Model checking of invariants and LTL properties is very useful. But it has some limitations:

1. Explicit-state model checking algorithms can only deal with finite sets of reachable states.
2. Even if an equational abstraction can be used to make the set of reachable states finite, the set of abstracted initial states of interest may be infinite.
3. More generally, state infinity can block the use of explicit-state model checking in two different ways: The number of states reachable from a given state is infinite. The number of initial states is infinite.

This suggests two other options: (1) symbolic model checking (automatic) and (2) deductive methods based on theorem proving (more general). We will explore logics for option (2) in this lecture.
Model checking of invariants and LTL properties is very useful. But it has some limitations:

1. Explicit-state model checking algorithms can only deal with finite sets of reachable states.
2. Even if an equational abstraction can be used to make the set of reachable states finite, the set of abstracted initial states of interest may be infinite.
3. More generally, state infinity can block the use of explicit-state model checking in two different ways: The number of states reachable from a given state is infinite. The number of initial states is infinite.

This suggests two other options: (1) symbolic model checking (automatic) and (2) deductive methods based on theorem proving (more general). We will explore logics for option (2) in this lecture.
Model checking of invariants and LTL properties is very useful. But it has some limitations:

1. Explicit-state model checking algorithms can only deal with *finite* sets of reachable states.
Model checking of invariants and LTL properties is very useful. But it has some limitations:

1. Explicit-state model checking algorithms can only deal with *finite* sets of reachable states.
2. Even if an *equational abstraction* can be used to make the set of reachable states finite,
Deductive Verification of Distributed Systems

Model checking of invariants and LTL properties is very useful. But it has some limitations:

1. Explicit-state model checking algorithms can only deal with finite sets of reachable states.
2. Even if an equational abstraction can be used to make the set of reachable states finite, the set of abstracted initial states of interest may be infinite.
Deductive Verification of Distributed Systems

Model checking of invariants and LTL properties is very useful. But it has some limitations:

1. Explicit-state model checking algorithms can only deal with \textit{finite} sets of reachable states.

2. Even if an \textit{equational abstraction} can be used to make the set of reachable states finite, the \textit{set of abstracted initial states} of interest may be \textit{infinite}.

3. More generally, \textit{state infinity} can block the use of explicit-state model checking in two different ways:
Deductive Verification of Distributed Systems

Model checking of invariants and LTL properties is very useful. But it has some limitations:

1. Explicit-state model checking algorithms can only deal with finite sets of reachable states.
2. Even if an *equational abstraction* can be used to make the set of reachable states finite, the set of abstracted initial states of interest may be infinite.
3. More generally, *state infinity* can block the use of explicit-state model checking in two different ways:
   - The number of states reachable from a given state is *infinite*.
Model checking of invariants and LTL properties is very useful. But it has some limitations:

1. Explicit-state model checking algorithms can only deal with *finite* sets of reachable states.

2. Even if an *equational abstraction* can be used to make the set of reachable states finite, the *set of abstracted initial states* of interest may be *infinite*.

3. More generally, *state infinity* can block the use of explicit-state model checking in two different ways:
   - The number of states reachable from a given states is *infinite*.
   - The number of initial states is *infinite*. 
Deductive Verification of Distributed Systems

Model checking of invariants and LTL properties is very useful. But it has some limitations:

1. Explicit-state model checking algorithms can only deal with finite sets of reachable states.
2. Even if an equational abstraction can be used to make the set of reachable states finite, the set of abstracted initial states of interest may be infinite.
3. More generally, state infinity can block the use of explicit-state model checking in two different ways:
   - The number of states reachable from a given state is infinite.
   - The number of initial states is infinite.

This suggests two other options: (1) symbolic model checking (automatic)
Deductive Verification of Distributed Systems

Model checking of invariants and LTL properties is very useful. But it has some limitations:

1. Explicit-state model checking algorithms can only deal with *finite* sets of reachable states.

2. Even if an *equational abstraction* can be used to make the set of reachable states finite, the *set of abstracted initial states* of interest may be *infinite*.

3. More generally, *state infinity* can block the use of explicit-state model checking in two different ways:
   - The number of states reachable from a given states is *infinite*.
   - The number of initial states is *infinite*.

This suggests two other options: (1) *symbolic model checking* (automatic) and (2) *deductive methods* based on theorem proving (more general).
Deductive Verification of Distributed Systems

Model checking of invariants and LTL properties is very useful. But it has some limitations:

1. Explicit-state model checking algorithms can only deal with finite sets of reachable states.
2. Even if an equational abstraction can be used to make the set of reachable states finite, the set of abstracted initial states of interest may be infinite.
3. More generally, state infinity can block the use of explicit-state model checking in two different ways:
   - The number of states reachable from a given states is infinite.
   - The number of initial states is infinite.

This suggests two other options: (1) symbolic model checking (automatic) and (2) deductive methods based on theorem proving (more general). We will explore logics for option (2) in this lecture.
Suppose that a concurrent system has been specified by a rewrite theory $\mathcal{R}$,
Suppose that a concurrent system has been specified by a rewrite theory $R$, a top sort $State$ of states has been chosen, and
Suppose that a concurrent system has been specified by a rewrite theory $\mathcal{R}$, a top sort $State$ of states has been chosen, and some state predicates $\Pi$ have also been defined.
Suppose that a concurrent system has been specified by a rewrite theory $\mathcal{R}$, a top sort $State$ of states has been chosen, and some state predicates $\Pi$ have also been defined.

We can then define properties of $\mathcal{R}$ in Hoare Logic by means of so-called Hoare Triples of the form:
Hoare Logic

Suppose that a concurrent system has been specified by a rewrite theory \( \mathcal{R} \), a top sort \( \text{State} \) of states has been chosen, and some state predicates \( \Pi \) have also been defined.

We can then define properties of \( \mathcal{R} \) in \textit{Hoare Logic} by means of so-called \textit{Hoare Triples} of the form: \( \{A\} \ \mathcal{R} \ \{B\} \),
Suppose that a concurrent system has been specified by a rewrite theory $\mathcal{R}$, a top sort $State$ of states has been chosen, and some state predicates $\Pi$ have also been defined.

We can then define properties of $\mathcal{R}$ in Hoare Logic by means of so-called Hoare Triples of the form: $\{A\} \mathcal{R} \{B\}$, where $A$ and $B$ are formulas on predicates $\Pi$ defining sets of states $[A]$ and $[B]$. 
Hoare Logic

Suppose that a concurrent system has been specified by a rewrite theory $\mathcal{R}$, a top sort $State$ of states has been chosen, and some state predicates $\Pi$ have also been defined.

We can then define properties of $\mathcal{R}$ in Hoare Logic by means of so-called Hoare Triples of the form: $\{A\} \mathcal{R} \{B\}$, where $A$ and $B$ are formulas on predicates $\Pi$ defining sets of states $[A]$ and $[B]$.

$A$ is called the precondition and $B$ the postcondition.
Suppose that a concurrent system has been specified by a rewrite theory $\mathcal{R}$, a top sort $State$ of states has been chosen, and some \textit{state predicates} $\Pi$ have also been defined.

We can then define properties of $\mathcal{R}$ in \textit{Hoare Logic} by means of so-called \textit{Hoare Triples} of the form: $\{A\} \mathcal{R} \{B\}$, where $A$ and $B$ are \textit{formulas} on predicates $\Pi$ defining \textit{sets of states} $[A]$ and $[B]$.

$A$ is called the \textit{precondition} and $B$ the \textit{postcondition}. The Hoare triple $\{A\} \mathcal{R} \{B\}$ is a \textit{partial correctness assertion} about $\mathcal{R}$:
Suppose that a concurrent system has been specified by a rewrite theory \( R \), a top sort \( \textit{State} \) of states has been chosen, and some \textit{state predicates} \( \Pi \) have also been defined.

We can then define properties of \( R \) in Hoare Logic by means of so-called \textit{Hoare Triples} of the form: \( \{ A \} R \{ B \} \), where \( A \) and \( B \) are \textit{formulas} on predicates \( \Pi \) defining \textit{sets of states} \( \llbracket A \rrbracket \) and \( \llbracket B \rrbracket \).

\( A \) is called the \textit{precondition} and \( B \) the \textit{postcondition}. The Hoare triple \( \{ A \} R \{ B \} \) is a \textit{partial correctness assertion} about \( R \):

- for each state \( \llbracket u_0 \rrbracket \in \mathcal{T}_{R, \textit{State}} \), if \( \llbracket u_0 \rrbracket \) satisfies the precondition \( A \), then,
Suppose that a concurrent system has been specified by a rewrite theory $\mathcal{R}$, a top sort $State$ of states has been chosen, and some state predicates $\Pi$ have also been defined.

We can then define properties of $\mathcal{R}$ in Hoare Logic by means of so-called Hoare Triples of the form: $\{A\} \mathcal{R} \{B\}$, where $A$ and $B$ are formulas on predicates $\Pi$ defining sets of states $\llbracket A \rrbracket$ and $\llbracket B \rrbracket$.

$A$ is called the precondition and $B$ the postcondition. The Hoare triple $\{A\} \mathcal{R} \{B\}$ is a partial correctness assertion about $\mathcal{R}$:

- for each state $[u_0] \in \mathcal{T}_{\mathcal{R},State}$, if $[u_0]$ satisfies the precondition $A$, then,
- for each terminating sequence of transitions

$$[u_0] \rightarrow_{\mathcal{R}} [u_1] \ldots [u_{n-1}] \rightarrow_{\mathcal{R}} [u_n]$$

the terminating state $[u_n]$ satisfies postcondition $B$. 
What formulas $A$ and $B$ shall we use in a Hoare triple \( \{ A \} \mathcal{R} \{ B \} \)?
What formulas \( A \) and \( B \) shall we use in a Hoare triple
\( \{ A \} R \{ B \} \)? Assuming \( R = (\Sigma, B, R) \) has constructors \( \Omega \), we can
use *pattern predicates* of the form \( u \mid \varphi \) where \( u \) is an \( \Omega \)-term of
sort \( State \) and \( \varphi \) is a \( \Sigma \)-condition.
What formulas $A$ and $B$ shall we use in a Hoare triple \{A\} $\mathcal{R}$ \{B\}? Assuming $\mathcal{R} = (\Sigma, B, R)$ has constructors $\Omega$, we can use *pattern predicates* of the form $u | \varphi$ where $u$ is an $\Omega$-term of sort $State$ and $\varphi$ is a $\Sigma$-condition. Then $u | \varphi$ denotes the set of its ground instance states:

Let $Y = \text{vars}(A) \cap \text{vars}(B)$. Then we call $Y$ the *parameters* of the Hoare triple \{A\} $\mathcal{R}$ \{B\}. Such a triple is in fact universally quantified on its parameters. That is, \{A\} $\mathcal{R}$ \{B\} implicitly means: $(\forall Y) \{A\} \mathcal{R} \{B\}$. Let us see an example of a parametric Hoare triple involving a slight modification of the CHOICE module in Lecture 16.
What formulas $A$ and $B$ shall we use in a Hoare triple
\{ $A$ \} $\mathcal{R}$ \{ $B$ \}? Assuming $\mathcal{R} = (\Sigma, B, R)$ has constructors $\Omega$, we can use pattern predicates of the form $u \mid \varphi$ where $u$ is an $\Omega$-term of sort $\text{State}$ and $\varphi$ is a $\Sigma$-condition. Then $u \mid \varphi$ denotes the set of its ground instance states:

$$\llbracket u \mid \varphi \rrbracket = \{ [u\rho]_B \mid \rho \in [X \to T_\Omega] \land E \cup B \models \varphi\rho \}.$$
What formulas $A$ and $B$ shall we use in a Hoare triple $\{A\} \mathcal{R} \{B\}$? Assuming $\mathcal{R} = (\Sigma, B, R)$ has constructors $\Omega$, we can use pattern predicates of the form $u \mid \varphi$ where $u$ is an $\Omega$-term of sort $State$ and $\varphi$ is a $\Sigma$-condition. Then $u \mid \varphi$ denotes the set of its ground instance states:

$$\llbracket u \mid \varphi \rrbracket = \{[u\rho]_B \mid \rho \in [X \rightarrow T_\Omega] \land E \cup B \models \varphi_\rho\}.$$ 

Let $Y = \text{vars}(A) \cap \text{vars}(B)$. Then we call $Y$ the parameters of the Hoare triple $\{A\} \mathcal{R} \{B\}$. 


What formulas $A$ and $B$ shall we use in a Hoare triple $\{A\} R \{B\}$? Assuming $R = (\Sigma, B, R)$ has constructors $\Omega$, we can use *pattern predicates* of the form $u \mid \varphi$ where $u$ is an $\Omega$-term of sort $State$ and $\varphi$ is a $\Sigma$-condition. Then $u \mid \varphi$ denotes the set of its ground instance states:

$$[[u \mid \varphi] = \{[u\rho]_B \mid \rho \in [X \to T_\Omega] \land E \cup B \models \varphi\}.$$ 

Let $Y = \text{vars}(A) \cap \text{vars}(B)$. Then we call $Y$ the *parameters* of the Hoare triple $\{A\} R \{B\}$. Such a triple is in fact *universally quantified* on its parameters. That is, $\{A\} R \{B\}$ implicitly means: $(\forall Y) \{A\} R \{B\}$. 

**Pattern Predicates and Parameters**
What formulas $A$ and $B$ shall we use in a Hoare triple $\{A\} \mathcal{R} \{B\}$? Assuming $\mathcal{R} = (\Sigma, B, R)$ has constructors $\Omega$, we can use *pattern predicates* of the form $u \mid \varphi$ where $u$ is an $\Omega$-term of sort $\text{State}$ and $\varphi$ is a $\Sigma$-condition. Then $u \mid \varphi$ denotes the set of its ground instance states:

$$[[u \mid \varphi]] = \{[u\rho]_B \mid \rho \in [X \to T\Omega] \land E \cup B \models \varphi\rho\}.$$  

Let $Y = \text{vars}(A) \cap \text{vars}(B)$. Then we call $Y$ the *parameters* of the Hoare triple $\{A\} \mathcal{R} \{B\}$. Such a triple is in fact *universally quantified* on its parameters. That is, $\{A\} \mathcal{R} \{B\}$ implicitly means: $(\forall Y) \{A\} \mathcal{R} \{B\}$.

Let us see an example of a parametric Hoare triple involving a slight modification of the CHOICE module in Lecture 16.
mod CHOICE is
  protecting NAT .
sorts MSet State Pred .
subsorts Nat < MSet .
  op __ : MSet MSet -> MSet [ctor assoc comm] .
  op {_} : MSet -> State .
  op tt : -> Pred [ctor] .
  op _=C_ : MSet MSet -> Pred [ctor] . *** MSet containment
vars U V : MSet . var N : Nat .
  eq U =C U = tt .
  eq U =C U V = tt .
rl [choice] : {U V} => {U} .
endm
The Hoare triple: \{\{M\} | \top\} CHOICE \{\{N\} | N \subseteq M = tt\} is parametric on \(M\).
A Hoare Triple for the CHOICE Module

mod CHOICE is
  protecting NAT .
sorts MSet State Pred .
subsorts Nat < MSet .
op __ : MSet MSet -> MSet [ctor assoc comm] .
op {_} : MSet -> State .
op tt : -> Pred [ctor] .
op _=C_ : MSet MSet -> Pred [ctor] . *** MSet containment
vars U V : MSet . var N : Nat .
eq U =C U = tt .
eq U =C U V = tt .
rl [choice] : {U V} => {U} .
endm

The Hoare triple: \{\{ M \} | \top \} \text{CHOICE} \{\{ N \} | N \subseteq M = tt \} is 
\textit{parametric} on $M$. It states that for each $M$ every final state 
reachable from $\{ M \}$ is a singleton set $\{ N \}$ with $N$ in $M$. 
Hoare logic is widely used to state and verify properties of an
imperative program $p$ in, say, Java or C.
Hoare logic is widely used to state and verify properties of an *imperative program* $p$ in, say, Java or C. It is then written in the form $\{A\} p \{B\}$.
Hoare logic is widely used to state and verify properties of an imperative program $p$ in, say, Java or C. It is then written in the form $\{A\} p \{B\}$. We shall see later in the course that this is just a special case of a Hoare triple of the form $\{A'(p)\} \mathcal{R}_\mathcal{L} \{B'\}$, where $\mathcal{L}$ is the imperative programming language, and $\mathcal{R}_\mathcal{L}$ is the rewriting logic semantics of $\mathcal{L}$. 
Hoare logic is widely used to state and verify properties of an imperative program \( p \) in, say, Java or C. It is then written in the form \( \{A\} p \{B\} \). We shall see later in the course that this is just a special case of a Hoare triple of the form \( \{A'(p)\} \mathcal{R}_L \{B'\} \), where \( L \) is the imperative programming language, and \( \mathcal{R}_L \) is the rewriting logic semantics of \( L \).

A serious difficulty with traditional Hoare logic is that it is language-dependent. There is a Hoare logic for Java, another for C, and so on.
Hoare logic is widely used to state and verify properties of an *imperative program* $p$ in, say, Java or C. It is then written in the form $\{A\} \ p \ {B}$. We shall see later in the course that this is just a special case of a Hoare triple of the form $\{A'(p)\} \ R_L \ {B'}$, where $L$ is the imperative programming language, and $R_L$ is the *rewriting logic semantics* of $L$.

A serious difficulty with traditional Hoare logic is that it is *language-dependent*. There is a Hoare logic for Java, another for $C$, and so on. Furthermore, for each language *different inference rules* must be defined and proved correct.
Hoare logic is widely used to state and verify properties of an imperative program $p$ in, say, Java or C. It is then written in the form $\{A\} p \{B\}$. We shall see later in the course that this is just a special case of a Hoare triple of the form $\{A'(p)\} R_L \{B'\}$, where $L$ is the imperative programming language, and $R_L$ is the rewriting logic semantics of $L$.

A serious difficulty with traditional Hoare logic is that it is language-dependent. There is a Hoare logic for Java, another for C, and so on. Furthermore for each language different inference rules must be defined and proved correct.

Roşu, Stefanescu et al. at UIUC have made Hoare logic programming-language-independent by generalizing it to reachability logic.
Hoare logic is widely used to state and verify properties of an imperative program $p$ in, say, Java or C. It is then written in the form $\{A\} p \{B\}$. We shall see later in the course that this is just a special case of a Hoare triple of the form $\{A'(p)\} \mathcal{R}_L \{B'\}$, where $\mathcal{L}$ is the imperative programming language, and $\mathcal{R}_L$ is the rewriting logic semantics of $\mathcal{L}$.

A serious difficulty with traditional Hoare logic is that it is language-dependent. There is a Hoare logic for Java, another for C, and so on. Furthermore for each language different inference rules must be defined and proved correct.

Roșu, Stefanescu et al. at UIUC have made Hoare logic programming-language-independent by generalizing it to reachability logic.

Skeirik, Stefanescu and Meseguer at UIUC have in turn made reachability logic rewrite-theory-independent by defining it for rewrite theories $\mathcal{R}$. 

---

**From Hoare Logic to Reachability Logic**
Reachability Logic (RL) is:

Reachability Logic (RL) is:
Reachability Logic (RL) is:

- parameterized over an underlying \textit{rewrite theory} $R$

\begin{align*}
\nu \mid \phi \rightarrow \star \lor \bigwedge_i \nu_i \mid \psi_i
\end{align*}
Reachability Logic (RL) is:

- parameterized over an underlying *rewrite theory* $\mathcal{R}$
- considers formulas $A \longrightarrow^{\otimes} B$ where $A$ is a *pattern predicate*, and $B$ a *disjunction of pattern predicates*.

\[ u \mid \varphi \longrightarrow^{\otimes} \bigvee_{i} v_i \mid \psi_i \]
Reachability Logic (RL) is:

- parameterized over an underlying *rewrite theory* $\mathcal{R}$
- considers formulas $A \rightarrow^\ast B$ where $A$ is a *pattern predicate*, and $B$ a *disjunction of pattern predicates*.

$$u \mid \varphi \rightarrow^\ast \bigvee_{i} v_i \mid \psi_i$$

- a generalization of Hoare Logic *partial correctness*, i.e., $A \rightarrow^\ast B$ generalizes $\{A\} \mathcal{R} \{B\}$
Reachability Logic

Introduction

Reachability Logic (RL) is:

- parameterized over an underlying *rewrite theory* $\mathcal{R}$
- considers formulas $A \rightarrow^* B$ where $A$ is a *pattern predicate*, and $B$ a *disjunction of pattern predicates*.

$$ u \mid \varphi \rightarrow^* \bigvee_{i} v_i \mid \psi_i $$

- a generalization of Hoare Logic *partial correctness*, i.e., $A \rightarrow^* B$ generalizes $\{A\} \mathcal{R} \{B\}$
- directly captures *inductive reasoning* in *any* theory $\mathcal{R}$, unlike Hoare Logic, special rules for loops, etc, *unnecessary*
Q: What does the relation $A \rightarrow^\ast B$ mean?

A: Suppose we have:

(1) a rewrite theory $\mathcal{R}$
(2) pattern formulas $A, B$
(3) and terminating states $T$

Then $A \rightarrow^\ast B$ means:
for each state $[t] \in [A]$
and rewrite path $p$ from $[t]$, either:
(1) $p$ crosses $[B]$ or
(2) $p$ is infinite

---

indicates counterex.
satisfies $A \rightarrow^\ast B$
vacuously satisfies
Let \( R = (\Sigma, E \cup B, R) \) be a rewrite theory with good executability conditions, and having a subsignature \( \Omega \) of constructors and a chosen top sort \( State \) of states.
Let $R = (\Sigma, E \cup B, R)$ be a rewrite theory with good executability conditions, and having a subsignature $\Omega$ of constructors and a chosen top sort $State$ of states. Let $C_R$ denote the canonical reachability model.
Reachability Logic
Precise Definition

Let $\mathcal{R} = (\Sigma, E \cup B, R)$ be a rewrite theory with good executability conditions, and having a subsignature $\Omega$ of constructors and a chosen top sort $State$ of states. Let $C_\mathcal{R}$ denote the canonical reachability model. For a reachability formula $A \rightarrow^\ast B$ call $Y = \text{vars}(A) \cap \text{vars}(B)$ its \textit{parameters}. 
Let $\mathcal{R} = (\Sigma, E \cup B, R)$ be a rewrite theory with good executability conditions, and having a subsignature $\Omega$ of constructors and a chosen top sort $State$ of states. Let $C_R$ denote the canonical reachability model. For a reachability formula $A \rightarrow^\ast B$ call $Y = \text{vars}(A) \cap \text{vars}(B)$ its parameters.

If $Y = \emptyset$, then we write $\mathcal{R} \models A \rightarrow^\ast B$ iff
Let $\mathcal{R} = (\Sigma, E \cup B, R)$ be a rewrite theory with good executability conditions, and having a subsignature $\Omega$ of constructors and a chosen top sort $\text{State}$ of states. Let $\mathcal{C}_R$ denote the canonical reachability model. For a reachability formula $A \rightarrow^* B$ call $Y = \text{vars}(A) \cap \text{vars}(B)$ its parameters.

If $Y = \emptyset$, then we write $\mathcal{R} \models A \rightarrow^* B$ iff for each $[u_0] \in \mathcal{C}_R,\text{State}$ such that $[u_0] \in [A]$
Let $\mathcal{R} = (\Sigma, E \cup B, R)$ be a rewrite theory with good executability conditions, and having a subsignature $\Omega$ of constructors and a chosen top sort $\text{State}$ of states. Let $\mathcal{C}_\mathcal{R}$ denote the canonical reachability model. For a reachability formula $A \rightarrow^\ast B$ call $Y = \text{vars}(A) \cap \text{vars}(B)$ its parameters.

If $Y = \emptyset$, then we write $\mathcal{R} \models A \rightarrow^\ast B$ iff for each $[u_0] \in \mathcal{C}_{\mathcal{R}, \text{State}}$ such that $[u_0] \in [A]$ and each terminating sequence:
Reachability Logic
Precise Definition

Let $\mathcal{R} = (\Sigma, E \cup B, R)$ be a rewrite theory with good executability conditions, and having a subsignature $\Omega$ of constructors and a chosen top sort $State$ of states. Let $\mathcal{C}_\mathcal{R}$ denote the canonical reachability model. For a reachability formula $A \rightarrow^\ast B$ call $Y = \text{vars}(A) \cap \text{vars}(B)$ its parameters.

If $Y = \emptyset$, then we write $\mathcal{R} \models A \rightarrow^\ast B$ iff for each $[u_0] \in \mathcal{C}_\mathcal{R,State}$ such that $[u_0] \in \llbracket A \rrbracket$ and each terminating sequence:

$$[u_0] \rightarrow_{\mathcal{C}_\mathcal{R}} [u_1] \ldots [u_{n-1}] \rightarrow_{\mathcal{C}_\mathcal{R}} [u_n]$$
Let $\mathcal{R} = (\Sigma, E \cup B, R)$ be a rewrite theory with good executability conditions, and having a subsignature $\Omega$ of constructors and a chosen top sort $State$ of states. Let $\mathcal{C}_\mathcal{R}$ denote the canonical reachability model. For a reachability formula $A \xrightarrow{\ast} B$ call $Y = \text{vars}(A) \cap \text{vars}(B)$ its parameters.

If $Y = \emptyset$, then we write $\mathcal{R} \models A \xrightarrow{\ast} B$ iff for each $[u_0] \in \mathcal{C}_\mathcal{R},State$ such that $[u_0] \in [A]$ and each terminating sequence:

$$[u_0] \xrightarrow{\mathcal{C}_\mathcal{R}} [u_1] \ldots [u_{n-1}] \xrightarrow{\mathcal{C}_\mathcal{R}} [u_n]$$

there exist $j$, $0 \leq j \leq n$ such that $[u_j] \in [B]$. 
Reachability Logic
Precise Definition

Let $\mathcal{R} = (\Sigma, E \cup B, R)$ be a rewrite theory with good executability conditions, and having a subsignature $\Omega$ of constructors and a chosen top sort $\text{State}$ of states. Let $\mathcal{C}_\mathcal{R}$ denote the canonical reachability model. For a reachability formula $A \rightarrow^\ast B$ call $Y = \text{vars}(A) \cap \text{vars}(B)$ its parameters.

If $Y = \emptyset$, then we write $\mathcal{R} \models A \rightarrow^\ast B$ iff for each $[u_0] \in \mathcal{C}_\mathcal{R},\text{State}$ such that $[u_0] \in [A]$ and each terminating sequence:

$$[u_0] \rightarrow_{\mathcal{C}_\mathcal{R}} [u_1] \ldots [u_{n-1}] \rightarrow_{\mathcal{C}_\mathcal{R}} [u_n]$$

there exist $j$, $0 \leq j \leq n$ such that $[u_j] \in [B]$.

If $Y \neq \emptyset$, then we write $\mathcal{R} \models A \rightarrow^\ast B$ iff
Reachability Logic
Precise Definition

Let $\mathcal{R} = (\Sigma, E \cup B, R)$ be a rewrite theory with good executability conditions, and having a subsignature $\Omega$ of constructors and a chosen top sort $State$ of states. Let $\mathcal{C}_\mathcal{R}$ denote the canonical reachability model. For a reachability formula $A \longrightarrow^\ast B$ call $Y = \text{vars}(A) \cap \text{vars}(B)$ its parameters.

If $Y = \emptyset$, then we write $\mathcal{R} \models A \longrightarrow^\ast B$ iff for each $[u_0] \in \mathcal{C}_{\mathcal{R},State}$ such that $[u_0] \in \llbracket A \rrbracket$ and each terminating sequence:

$$[u_0] \rightarrow_{\mathcal{C}_\mathcal{R}} [u_1] \ldots [u_{n-1}] \rightarrow_{\mathcal{C}_\mathcal{R}} [u_n]$$

there exist $j$, $0 \leq j \leq n$ such that $[u_j] \in \llbracket B \rrbracket$.

If $Y \neq \emptyset$, then we write $\mathcal{R} \models A \longrightarrow^\ast B$ iff for each $\rho \in [Y \rightarrow T_\Omega]$ we have $\mathcal{R} \models A\rho \longrightarrow^\ast B\rho$. 
Let $\mathcal{R} = (\Sigma, E \cup B, R)$ be a rewrite theory with good executability conditions, and having a subsignature $\Omega$ of constructors and a chosen top sort $State$ of states. Let $C_\mathcal{R}$ denote the canonical reachability model. For a reachability formula $A \rightarrow^* B$ call $Y = \text{vars}(A) \cap \text{vars}(B)$ its parameters.

If $Y = \emptyset$, then we write $\mathcal{R} \models A \rightarrow^* B$ iff for each $[u_0] \in C_\mathcal{R},State$ such that $[u_0] \in [A]$ and each terminating sequence:

$$[u_0] \rightarrow C_\mathcal{R} [u_1] \ldots [u_{n-1}] \rightarrow C_\mathcal{R} [u_n]$$

there exist $j$, $0 \leq j \leq n$ such that $[u_j] \in [B]$.

If $Y \neq \emptyset$, then we write $\mathcal{R} \models A \rightarrow^* B$ iff for each $\rho \in [Y \rightarrow T_\Omega]$ we have $\mathcal{R} \models A\rho \rightarrow^* B\rho$.

That is, the parameters $Y$ in $A \rightarrow^* B$ are universally quantified,
Reachability Logic
Precise Definition

Let \( \mathcal{R} = (\Sigma, E \cup B, R) \) be a rewrite theory with good executability conditions, and having a subsignature \( \Omega \) of constructors and a chosen top sort \( \text{State} \) of states. Let \( \mathcal{C}_\mathcal{R} \) denote the canonical reachability model. For a reachability formula \( A \rightarrow^* B \) call \( Y = \text{vars}(A) \cap \text{vars}(B) \) its parameters.

If \( Y = \emptyset \), then we write \( \mathcal{R} \models A \rightarrow^* B \) iff for each \( [u_0] \in \mathcal{C}_\mathcal{R},\text{State} \) such that \( [u_0] \in [A] \) and each terminating sequence:

\[
[u_0] \rightarrow_{\mathcal{C}_\mathcal{R}} [u_1] \ldots [u_{n-1}] \rightarrow_{\mathcal{C}_\mathcal{R}} [u_n]
\]

there exist \( j, 0 \leq j \leq n \) such that \( [u_j] \in [B] \).

If \( Y \neq \emptyset \), then we write \( \mathcal{R} \models A \rightarrow^* B \) iff for each \( \rho \in [Y \rightarrow T_\Omega] \) we have \( \mathcal{R} \models A\rho \rightarrow^* B\rho \).

That is, the parameters \( Y \) in \( A \rightarrow^* B \) are universally quantified, so that \( A \rightarrow^* B \) implicitly means: \((\forall Y) A \rightarrow^* B\).
Q: How is a Hoare triple \( \{A\} R \{B\} \) expressed in reachability logic?

A: as the formula \( A \overset{\text{→}}{\rightarrow} \text{⊛}(B \land T) \), with \( J \rightarrow T \rightarrow K \) the terminating states.

Q: How is a reachability logic sequent \( A \overset{\text{→}}{\rightarrow} \text{⊛} B \) expressed in linear temporal logic?

A: as the LTL formula \( A \rightarrow (\Box \text{enabled}) \lor \Diamond B \).

Example. For \textit{CHOICE}, the formula \( \{M\} |\top \overset{\text{→}}{\rightarrow} \text{⊛} \{M\}' |M' \subseteq M = \text{tt} \) is parametric on \( M \).

It states that for each \( M \) every state reachable from \( \{M\} \) is a submultiset \( M' \) of \( M \).

Note that this reachability property cannot be expressed by a Hoare triple.
Q: How is a Hoare triple $\{A\} \mathcal{R} \{B\}$ expressed in reachability logic?

A: as the formula $A \rightarrow^{\circ} (B \land T)$, with $\lbrack T\rbrack$ the terminating states.
Q: How is a Hoare triple $\{A\} \mathcal{R} \{B\}$ expressed in reachability logic?

A: as the formula $A \rightarrow^{\Diamond} (B \land T)$, with $\lceil T \rceil$ the terminating states.

Q: How is a reachability logic sequent $A \rightarrow^{\Diamond} B$ expressed in linear temporal logic?

Example. For CHOICE, the formula $\{M\} |\top \rightarrow^{\Diamond} \{M\}' |M' \subseteq M = \text{tt}$ is parametric on $M$. It states that for each $M$, every state reachable from $\{M\}$ is a submultiset $M'$ of $M$. Note that this reachability property cannot be expressed by a Hoare triple.
Q: How is a Hoare triple \( \{ A \} R \{ B \} \) expressed in reachability logic?

A: as the formula \( A \longrightarrow^\bullet (B \land T) \), with \([T]\) the terminating states.

Q: How is a reachability logic sequent \( A \longrightarrow^\bullet B \) expressed in linear temporal logic?

A: as the LTL formula \( A \rightarrow (\Box enabled) \lor \Diamond B \).
Q: How is a Hoare triple \( \{A\} R \{B\} \) expressed in reachability logic?

A: as the formula \( A \rightarrow^* (B \land T) \), with \([T]\) the terminating states.

Q: How is a reachability logic sequent \( A \rightarrow^* B \) expressed in linear temporal logic?

A: as the LTL formula \( A \rightarrow (\Box \text{enabled}) \lor \Diamond B \).

Example. For \texttt{CHOICE}, the formula

\[
\{M\} | \top \rightarrow^* \{M'\} \mid M' \subseteq M = tt
\]
Q: How is a Hoare triple $\{A\} R \{B\}$ expressed in reachability logic?

A: as the formula $A \rightarrow^\star (B \land T)$, with $[T]$ the terminating states.

Q: How is a reachability logic sequent $A \rightarrow^\star B$ expressed in linear temporal logic?

A: as the LTL formula $A \rightarrow (\square enabled) \lor \diamond B$.

Example. For CHOICE, the formula

\[
\{M\} \mid \top \rightarrow^\star \{M'\} \mid M' \subseteq M = tt
\]

is parametric on $M$. 
Q: How is a Hoare triple $\{A\} \mathcal{R} \{B\}$ expressed in reachability logic?

A: as the formula $A \rightarrow^{\star} (B \land T)$, with $[T]$ the terminating states.

Q: How is a reachability logic sequent $A \rightarrow^{\star} B$ expressed in linear temporal logic?

A: as the LTL formula $A \rightarrow (\Box enabled) \lor \Diamond B$.

Example. For CHOICE, the formula

\[
\{ M \} | \top \rightarrow^{\star} \{ M' \} | M' \subseteq M = \text{tt}
\]

is parametric on $M$. It states that for each $M$ every state reachable from $\{ M \}$ is a submultiset $M'$ of $M$. 
Q: How is a Hoare triple \( \{ A \} R \{ B \} \) expressed in reachability logic?

A: as the formula \( A \rightarrow^{\ast} (B \land T) \), with \( [T] \) the terminating states.

Q: How is a reachability logic sequent \( A \rightarrow^{\ast} B \) expressed in linear temporal logic?

A: as the LTL formula \( A \rightarrow (\square \text{enabled}) \lor \Diamond B \).

Example. For \textsc{choice}, the formula

\[
\{ M \} \mid \top \rightarrow^{\ast} \{ M' \} \mid M' \subseteq M = \text{tt}
\]

is \textit{parametric} on \( M \). It states that for each \( M \) every state reachable from \( \{ M \} \) is a submultiset \( M' \) of \( M \). Note that this reachability property \textit{cannot} be expressed by a Hoare triple.
Consider the readers and writers example (Lecture 18):
The Invariant Paradox

Consider the readers and writers example (Lecture 18):

modifiable READERS-WRITERS is
protecting NAT .
sort State .
op <_,_> : Nat Nat -> State [ctor] . --- readers/writers
vars R W : Nat .
rl < 0, 0 > => < 0, s(0) > .
rl < R, s(W) > => < R, W > .
rl < R, 0 > => < s(R), 0 > .
rl < s(R), W > => < R, W > .
endmod
The Invariant Paradox

Consider the readers and writers example (Lecture 18):

mod READERS-WRITERS is
protecting NAT .
sort State .
op <_,_> : Nat Nat -> State [ctor] . --- readers/writers
vars R W : Nat .
rl < 0, 0 > => < 0, s(0) > .
rl < R, s(W) > => < R, W > .
rl < R, 0 > => < s(R), 0 > .
rl < s(R), W > => < R, W > .
endm

Q: How can we express its *mutual exclusion* invariant as a reachability formula $A \rightarrow^\ast B$?
Consider the readers and writers example (Lecture 18):

mod READERS-WRITERS is
  protecting NAT .
sort State .
op <_,_> : Nat Nat -> State [ctor] . --- readers/writers
vars R W : Nat .
rl < 0, 0 > => < 0, s(0) > .
rl < R, s(W) > => < R, W > .
rl < R, 0 > => < s(R), 0 > .
rl < s(R), W > => < R, W > .
endm

Q: How can we express its *mutual exclusion* invariant as a reachability formula $A \xrightarrow{\ast} B$?

A: Since:
The Invariant Paradox

Consider the readers and writers example (Lecture 18):

\[
\text{mod READERS-WRITERS is}
\] protecting NAT.

\[
\text{sort State .}
\]

\[
\text{op < _, _> : Nat Nat -> State [ctor] . --- readers/writers}
\]

\[
\text{vars R W : Nat .}
\]

\[
\text{rl < 0, 0 > => < 0, s(0) > .}
\]

\[
\text{rl < R, s(W) > => < R, W > .}
\]

\[
\text{rl < R, 0 > => < s(R), 0 > .}
\]

\[
\text{rl < s(R), W > => < R, W > .}
\]

\endm

**Q:** How can we express its *mutual exclusion* invariant as a reachability formula \( A \rightarrow^* B \)?

**A:** Since: (i) \( A \rightarrow^* B \) just means \( A \rightarrow (\square \text{enabled}) \lor \Diamond B, \) and
Consider the readers and writers example (Lecture 18):

\begin{verbatim}
mod READERS-WRITERS is
  protecting NAT .
  sort State .
  op <_,_> : Nat Nat -> State [ctor] . --- readers/writers
  vars R W : Nat .
  rl < 0, 0 > => < 0, s(0) > .
  rl < R, s(W) > => < R, W > .
  rl < R, 0 > => < s(R), 0 > .
  rl < s(R), W > => < R, W > .
endm

Q: How can we express its \textit{mutual exclusion} invariant as a reachability formula $A \xrightarrow{\ast} B$?

A: Since: (i) $A \xrightarrow{\ast} B$ just means $A \rightarrow (\square \text{enabled}) \lor \diamond B$, and (ii) READERS-WRITERS is a \textit{never terminating} rewrite theory,
Consider the readers and writers example (Lecture 18):

\[
\text{mod READERS-WRITERS is}
\]
\[
\text{protecting NAT .}
\]
\[
\text{sort State .}
\]
\[
\text{op \(_{\text{_,_}}\) : Nat Nat \rightarrow State [ctor] . --- readers/writers}
\]
\[
\text{vars R W : Nat .}
\]
\[
\text{rl \(_{\text{< 0, 0 >}}\) \rightarrow \(_{\text{< 0, s(0) >}}\) .}
\]
\[
\text{rl \(_{\text{< R, s(W) >}}\) \rightarrow \(_{\text{< R, W >}}\) .}
\]
\[
\text{rl \(_{\text{< R, 0 >}}\) \rightarrow \(_{\text{< s(R), 0 >}}\) .}
\]
\[
\text{rl \(_{\text{< s(R), W >}}\) \rightarrow \(_{\text{< R, W >}}\).}
\]
\[
\text{endm}
\]

Q: How can we express its \textit{mutual exclusion} invariant as a reachability formula \(A \longrightarrow^\ast B\)?

A: Since: (i) \(A \longrightarrow^\ast B\) just means \(A \rightarrow (\square \text{enabled}) \lor \Diamond B\), and
(ii) READERS-WRITERS is a \textit{never terminating} rewrite theory, all formulas \(A \longrightarrow^\ast B\) are satisfied!!
Consider the readers and writers example (Lecture 18):

```plaintext
mod READERS-WRITERS is
  protecting NAT .
sort State .
op <_,_> : Nat Nat -> State [ctor] . --- readers/writers
vars R W : Nat .
rl < 0, 0 > => < 0, s(0) > .
rl < R, s(W) > => < R, W > .
rl < R, 0 > => < s(R), 0 > .
rl < s(R), W > => < R, W > .
endm
```

Q: How can we express its mutual exclusion invariant as a reachability formula $A \longrightarrow \ast B$?

A: Since: (i) $A \longrightarrow \ast B$ just means $A \rightarrow (\square \text{enabled}) \lor \Diamond B$, and (ii) READERS-WRITERS is a never terminating rewrite theory, all formulas $A \longrightarrow \ast B$ are satisfied!! So we cannot!!
The Invariant Paradox

Consider the readers and writers example (Lecture 18):

mod READERS-WRITERS is
  protecting NAT .
sort State .
op <_,_> : Nat Nat -> State [ctor] . --- readers/writers
vars R W : Nat .
rl < 0, 0 > => < 0, s(0) > .
rl < R, s(W) > => < R, W > .
rl < R, 0 > => < s(R), 0 > .
rl < s(R), W > => < R, W > .
endm

Q: How can we express its \textit{mutual exclusion} invariant as a reachability formula $A \longrightarrow^\ast B$?

A: Since: (i) $A \longrightarrow^\ast B$ just means $A \rightarrow (\Box \text{enabled}) \lor \Diamond B$, and (ii) READERS-WRITERS is a \textit{never terminating} rewrite theory, \textit{all} formulas $A \longrightarrow^\ast B$ are satisfied!! So we cannot!! (Paradox!!).
Solving the Invariant Paradox

Let us add a *stopwatch* to READERS-WRITERS as follows:

```
let us add a stopwatch to READERS-WRITERS as follows:
```

```mod READERS-WRITERS-stop is
protecting NAT .
sort State .
vars R W : Nat .
rl < 0, 0 > => < 0, s(0) > .
rl < R, s(W) > => < R, W > .
rl < R, 0 > => < s(R), 0 > .
rl < s(R), W > => < R, W > .
endm```

The rule `< R, W > => [R,W]` can now stop any state and make it terminating.

For any pattern predicate `B = ⟨ u,v ⟩|ϕ` let `[B]` denote the pattern predicate `[B] = [u,v]|ϕ`.

**Fact.** `B` is an invariant from initial states `S₀` in READERS-WRITERS iff `S₀ → ⊛[B]` holds in READERS-WRITERS-stop.
Solving the Invariant Paradox

Let us add a *stopwatch* to READERS–WRITERS as follows:

```plaintext
mod READERS-WRITERS-stop is
  protecting NAT .
  sort State .
  vars R W : Nat .
  rl < 0, 0 > => < 0, s(0) > .
  rl < R, s(W) > => < R, W > .
  rl < R, 0 > => < s(R), 0 > .
  rl < s(R), W > => < R, W > .
endm
```

The rule `< R, W > => [R,W]` can now stop any state and make it terminating. For any pattern predicate \( B = \langle u,v \rangle | \phi \) let \([B]\) denote the pattern predicate \([u,v]\) | \(\phi\).
Let us add a *stopwatch* to READERS–WRITERS as follows:

\[
\text{mod READERS–WRITERS-stop is }
\]

\[
\text{protecting NAT .}
\]

\[
\text{sort State .}
\]

\[
\text{op \( \langle \_, \_ \rangle \) : Nat Nat \rightarrow State [ctor] .}
\]

\[
\text{op \([\_, \_]\) : Nat Nat \rightarrow State [ctor] .}
\]

\[
\text{vars R W : Nat .}
\]

\[
\text{rl \( \langle 0, 0 \rangle \rightarrow \langle 0, s(0) \rangle \) .}
\]

\[
\text{rl \( \langle R, s(W) \rangle \rightarrow \langle R, W \rangle \) .}
\]

\[
\text{rl \( \langle R, 0 \rangle \rightarrow \langle s(R), 0 \rangle \) .}
\]

\[
\text{rl \( \langle s(R), W \rangle \rightarrow \langle R, W \rangle \) .}
\]

\[
\text{rl \( \langle R, W \rangle \rightarrow [R,W] \) .}
\]

\[
\text{endm}
\]

The rule \( \langle R, W \rangle \rightarrow [R,W] \) can now *stop* any state and make it terminating.
Let us add a *stopwatch* to READERS–WRITERS as follows:

mod READERS–WRITERS–stop is

protecting NAT .

sort State .


vars R W : Nat .

rl < 0, 0 > => < 0, s(0) > .

rl < R, s(W) > => < R, W > .

rl < R, 0 > => < s(R), 0 > .

rl < s(R), W > => < R, W > .


dendm

The rule < R, W > => [R,W] can now *stop* any state and make it terminating. For any pattern predicate $B = \langle u, v \rangle \mid \varphi$ let $[B]$ denote the pattern predicate $[B] = [u, v] \mid \varphi$. 
Solving the Invariant Paradox

Let us add a *stopwatch* to READERS–WRITERS as follows:

\[
\text{mod READERS–WRITERS–stop is}
\]

\[
\text{protecting NAT .}
\]

\[
\text{sort State .}
\]

\[
\text{op \(_{\_}\_\_\_\) : Nat Nat \rightarrow State [ctor] .}
\]

\[
\text{op \([\_\_\_\_] \) : Nat Nat \rightarrow State [ctor] .}
\]

\[
\text{vars R W : Nat .}
\]

\[
\text{rl \(< 0, 0 > \Rightarrow < 0, s(0) > .}
\]

\[
\text{rl \(< R, s(W) > \Rightarrow < R, W > .}
\]

\[
\text{rl \(< R, 0 > \Rightarrow < s(R), 0 > .}
\]

\[
\text{rl \(< s(R), W > \Rightarrow < R, W > .}
\]

\[
\text{rl \(< R, W > \Rightarrow [R,W] .}
\]

\[
\text{endm}
\]

The rule \(< R, W > \Rightarrow [R,W]\) can now *stop* any state and make it terminating. For any pattern predicate \(B = \langle u, v \rangle | \varphi\) let \([B]\) denote the pattern predicate \([B] = [u, v] | \varphi\).

**Fact.** \(B\) is an *invariant* from initial states \(S_0\) in READERS–WRITERS iff
Let us add a *stopwatch* to READERS–WRITERS as follows:

mod READERS–WRITERS–stop is
  protecting NAT.

sort State.


vars R W : Nat .

rl < 0, 0 > => < 0, s(0) > .
rl < R, s(W) > => < R, W > .
rl < R, 0 > => < s(R), 0 > .
rl < s(R), W > => < R, W > .
endm

The rule < R, W > => [R,W] can now stop any state and make it terminating. For any pattern predicate $B = \langle u, v \rangle | \phi$ let $[B]$ denote the pattern predicate $[B] = [u, v] | \phi$.

**Fact.** $B$ is an invariant from initial states $S_0$ in READERS–WRITERS iff $S_0 \rightarrow^\circ [B]$ holds in READERS–WRITERS–stop.
Solving the Invariant Paradox (General Case)

Suppose $\mathcal{R}$ is *never terminating* (has no terminating states),
Suppose $\mathcal{R}$ is never terminating (has no terminating states), $State$ has a single constructor $\langle \_, \ldots, \_ \rangle : s_1 \ldots s_n \to State$, 

Theorem $B$ is an invariant for $\mathcal{R}$ from initial states $S_0$ iff $S_0 \rightarrow^* \emptyset[B]$ holds in $\mathcal{R}_{stop}$.

Corollary If $J S_0 K \subseteq J B K$ and $B \rightarrow^* \emptyset[B]$ holds in $\mathcal{R}_{stop}$, then $B$ is an invariant for $\mathcal{R}$ from initial states $S_0$.

Example. Mutual exclusion from $\langle 0, 0 \rangle$ in READERS-WRITERS is the predicate: $\text{Mutex} = \langle R, W \rangle | W = 0 \lor (W = 1 \land R = 0)$.

We can prove it by showing:

(i) $\langle 0, 0 \rangle \in \text{Mutex}$ (easy), and

(ii) $\text{Mutex} \rightarrow^* \emptyset[\text{Mutex}]$ in $\text{READERS-WRITERS}_{\text{stop}}$. 


Suppose $\mathcal{R}$ is *never terminating* (has no terminating states), $\text{State}$ has a single constructor $\langle \_, \ldots, \_ \rangle : s_1 \ldots s_n \rightarrow \text{State}$, and all rules are between terms of sort $\text{State}$. 

---

**Theorem B** is an invariant for $\mathcal{R}$ from initial states $S_0$ iff $S_0 \rightarrow \mapsto \lbrack B \rbrack$ holds in $\mathcal{R}_{\text{stop}}$.

**Corollary** If $J S_0 K \subseteq J B K$ and $B \rightarrow \mapsto \lbrack B \rbrack$ holds in $\mathcal{R}_{\text{stop}}$, then $B$ is an invariant for $\mathcal{R}$ from initial states $S_0$.

**Example.** Mutual exclusion from $\langle 0, 0 \rangle$ in READERS-WRITERS is the predicate:

$$\text{Mutex} = \langle R, W \rangle | W = 0 \lor (W = 1 \land R = 0).$$

We can prove it by showing:

(i) $\langle 0, 0 \rangle \in \text{Mutex}$ (easy), and
(ii) $\text{Mutex} \rightarrow \mapsto \lbrack \text{Mutex} \rbrack$ in READERS-WRITERS-stop.
Suppose $\mathcal{R}$ is *never terminating* (has no terminating states), $\text{State}$ has a single constructor $\langle \_, \ldots, \_ \rangle : s_1 \ldots s_n \rightarrow \text{State}$, and all rules are between terms of sort $\text{State}$. Call $\mathcal{R}_{\text{stop}}$ the rewrite theory extending $\mathcal{R}$ by adding:

1. $\langle \_, \ldots, \_ \rangle : s_1 \ldots s_n \rightarrow \text{State}$, and
2. $\langle x_1, \ldots, x_n \rangle \rightarrow \langle x_1, \ldots, x_n \rangle$. 

Then:

**Theorem** $B$ is an invariant for $\mathcal{R}$ from initial states $S_0$ iff $S_0 \Rightarrow ^* \Box B$ holds in $\mathcal{R}_{\text{stop}}$.

**Corollary** If $J S_0 K \subseteq J B K$ and $B \Rightarrow ^* \Box B$ holds in $\mathcal{R}_{\text{stop}}$, then $B$ is an invariant for $\mathcal{R}$ from initial states $S_0$.

**Example.** Mutual exclusion from $\langle 0, 0 \rangle$ in READERS-WRITERS is the predicate:

$\text{Mutex} = \langle R, W \rangle | W = 0 \lor (W = 1 \land R = 0)$.

We can prove it by showing:

1. $\langle 0, 0 \rangle \in \text{Mutex}$ (easy), and
2. $\text{Mutex} \Rightarrow ^* \Box \text{Mutex}$ in $\text{READERS-WRITERS-stop}$. 

Suppose $\mathcal{R}$ is *never terminating* (has no terminating states), $\text{State}$ has a single constructor $\langle _, \ldots, _ \rangle : s_1 \ldots s_n \rightarrow \text{State}$, and all rules are between terms of sort $\text{State}$. Call $\mathcal{R}_{\text{stop}}$ the rewrite theory extending $\mathcal{R}$ by adding: (i) $\langle _, \ldots, _ \rangle : s_1 \ldots s_n \rightarrow \text{State}$, and
Suppose $\mathcal{R}$ is \textit{never terminating} (has no terminating states), $\text{State}$ has a single constructor $\langle _{, \ldots , _} \rangle : s_1 \ldots s_n \rightarrow \text{State}$, and all rules are between terms of sort $\text{State}$. Call $\mathcal{R}_{\text{stop}}$ the rewrite theory extending $\mathcal{R}$ by adding: (i) $\langle _{, \ldots , _} \rangle : s_1 \ldots s_n \rightarrow \text{State}$, and (ii) a stop rule $\langle x_1, \ldots , x_n \rangle \rightarrow [x_1, \ldots , x_n]$. 

**Theorem**

$B$ is an invariant for $\mathcal{R}$ from initial states $S_0$ iff $S_0 \rightarrow \Box [B]$ holds in $\mathcal{R}_{\text{stop}}$.

**Corollary**

If $J S_0 K \subseteq J B K$ and $B \rightarrow \Box [B]$ holds in $\mathcal{R}_{\text{stop}}$, then $B$ is an invariant for $\mathcal{R}$ from initial states $S_0$.

**Example**

Mutual exclusion from $\langle 0, 0 \rangle$ in READERS-WRITERS is the predicate: $\text{Mutex} = \langle R, W \rangle | W = 0 \lor (W = 1 \land R = 0)$. We can prove it by showing: (i) $\langle 0, 0 \rangle \in \text{Mutex}$ (easy), and (ii) $\text{Mutex} \rightarrow \Box [\text{Mutex}]$ in $\text{READERS-WRITERS-stop}$. 


Suppose $\mathcal{R}$ is *never terminating* (has no terminating states), $\textit{State}$ has a single constructor $\langle -, \ldots, - \rangle : s_1 \ldots s_n \rightarrow \textit{State}$, and all rules are between terms of sort $\textit{State}$. Call $\mathcal{R}_{\text{stop}}$ the rewrite theory extending $\mathcal{R}$ by adding: (i) $[\langle -, \ldots, - \rangle : s_1 \ldots s_n \rightarrow \textit{State}$, and (ii) a *stop rule* $\langle x_1, \ldots, x_n \rangle \rightarrow [x_1, \ldots, x_n]$. Then:
Suppose $\mathcal{R}$ is *never terminating* (has no terminating states), $\text{State}$ has a single constructor $\langle \_, \ldots, \_ \rangle : s_1 \ldots s_n \to \text{State}$, and all rules are between terms of sort $\text{State}$. Call $\mathcal{R}_{\text{stop}}$ the rewrite theory extending $\mathcal{R}$ by adding: (i) $\langle \_, \ldots, \_ \rangle : s_1 \ldots s_n \to \text{State}$, and (ii) a *stop rule* $\langle x_1, \ldots, x_n \rangle \to [x_1, \ldots, x_n]$. Then:

**Theorem**

$B$ is an invariant for $\mathcal{R}$ from initial states $S_0$ iff $S_0 \xrightarrow{\otimes} [B]$ holds in $\mathcal{R}_{\text{stop}}$. 

**Example.** Mutual exclusion from $\langle 0, 0 \rangle$ in READERS-WRITERS is the predicate:

$$
\text{Mutex} = \langle R, W \rangle| W = 0 \lor (W = 1 \land R = 0).
$$

We can prove it by showing: (i) $\langle 0, 0 \rangle \in \text{Mutex}$ (easy), and (ii) $\text{Mutex} \xrightarrow{\otimes} [\text{Mutex}]$ in $\text{READERS-WRITERS}_{\text{stop}}$. 


Solving the Invariant Paradox (General Case)

Suppose $\mathcal{R}$ is never terminating (has no terminating states), $\text{State}$ has a single constructor $\langle , \ldots , \rangle : s_1 \ldots s_n \rightarrow \text{State}$, and all rules are between terms of sort $\text{State}$. Call $\mathcal{R}_{\text{stop}}$ the rewrite theory extending $\mathcal{R}$ by adding: (i) $\langle , \ldots , \rangle : s_1 \ldots s_n \rightarrow \text{State}$, and (ii) a stop rule $\langle x_1, \ldots, x_n \rangle \rightarrow [x_1, \ldots, x_n]$. Then:

**Theorem**

$B$ is an invariant for $\mathcal{R}$ from initial states $S_0$ iff $S_0 \rightarrow^\ast [B]$ holds in $\mathcal{R}_{\text{stop}}$.

**Corollary**

If $[S_0] \subseteq [B]$ and $B \rightarrow^\ast [B]$ holds in $\mathcal{R}_{\text{stop}}$, then $B$ is an invariant for $\mathcal{R}$ from initial states $S_0$.  

Example. Mutual exclusion from $\langle 0, 0 \rangle$ in READERS-WRITERS is the predicate:

$$\text{Mutex} = \langle R, W \rangle | W = 0 \lor (W = 1 \land R = 0).$$

We can prove it by showing:

(i) $\langle 0, 0 \rangle \in \text{Mutex}$ (easy), and

(ii) $\text{Mutex} \rightarrow^\ast [\text{Mutex}]$ in $\text{READERS-WRITERS-stop}$. 
Solving the Invariant Paradox (General Case)

Suppose $\mathcal{R}$ is *never terminating* (has no terminating states), $\text{State}$ has a single constructor $\langle \_, \ldots, \_ \rangle : s_1 \ldots s_n \rightarrow \text{State}$, and all rules are between terms of sort $\text{State}$. Call $\mathcal{R}_{\text{stop}}$ the rewrite theory extending $\mathcal{R}$ by adding: (i) $\langle \_, \ldots, \_ \rangle : s_1 \ldots s_n \rightarrow \text{State}$, and (ii) a *stop rule* $\langle x_1, \ldots, x_n \rangle \rightarrow [x_1, \ldots, x_n]$. Then:

**Theorem**

$B$ is an invariant for $\mathcal{R}$ from initial sates $S_0$ iff $S_0 \xrightarrow{\ast} [B]$ holds in $\mathcal{R}_{\text{stop}}$.

**Corollary**

If $[S_0] \subseteq [B]$ and $B \xrightarrow{\ast} [B]$ holds in $\mathcal{R}_{\text{stop}}$, then $B$ is an invariant for $\mathcal{R}$ from initial sates $S_0$.

**Example.** Mutual exclusion from $\langle 0, 0 \rangle$ in READERS–WRITERS is the predicate:
Solving the Invariant Paradox (General Case)

Suppose \( R \) is *never terminating* (has no terminating states), \( \text{State} \) has a single constructor \( ⟨\_,\ldots,\_⟩ : s_1 \ldots s_n \rightarrow \text{State} \), and all rules are between terms of sort \( \text{State} \). Call \( R_{\text{stop}} \) the rewrite theory extending \( R \) by adding: (i) \( [\_,\ldots,\_] : s_1 \ldots s_n \rightarrow \text{State} \), and (ii) a *stop rule* \( ⟨x_1,\ldots,x_n⟩ \rightarrow [x_1,\ldots,x_n] \). Then:

**Theorem**

\( B \) is an invariant for \( R \) from initial states \( S_0 \) iff \( S_0 \rightarrow^* [B] \) holds in \( R_{\text{stop}} \).

**Corollary**

If \( [S_0] \subseteq [B] \) and \( B \rightarrow^* [B] \) holds in \( R_{\text{stop}} \), then \( B \) is an invariant for \( R \) from initial states \( S_0 \).

**Example.** Mutual exclusion from \( \langle 0, 0 \rangle \) in READERS–WRITERS is the predicate: \( \text{Mutex} = \langle R, W \rangle \mid W = 0 \lor (W = 1 \land R = 0) \).
Suppose $\mathcal{R}$ is *never terminating* (has no terminating states), $\textit{State}$ has a single constructor $\langle \_ , \ldots , \_ \rangle : s_1 \ldots s_n \rightarrow \textit{State}$, and all rules are between terms of sort $\textit{State}$. Call $\mathcal{R}_{\text{stop}}$ the rewrite theory extending $\mathcal{R}$ by adding: (i) $\langle \_ , \ldots , \_ \rangle : s_1 \ldots s_n \rightarrow \textit{State}$, and (ii) a *stop rule* $\langle x_1 , \ldots , x_n \rangle \rightarrow [x_1 , \ldots , x_n]$. Then:

**Theorem**

$B$ is an invariant for $\mathcal{R}$ from initial states $S_0$ iff $S_0 \stackrel{\ast}{\longrightarrow} [B]$ holds in $\mathcal{R}_{\text{stop}}$.

**Corollary**

If $[S_0] \subseteq [B]$ and $B \stackrel{\ast}{\longrightarrow} [B]$ holds in $\mathcal{R}_{\text{stop}}$, then $B$ is an invariant for $\mathcal{R}$ from initial states $S_0$.

**Example.** Mutual exclusion from $\langle 0, 0 \rangle$ in READERS–WRITERS is the predicate: $\textit{Mutex} = \langle R, W \rangle \mid W = 0 \lor (W = 1 \land R = 0)$. We can prove it by showing:
Suppose \( \mathcal{R} \) is *never terminating* (has no terminating states), \( \text{State} \) has a single constructor \( \langle \_, \ldots, \_ \rangle : s_1 \ldots s_n \rightarrow \text{State} \), and all rules are between terms of sort \( \text{State} \). Call \( \mathcal{R}_{\text{stop}} \) the rewrite theory extending \( \mathcal{R} \) by adding: (i) \( \langle \_, \ldots, \_ \rangle : s_1 \ldots s_n \rightarrow \text{State} \), and (ii) a stop rule \( \langle x_1, \ldots, x_n \rangle \rightarrow [x_1, \ldots, x_n] \). Then:

**Theorem**

\( B \) is an invariant for \( \mathcal{R} \) from initial sates \( S_0 \) iff \( S_0 \xrightarrow{\ast} [B] \) holds in \( \mathcal{R}_{\text{stop}} \).

**Corollary**

If \( [S_0] \subseteq [B] \) and \( B \xrightarrow{\ast} [B] \) holds in \( \mathcal{R}_{\text{stop}} \), then \( B \) is an invariant for \( \mathcal{R} \) from initial sates \( S_0 \).

**Example**. Mutual exclusion from \( \langle 0, 0 \rangle \) in READERS–WRITERS is the predicate: \( \text{Mutex} = \langle R, W \rangle \mid W = 0 \vee (W = 1 \land R = 0) \). We can prove it by showing: (i) \( \langle 0, 0 \rangle \in \text{Mutex} \) (easy), and
Suppose $\mathcal{R}$ is *never terminating* (has no terminating states), $\textit{State}$ has a single constructor $\langle \_, \ldots, \_ \rangle : s_1 \ldots s_n \rightarrow \textit{State}$, and all rules are between terms of sort $\textit{State}$. Call $\mathcal{R}_{\text{stop}}$ the rewrite theory extending $\mathcal{R}$ by adding: (i) $\langle \_, \ldots, \_ \rangle : s_1 \ldots s_n \rightarrow \textit{State}$, and (ii) a *stop rule* $\langle x_1, \ldots, x_n \rangle \rightarrow [x_1, \ldots, x_n]$. Then:

**Theorem**

$B$ is an invariant for $\mathcal{R}$ from initial states $S_0$ iff $S_0 \xrightarrow{\ast} [B]$ holds in $\mathcal{R}_{\text{stop}}$.

**Corollary**

If $[S_0] \subseteq [B]$ and $B \xrightarrow{\ast} [B]$ holds in $\mathcal{R}_{\text{stop}}$, then $B$ is an invariant for $\mathcal{R}$ from initial states $S_0$.

**Example.** Mutual exclusion from $\langle 0, 0 \rangle$ in READERS–WRITERS is the predicate: $\textit{Mutex} = \langle R, W \rangle \mid W = 0 \vee (W = 1 \land R = 0)$. We can prove it by showing: (i) $\langle 0, 0 \rangle \in \textit{Mutex}$ (easy), and (ii) $\textit{Mutex} \xrightarrow{\ast} [\textit{Mutex}]$ in READERS–WRITERS–stop.
Q: Then given RWL theory $\mathcal{R}$, how do we prove $A \xrightarrow{\oplus} B$?
Q: Then given RWL theory $\mathcal{R}$, how do we prove $A \xrightarrow{\odot} B$?

A: Perhaps surprisingly, two proof rules are enough.
Q: Then given RWL theory $\mathcal{R}$, how do we prove $A \rightarrow^\otimes B$?

A: Perhaps surprisingly, two proof rules are enough

- A rule that traces *rewrite steps* of *symbolic* states in $\mathcal{R}$
Q: Then given RWL theory $\mathcal{R}$, how do we prove $A \xrightarrow{\text{\tiny \circledast}} B$?

A: Perhaps surprisingly, two proof rules are enough

- A rule that traces *rewrite steps* of *symbolic* states in $\mathcal{R}$
- A rule that captures *circular behavior* of $\mathcal{R}$
Q: Then given RWL theory $\mathcal{R}$, how do we prove $A \rightarrow^{\circ} B$?
A: Perhaps surprisingly, two proof rules are enough

- A rule that traces *rewrite steps* of *symbolic* states in $\mathcal{R}$
- A rule that captures *circular behavior* of $\mathcal{R}$

We call these two rules *Step+Subsumption* and *Axiom* resp.
Q: Then given RWL theory $\mathcal{R}$, how do we prove $A \rightarrow^{\circlearrowright} B$?

A: Perhaps surprisingly, two proof rules are enough

- A rule that traces *rewrite steps* of *symbolic* states in $\mathcal{R}$
- A rule that captures *circular behavior* of $\mathcal{R}$

We call these two rules *Step+Subsumption* and *Axiom* resp.

The key ideas are:
Q: Then given RWL theory $\mathcal{R}$, how do we prove $A \xrightarrow{\star} B$?

A: Perhaps surprisingly, two proof rules are enough

- A rule that traces rewrite steps of symbolic states in $\mathcal{R}$
- A rule that captures circular behavior of $\mathcal{R}$

We call these two rules \textit{Step+Subsumption} and \textit{Axiom} resp.

The key ideas are: (i) to prove $A \xrightarrow{\star} B$ we may need some \textit{auxiliary lemmas}. 
Q: Then given RWL theory $\mathcal{R}$, how do we prove $A \xrightarrow{\Diamond} B$?

A: Perhaps surprisingly, two proof rules are enough

- A rule that traces \textit{rewrite steps} of \textit{symbolic} states in $\mathcal{R}$
- A rule that captures \textit{circular behavior} of $\mathcal{R}$

We call these two rules \textit{Step+Subsumption} and \textit{Axiom} resp.

The key ideas are: (i) to prove $A \xrightarrow{\Diamond} B$ we may need some \textit{auxiliary lemmas}. Call $\mathcal{C}$ the formulas $A \xrightarrow{\Diamond} B$ plus these lemmas;
Q: Then given RWL theory $\mathcal{R}$, how do we prove $A \rightarrow^{\ominus} B$?

A: Perhaps surprisingly, two proof rules are enough

- A rule that traces *rewrite steps* of *symbolic* states in $\mathcal{R}$
- A rule that captures *circular behavior* of $\mathcal{R}$

We call these two rules *Step+Subsumption* and *Axiom* resp.

The key ideas are: (i) to prove $A \rightarrow^{\ominus} B$ we may need some *auxiliary lemmas*. Call $C$ the formulas $A \rightarrow^{\ominus} B$ plus these lemmas; (ii) we start with labeled sequents of the form $[\emptyset, C] \vdash_T \ u \mid \varphi \rightarrow^{\ominus} \bigvee_i \nu_i \mid \psi_i$ for all formulas in $C$;
Q: Then given RWL theory $\mathcal{R}$, how do we prove $A \rightarrow^{\oplus} B$?

A: Perhaps surprisingly, two proof rules are enough

- A rule that traces *rewrite steps* of *symbolic* states in $\mathcal{R}$
- A rule that captures *circular behavior* of $\mathcal{R}$

We call these two rules *Step+Subsumption* and *Axiom* resp.

The key ideas are: (i) to prove $A \rightarrow^{\oplus} B$ we may need some *auxiliary lemmas*. Call $C$ the formulas $A \rightarrow^{\oplus} B$ plus these lemmas; (ii) we start with labeled sequents of the form $[\emptyset, C] \vdash_T u | \phi \rightarrow^{\oplus} \bigvee_i v_i | \psi_i$ for all formulas in $C$; (iii) the first component ($\emptyset$) are the formulas we can assume as *axioms* (none);
**Reachability Logic**

**Proof Rules**

**Q:** Then given RWL theory $\mathcal{R}$, how do we prove $A \longrightarrow^{\ast} B$?

**A:** Perhaps surprisingly, two proof rules are enough

- A rule that traces *rewrite steps* of *symbolic* states in $\mathcal{R}$
- A rule that captures *circular behavior* of $\mathcal{R}$

We call these two rules *Step+Subsumption* and *Axiom* resp.

The key ideas are: (i) to prove $A \longrightarrow^{\ast} B$ we may need some *auxiliary lemmas*. Call $C$ the formulas $A \longrightarrow^{\ast} B$ plus these lemmas; (ii) we start with labeled sequents of the form  

$[\emptyset, C] \vdash_{T} u \mid \varphi \longrightarrow^{\ast} \bigvee_{i} v_{i} \mid \psi_{i}$  

for all formulas in $C$; (iii) the first component ($\emptyset$) are the formulas we can assume as *axioms* (none); (iv) the second ($C$) the formulas we need to prove and cannot yet assume;
Q: Then given RWL theory $\mathcal{R}$, how do we prove $A \rightarrow^{\circlearrowright} B$?

A: Perhaps surprisingly, two proof rules are enough

- A rule that traces rewrite steps of symbolic states in $\mathcal{R}$
- A rule that captures circular behavior of $\mathcal{R}$

We call these two rules *Step+Subsumption* and *Axiom* resp.

The key ideas are: (i) to prove $A \rightarrow^{\circlearrowright} B$ we may need some auxiliary lemmas. Call $C$ the formulas $A \rightarrow^{\circlearrowright} B$ plus these lemmas; (ii) we start with labeled sequents of the form $[\emptyset, C] \vdash_{T} u \mid \varphi \rightarrow^{\circlearrowright} \lor_{i} v_{i} \mid \psi_{i}$ for all formulas in $C$; (iii) the first component ($\emptyset$) are the formulas we can assume as axioms (none); (iv) the second ($C$) the formulas we need to prove and cannot yet assume; (v) the *Step+Subsumption* rule allows us to inductively assume $C$ after a rewrite step with rules $R = \{l_{j} \rightarrow r_{j} \mid \phi_{j}\}$. 
Reachability Logic
Proof Rules

\[ \bigwedge_{(j, \alpha) \in \text{UNIFY}(u \mid \varphi', R)} [A \cup C, \emptyset] \vdash_T (r_j \mid \varphi' \land \phi_j)\alpha \rightarrow^* \bigvee_i (v_i \mid \psi_i)\alpha \]

\[ [A, C] \vdash_T u \mid \varphi \rightarrow^* \bigvee_i v_i \mid \psi_i \]

\[ \bigwedge_j [\{u' \mid \varphi' \rightarrow^* \bigvee_j v'_j \mid \psi'_j\} \cup A, \emptyset] \vdash_T v'_j\alpha \mid \varphi \land \psi'_j\alpha \rightarrow^* \bigvee_i v_i \mid \psi_i \]

\[ [\{u' \mid \varphi' \rightarrow^* \bigvee_j v'_j \mid \psi'_j\} \cup A, \emptyset] \vdash_T u \mid \varphi \rightarrow^* \bigvee_i v_i \mid \psi_i \]

The \textit{Step+Subsumption} and \textit{Axiom} Rules
Q: So what work has been done already?
Q: So what work has been done already?

A: A substantial RL framework is already in place with:

- full semantics for RL developed in terms of RWL
- soundness proof for proof system and semantics
- Maude tool semi-automating the proof system
- a collection of case studies.

Next lecture will illustrate the use of the Maude Reachability Logic tool by means of examples.
Q: So what work has been done already?

A: A substantial RL framework is already in place with:

- full semantics for RL developed in terms of RWL
Q: So what work has been done already?

A: A substantial RL framework is already in place with:
- full semantics for RL developed in terms of RWL
- soundness proof for proof system and semantics
Q: So what work has been done already?

A: A substantial RL framework is already in place with:
   - full semantics for RL developed in terms of RWL
   - soundness proof for proof system and semantics
   - Maude tool semi-automating the proof system
Q: So what work has been done already?

A: A substantial RL framework is already in place with:
- full semantics for RL developed in terms of RWL
- soundness proof for proof system and semantics
- Maude tool semi-automating the proof system
- a collection of case studies.
Q: So what work has been done already?

A: A substantial RL framework is already in place with:
  - full semantics for RL developed in terms of RWL
  - soundness proof for proof system and semantics
  - Maude tool semi-automating the proof system
  - a collection of case studies.

Next lecture will illustrate the use of the Maude Reachability Logic tool by means of examples.