

# Infinite-State Verification of the Basic Tense Logic on Rational Kripke Models

Wilmari Bekker and Valentin Goranko

**Infinity in logic and computation,**  
University of Cape Town, 3 November 2007.

To do verification on an infinite structure:

- The structure must be **finitely presentable**.
- Model checking of formulas from the relevant logic must be **decidable**.
- Language must satisfy **minimal requirements** to be **adequate** for symbolic model checking [Kesten et al., TCS, 2001.].

We propose:

- **Rational Kripke models** - (infinite) structures that are finitely presentable using machines.
- **The basic tense logic**
  - Model checking of its formulas is decidable on rational Kripke models
  - Satisfies the minimum requirements.

To do verification on an infinite structure:

- The structure must be **finitely presentable**.
- Model checking of formulas from the relevant logic must be **decidable**.
- Language must satisfy **minimal requirements** to be **adequate** for symbolic model checking [Kesten et al., TCS, 2001].

We propose:

- **Rational Kripke models** - (infinite) structures that are finitely presentable using machines.
- **The basic tense logic**
  - Model checking of its formulas is decidable on rational Kripke models
  - Satisfies the minimum requirements.

To do verification on an infinite structure:

- The structure must be **finitely presentable**.
- Model checking of formulas from the relevant logic must be **decidable**.
- Language must satisfy **minimal requirements** to be **adequate** for symbolic model checking [Kesten et al., TCS, 2001].

We propose:

- **Rational Kripke models** - (infinite) structures that are finitely presentable using machines.
- **The basic tense logic**
  - Model checking of its formulas is decidable on rational Kripke models
  - Satisfies the minimum requirements.

To do verification on an infinite structure:

- The structure must be **finitely presentable**.
- Model checking of formulas from the relevant logic must be **decidable**.
- Language must satisfy **minimal requirements** to be **adequate** for symbolic model checking [Kesten et al., TCS, 2001.].

We propose:

- **Rational Kripke models** - (infinite) structures that are finitely presentable using machines.
- **The basic tense logic**
  - Model checking of its formulas is decidable on rational Kripke models
  - Satisfies the minimum requirements.

To do verification on an infinite structure:

- The structure must be **finitely presentable**.
- Model checking of formulas from the relevant logic must be **decidable**.
- Language must satisfy **minimal requirements** to be **adequate** for symbolic model checking [Kesten et al., TCS, 2001].

We propose:

- **Rational Kripke models** - (infinite) structures that are finitely presentable using machines.
- **The basic tense logic**
  - Model checking of its formulas is decidable on rational Kripke models
  - Satisfies the minimum requirements.

To do verification on an infinite structure:

- The structure must be **finitely presentable**.
- Model checking of formulas from the relevant logic must be **decidable**.
- Language must satisfy **minimal requirements** to be **adequate** for symbolic model checking [Kesten et al., TCS, 2001.].

We propose:

- **Rational Kripke models** - (infinite) structures that are finitely presentable using machines.
- **The basic tense logic**
  - Model checking of its formulas is decidable on rational Kripke models
  - Satisfies the minimum requirements.

To do verification on an infinite structure:

- The structure must be **finitely presentable**.
- Model checking of formulas from the relevant logic must be **decidable**.
- Language must satisfy **minimal requirements** to be **adequate** for symbolic model checking [Kesten et al., TCS, 2001.].

We propose:

- **Rational Kripke models** - (infinite) structures that are finitely presentable using machines.
- **The basic tense logic**
  - Model checking of its formulas is decidable on rational Kripke models
  - Satisfies the minimum requirements.

# The Basic Tense Logic

## Definition

For a Kripke model  $\mathcal{M} = (S, R, V)$  and  $\Phi$  the set of atomic propositions, the **basic tense logic**  $K_t$  is the extension of the propositional logic with the modal operators  $\langle R \rangle$  and  $\langle R^{-1} \rangle$ .

Kripke semantics:

$\mathcal{M}, u \models \langle R \rangle \varphi \iff \mathcal{M}, w \models \varphi$  for  $w$  an immediate successor of  $u$ , i.e.  $uRw$ .  
 $\mathcal{M}, u \models \langle R^{-1} \rangle \varphi \iff \mathcal{M}, w \models \varphi$  for  $w$  an immediate predecessor of  $u$ , i.e.  $wRu$ .

The dual operators  $[R]$  and  $[R^{-1}]$  can be defined in the usual way.

$K_t$  can express local properties but not reachability properties.

# The Basic Tense Logic

## Definition

For a Kripke model  $\mathcal{M} = (S, R, V)$  and  $\Phi$  the set of atomic propositions, the **basic tense logic**  $K_t$  is the extension of the propositional logic with the modal operators  $\langle R \rangle$  and  $\langle R^{-1} \rangle$ .

Kripke semantics:

$\mathcal{M}, u \models \langle R \rangle \varphi \iff \mathcal{M}, w \models \varphi$  for  $w$  an immediate successor of  $u$ , i.e.  $uRw$ .  
 $\mathcal{M}, u \models \langle R^{-1} \rangle \varphi \iff \mathcal{M}, w \models \varphi$  for  $w$  an immediate predecessor of  $u$ , i.e.  $wRu$ .

The dual operators  $[R]$  and  $[R^{-1}]$  can be defined in the usual way.

$K_t$  can express local properties but not reachability properties.

# The Basic Tense Logic

## Definition

For a Kripke model  $\mathcal{M} = (S, R, V)$  and  $\Phi$  the set of atomic propositions, the **basic tense logic**  $K_t$  is the extension of the propositional logic with the modal operators  $\langle R \rangle$  and  $\langle R^{-1} \rangle$ .

Kripke semantics:

$\mathcal{M}, u \models \langle R \rangle \varphi \iff \mathcal{M}, w \models \varphi$  for  $w$  an immediate successor of  $u$ , i.e.  $uRw$ .  
 $\mathcal{M}, u \models \langle R^{-1} \rangle \varphi \iff \mathcal{M}, w \models \varphi$  for  $w$  an immediate predecessor of  $u$ , i.e.  $wRu$ .

The dual operators  $[R]$  and  $[R^{-1}]$  can be defined in the usual way.

$K_t$  can express local properties but not reachability properties.

## Definition

A **rational transducer** is a tuple  $\mathcal{T} = \langle Q, \Sigma, \Gamma, q^0, F, \rho \rangle$  where

- 1  $Q$  is a finite set of **states**;
- 2  $\Sigma$  is a finite **input alphabet**;
- 3  $\Gamma$  is a finite **output alphabet**;
- 4  $q^0 \in Q$  is the **initial state**;
- 5  $F \subseteq Q$  is a set of **accepting states**; and
- 6  $\rho \subseteq Q \times \Sigma^* \times \Gamma^* \times Q$  is a **transition relation**.

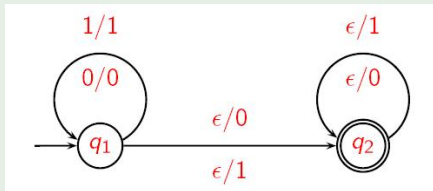
# An example of a rational transducer

## Example

Let  $\mathcal{T}$  be the rational transducer defined by:

- 1  $Q = \{q_1, q_2\}$ ;
- 2  $\Sigma = \{0, 1\}$
- 3  $\Gamma = \Sigma$ ;
- 4  $q^0 = q_1$ ;
- 5  $F = \{q_2\}$ ; and
- 6  $\rho = \left\{ q_1 \xrightarrow{x/x} q_1, q_1 \xrightarrow{\epsilon/x} q_2, q_2 \xrightarrow{\epsilon/x} q_2 \mid x \in \Sigma \right\}$

The empty word is denoted by  $\epsilon$ .



## Definition

A relation  $R \subseteq \Sigma^* \times \Gamma^*$  is **rational** if it is the relation recognised by some rational transducer.

Assume that  $\Gamma = \Sigma$  in the sequel.

## Definition

A relation  $R \subseteq \Sigma^* \times \Gamma^*$  is **rational** if it is the relation recognised by some rational transducer.

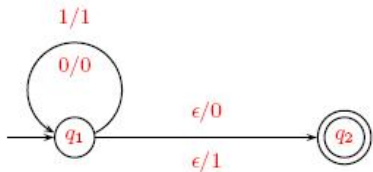
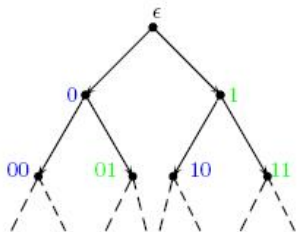
Assume that  $\Gamma = \Sigma$  in the sequel.

# Rational graphs

## Definition

Let  $\Sigma$  be a finite alphabet. A graph  $\mathcal{G} = (W, R)$  where  $W \subseteq \Sigma^*$  is a regular language and  $R \subseteq \Sigma^* \times \Sigma^*$  a rational relation is called a **rational graph**.

## Example



## Definition

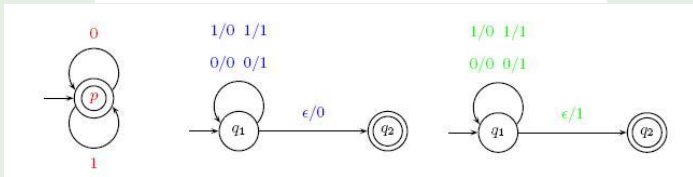
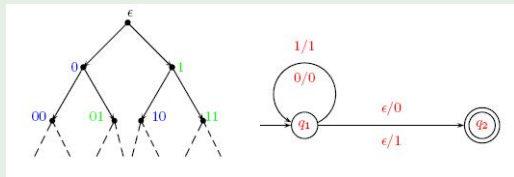
A Kripke model  $\mathcal{M} = (W, R, V)$  is **rational** if

- 1 the frame  $(W, R)$  on which it is based is a **rational graph**, and
- 2 the valuation  $V : \Phi \rightarrow \mathcal{P}(W)$  is **rational**, i.e.  $V(p)$  is a regular language for every  $p \in \Phi$ .

# Rational Kripke Models - Example

## Example

For  $\Sigma = \{0, 1\}$ , consider the rational Kripke model  $\mathcal{M} = (\Sigma^*, R, V)$  where the frame  $(\Sigma^*, R)$  is the complete binary tree and  $V(p)$  is the regular language containing all **left successors** and  $V(q)$  the regular language containing all **right successors** for  $\Phi = \{p, q\}$ .



# $\langle R \rangle X$ is Regular

Given a relation  $R$  and a language  $X$  define the language:

$$\langle R \rangle X = \{u \in \Sigma^* \mid \exists v \in X (uRv)\}$$

Lemma (Regularity Preservation Lemma)

Let  $\Sigma$  be a finite non-empty alphabet,  $X \subseteq \Sigma^*$  a regular language and  $R \subseteq \Sigma^* \times \Sigma^*$  a rational relation, then the language  $\langle R \rangle X$  is *regular*.

Proof.

**SKETCH.** A rational transducer  $\mathcal{T}$  recognising  $R$  and an automaton  $\mathcal{A}$  recognising  $X$  can be synchronised to form the synchronised product of the two, namely an automaton that recognises the  $\langle R \rangle X$ .  $\square$

This result also follows from Nivat's theorem.

# $\langle R \rangle X$ is Regular

Given a relation  $R$  and a language  $X$  define the language:

$$\langle R \rangle X = \{u \in \Sigma^* \mid \exists v \in X (uRv)\}$$

## Lemma (Regularity Preservation Lemma)

Let  $\Sigma$  be a finite non-empty alphabet,  $X \subseteq \Sigma^*$  a regular language and  $R \subseteq \Sigma^* \times \Sigma^*$  a rational relation, then the language  $\langle R \rangle X$  is **regular**.

Proof.

**SKETCH.** A rational transducer  $\mathcal{T}$  recognising  $R$  and an automaton  $\mathcal{A}$  recognising  $X$  can be synchronised to form the synchronised product of the two, namely an automaton that recognises the  $\langle R \rangle X$ .  $\square$

This result also follows from Nivat's theorem.

# $\langle R \rangle X$ is Regular

Given a relation  $R$  and a language  $X$  define the language:

$$\langle R \rangle X = \{u \in \Sigma^* \mid \exists v \in X (uRv)\}$$

## Lemma (Regularity Preservation Lemma)

Let  $\Sigma$  be a finite non-empty alphabet,  $X \subseteq \Sigma^*$  a regular language and  $R \subseteq \Sigma^* \times \Sigma^*$  a rational relation, then the language  $\langle R \rangle X$  is **regular**.

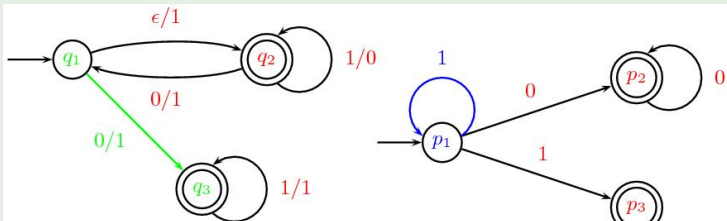
## Proof.

**SKETCH.** A rational transducer  $\mathcal{T}$  recognising  $R$  and an automaton  $\mathcal{A}$  recognising  $X$  can be synchronised to form the synchronised product of the two, namely an automaton that recognises the  $\langle R \rangle X$ .  $\square$

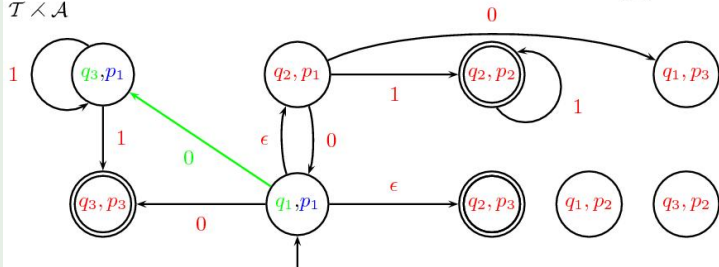
This result also follows from Nivat's theorem.

# $\langle R \rangle X$ is Regular - Example

## Example



$\mathcal{T} \times \mathcal{A}$



# Model Checking the Basic Tense Logic on Rational Kripke Models - 1

For a Kripke model  $\mathcal{M}$  and a formula  $\varphi \in K_t$ , let  $[[\varphi]]_{\mathcal{M}}$  denote the set of all states where  $\varphi$  is true.

## Theorem

*For every rational Kripke model  $\mathcal{M}$  and every formula  $\varphi \in K_t$ , the set  $[[\varphi]]_{\mathcal{M}}$  is an effectively computable **regular language**.*

## Proof.

The proof consists of structural induction on  $\varphi$ , using the **closure** of regular languages under **Booleans** and the **Regularity Preservation Lemma** from the previous slide. □

# Model checking tasks

Let  $\mathcal{M}$  be a Kripke model,  $u$  a state in  $\mathcal{M}$  and  $\varphi \in \mathcal{K}_t$ .

- 1 **Local model checking:** determine whether  $\mathcal{M}, u \models \varphi$ ;
- 2 **Global model checking:** determine the set  $[[\varphi]]_{\mathcal{M}}$ ; and
- 3 **Model satisfiability checking:** determine whether  $[[\varphi]]_{\mathcal{M}} \neq \emptyset$ .

# Model checking tasks

Let  $\mathcal{M}$  be a Kripke model,  $u$  a state in  $\mathcal{M}$  and  $\varphi \in \mathcal{K}_t$ .

- 1 **Local model checking:** determine whether  $\mathcal{M}, u \models \varphi$ ;
- 2 **Global model checking:** determine the set  $[[\varphi]]_{\mathcal{M}}$ ; and
- 3 **Model satisfiability checking:** determine whether  $[[\varphi]]_{\mathcal{M}} \neq \emptyset$ .

# Model checking tasks

Let  $\mathcal{M}$  be a Kripke model,  $u$  a state in  $\mathcal{M}$  and  $\varphi \in \mathcal{K}_t$ .

- 1 **Local model checking**: determine whether  $\mathcal{M}, u \models \varphi$ ;
- 2 **Global model checking**: determine the set  $[[\varphi]]_{\mathcal{M}}$ ; and
- 3 **Model satisfiability checking**: determine whether  $[[\varphi]]_{\mathcal{M}} \neq \emptyset$ .

# Model checking tasks

Let  $\mathcal{M}$  be a Kripke model,  $u$  a state in  $\mathcal{M}$  and  $\varphi \in \mathcal{K}_t$ .

- 1 **Local model checking:** determine whether  $\mathcal{M}, u \models \varphi$ ;
- 2 **Global model checking:** determine the set  $[[\varphi]]_{\mathcal{M}}$ ; and
- 3 **Model satisfiability checking:** determine whether  $[[\varphi]]_{\mathcal{M}} \neq \emptyset$ .

# Model Checking the Basic Tense Logic on rational Kripke models - 2

## Corollary

*Local model checking, global model checking, and model satisfiability checking of formulas of  $K_t$ -formulas in rational Kripke models are **algorithmically decidable**.*

## Definition

The **basic hybrid tense logic**  $\mathbf{H}_t$  extends the basic tense logic  $\mathbf{K}_t$  with a set of new atomic symbols  $\Theta$  called **nominals**. Syntactically the nominals form a second type of atomic formulae and are evaluated in Kripke models in **singleton sets** of states.

Nominals can be used to refer directly to states.

## Definition

$\mathbf{H}_t(U)$  is an extension of  $\mathbf{H}_t$ : add the **universal modality**  $[U]$  with semantics:

$$\mathcal{M}, u \models [U] \varphi \iff \mathcal{M}, w \models \varphi \text{ for every } w \in \mathcal{M}.$$

## Definition

The **basic hybrid tense logic**  $\mathbf{H}_t$  extends the basic tense logic  $\mathbf{K}_t$  with a set of new atomic symbols  $\Theta$  called **nominals**. Syntactically the nominals form a second type of atomic formulae and are evaluated in Kripke models in **singleton sets** of states.

Nominals can be used to refer directly to states.

## Definition

$\mathbf{H}_t(U)$  is an extension of  $\mathbf{H}_t$ : add the **universal modality**  $[U]$  with semantics:

$$\mathcal{M}, u \models [U]\varphi \iff \mathcal{M}, w \models \varphi \text{ for every } w \in \mathcal{M}.$$

# Model Checking $H_t(U)$ on rational Kripke models

## Theorem

*Local model checking, global model checking, and model satisfiability checking of formulas of  $K_t$ -formulas in rational Kripke models are **algorithmically decidable**.*

## Proof.

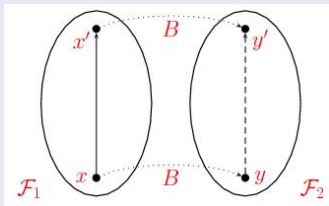
Valuations of nominals are **rational sets** since they are **singleton sets**.  
 $\llbracket [U]\varphi \rrbracket_{\mathcal{M}}$  is either **entire universe** of the model or the **empty set**.  
Hence, this claim follows from the decidability of model checking  $K_t$  on rational Kripke models. □

# Bisimulation Equivalence - 1

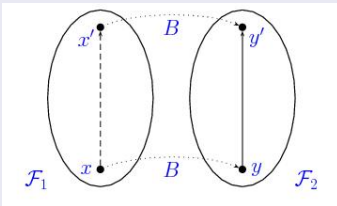
## Definition

Let  $\mathcal{F}_1 = (W_1, R_1)$  and  $\mathcal{F}_2 = (W_2, R_2)$  be rational Kripke frames.  $B \subseteq W_1 \times W_2$  is a **bisimulation** between  $\mathcal{F}_1$  and  $\mathcal{F}_2$  if it satisfies:

- 1 The forth condition:



- 2 The back condition:



## Definition

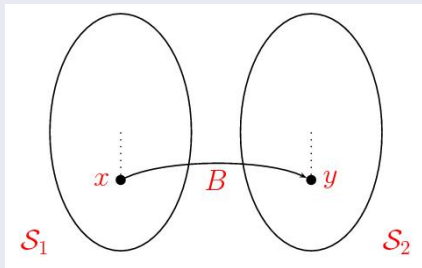
If  $\mathcal{M}_1 = (\mathcal{F}_1, V_1)$  and  $\mathcal{M}_2 = (\mathcal{F}_2, V_2)$  are two Kripke models  $B \subseteq W_1 \times W_2$  is a **bisimulation** between  $\mathcal{M}_1$  and  $\mathcal{M}_2$  if:

- 1 B is a bisimulation from  $\mathcal{F}_1$  to  $\mathcal{F}_2$ , and
- 2 if  $(x, y) \in B$  then  $x \in V_1(p) \iff y \in V_2(p)$  for  $p \in \Phi$ .

# Bisimilarity

## Definition

The **pointed** frames (models)  $(\mathcal{S}_1, x)$  and  $(\mathcal{S}_2, y)$  are **bisimilar** or **bisimulation equivalent**, if there is a bisimulation  $B$  between  $\mathcal{S}_1$  and  $\mathcal{S}_2$  such that  $xBy$ .



## Definition

If  $B$  is a bisimulation between two Kripke frames (models)  $\mathcal{S}_1$  and  $\mathcal{S}_2$ , such that every element in  $\mathcal{S}_1$  is related to some element in  $\mathcal{S}_2$  and vice versa, then  $B$  is a **global bisimulation** between the two structures.  $\mathcal{S}_1$  and  $\mathcal{S}_2$  are said to be **globally bisimilar**.

# Bisimulation Equivalence Results - 1

## Theorem

It is *undecidable* whether two given pointed rational Kripke frames are bisimilar.

## Proof.

SKETCH. [Jančar, STCS', 1994] proved that bisimilarity is undecidable for labeled Petri nets. But, the configuration graphs of Petri nets are rational graphs, and therefore Jančar's result carries over to rational Kripke frames. □

## Corollary

*It is **undecidable** whether two given rational Kripke frames are globally bisimilar.*

## Corollary

*It is **undecidable** whether two given pointed rational Kripke models are bisimilar, or whether two given rational Kripke models are globally bisimilar.*

## Theorem

It is *decidable* whether a given pointed rational Kripke model  $(\mathcal{M}_r, x)$  and given *finite* pointed Kripke model  $(\mathcal{M}_f, y)$  are bisimilar.

## Proof.

**SKETCH.** Two semi-algorithms can be run simultaneously:

- 1 A modified version of the [Paige-Tarjan algorithm](#)[SIAM J. Comput., 1987] symbolically computes the finite bisimulation quotient if it exists. Since two pointed Kripke structures are bisimilar if and only if their bisimulation quotients are isomorphic, the answer is positive if the procedure produces a finite Kripke model bisimilar to the given one.
- 2 A semi-algorithm subsequently tests for  $n$ -bisimulations between the models. If the two models are not bisimilar then for a large enough  $n$  there are no  $n$ -bisimulations.



## OPEN PROBLEMS:

- 1 **Generalise** to tree-rational and  $\omega$ -tree rational models.
- 2 What is the **strongest modal language** for which **model checking** is **decidable** on rational Kripke models?
- 3 Identify **natural subclasses** of rational Kripke models where model checking of  $K_t$  extended with **reachability** is decidable.
- 4 Is it the case that when a modal formula  $\varphi$  is satisfiable in a rational Kripke frame (i.e. there exists a valuation and state where it is true) then there exists a rational valuation satisfying  $\varphi$ ?