Model checking modal transition systems using Kripke structures

Michael Huth
Department of Computing
Imperial College of Science, Technology, and Medicine
London, United Kingdom

Relevant papers: see www.doc.ic.ac.uk/˜mrh/research.html
This talk: see www.doc.ic.ac.uk/˜mrh/vmcai2002.ps

Outline of talk

1. Motivation for this work;

Outline of talk

1. Motivation for this work;
2. abstraction-based model-checking using Kripke modal transition systems;

Outline of talk

1. Motivation for this work;
2. abstraction-based model-checking using Kripke modal transition systems;
3. reduction to model checking Kripke structures;

Outline of talk

1. Motivation for this work;
2. abstraction-based model-checking using Kripke modal transition systems;
3. reduction to model checking Kripke structures;
4. assessment of this reduction;

Outline of talk

1. Motivation for this work;
2. abstraction-based model-checking using Kripke modal transition systems;
3. reduction to model checking Kripke structures;
4. assessment of this reduction;
5. related work.

Motivation for this work

- Two principal reasons for using three-valued model checking:

Motivation for this work

- Two principal reasons for using three-valued model checking:
  1. specifier has explicit means of distinguishing between **guaranteed** and merely **possible** state and behavior;

Motivation for this work

- Two principal reasons for using three-valued model checking:
  1. specifier has explicit means of distinguishing between **guaranteed** and merely **possible** state and behavior;
  2. abstraction-based model checking is sound for a logic with **unrestricted** negation and quantification.

Motivation for this work

- Two principal reasons for using three-valued model checking:
  1. specifier has explicit means of distinguishing between **guaranteed** and merely **possible** state and behavior;
  2. abstraction-based model checking is sound for a logic with **unrestricted** negation and quantification.
- Beneficial to reduce three-valued models and checks to standard two-valued ones: pioneered by **(Bruns & Godefroid'00)** for partial **Kripke structures**;

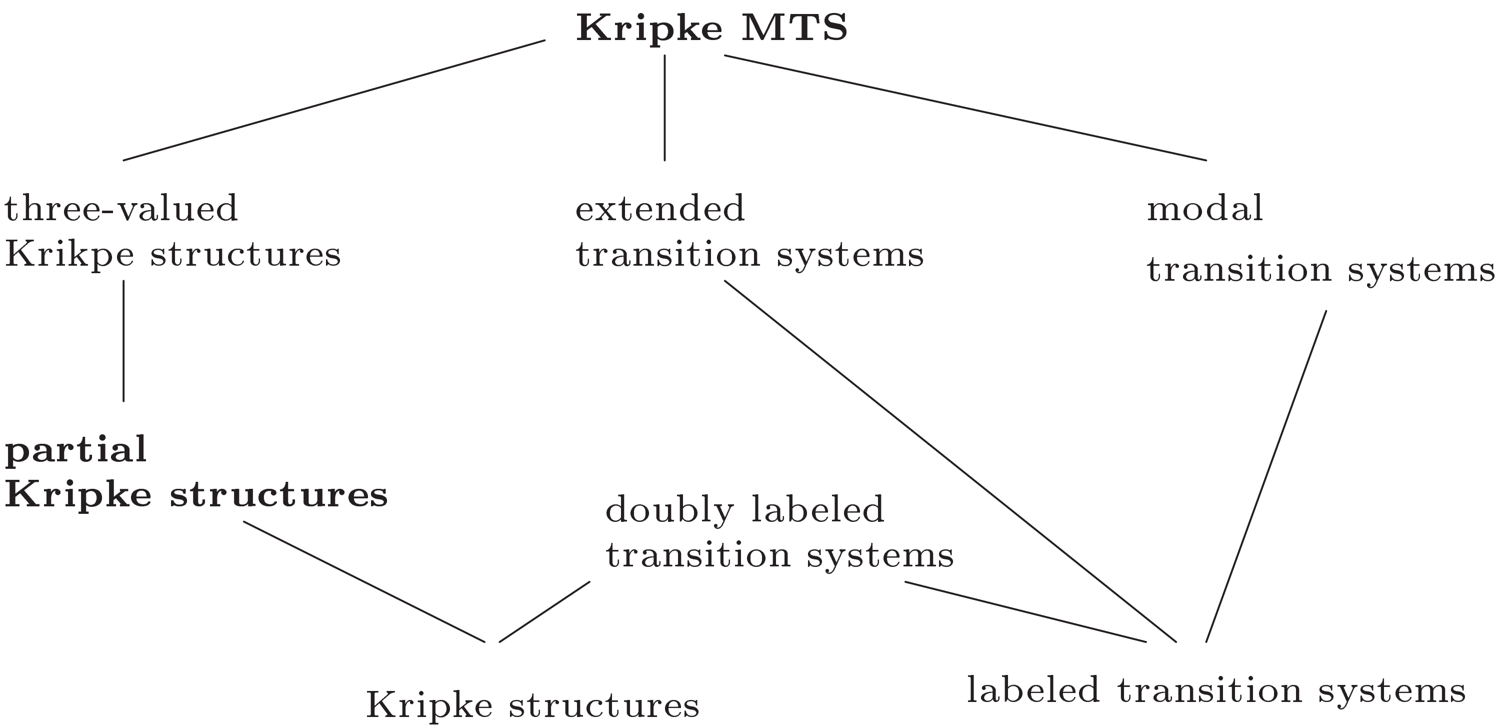
Motivation for this work

- Two principal reasons for using three-valued model checking:
  1. specifier has explicit means of distinguishing between **guaranteed** and merely **possible** state and behavior;
  2. abstraction-based model checking is sound for a logic with **unrestricted** negation and quantification.
- Beneficial to reduce three-valued models and checks to standard two-valued ones: pioneered by **(Bruns & Godefroid'00)** for partial **Kripke structures**;
- For models that are three-valued on states **and** behavior, such a reduction serves as a **blueprint for tool interfaces**.

Motivation for this work

- Two principal reasons for using three-valued model checking:
  1. specifier has explicit means of distinguishing between **guaranteed** and merely **possible** state and behavior;
  2. abstraction-based model checking is sound for a logic with **unrestricted** negation and quantification.
- Beneficial to reduce three-valued models and checks to standard two-valued ones: pioneered by **(Bruns & Godefroid'00)** for partial **Kripke structures**;
- For models that are three-valued on states **and** behavior, such a reduction serves as a **blueprint for tool interfaces**.
- Does such a reduction support techniques important in practice (e.g. **fairness constraints**)?

A hierarchy of two/three-valued models



A Hasse diagram of classes of two-valued (doubly labeled transition systems, Kripke structures, and labeled transition systems) and three-valued (all other classes) models, where the order represents class inclusion up to isomorphism.

Kripke modal transition systems

- A **Kripke MTS** $\mathcal{M}$ (HJS'01) with signature $(\mathtt{Act}, \mathtt{AP})$ is a pair $(\mathcal{M}^{\mathrm{a}}, \mathcal{M}^{\mathrm{c}})$, with $\mathcal{M}^{\mathrm{m}} = (\Sigma, R^{\mathrm{m}}, L^{\mathrm{m}})$ such that

$$R^{\mathrm{m}} \subseteq \Sigma \times \mathtt{Act} \times \Sigma$$

$$L^{\mathrm{m}} : \Sigma \to \mathcal{P}(\mathtt{AP})$$

for each $\mathrm{m} \in \{\mathrm{a}, \mathrm{c}\}$.

Kripke modal transition systems

- A **Kripke MTS** $\mathcal{M}$ (HJS'01) with signature $(\mathtt{Act}, \mathtt{AP})$ is a pair $(\mathcal{M}^{\mathrm{a}}, \mathcal{M}^{\mathrm{c}})$, with $\mathcal{M}^{\mathrm{m}} = (\Sigma, R^{\mathrm{m}}, L^{\mathrm{m}})$ such that

$$R^{\mathrm{m}} \subseteq \Sigma \times \mathtt{Act} \times \Sigma$$

$$L^{\mathrm{m}} : \Sigma \to \mathcal{P}(\mathtt{AP})$$

  for each $\mathrm{m} \in \{\mathrm{a}, \mathrm{c}\}$.

- $\mathcal{M}^{\mathrm{a}}$ specifies **guaranteed** state and behavior, $\mathcal{M}^{\mathrm{c}}$ specifies **possible** state and behavior.

Kripke modal transition systems

- A **Kripke MTS** $\mathcal{M}$ (HJS'01) with signature $(\mathtt{Act}, \mathtt{AP})$ is a pair $(\mathcal{M}^{\mathrm{a}}, \mathcal{M}^{\mathrm{c}})$, with $\mathcal{M}^{\mathrm{m}} = (\Sigma, R^{\mathrm{m}}, L^{\mathrm{m}})$ such that

$$R^{\mathrm{m}} \subseteq \Sigma \times \mathtt{Act} \times \Sigma$$

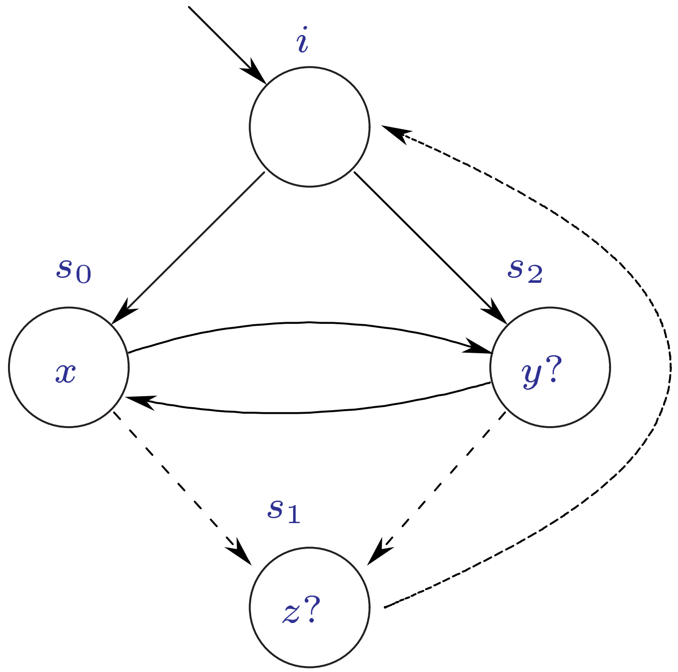
$$L^{\mathrm{m}} : \Sigma \to \mathcal{P}(\mathtt{AP})$$

  for each $\mathrm{m} \in \{\mathrm{a}, \mathrm{c}\}$.

- $\mathcal{M}^{\mathrm{a}}$ specifies **guaranteed** state and behavior, $\mathcal{M}^{\mathrm{c}}$ specifies **possible** state and behavior.

- Models with $\mathcal{M}^{\mathrm{a}} = \mathcal{M}^{\mathrm{c}}$ correspond to doubly labeled transition systems.

Modeling laptop modes



A Kripke MTS modeling laptop modes, where x, y, and z denote "AC powered", "battery powered", and "in suspend mode" (respectively).

Sound property semantics

$$
\begin{aligned}
[\![\, p \,]\!]^{\mathrm{m}}_{\rho} &\stackrel{\mathrm{def}}{=} \{s \in \Sigma \mid p \in L^{\mathrm{m}}(s)\} \\
[\![\, Z \,]\!]^{\mathrm{m}}_{\rho} &\stackrel{\mathrm{def}}{=} \rho^{\mathrm{m}}(Z) \\
[\![\, \neg\phi \,]\!]^{\mathrm{m}}_{\rho} &\stackrel{\mathrm{def}}{=} \Sigma \setminus [\![\, \phi \,]\!]^{\neg\mathrm{m}}_{\rho} \\
[\![\, \phi_1 \wedge \phi_2 \,]\!]^{\mathrm{m}}_{\rho} &\stackrel{\mathrm{def}}{=} [\![\, \phi_1 \,]\!]^{\mathrm{m}}_{\rho} \cap [\![\, \phi_2 \,]\!]^{\mathrm{m}}_{\rho} \\
[\![\, (\exists\alpha)\,\phi \,]\!]^{\mathrm{m}}_{\rho} &\stackrel{\mathrm{def}}{=} \mathrm{pre}^{\mathrm{m}}_{\alpha}([\![\, \phi \,]\!]^{\mathrm{m}}_{\rho}) \\
[\![\, \mu Z.\phi \,]\!]^{\mathrm{m}}_{\rho}\, s &\stackrel{\mathrm{def}}{=} \mathrm{lfp}\, F^{\mathrm{m}};\ \text{where } F^{\mathrm{m}}(A) \stackrel{\mathrm{def}}{=} [\![\, \phi \,]\!]^{\mathrm{m}}_{\rho^{\mathrm{m}}[Z \mapsto A]}.
\end{aligned}
$$

Sound property semantics

$$
\begin{aligned}
\llbracket\, p \,\rrbracket_\rho^{\mathrm{m}} &\stackrel{\mathrm{def}}{=} \{ s \in \Sigma \mid p \in L^{\mathrm{m}}(s) \} \\
\llbracket\, Z \,\rrbracket_\rho^{\mathrm{m}} &\stackrel{\mathrm{def}}{=} \rho^{\mathrm{m}}(Z) \\
\llbracket\, \neg\phi \,\rrbracket_\rho^{\mathrm{m}} &\stackrel{\mathrm{def}}{=} \Sigma \setminus \llbracket\, \phi \,\rrbracket_\rho^{\neg\mathrm{m}} \\
\llbracket\, \phi_1 \wedge \phi_2 \,\rrbracket_\rho^{\mathrm{m}} &\stackrel{\mathrm{def}}{=} \llbracket\, \phi_1 \,\rrbracket_\rho^{\mathrm{m}} \cap \llbracket\, \phi_2 \,\rrbracket_\rho^{\mathrm{m}} \\
\llbracket\, (\exists\alpha)\, \phi \,\rrbracket_\rho^{\mathrm{m}} &\stackrel{\mathrm{def}}{=} \mathrm{pre}_\alpha^{\mathrm{m}}(\llbracket\, \phi \,\rrbracket_\rho^{\mathrm{m}}) \\
\llbracket\, \mu Z.\phi \,\rrbracket_\rho^{\mathrm{m}}\, s &\stackrel{\mathrm{def}}{=} \mathrm{lfp}\, F^{\mathrm{m}};\ \text{where } F^{\mathrm{m}}(A) \stackrel{\mathrm{def}}{=} \llbracket\, \phi \,\rrbracket^{\mathrm{m}}_{\rho^{\mathrm{m}}[Z \mapsto A]}.
\end{aligned}
$$

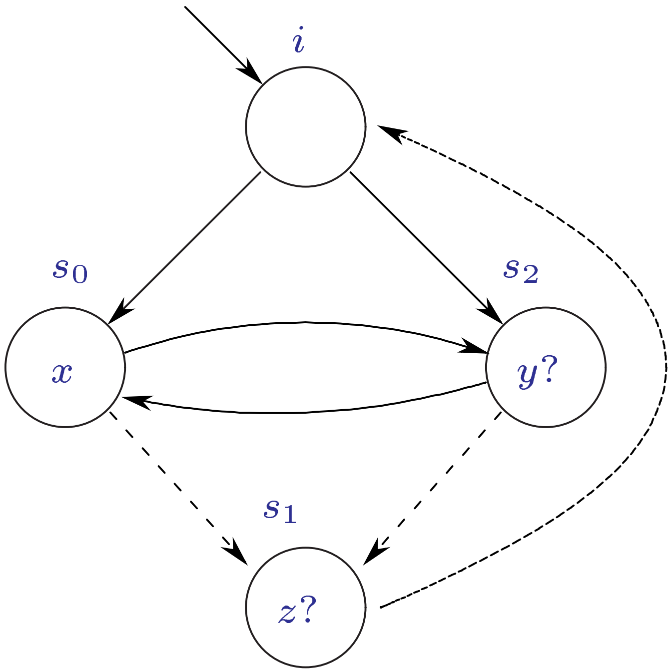
Except for treatment of negation, the property semantics over Kripke MTSs is as for doubly labeled transition systems.

Sound property semantics

$$
\begin{aligned}
\llbracket\, p \,\rrbracket_\rho^{\mathrm{m}} &\stackrel{\mathrm{def}}{=} \{s \in \Sigma \mid p \in L^{\mathrm{m}}(s)\} \\
\llbracket\, Z \,\rrbracket_\rho^{\mathrm{m}} &\stackrel{\mathrm{def}}{=} \rho^{\mathrm{m}}(Z) \\
\llbracket\, \neg\phi \,\rrbracket_\rho^{\mathrm{m}} &\stackrel{\mathrm{def}}{=} \Sigma \setminus \llbracket\, \phi \,\rrbracket_\rho^{\neg\mathrm{m}} \\
\llbracket\, \phi_1 \wedge \phi_2 \,\rrbracket_\rho^{\mathrm{m}} &\stackrel{\mathrm{def}}{=} \llbracket\, \phi_1 \,\rrbracket_\rho^{\mathrm{m}} \cap \llbracket\, \phi_2 \,\rrbracket_\rho^{\mathrm{m}} \\
\llbracket\, (\exists\alpha)\,\phi \,\rrbracket_\rho^{\mathrm{m}} &\stackrel{\mathrm{def}}{=} \mathrm{pre}_\alpha^{\mathrm{m}}(\llbracket\, \phi \,\rrbracket_\rho^{\mathrm{m}}) \\
\llbracket\, \mu Z.\phi \,\rrbracket_\rho^{\mathrm{m}}\, s &\stackrel{\mathrm{def}}{=} \mathrm{lfp}\, F^{\mathrm{m}};\ \text{where } F^{\mathrm{m}}(A) \stackrel{\mathrm{def}}{=} \llbracket\, \phi \,\rrbracket_{\rho^{\mathrm{m}}[Z \mapsto A]}^{\mathrm{m}}.
\end{aligned}
$$

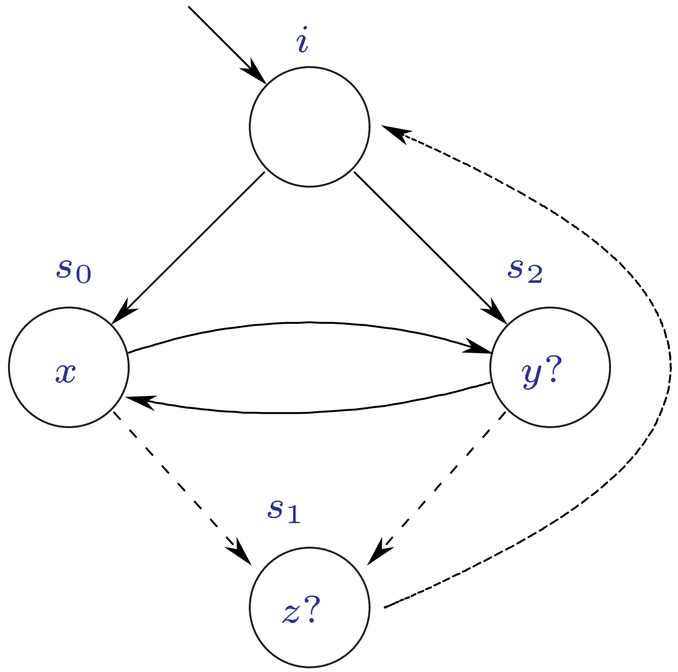
Except for treatment of negation, the property semantics over Kripke MTSs is as for doubly labeled transition systems. We have **soundness** for all ϕ: if $s \prec t$, then (i) $s \in \llbracket\, \phi \,\rrbracket_\rho^{\mathrm{c}}$ implies $t \in \llbracket\, \phi \,\rrbracket_\rho^{\mathrm{c}}$ and (ii) $t \in \llbracket\, \phi \,\rrbracket_\rho^{\mathrm{a}}$ implies $s \in \llbracket\, \phi \,\rrbracket_\rho^{\mathrm{a}}$.

An example check



The evaluation of $(\mathcal{M}, i) \models^{\mathrm{a}} \mathrm{AG}\,\mathrm{EF}\, z$ effectively checks whether all R^{c}-reachable states contain a R^{a}-path to a state s, where $z \in L^{\mathrm{a}}(s)$.

An example check



The evaluation of $(\mathcal{M}, i) \models^{\mathrm{a}} \mathrm{AG}\,\mathrm{EF}\, z$ effectively checks whether all R^{c}-reachable states contain a R^{a}-path to a state s, where $z \in L^{\mathrm{a}}(s)$. The evaluation of $(\mathcal{M}, i) \models^{\mathrm{c}} \mathrm{AG}\,\mathrm{EF}\, z$ conducts the same analysis, except that the modalities of paths are swapped.

Stage #1 of reduction [GHJ'01]

Reduce the model-checking problem for Kripke MTSs $\mathcal{M}$ with signature $(\mathtt{Act}, \mathtt{AP})$ to two model-checking problems for doubly labeled transition systems $\mathcal{M}^{\mathrm{p}} = (\Sigma, R^{\mathrm{p}}, L^{\mathrm{a}})$ and $\mathcal{M}^{\mathrm{o}} = (\Sigma, R^{\mathrm{o}}, L^{\mathrm{c}})$ with signature $(\overline{\mathtt{Act}}, \mathtt{AP})$, where

Stage #1 of reduction [GHJ'01]

Reduce the model-checking problem for Kripke MTSs $\mathcal{M}$ with signature $(\mathtt{Act}, \mathtt{AP})$ to two model-checking problems for doubly labeled transition systems $\mathcal{M}^{\mathrm{p}} = (\Sigma, R^{\mathrm{p}}, L^{\mathrm{a}})$ and $\mathcal{M}^{\mathrm{o}} = (\Sigma, R^{\mathrm{o}}, L^{\mathrm{c}})$ with signature $(\overline{\mathtt{Act}}, \mathtt{AP})$, where

$$\overline{\mathtt{Act}} \stackrel{\text{def}}{=} \{\alpha_\forall \mid \alpha \in \mathtt{Act}\} \cup \{\alpha_\exists \mid \alpha \in \mathtt{Act}\}$$

Stage #1 of reduction [GHJ'01]

Reduce the model-checking problem for Kripke MTSs $\mathcal{M}$ with signature $(\mathtt{Act}, \mathtt{AP})$ to two model-checking problems for doubly labeled transition systems $\mathcal{M}^{\mathrm{p}} = (\Sigma, R^{\mathrm{p}}, L^{\mathrm{a}})$ and $\mathcal{M}^{\mathrm{o}} = (\Sigma, R^{\mathrm{o}}, L^{\mathrm{c}})$ with signature $(\overline{\mathtt{Act}}, \mathtt{AP})$, where

$$\overline{\mathtt{Act}} \stackrel{\mathrm{def}}{=} \{\alpha_\forall \mid \alpha \in \mathtt{Act}\} \cup \{\alpha_\exists \mid \alpha \in \mathtt{Act}\}$$

$$R^{\mathrm{p}} \stackrel{\mathrm{def}}{=} \{(s, \alpha_\forall, s') \mid (s, \alpha, s') \in R^{\mathrm{c}}\} \cup \{(s, \alpha_\exists, s') \mid (s, \alpha, s') \in R^{\mathrm{a}}\}$$

$$R^{\mathrm{o}} \stackrel{\mathrm{def}}{=} \{(s, \alpha_\forall, s') \mid (s, \alpha, s') \in R^{\mathrm{a}}\} \cup \{(s, \alpha_\exists, s') \mid (s, \alpha, s') \in R^{\mathrm{c}}\}.$$

Stage #1 of reduction [GHJ'01]

Reduce the model-checking problem for Kripke MTSs $\mathcal{M}$ with signature $(\mathtt{Act}, \mathtt{AP})$ to two model-checking problems for doubly labeled transition systems $\mathcal{M}^{\mathrm{p}} = (\Sigma, R^{\mathrm{p}}, L^{\mathrm{a}})$ and $\mathcal{M}^{\mathrm{o}} = (\Sigma, R^{\mathrm{o}}, L^{\mathrm{c}})$ with signature $(\overline{\mathtt{Act}}, \mathtt{AP})$, where

$$\overline{\mathtt{Act}} \stackrel{\mathrm{def}}{=} \{\alpha_\forall \mid \alpha \in \mathtt{Act}\} \cup \{\alpha_\exists \mid \alpha \in \mathtt{Act}\}$$

$$R^{\mathrm{p}} \stackrel{\mathrm{def}}{=} \{(s, \alpha_\forall, s') \mid (s, \alpha, s') \in R^{\mathrm{c}}\} \cup \{(s, \alpha_\exists, s') \mid (s, \alpha, s') \in R^{\mathrm{a}}\}$$

$$R^{\mathrm{o}} \stackrel{\mathrm{def}}{=} \{(s, \alpha_\forall, s') \mid (s, \alpha, s') \in R^{\mathrm{a}}\} \cup \{(s, \alpha_\exists, s') \mid (s, \alpha, s') \in R^{\mathrm{c}}\}.$$

$\mathcal{M}^{\mathrm{p}}$ is the **pessimist** and $\mathcal{M}^{\mathrm{o}}$ is the **optimist** (Bruns & Godefroid'00).

Stage #1 of reduction [GHJ'01]

Reduce the model-checking problem for Kripke MTSs $\mathcal{M}$ with signature $(\texttt{Act}, \texttt{AP})$ to two model-checking problems for doubly labeled transition systems $\mathcal{M}^{\mathrm{p}} = (\Sigma, R^{\mathrm{p}}, L^{\mathrm{a}})$ and $\mathcal{M}^{\mathrm{o}} = (\Sigma, R^{\mathrm{o}}, L^{\mathrm{c}})$ with signature $(\overline{\texttt{Act}}, \texttt{AP})$, where

$$\overline{\texttt{Act}} \stackrel{\mathrm{def}}{=} \{\alpha_\forall \mid \alpha \in \texttt{Act}\} \cup \{\alpha_\exists \mid \alpha \in \texttt{Act}\}$$

$$R^{\mathrm{p}} \stackrel{\mathrm{def}}{=} \{(s, \alpha_\forall, s') \mid (s, \alpha, s') \in R^{\mathrm{c}}\} \cup \{(s, \alpha_\exists, s') \mid (s, \alpha, s') \in R^{\mathrm{a}}\}$$

$$R^{\mathrm{o}} \stackrel{\mathrm{def}}{=} \{(s, \alpha_\forall, s') \mid (s, \alpha, s') \in R^{\mathrm{a}}\} \cup \{(s, \alpha_\exists, s') \mid (s, \alpha, s') \in R^{\mathrm{c}}\}.$$

$\mathcal{M}^{\mathrm{p}}$ is the **pessimist** and $\mathcal{M}^{\mathrm{o}}$ is the **optimist** (Bruns & Godefroid'00). Note that each DLTS **mixes** elements of R^{a} and R^{c}!

Correctness of first stage [GHJ'01]

First, we transform every ϕ with signature $(\mathtt{Act}, \mathtt{AP})$ to its formula ϕ^+ in negation normal form.

Correctness of first stage [GHJ'01]

First, we transform every ϕ with signature $(\mathtt{Act}, \mathtt{AP})$ to its formula ϕ^+ in negation normal form.

Second, $T(\phi^+)$ is a formulas with signature $(\overline{\mathtt{Act}}, \mathtt{AP})$ and is computed from ϕ^+ as follows: for all $\alpha \in \mathtt{Act}$, we replace all occurrences of $(\forall\alpha)$ in ϕ^+ by $(\forall\alpha_\forall)$ and all occurrences of $(\exists\alpha)$ in ϕ^+ by $(\exists\alpha_\exists)$.

Correctness of first stage [GHJ'01]

First, we transform every ϕ with signature $(\mathtt{Act}, \mathtt{AP})$ to its formula ϕ^+ in negation normal form.

Second, $T(\phi^+)$ is a formulas with signature $(\overline{\mathtt{Act}}, \mathtt{AP})$ and is computed from ϕ^+ as follows: for all $\alpha \in \mathtt{Act}$, we replace all occurrences of $(\forall\alpha)$ in ϕ^+ by $(\forall\alpha_\forall)$ and all occurrences of $(\exists\alpha)$ in ϕ^+ by $(\exists\alpha_\exists)$.

Correctness: For any state $s \in \Sigma$, we then have

$$(\mathcal{M}, s) \models^{\mathrm{a}}_{\rho} \phi \qquad \text{iff} \qquad (\mathcal{M}^{\mathrm{p}}, s) \models_{\rho} T(\phi^+)$$

$$(\mathcal{M}, s) \models^{\mathrm{c}}_{\rho} \phi \qquad \text{iff} \qquad (\mathcal{M}^{\mathrm{o}}, s) \models_{\rho} T(\phi^+).$$

Stage #2 of reduction: formulas

First, we translate any DLTS formula with signature $(\overline{\mathtt{Act}}, \mathtt{AP})$ into Kripke structure formulas with signature $\overline{\mathtt{Act}} + \mathtt{AP}$:

$$
\begin{aligned}
K(\bot) &\stackrel{\text{def}}{=} \bot & K(\top) &\stackrel{\text{def}}{=} \top \\
K(Z) &\stackrel{\text{def}}{=} Z & K(p) &\stackrel{\text{def}}{=} p \\
K(\neg\phi) &\stackrel{\text{def}}{=} \neg K(\phi) \\
K(\phi_1 \wedge \phi_2) &\stackrel{\text{def}}{=} K(\phi_1) \wedge K(\phi_2) & K(\phi_1 \vee \phi_2) &\stackrel{\text{def}}{=} K(\phi_1) \vee K(\phi_2) \\
K((\exists\alpha)\phi) &\stackrel{\text{def}}{=} \mathrm{EX}\,(K(\phi) \wedge \alpha) & K((\forall\alpha)\phi) &\stackrel{\text{def}}{=} \mathrm{AX}\,(\neg\alpha \vee K(\phi)) \\
K(\mu Z.\phi) &\stackrel{\text{def}}{=} \mu Z.K(\phi) & K(\nu Z.\phi) &\stackrel{\text{def}}{=} \nu Z.K(\phi).
\end{aligned}
$$

Stage #2 of reduction: formulas

First, we translate any DLTS formula with signature $(\overline{\mathtt{Act}}, \mathtt{AP})$ into Kripke structure formulas with signature $\overline{\mathtt{Act}} + \mathtt{AP}$:

$$
\begin{array}{llll}
K(\bot) \stackrel{\text{def}}{=} \bot & & K(\top) \stackrel{\text{def}}{=} \top \\
K(Z) \stackrel{\text{def}}{=} Z & & K(p) \stackrel{\text{def}}{=} p \\
K(\neg\phi) \stackrel{\text{def}}{=} \neg K(\phi) & & \\
K(\phi_1 \wedge \phi_2) \stackrel{\text{def}}{=} K(\phi_1) \wedge K(\phi_2) & & K(\phi_1 \vee \phi_2) \stackrel{\text{def}}{=} K(\phi_1) \vee K(\phi_2) \\
K((\exists\alpha)\phi) \stackrel{\text{def}}{=} \mathrm{EX}\,(K(\phi) \wedge \alpha) & & K((\forall\alpha)\phi) \stackrel{\text{def}}{=} \mathrm{AX}\,(\neg\alpha \vee K(\phi)) \\
K(\mu Z.\phi) \stackrel{\text{def}}{=} \mu Z.K(\phi) & & K(\nu Z.\phi) \stackrel{\text{def}}{=} \nu Z.K(\phi).
\end{array}
$$

This translation preserves the fixed-point structure of formulas (alternation-depth fragments).

Stage #2 of reduction: models

Second, given a DLTS $\mathcal{L} = (\Sigma, R, L)$ with signature $(\mathtt{Act}, \mathtt{AP})$, we define a Kripke structure $\mathrm{K}[\mathcal{L}] = (\Sigma \times \mathtt{Act}, \bar{R}, \bar{L})$ with signature $\mathtt{Act} + \mathtt{AP}$ where

$$\bar{R} \stackrel{\text{def}}{=} \{((s, \alpha), (s', \beta)) \mid \alpha \in \mathtt{Act},\ (s, \beta, s') \in R\}$$

$$\bar{L}(s, \alpha) \stackrel{\text{def}}{=} L(s) + \{\alpha\}.$$

Stage #2 of reduction: models

Second, given a DLTS $\mathcal{L} = (\Sigma, R, L)$ with signature $(\mathtt{Act}, \mathtt{AP})$, we define a Kripke structure $\mathrm{K}[\mathcal{L}] = (\Sigma \times \mathtt{Act}, \bar{R}, \bar{L})$ with signature $\mathtt{Act} + \mathtt{AP}$ where

$$\bar{R} \stackrel{\text{def}}{=} \{((s,\alpha),(s',\beta)) \mid \alpha \in \mathtt{Act},\ (s,\beta,s') \in R\}$$

$$\bar{L}(s,\alpha) \stackrel{\text{def}}{=} L(s) + \{\alpha\}.$$

Correctness: For any ϕ with signature $(\mathtt{Act}, \mathtt{AP})$ and any $s \in \Sigma$, and any ρ as above, we have

$$[\![\, \phi \,]\!]_\rho \times \mathtt{Act} = [\![\, K(\phi) \,]\!]_{\rho_{\mathcal{K}}}.$$

where $\rho_{\mathcal{K}}(Z) \stackrel{\text{def}}{=} \rho(Z) \times \mathtt{Act}$.

Assessment of this reduction

Our reduction, the composition of the two stages,

1. is correct and has a linear blowup,

Assessment of this reduction

Our reduction, the composition of the two stages,

1. is correct and has a linear blowup,

2. preserves alternation-depth fragments,

Assessment of this reduction

Our reduction, the composition of the two stages,

1. is correct and has a linear blowup,
2. preserves alternation-depth fragments,
3. enables the use of standard and novel model checkers for Kripke structures (e.g. SMV and hesitant alternating automata),

Assessment of this reduction

Our reduction, the composition of the two stages,

1. is correct and has a linear blowup,
2. preserves alternation-depth fragments,
3. enables the use of standard and novel model checkers for Kripke structures (e.g. SMV and hesitant alternating automata),
4. can hardwire (simple) fairness in the logic (potentially expensive),

Assessment of this reduction

Our reduction, the composition of the two stages,

1. is correct and has a linear blowup,
2. preserves alternation-depth fragments,
3. enables the use of standard and novel model checkers for Kripke structures (e.g. SMV and hesitant alternating automata),
4. can hardwire (simple) fairness in the logic (potentially expensive),
5. but cannot separate fairness algorithmically as the first reduction mixes elements of R^{a} and R^{c}.

Conclusions

- Efficient reduction of three-valued model checking to two-valued model checking for Kripke MTSs **is** possible.

Conclusions

- Efficient reduction of three-valued model checking to two-valued model checking for Kripke MTSs **is** possible.
- Such reductions may **limit** use of additional techniques (e.g. algorithmic separation of fairness).

Conclusions

- Efficient reduction of three-valued model checking to two-valued model checking for Kripke MTSs **is** possible.
- Such reductions may **limit** use of additional techniques (e.g. algorithmic separation of fairness).
- . . . mixed message and a case for three-valued tools?

Related work

(Bruns & Godefroid'00): pioneered such reductions for **partial Kripke structures** $\mathcal{K} = (\Sigma, R, L)$, where $L\colon \Sigma \times \mathtt{AP} \to \{\text{false}, \text{true}, \perp\}$.

Related work

(Bruns & Godefroid'00): pioneered such reductions for **partial Kripke structures** $\mathcal{K} = (\Sigma, R, L)$, where $L\colon \Sigma \times \mathtt{AP} \to \{\text{false}, \text{true}, \perp\}$.

Question: Is there a translation of Kripke MTSs to partial Kripke structures that preserves and reflects refinements? If so, this offers another reduction to Kripke structures; presumably with similar limitations regarding fairness?

Related work

(Bruns & Godefroid'00): pioneered such reductions for **partial Kripke structures** $\mathcal{K} = (\Sigma, R, L)$, where $L\colon \Sigma \times \mathtt{AP} \to \{\mathrm{false}, \mathrm{true}, \perp\}$.

Question: Is there a translation of Kripke MTSs to partial Kripke structures that preserves and reflects refinements? If so, this offers another reduction to Kripke structures; presumably with similar limitations regarding fairness?

(Dams, Gerth & Grumberg'00): study fair CTL* over mixed transition systems, transitions and propositions come in two flavors: free and constrained ones; convert ϕ into positive normal form and annotate ϕ on path quantifiers and atomic propositions; annotations guide the satisfaction relation in its choice of free or constrained fair paths; soundness of that approach for fair CTL* over mixed transition systems is proved.