mathcal{W}}$ *deterministic*
- $\mathcal{L}(\widehat{\mathcal{W}}) = \mathcal{L}(\mathcal{W})$

Using the ideal completion

Proposition

If X is an inductive invariant for $\mathcal{W}$,

then its ideal decomposition $\textsc{Idec}(X)\downarrow$

is a finitely-represented inductive invariant for $\widehat{\mathcal{W}}$.

Using the ideal completion

Proposition

If X is an inductive invariant for $\mathcal{W}$,

then its ideal decomposition $\textsc{Idec}(X){\downarrow}$

is a finitely-represented inductive invariant for $\widehat{\mathcal{W}}$.

Proof.

Property of being an inductive invariant carries over

Any set of the shape $\textsc{Idec}(Y){\downarrow}$ is finitely-represented in $\widehat{\mathcal{W}}$ $\square$

Using the ideal completion

Proposition

If X is an inductive invariant for $\mathcal{W}$,

then its ideal decomposition $\textsc{Idec}(X)\downarrow$

is a finitely-represented inductive invariant for $\widehat{\mathcal{W}}$.

Proof.

Property of being an inductive invariant carries over

Any set of the shape $\textsc{Idec}(Y)\downarrow$ is finitely-represented in $\widehat{\mathcal{W}}$ $\square$

Result in particular applies to $\mathsf{Cover} = \mathsf{Post}^*(I_1 \times I_2)\downarrow$.

Using the ideal completion

Proposition

If X is an inductive invariant for $\mathcal{W}$,

then its ideal decomposition $\textsc{Idec}(X)\downarrow$

is a finitely-represented inductive invariant for $\widehat{\mathcal{W}}$.

Proof.

Property of being an inductive invariant carries over

Any set of the shape $\textsc{Idec}(Y)\downarrow$ is finitely-represented in $\widehat{\mathcal{W}}$ $\square$

Result in particular applies to $\mathrm{Cover} = \mathrm{Post}^*(I_1 \times I_2)\downarrow$.

Remark: $\widehat{\mathcal{W}}$ is not necessarily a WSTS.

Conclusion

Regular separability for WSTS languages

Theorem

If two WSTS languages are disjoint,

one of them finitely branching or deterministic or ω^2,

then they are regularly separable.

Also in the paper...

1. A similar result for downward-compatible WSTS

Theorem

If two DWSTS languages, one of them deterministic, are disjoint, then they are regularly separable

Also in the paper...

1. A similar result for downward-compatible WSTS

Theorem

If two DWSTS languages, one of them deterministic, are disjoint, then they are regularly separable

2. A size estimation for the case of Petri nets

Theorem

Given two Petri nets, their coverability languages can be separated by

- *Upper bound: an NFA of triply-exponential size*
- *Lower bound: a DFA of triply-exponential size*

Open problems

Expressibility results:

Are the inclusions strict?

$$\begin{aligned} \omega^2 - \text{WSTS languages} &\subseteq \text{det. WSTS languages} \\ \text{deterministic WSTS languages} &\subseteq \text{all WSTS languages} \end{aligned}$$

Expressibility results:
Are the inclusions strict?

$$\begin{aligned} \omega^2 - \text{WSTS languages} &\subseteq \text{det. WSTS languages} \\ \text{deterministic WSTS languages} &\subseteq \text{all WSTS languages} \end{aligned}$$

Separability results:
Are disjoint WSTS languages always regularly separable?

Open problems

Expressibility results:
Are the inclusions strict?

$$\begin{aligned} \omega^2 - \text{WSTS languages} &\subseteq \text{det. WSTS languages} \\ \text{deterministic WSTS languages} &\subseteq \text{all WSTS languages} \end{aligned}$$

Separability results:
Are disjoint WSTS languages always regularly separable?

Crucial for both problems:
Expressiveness of infinitely-branching Rado WSTS

Thank you!

Questions?

References

References 1/5

[PZ16] T. Place, M. Zeitoun
Separating regular languages with first-order logic
LMCS, 2016

[SW76] T. G. Szymanski, J. H. Williams
Noncanonical extensions of bottom-up parsing techniques
SIAM Journal on Computing, 1976

[K16] E. Kopczynski
Invisible pushdown languages
LICS, 2016

[CL17] W. Czerwiński, S. Lasota
Regular separability of one counter automata
LICS, 2017

[CCLP17a] L. Clemente, W. Czerwiński, S. Lasota, C. Paperman
Regular separability of Parikh automata
ICALP, 2017

[CCLP17b] L. Clemente, W. Czerwiński, S. Lasota, C. Paperman
Separability of reachability sets of vector addition systems
STACS, 2017

[F87] A. Finkel
A generalization of the procedure of Karp and Miller to well structured transition systems
ICALP, 1987

[ACJT96] P. A. Abdulla, K. Cerans, B. Jonsson, Y.-K. Tsay
General decidability theorems for infinite-state systems
ICALP, 1996

References 3/5

[FS01] A. Finkel and P. Schnoebelen
Well-structured transition systems everywhere!
Theor. Comput. Sci., 2001

[AJ93] P. A. Abdulla, B. Jonsson
Verifying programs with unreliable channels
LICS, 1993

[MKR98a] M. Mukund, K. N. Kumar, J. Radhakrishnan, M. A. Sohoni
Robust asynchronous protocols are finite-state
ICALP, 1998

[MKR98b] M. Mukund, K. N. Kumar, J. Radhakrishnan, M. A. Sohoni
Towards a characterisation of finite-state message-passing systems
ASIAN, 1998

[MP95] Z. Manna and A. Pnueli
Temporal verification of reactive systems - Safety
1995

[KP92] M. Kabil, M. Pouzet
Une extension d'un théorème de P. Jullien sur les âges de mots
ITA, 1992

[FG12] A. Finkel, J. Goubault-Larrecq
Forward analysis for wsts, part II: Complete WSTS
LMCS, 2012

References 5/5

[BFM14] M. Blondin, A. Finkel, P. McKenzie
Handling infinitely branching WSTS
ICALP, 2014

[BFM17] M. Blondin, A. Finkel, P. McKenzie
Well behaved transition systems
LMCS, 2017