

Putting it All Together

When we design a system, we would like to be sure that it will satisfy all requirements, such as safety.

What we can do:

- ▶ formally represent our system as a transition system (the symbolic representation);
- ▶ express the desired properties of the system in temporal logic.

What is missing?

Putting it All Together

When we design a system, we would like to be sure that it will satisfy all requirements, such as safety.

What we can do:

- ▶ formally represent our system as a transition system (the symbolic representation);
- ▶ express the desired properties of the system in temporal logic.

What is missing?

The Model Checking Problem

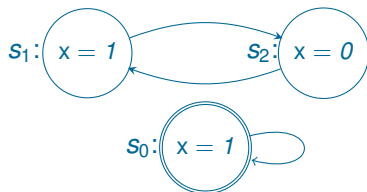
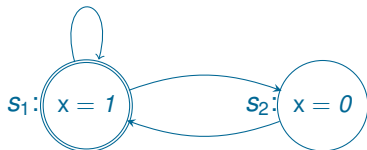
Given

1. a **symbolic representation** of a transition system;
2. a **temporal formula** F ,

check if every (some) computation of the system satisfies this formula, preferably in a **fully automatic way**.

Symbolic Representation and Transition Systems

Consider the transition systems with the following state transition graphs:



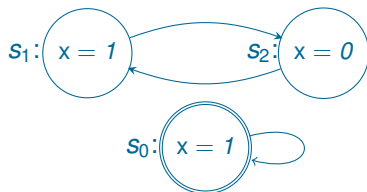
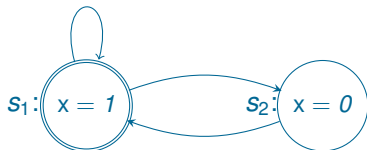
They have the same symbolic representation but satisfy different LTL formulas. For example, $\diamond \neg x$ is true in the first one but false in the second.

This may happen only if one of the transition systems has more than one different state with the same labelling function (states s_0 and s_1 in the second system).

We call such symbolic representations inadequate: one cannot distinguish two different states by a formula.

Symbolic Representation and Transition Systems

Consider the transition systems with the following state transition graphs:



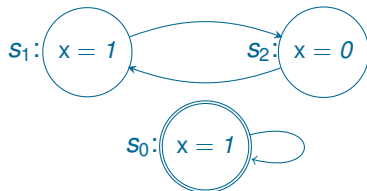
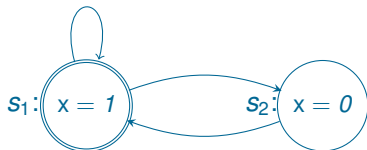
They have the **same symbolic representation** but satisfy **different LTL formulas**. For example, $\diamond \neg x$ is true in the first one but false in the second.

This may happen only if one of the transition systems has **more than one different state with the same labelling function** (states s_0 and s_1 in the second system).

We call such symbolic representations **inadequate**: one cannot distinguish two different states by a formula.

Symbolic Representation and Transition Systems

Consider the transition systems with the following state transition graphs:



They have the **same symbolic representation** but satisfy **different LTL formulas**. For example, $\diamond \neg x$ is true in the first one but false in the second.

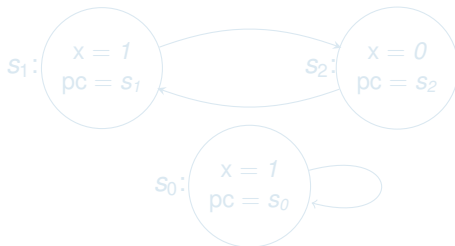
This may happen only if one of the transition systems has **more than one different state with the same labelling function** (states s_0 and s_1 in the second system).

We call such symbolic representations **inadequate**: one cannot distinguish two different states by a formula.

Making an Adequate Representation

If a transition system has **different states labeled by the same interpretation**, then introduce a **new state variable** that will distinguish any such pair of states.

For example, one can add a variable `pc` (program counter) ranging over all states such the value of `pc` at a state `s` is `s`.

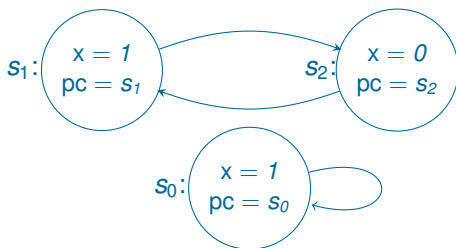


We assume that different states always have different labellings.

Making an Adequate Representation

If a transition system has **different states labeled by the same interpretation**, then introduce a **new state variable** that will distinguish any such pair of states.

For example, one can add a variable **pc** (program counter) ranging over all states such the value of **pc** at a state **s** is **s**.

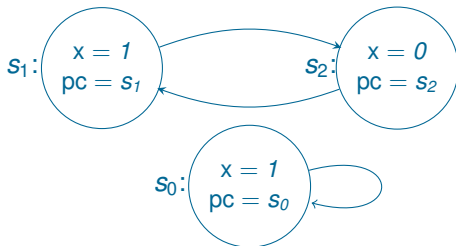


We assume that different states always have different labellings.

Making an Adequate Representation

If a transition system has **different states labeled by the same interpretation**, then introduce a **new state variable** that will distinguish any such pair of states.

For example, one can add a variable **pc** (program counter) ranging over all states such the value of **pc** at a state **s** is **s**.



We assume that different states always have different labellings.

Reachability and Safety Properties

A **reachability property** is expressed by a formula

$$\diamond F,$$

where F is a propositional formula.

A **safety property** is expressed by a formula

$$\square F,$$

where F is a propositional formula.

Reachability and Safety Properties

A **reachability property** is expressed by a formula

$$\diamond F,$$

where F is a propositional formula.

A **safety property** is expressed by a formula

$$\square F,$$

where F is a propositional formula.