Reachability Analysis with State-Coherent Automata

Bertram Felgenhauer and René Thiemann

University of Innsbruck

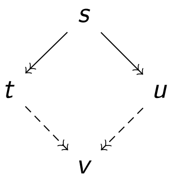
8th International Conference on
Language and Automata Theory and Applications
Madrid 2014-03-10

Contents

- Introduction
- State-Compatible Automata
- Conclusion

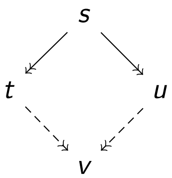
Motivation

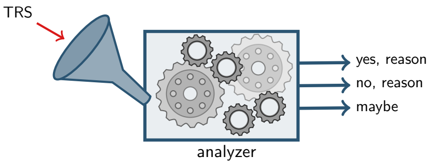
- Confluence of Term Rewrite Systems
  e.g. $\{\mathsf{F}(x,x) \to \mathsf{A}, \mathsf{G}(x) \to \mathsf{F}(x, \mathsf{G}(x)), \mathsf{C} \to \mathsf{G}(\mathsf{C})\}$



Motivation

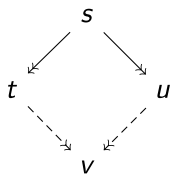
- Confluence of Term Rewrite Systems
  e.g. $\{\mathsf{F}(x,x) \to \mathsf{A}, \mathsf{G}(x) \to \mathsf{F}(x,\mathsf{G}(x)), \mathsf{C} \to \mathsf{G}(\mathsf{C})\}$
- Automation (CSI)
  but can we trust the tool?

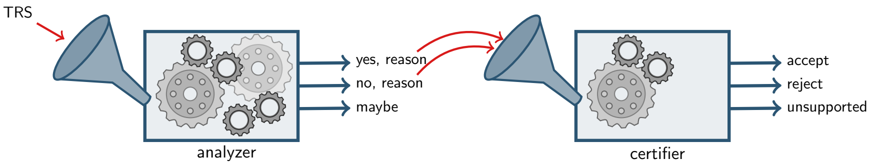




Motivation

- Confluence of Term Rewrite Systems
  e.g. $\{\mathsf{F}(x,x) \to \mathsf{A}, \mathsf{G}(x) \to \mathsf{F}(x,\mathsf{G}(x)), \mathsf{C} \to \mathsf{G}(\mathsf{C})\}$
- Automation (CSI)
  but can we trust the tool?
- Certification (CeTA)
  two tools are better than one
  especially if one is proved correct





Application: Non-Confluence

$\mathcal{R}: \qquad \mathsf{F}(x,x) \to \mathsf{A} \qquad \mathsf{G}(x) \to \mathsf{F}(x,\mathsf{G}(x)) \qquad \mathsf{C} \to \mathsf{G}(\mathsf{C})$

Rewriting

- rules $\ell \to r \in \mathcal{R}$, where $\ell, r \in \mathcal{T}(\mathcal{F},\mathcal{V})$ and $\mathcal{V}\mathrm{ar}(r) \subseteq \mathcal{V}\mathrm{ar}(\ell)$

Application: Non-Confluence

$$\mathcal{R}: \qquad \mathsf{F}(x,x) \to \mathsf{A} \qquad \mathsf{G}(x) \to \mathsf{F}(x,\mathsf{G}(x)) \qquad \mathsf{C} \to \mathsf{G}(\mathsf{C})$$

Rewriting

- rules $\ell \to r \in \mathcal{R}$, where $\ell, r \in \mathcal{T}(\mathcal{F},\mathcal{V})$ and $\mathcal{V}\mathsf{ar}(r) \subseteq \mathcal{V}\mathsf{ar}(\ell)$
- rewrite relation $C[\ell\tau] \to_{\mathcal{R}} C[r\tau]$, where $\tau : \mathcal{V} \to \mathcal{T}(\mathcal{F},\mathcal{V})$

Application: Non-Confluence

$$\mathcal{R}: \qquad \mathsf{F}(x,x) \to \mathsf{A} \qquad \mathsf{G}(x) \to \mathsf{F}(x,\mathsf{G}(x)) \qquad \mathsf{C} \to \mathsf{G}(\mathsf{C})$$

Rewriting

- rules $\ell \to r \in \mathcal{R}$, where $\ell, r \in \mathcal{T}(\mathcal{F},\mathcal{V})$ and $\mathcal{V}\mathsf{ar}(r) \subseteq \mathcal{V}\mathsf{ar}(\ell)$
- rewrite relation $C[\ell\tau] \to_{\mathcal{R}} C[r\tau]$, where $\tau : \mathcal{V} \to \mathcal{T}(\mathcal{F},\mathcal{V})$
- $\mathsf{G}(\mathsf{C}) \to \mathsf{F}(\mathsf{C},\mathsf{G}(\mathsf{C})) \to \mathsf{F}(\mathsf{G}(\mathsf{C}),\mathsf{G}(\mathsf{C})) \to \mathsf{A}$

Application: Non-Confluence

$\mathcal{R}: \quad \mathsf{F}(x,x) \to \mathsf{A} \qquad \mathsf{G}(x) \to \mathsf{F}(x,\mathsf{G}(x)) \qquad \mathsf{C} \to \mathsf{G}(\mathsf{C})$

Rewriting

- rules $\ell \to r \in \mathcal{R}$, where $\ell, r \in \mathcal{T}(\mathcal{F},\mathcal{V})$ and $\mathcal{V}\mathrm{ar}(r) \subseteq \mathcal{V}\mathrm{ar}(\ell)$
- rewrite relation $C[\ell\tau] \to_{\mathcal{R}} C[r\tau]$, where $\tau : \mathcal{V} \to \mathcal{T}(\mathcal{F},\mathcal{V})$
- $\mathsf{G}(\mathsf{C}) \to \mathsf{F}(\mathsf{C},\mathsf{G}(\mathsf{C})) \to \mathsf{F}(\mathsf{G}(\mathsf{C}),\mathsf{G}(\mathsf{C})) \to \mathsf{A}$
- $\mathsf{G}(\mathsf{C}) \to \mathsf{G}(\mathsf{G}(\mathsf{C})) \to^* \mathsf{G}(\mathsf{A})$

Application: Non-Confluence

$$\mathcal{R}: \qquad \mathsf{F}(x,x) \to \mathsf{A} \qquad \mathsf{G}(x) \to \mathsf{F}(x,\mathsf{G}(x)) \qquad \mathsf{C} \to \mathsf{G}(\mathsf{C})$$

Rewriting

- rules $\ell \to r \in \mathcal{R}$, where $\ell, r \in \mathcal{T}(\mathcal{F},\mathcal{V})$ and $\mathcal{V}\mathsf{ar}(r) \subseteq \mathcal{V}\mathsf{ar}(\ell)$
- rewrite relation $C[\ell\tau] \to_{\mathcal{R}} C[r\tau]$, where $\tau : \mathcal{V} \to \mathcal{T}(\mathcal{F},\mathcal{V})$
- $\mathsf{G}(\mathsf{C}) \to \mathsf{F}(\mathsf{C},\mathsf{G}(\mathsf{C})) \to \mathsf{F}(\mathsf{G}(\mathsf{C}),\mathsf{G}(\mathsf{C})) \to \mathsf{A}$
- $\mathsf{G}(\mathsf{C}) \to \mathsf{G}(\mathsf{G}(\mathsf{C})) \to^* \mathsf{G}(\mathsf{A})$

Idea

- $\mathcal{R}^*(\mathsf{A})$ and $\mathcal{R}^*(\mathsf{G}(\mathsf{A}))$ are disjoint:
- $\mathcal{R}^*(\mathsf{A}) = \{\mathsf{A}\}$
- $\mathcal{R}^*(\mathsf{G}(\mathsf{A})) = \{\mathsf{G}(\mathsf{A}), \mathsf{F}(\mathsf{A},\mathsf{G}(\mathsf{A})), \mathsf{F}(\mathsf{A},\mathsf{F}(\mathsf{A},\mathsf{G}(\mathsf{A}))), \dots\}$

Application: Non-Confluence

$$\mathcal{R}: \quad \mathsf{F}(x,x) \to \mathsf{A} \qquad \mathsf{G}(x) \to \mathsf{F}(x,\mathsf{G}(x)) \qquad \mathsf{C} \to \mathsf{G}(\mathsf{C})$$

Rewriting

- rules $\ell \to r \in \mathcal{R}$, where $\ell, r \in \mathcal{T}(\mathcal{F},\mathcal{V})$ and $\mathcal{V}\mathsf{ar}(r) \subseteq \mathcal{V}\mathsf{ar}(\ell)$
- rewrite relation $C[\ell\tau] \to_{\mathcal{R}} C[r\tau]$, where $\tau : \mathcal{V} \to \mathcal{T}(\mathcal{F},\mathcal{V})$
- $\mathsf{G}(\mathsf{C}) \to \mathsf{F}(\mathsf{C},\mathsf{G}(\mathsf{C})) \to \mathsf{F}(\mathsf{G}(\mathsf{C}),\mathsf{G}(\mathsf{C})) \to \mathsf{A}$
- $\mathsf{G}(\mathsf{C}) \to \mathsf{G}(\mathsf{G}(\mathsf{C})) \to^* \mathsf{G}(\mathsf{A})$

Idea

- $\mathcal{R}^*(\mathsf{A})$ and $\mathcal{R}^*(\mathsf{G}(\mathsf{A}))$ are disjoint:
- $\mathcal{R}^*(\mathsf{A}) = \{\mathsf{A}\}$
- $\mathcal{R}^*(\mathsf{G}(\mathsf{A})) = \{\mathsf{G}(\mathsf{A}), \mathsf{F}(\mathsf{A},\mathsf{G}(\mathsf{A})), \mathsf{F}(\mathsf{A},\mathsf{F}(\mathsf{A},\mathsf{G}(\mathsf{A}))), \dots\}$

$\Rightarrow$ Overapproximate $\mathcal{R}^*(t)$

Setup

Observation

If $\mathcal{L}(\mathcal{A})$ is closed under $\to_{\mathcal{R}}$ and $t \in \mathcal{L}(\mathcal{A})$ then $\mathcal{R}^*(t) \subseteq \mathcal{L}(\mathcal{A})$.

Setup

Observation

If $\mathcal{L}(\mathcal{A})$ is closed under $\to_{\mathcal{R}}$ and $t \in \mathcal{L}(\mathcal{A})$ then $\mathcal{R}^*(t) \subseteq \mathcal{L}(\mathcal{A})$.

Tree Automata

- $\mathcal{A} = (\mathcal{F}, Q, Q_f, \Delta)$

Setup

Observation

If $\mathcal{L}(\mathcal{A})$ is closed under $\to_{\mathcal{R}}$ and $t \in \mathcal{L}(\mathcal{A})$ then $\mathcal{R}^*(t) \subseteq \mathcal{L}(\mathcal{A})$.

Tree Automata

- $\mathcal{A} = (\mathcal{F}, Q, Q_f, \Delta)$
- signature $\mathcal{F}$, states Q, final states $Q_f \subseteq Q$

Setup

Observation

If $\mathcal{L}(\mathcal{A})$ is closed under $\to_{\mathcal{R}}$ and $t \in \mathcal{L}(\mathcal{A})$ then $\mathcal{R}^*(t) \subseteq \mathcal{L}(\mathcal{A})$.

Tree Automata

- $\mathcal{A} = (\mathcal{F}, Q, Q_f, \Delta)$
- signature $\mathcal{F}$, states Q, final states $Q_f \subseteq Q$
- transitions $f(q_1, \ldots, q_n) \to q \in \Delta$

Setup

Observation

If $\mathcal{L}(\mathcal{A})$ is closed under $\to_{\mathcal{R}}$ and $t \in \mathcal{L}(\mathcal{A})$ then $\mathcal{R}^*(t) \subseteq \mathcal{L}(\mathcal{A})$.

Tree Automata

- $\mathcal{A} = (\mathcal{F}, Q, Q_f, \Delta)$
- signature $\mathcal{F}$, states Q, final states $Q_f \subseteq Q$
- transitions $f(q_1, \ldots, q_n) \to q \in \Delta$
- language $\mathcal{L}(\mathcal{A}) = \{t \in \mathcal{T}(\mathcal{F}) \mid t \to_\Delta^* q \text{ for some } q \in Q_f\}$

Setup

Observation

If $\mathcal{L}(\mathcal{A})$ is closed under $\to_{\mathcal{R}}$ and $t \in \mathcal{L}(\mathcal{A})$ then $\mathcal{R}^*(t) \subseteq \mathcal{L}(\mathcal{A})$.

Tree Automata

- $\mathcal{A} = (\mathcal{F}, Q, Q_f, \Delta)$
- signature $\mathcal{F}$, states Q, final states $Q_f \subseteq Q$
- transitions $f(q_1, \ldots, q_n) \to q \in \Delta$
- language $\mathcal{L}(\mathcal{A}) = \{t \in \mathcal{T}(\mathcal{F}) \mid t \to_{\Delta}^* q \text{ for some } q \in Q_f\}$

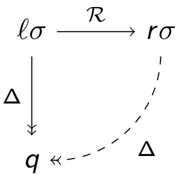
Question

Given a BTA $\mathcal{A}$, and a TRS $\mathcal{R}$, is $\mathcal{L}(\mathcal{A})$ closed under $\to_{\mathcal{R}}$?

Contents

- Introduction
- State-Compatible Automata
- Conclusion

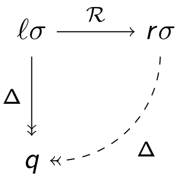
Compatibility



Definition

$\mathcal{A}$ is compatible with $\mathcal{R}$ if for all $\sigma : \mathcal{V} \to Q$ and $\ell \to r \in \mathcal{R}$, $\ell\sigma \to_\Delta^* q \in Q$ implies $r\sigma \to_\Delta^* q$.

Compatibility



Definition

$\mathcal{A}$ is compatible with $\mathcal{R}$ if for all $\sigma : \mathcal{V} \to Q$ and $\ell \to r \in \mathcal{R}$, $\ell\sigma \to_{\Delta}^{*} q \in Q$ implies $r\sigma \to_{\Delta}^{*} q$.

Theorem (Genet 1998)

If $\mathcal{A}$ is compatible with $\mathcal{R}$ then $\mathcal{L}(\mathcal{A})$ is closed under $\to_{\mathcal{R}}$ if $\mathcal{R}$ is left-linear or $\mathcal{A}$ is deterministic.

A Limitation

$$\mathcal{R}: \qquad \mathsf{F}(x,x) \to \mathsf{B} \qquad \mathsf{B} \to \mathsf{A}$$

Claim

$\{\mathsf{F}(\mathsf{A},\mathsf{A}), \mathsf{B}, \mathsf{A}\}$ is not accepted by a deterministic, compatible automaton.

A Limitation

$\mathcal{R}: \quad F(x,x) \to B \quad B \to A$

Claim

$\{F(A,A), B, A\}$ is not accepted by a deterministic, compatible automaton.

- by compatibility, $F(A,A), B, A$ are accepted in the same state $q \in Q_f$

A Limitation

$\mathcal{R}$: $\mathsf{F}(x, x) \to \mathsf{B}$ $\mathsf{B} \to \mathsf{A}$

Claim

$\{\mathsf{F}(\mathsf{A}, \mathsf{A}), \mathsf{B}, \mathsf{A}\}$ is not accepted by a deterministic, compatible automaton.

- by compatibility, $\mathsf{F}(\mathsf{A}, \mathsf{A}), \mathsf{B}, \mathsf{A}$ are accepted in the same state $q \in Q_f$
- by determinism, $\{\mathsf{F}(q, q) \to q, \mathsf{B} \to q, \mathsf{A} \to q\} \subseteq \Delta$

A Limitation

$\mathcal{R}$: $\mathsf{F}(x, x) \to \mathsf{B}$ $\mathsf{B} \to \mathsf{A}$

Claim

$\{\mathsf{F}(\mathsf{A}, \mathsf{A}), \mathsf{B}, \mathsf{A}\}$ is not accepted by a deterministic, compatible automaton.

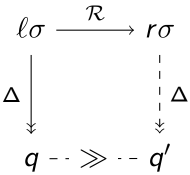
- by compatibility, $\mathsf{F}(\mathsf{A}, \mathsf{A}), \mathsf{B}, \mathsf{A}$ are accepted in the same state $q \in Q_f$
- by determinism, $\{\mathsf{F}(q, q) \to q, \mathsf{B} \to q, \mathsf{A} \to q\} \subseteq \Delta$
- $\mathcal{T}(\{\mathsf{F}, \mathsf{B}, \mathsf{A}\}) \subseteq \mathcal{L}(\mathcal{A})$ ∎

State-Compatibility

Definition

Let $\gg \subseteq Q \times Q$.

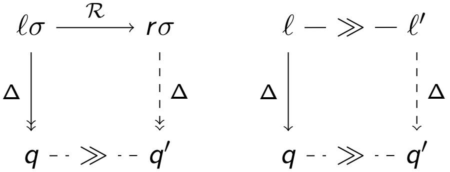
State-Compatibility



Definition

Let $\gg \subseteq Q \times Q$.
$(\mathcal{A}, \gg)$ is state-compatible with $\mathcal{R}$ if for all $\sigma : \mathcal{V} \to Q$ and $\ell \to r \in \mathcal{R}$,
$\ell\sigma \to_{\Delta}^{*} q$ implies $r\sigma \to_{\Delta}^{*} q'$ for some q' with $q \gg q'$.

State-Compatibility



Definition

Let $\gg \subseteq Q \times Q$.
$(\mathcal{A}, \gg)$ is state-compatible with $\mathcal{R}$ if for all $\sigma : \mathcal{V} \to Q$ and $\ell \to r \in \mathcal{R}$, $\ell\sigma \to_\Delta^* q$ implies $r\sigma \to_\Delta^* q'$ for some q' with $q \gg q'$.
$(\mathcal{A}, \gg)$ is state-coherent if $q \gg q'$ and $q \in Q_f$ implies $q' \in Q_f$, and for all $f(q_1, \ldots, q_n) \to q \in \Delta$ and $q_i \gg q_i'$, $f(q_1, \ldots, q_i', \ldots, q_n) \to q' \in \Delta$ for some some q' with $q \gg q'$.

Soundness

Theorem

If $(\mathcal{A}, \gg)$ is state-coherent and state-compatible with $\mathcal{R}$ then $\mathcal{L}(\mathcal{A})$ is closed under $\to_{\mathcal{R}}$ if $\mathcal{R}$ is left-linear or $\mathcal{A}$ is deterministic.

Soundness

Theorem

If $(\mathcal{A}, \gg)$ is state-coherent and state-compatible with $\mathcal{R}$ then $\mathcal{L}(\mathcal{A})$ is closed under $\to_{\mathcal{R}}$ if $\mathcal{R}$ is left-linear or $\mathcal{A}$ is deterministic.

$$\begin{array}{ccc} \mathcal{L}(\mathcal{A}) \ni & C[\ell\tau] \\ & \mathcal{R} \Big\downarrow \\ & C[r\tau] \end{array}$$

- $\tau : \mathcal{V} \to \mathcal{T}(\mathcal{F}, \mathcal{V})$

Soundness

Theorem

If $(\mathcal{A}, \gg)$ is state-coherent and state-compatible with $\mathcal{R}$ then $\mathcal{L}(\mathcal{A})$ is closed under $\to_{\mathcal{R}}$ if $\mathcal{R}$ is left-linear or $\mathcal{A}$ is deterministic.

$$\begin{array}{ccccccccc} \mathcal{L}(\mathcal{A}) \ni & C[\ell\tau] & \xrightarrow{\Delta}\!\!\!\!\rightarrow & C[\ell\sigma] & \xrightarrow{\Delta}\!\!\!\!\rightarrow & C[q] & \xrightarrow{\Delta}\!\!\!\!\rightarrow & q_\bullet & \in Q_f \\ & \mathcal{R}\downarrow & & & & & & & \\ & C[r\tau] & & & & & & & \end{array}$$

- $\tau : \mathcal{V} \to \mathcal{T}(\mathcal{F}, \mathcal{V})$, $\sigma : \mathcal{V} \to Q$

Soundness

Theorem

If $(\mathcal{A}, \gg)$ is state-coherent and state-compatible with $\mathcal{R}$ then $\mathcal{L}(\mathcal{A})$ is closed under $\to_{\mathcal{R}}$ if $\mathcal{R}$ is left-linear or $\mathcal{A}$ is deterministic.

$$\begin{array}{ccccccc}
\mathcal{L}(\mathcal{A}) \ni C[\ell\tau] & \xrightarrow{\Delta}\!\!\!\!\rightarrow & C[\ell\sigma] & \xrightarrow{\Delta}\!\!\!\!\rightarrow & C[q] & \xrightarrow{\Delta}\!\!\!\!\rightarrow & q_\bullet \in Q_f \\
\mathcal{R}\downarrow & ① & \mathcal{R}\downarrow & & & & \\
C[r\tau] & \xrightarrow[\Delta]{}\!\!\!\!\rightarrow & C[r\sigma] & & & &
\end{array}$$

- $\tau : \mathcal{V} \to \mathcal{T}(\mathcal{F}, \mathcal{V})$, $\sigma : \mathcal{V} \to Q$

① left-linearity of $\mathcal{R}$ or determinism of $\mathcal{A}$

Soundness

Theorem

If $(\mathcal{A}, \gg)$ is state-coherent and state-compatible with $\mathcal{R}$ then $\mathcal{L}(\mathcal{A})$ is closed under $\to_{\mathcal{R}}$ if $\mathcal{R}$ is left-linear or $\mathcal{A}$ is deterministic.

$$\begin{array}{ccccccc}
\mathcal{L}(\mathcal{A}) \ni C[\ell\tau] & \xrightarrow{\Delta}\!\!\!\!\rightarrow & C[\ell\sigma] & \xrightarrow{\Delta}\!\!\!\!\rightarrow & C[q] & \xrightarrow{\Delta}\!\!\!\!\rightarrow & q_\bullet \in Q_f \\
\mathcal{R} \downarrow & ① & \mathcal{R} \downarrow & ② & \Downarrow\!\!\!\!\!\vee & & \\
C[r\tau] & \xrightarrow[\Delta]{}\!\!\!\!\rightarrow & C[r\sigma] & \xrightarrow[\Delta]{}\!\!\!\!\rightarrow & C[q'] & &
\end{array}$$

- $\tau : \mathcal{V} \to \mathcal{T}(\mathcal{F}, \mathcal{V})$, $\sigma : \mathcal{V} \to Q$

① left-linearity of $\mathcal{R}$ or determinism of $\mathcal{A}$

② state-compatibility

Soundness

Theorem

If $(\mathcal{A}, \gg)$ is state-coherent and state-compatible with $\mathcal{R}$ then $\mathcal{L}(\mathcal{A})$ is closed under $\to_{\mathcal{R}}$ if $\mathcal{R}$ is left-linear or $\mathcal{A}$ is deterministic.

$$
\begin{array}{ccccccccc}
\mathcal{L}(\mathcal{A}) \ni C[\ell\tau] & \xrightarrow{\Delta}\!\!\!\!\rightarrow & C[\ell\sigma] & \xrightarrow{\Delta}\!\!\!\!\rightarrow & C[q] & \xrightarrow{\Delta}\!\!\!\!\rightarrow & q_\bullet \in Q_f \\
\mathcal{R} \downarrow & ① & \mathcal{R} \downarrow & ② & \Downarrow\!\!\!\!\!\downarrow & ③ & \Downarrow\!\!\!\!\!\downarrow \\
C[r\tau] & \xrightarrow[\Delta]{}\!\!\!\!\rightarrow & C[r\sigma] & \xrightarrow[\Delta]{}\!\!\!\!\rightarrow & C[q'] & \xrightarrow[\Delta]{}\!\!\!\!\rightarrow & q'_\bullet
\end{array}
$$

- $\tau : \mathcal{V} \to \mathcal{T}(\mathcal{F}, \mathcal{V})$, $\sigma : \mathcal{V} \to Q$

① left-linearity of $\mathcal{R}$ or determinism of $\mathcal{A}$

② state-compatibility

③ state-coherence

Soundness

Theorem

If $(\mathcal{A}, \gg)$ is state-coherent and state-compatible with $\mathcal{R}$ then $\mathcal{L}(\mathcal{A})$ is closed under $\to_{\mathcal{R}}$ if $\mathcal{R}$ is left-linear or $\mathcal{A}$ is deterministic.

$$
\begin{array}{ccccccccc}
\mathcal{L}(\mathcal{A}) \ni & C[\ell\tau] & \xrightarrow{\Delta}\!\!\!\!\rightarrow & C[\ell\sigma] & \xrightarrow{\Delta}\!\!\!\!\rightarrow & C[q] & \xrightarrow{\Delta}\!\!\!\!\rightarrow & q_\bullet & \in Q_f \\
\mathcal{R} & \Big\downarrow & ① & \mathcal{R}\ \Big\downarrow & ② & \Big\Downarrow\!\!\!\vee & ③ & \Big\Downarrow\!\!\!\vee & ③ \\
\mathcal{L}(\mathcal{A}) \ni & C[r\tau] & \xrightarrow[\Delta]{}\!\!\!\!\rightarrow & C[r\sigma] & \xrightarrow[\Delta]{}\!\!\!\!\rightarrow & C[q'] & \xrightarrow[\Delta]{}\!\!\!\!\rightarrow & q'_\bullet & \in Q_f
\end{array}
$$

- $\tau : \mathcal{V} \to \mathcal{T}(\mathcal{F}, \mathcal{V})$, $\sigma : \mathcal{V} \to Q$

① left-linearity of $\mathcal{R}$ or determinism of $\mathcal{A}$

② state-compatibility

③ state-coherence

No Limitation

$\mathcal{R}:$ $\quad \mathsf{F}(x,x) \to \mathsf{B} \quad \mathsf{B} \to \mathsf{A}$

Claim

$\{\mathsf{F}(\mathsf{A},\mathsf{A}), \mathsf{B}, \mathsf{A}\}$ is accepted by a deterministic, state-compatible and state-coherent automaton.

No Limitation

$$\mathcal{R}: \qquad \mathsf{F}(x,x) \to \mathsf{B} \qquad \mathsf{B} \to \mathsf{A}$$

Claim

$\{\mathsf{F}(\mathsf{A},\mathsf{A}),\mathsf{B},\mathsf{A}\}$ is accepted by a deterministic, state-compatible and state-coherent automaton.

- $Q = Q_f = \{0,1\}$, $1 \gg 0$
- $\Delta = \{\mathsf{A} \to 0, \mathsf{B} \to 1, \mathsf{F}(0,0) \to 1\}$ ■

No Limitation

$\mathcal{R}:$ $\mathsf{F}(x,x) \to \mathsf{B}$ $\mathsf{B} \to \mathsf{A}$

Claim

$\{\mathsf{F}(\mathsf{A},\mathsf{A}),\mathsf{B},\mathsf{A}\}$ is accepted by a deterministic, state-compatible and state-coherent automaton.

- $Q = Q_f = \{0,1\}$, $1 \gg 0$
- $\Delta = \{\mathsf{A} \to 0, \mathsf{B} \to 1, \mathsf{F}(0,0) \to 1\}$ ■

Theorem (Completeness)

Let $\mathcal{A}$ be deterministic and trim, and $\mathcal{L}(\mathcal{A})$ be closed under $\to_{\mathcal{R}}$. Then $(\mathcal{A},\gg)$ is state-coherent and state-compatible with $\mathcal{R}$ for some $\gg$.

Decidability

Theorem

Let $\mathcal{A}$ be a BTA and $\mathcal{R}$ be a TRS. It is decidable whether $\mathcal{L}(\mathcal{A})$ is closed under $\rightarrow_{\mathcal{R}}$.

Decidability

Theorem

Let $\mathcal{A}$ be a BTA and $\mathcal{R}$ be a TRS. It is decidable whether $\mathcal{L}(\mathcal{A})$ is closed under $\to_{\mathcal{R}}$.

1. determinize and trim $\mathcal{A}$

Decidability

Theorem

Let $\mathcal{A}$ be a BTA and $\mathcal{R}$ be a TRS. It is decidable whether $\mathcal{L}(\mathcal{A})$ is closed under $\to_{\mathcal{R}}$.

1. determinize and trim $\mathcal{A}$
2. compute minimal relation $\gg$ that makes $\mathcal{A}$ state-compatible with $\mathcal{R}$ and state-coherent
   - return no if $\ell\sigma \to_{\Delta}^{*} q$ but not $r\sigma \to_{\Delta}^{*} q'$ for any $q' \in Q$; otherwise, add $q \gg q'$
   - return no if $f(q_1, \dots, q_n) \to q \in \Delta$, $q_i \gg q_i'$ but not $f(q_1, \dots, q_i', \dots, q_n) \to q' \in \Delta$ for any $q' \in Q$; otherwise, add $q \gg q'$
   - return no if $q \in Q_f$, $q \gg q'$ but not $q' \in Q_f$

Decidability

Theorem

Let $\mathcal{A}$ be a BTA and $\mathcal{R}$ be a TRS. It is decidable whether $\mathcal{L}(\mathcal{A})$ is closed under $\to_{\mathcal{R}}$.

1. determinize and trim $\mathcal{A}$
2. compute minimal relation $\gg$ that makes $\mathcal{A}$ state-compatible with $\mathcal{R}$ and state-coherent
   - return no if $\ell\sigma \to_{\Delta}^{*} q$ but not $r\sigma \to_{\Delta}^{*} q'$ for any $q' \in Q$; otherwise, add $q \gg q'$
   - return no if $f(q_1, \ldots, q_n) \to q \in \Delta$, $q_i \gg q_i'$ but not $f(q_1, \ldots, q_i', \ldots, q_n) \to q' \in \Delta$ for any $q' \in Q$; otherwise, add $q \gg q'$
   - return no if $q \in Q_f$, $q \gg q'$ but not $q' \in Q_f$
3. return yes

Implementation

IsaFoR + CeTA

- soundness and completeness: formalized in IsaFoR, executable
- also formalized tree automata intersection and emptiness check

Implementation

IsaFoR + CeTA

- soundness and completeness: formalized in IsaFoR, executable
- also formalized tree automata intersection and emptiness check

$\Rightarrow$ CeTA can now certify tree-automata based non-confluence proofs

Implementation

IsaFoR + CeTA

- soundness and completeness: formalized in IsaFoR, executable
- also formalized tree automata intersection and emptiness check

⇒ CeTA can now certify tree-automata based non-confluence proofs

CSI

- CSI can produce state-coherent, state-compatible automata for non-confluence proofs

Contents

- Introduction
- State-Compatible Automata
- Conclusion

Summary

Done

- state-compatible, state-coherent automata
- simple, sound and complete
- most important results formalized in IsaFoR
- non-confluence support in CSI, CeTA
- ...

Summary

Done

- state-compatible, state-coherent automata
- simple, sound and complete
- most important results formalized in IsaFoR
- non-confluence support in CSI, CeTA
- ...

Future work

- match-bounds
- do completion directly on state-compatible automata

Summary

Done

- state-compatible, state-coherent automata
- simple, sound and complete
- most important results formalized in IsaFoR
- non-confluence support in CSI, CeTA
- ...

Future work

- match-bounds
- do completion directly on state-compatible automata

Thank you!