02246 - Model Checking

$$M \models \Phi?$$

Lecture 05 - Bisimulations

Technical University of Denmark

Relating models

very abstract model

$$\begin{tikzcd} t_0 & T_0 \arrow[l, "\text{reduce}"'] \arrow[r, leftrightarrow] \arrow[d, bend left, "\text{refine}"] & T_0' \\ & T_1 \arrow[u, bend left, "\text{abstract}"] \arrow[d, bend left, "\text{refine}"] & \\ & \cdots \arrow[u, bend left, "\text{abstract}"] & \end{tikzcd}$$

alternative model
or new version

(implementation)

Are all these models “equivalent”?
Do they satisfy the same properties?

Key points of this lecture

Definition of bisimulation relation, a formal way to relate transition systems and states that have the same properties.

Definition of bisimulation equivalence, the most precise bisimulation relation.

Definition of bisimulation quotient, the smallest “reduced” transition system equivalent to a given one.

Bisimulation equivalence and CTL equivalence coincide! This means bisimilar transition systems satisfy the same CTL properties.

Bisimulations

- Reading material
- Bisimulation relations and bisimulation equivalence
- Computing bisimulations and reducing systems
- Bisimulations equivalence vs other equivalences
- Exercises & Homework

Reading material

Section 7, 7.1 and 7.2 of “Principles of Model Checking”

Bisimulations

- Reading material
- Bisimulation relations and bisimulation equivalence
- Computing bisimulations and reducing systems
- Bisimulations equivalence vs other equivalences
- Exercises & Homework

Definition of bisimulation between two transition systems

Let T and T' be transition systems.

A relation $R \subseteq S \times S'$ is a **bisimulation relation** iff

(0) Each initial state is related to at least another initial state

$\forall s \in I \,.\, \exists s' \in I' \,.\, (s, s') \in R$ and $\forall s' \in I' \,.\, \exists s \in I \,.\, (s, s') \in R$

Definition of bisimulation between two transition systems

Let T and T' be transition systems.

A relation $R \subseteq S \times S'$ is a **bisimulation relation** iff

(0) Each initial state is related to at least another initial state

$\forall s \in I\,.\, \exists s' \in I'\,.\, (s, s') \in R$ and $\forall s' \in I'\,.\, \exists s \in I\,.\, (s, s') \in R$

(1) Related states have the same labels

$(s, s') \in R \;\Rightarrow\; L(s) = L(s')$

Definition of bisimulation between two transition systems

Let T and T' be transition systems.

A relation $R \subseteq S \times S'$ is a **bisimulation relation** iff

(0) Each initial state is related to at least another initial state

$$\forall s \in I \,.\, \exists s' \in I' \,.\, (s, s') \in R \;\text{ and }\; \forall s' \in I' \,.\, \exists s \in I \,.\, (s, s') \in R$$

(1) Related states have the same labels

$$(s, s') \in R \;\Rightarrow\; L(s) = L(s')$$

(2) If T and T' are in related states, then T' can mimic T

$$(s, s') \in R \;\Rightarrow\; \forall s \rightarrow t \,.\, \exists s' \rightarrow t' \,.\, (t, t') \in R$$

$$\begin{tikzcd} s \arrow[d] & R & s' \\ t & & \end{tikzcd}$$

Definition of bisimulation between two transition systems

Let T and T' be transition systems.

A relation $R \subseteq S \times S'$ is a **bisimulation relation** iff

(0) Each initial state is related to at least another initial state

$$\forall s \in I \,.\, \exists s' \in I' \,.\, (s, s') \in R \quad \text{and} \quad \forall s' \in I' \,.\, \exists s \in I \,.\, (s, s') \in R$$

(1) Related states have the same labels

$$(s, s') \in R \;\Rightarrow\; L(s) = L(s')$$

(2) If T and T' are in related states, then T' can mimic T

$$(s, s') \in R \;\Rightarrow\; \forall s \to t \,.\, \exists s' \to t' \,.\, (t, t') \in R$$

$$\begin{tikzcd} s \arrow[d] & R & s' \arrow[d] \\ t & R & t' \end{tikzcd}$$

Definition of bisimulation between two transition systems

Let T and T' be transition systems.

A relation $R \subseteq S \times S'$ is a **bisimulation relation** iff

(0) Each initial state is related to at least another initial state

$$\forall s \in I \,.\, \exists s' \in I' \,.\, (s, s') \in R \quad \text{and} \quad \forall s' \in I' \,.\, \exists s \in I \,.\, (s, s') \in R$$

(1) Related states have the same labels

$$(s, s') \in R \;\Rightarrow\; L(s) = L(s')$$

(2) If T and T' are in related states, then T' can mimic T

$$(s, s') \in R \;\Rightarrow\; \forall s \to t \,.\, \exists s' \to t' \,.\, (t, t') \in R$$

$$\begin{tikzcd} s \arrow[d] & R & s' \arrow[d] \\ t & R & t' \end{tikzcd}$$

(3) Vice versa, T can also mimic T'.

$$(s, s') \in R \;\Rightarrow\; \forall s' \to t' \,.\, \exists s \to t \,.\, (t, t') \in R$$

$$\begin{tikzcd} s \arrow[d] & R & s' \arrow[d] \\ t & R & t' \end{tikzcd}$$

Definition of bisimulation between two transition systems

With bisimulation we can see if two models **behave** in the same way

Let T and T' be transition systems.

A relation $R \subseteq S \times S'$ is a **bisimulation relation** iff

(0) Each initial state is related to at least another initial state

$$\forall s \in I \,.\, \exists s' \in I' \,.\, (s, s') \in R \quad \text{and} \quad \forall s' \in I' \,.\, \exists s \in I \,.\, (s, s') \in R$$

(1) Related states have the same labels

$$(s, s') \in R \;\Rightarrow\; L(s) = L(s')$$

(2) If T and T' are in related states, then T' can mimic T

$$(s, s') \in R \;\Rightarrow\; \forall s \to t \,.\, \underline{\exists s' \to t' \,.\, (t, t') \in R}$$

$$\begin{tikzcd} s \arrow[d] \arrow[r, phantom, "R"] & s' \arrow[d] \\ t \arrow[r, phantom, "R"] & t' \end{tikzcd}$$

(3) Vice versa, T can also mimic T'.

$$(s, s') \in R \;\Rightarrow\; \forall s' \to t' \,.\, \underline{\exists s \to t \,.\, (t, t') \in R}$$

$$\begin{tikzcd} s \arrow[d] \arrow[r, phantom, "R"] & s' \arrow[d] \\ t \arrow[r, phantom, "R"] & t' \end{tikzcd}$$

Definition of bisimulation for just one transition system

Let T be a transition system.

A relation $R \subseteq S \times S$ is a **bisimulation relation** iff

(1) Related states have the same labels

$$(s, s') \in R \;\Rightarrow\; L(s) = L(s')$$

$$\begin{array}{ccc} s & R & s' \\ \downarrow & & \downarrow \\ t & R & t' \end{array}$$

(2) Related states can mimic each other

$$(s, s') \in R \;\Rightarrow\; \forall s \to t \,.\, \underline{\exists s' \to t' \,.\, (t, t') \in R}$$

$$(s, s') \in R \;\Rightarrow\; \forall s' \to t' \,.\, \underline{\exists s \to t \,.\, (t, t') \in R}$$

$$\begin{array}{ccc} s & R & s' \\ \downarrow & & \downarrow \\ t & R & t' \end{array}$$

Definition of bisimulation for just one transition system

Let T be a transition system.

A relation $R \subseteq S \times S$ is a **bisimulation relation** iff

(1) Related states have the same labels

$$(s, s') \in R \;\Rightarrow\; L(s) = L(s')$$

(2) Related states can mimic each other

$$(s, s') \in R \;\Rightarrow\; \forall s \to t \,.\, \exists s' \to t' \,.\, (t, t') \in R$$

$$\begin{tikzcd} s \arrow[d] \arrow[r, phantom, "R"] & s' \arrow[d] \\ t \arrow[r, phantom, "R"] & t' \end{tikzcd}$$

$$(s, s') \in R \;\Rightarrow\; \forall s' \to t' \,.\, \exists s \to t \,.\, (t, t') \in R$$

$$\begin{tikzcd} s \arrow[d] \arrow[r, phantom, "R"] & s' \arrow[d] \\ t \arrow[r, phantom, "R"] & t' \end{tikzcd}$$

The most "naive" bisimulation is the identity relation: **just relate each state with itself!**

Bisimulation equivalence

We say that **T and T' are bisimulation equivalent**, written

$$T \sim T'$$

iff there exists a bisimulation relation $R \subseteq S \times S'$

We say that **states s and s' are bisimulation equivalent**, written

$$s \sim s'$$

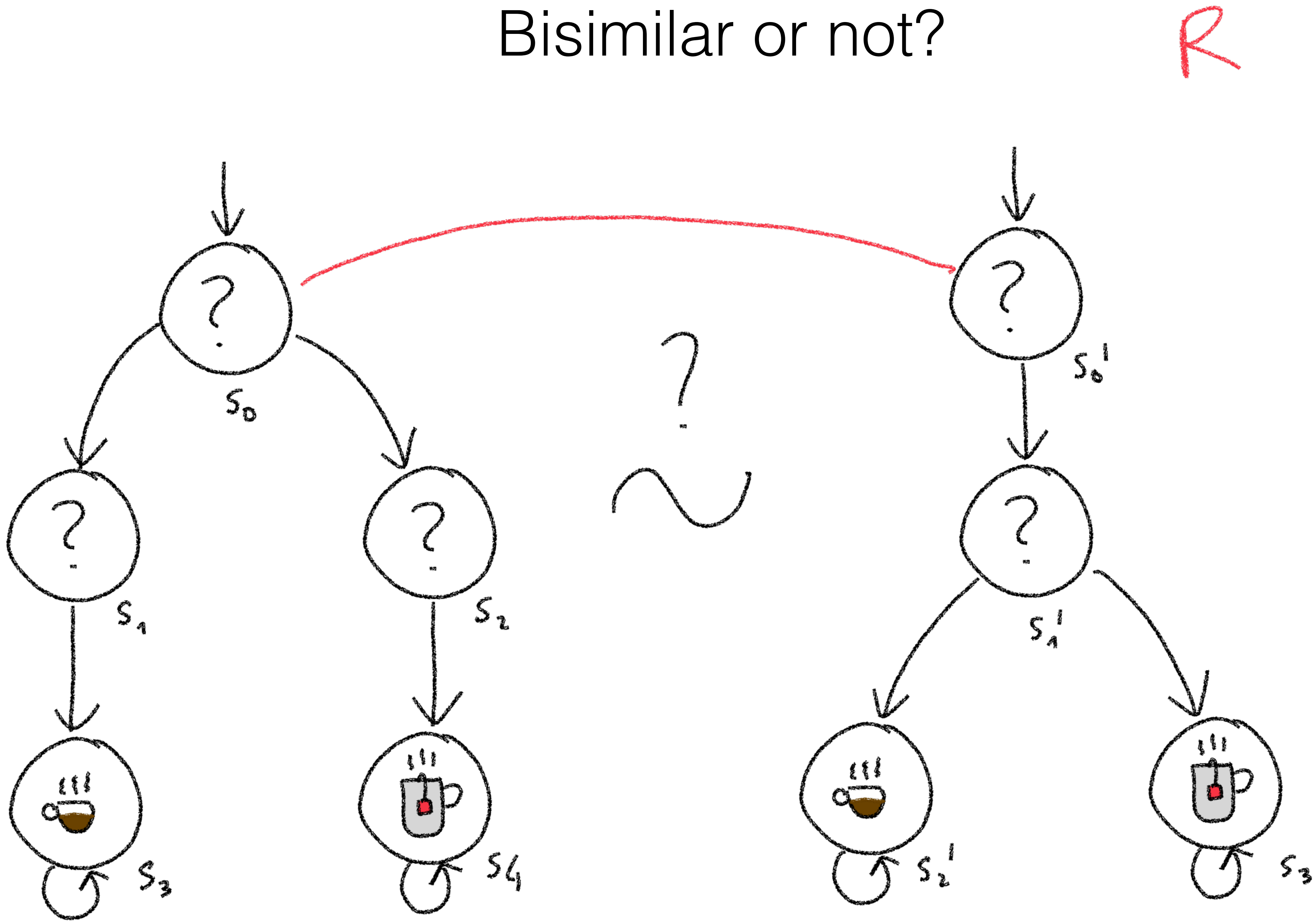
iff there exists a bisimulation relation $R \subseteq S \times S'$ such that

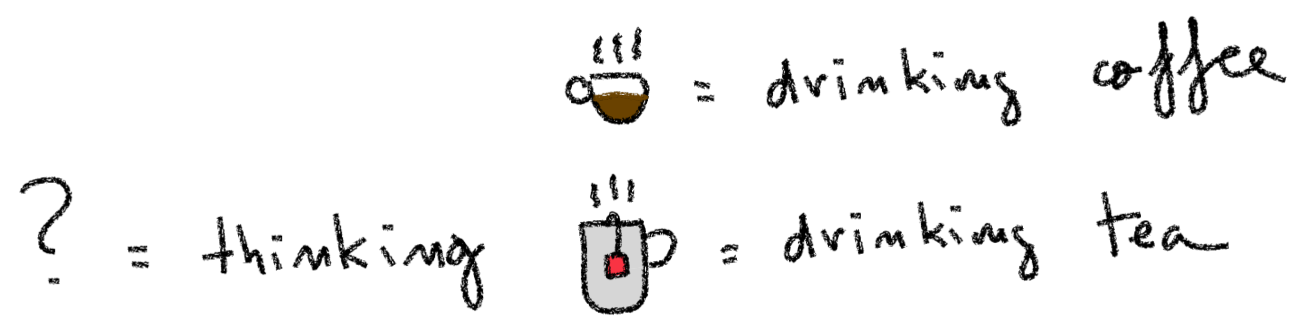
$$(s, s') \in R$$

Symbol ~ is also used for the **largest bisimulation relation** (called **bisimilarity**) for a given pair of transition systems (or a single one).

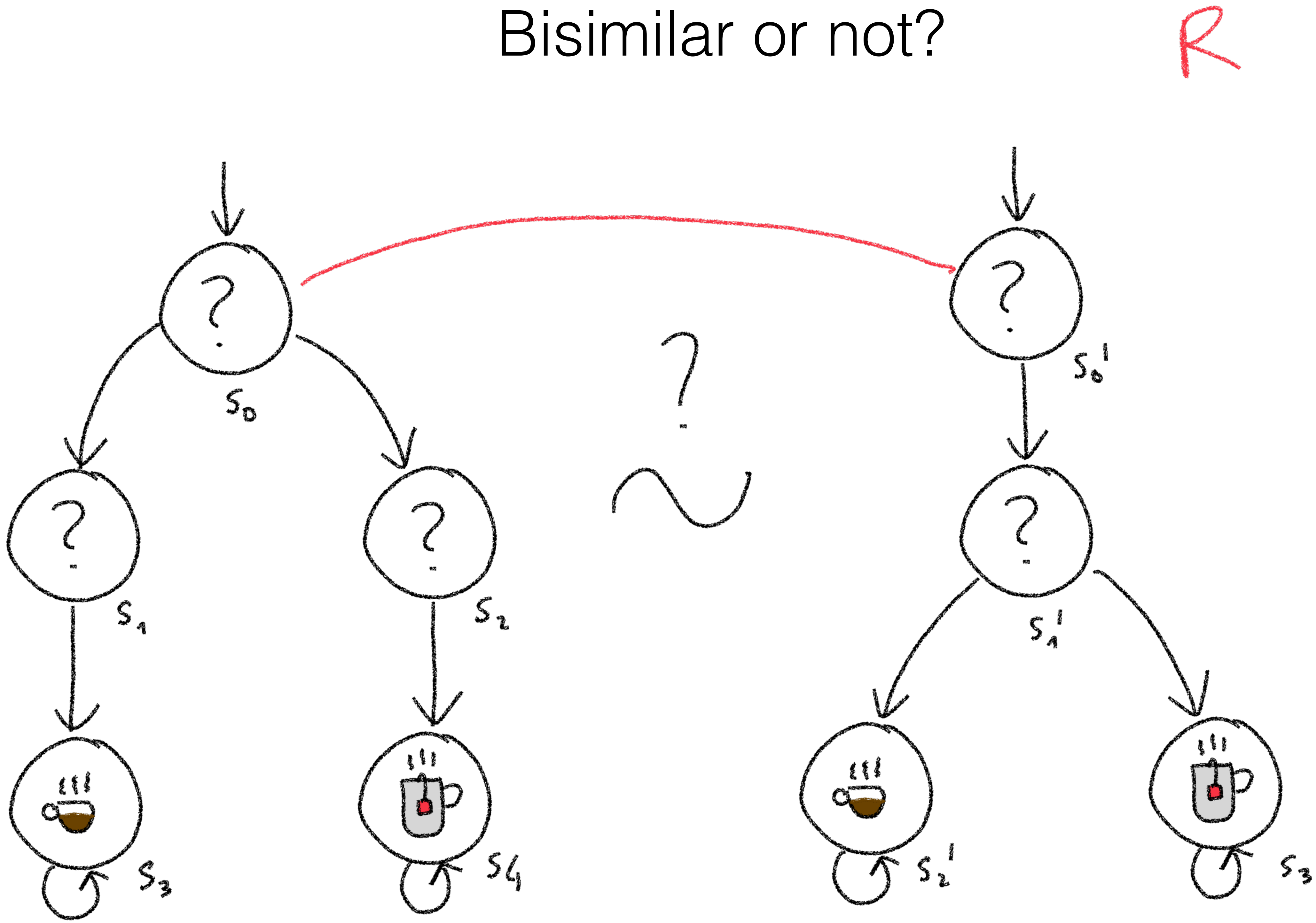
Bisimilarity happens to be the **union of all bisimulation relations**.

Bisimilar or not?



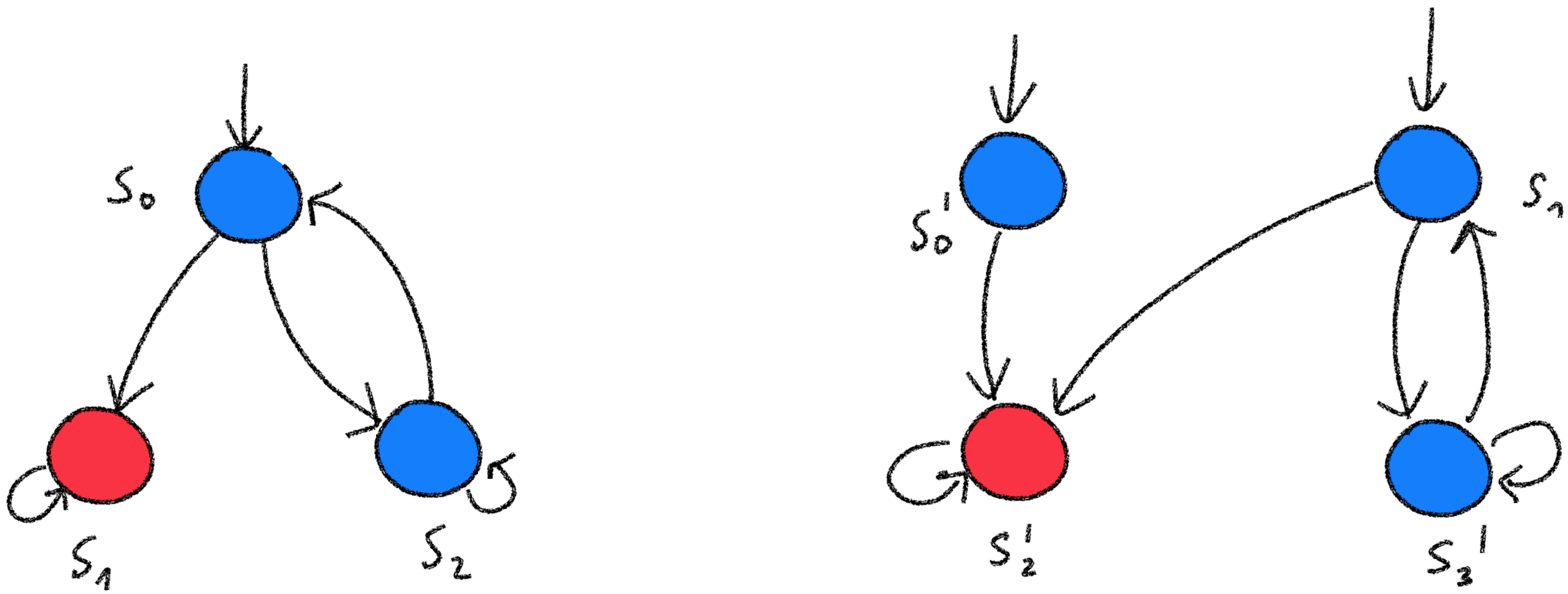


Bisimilar or not?

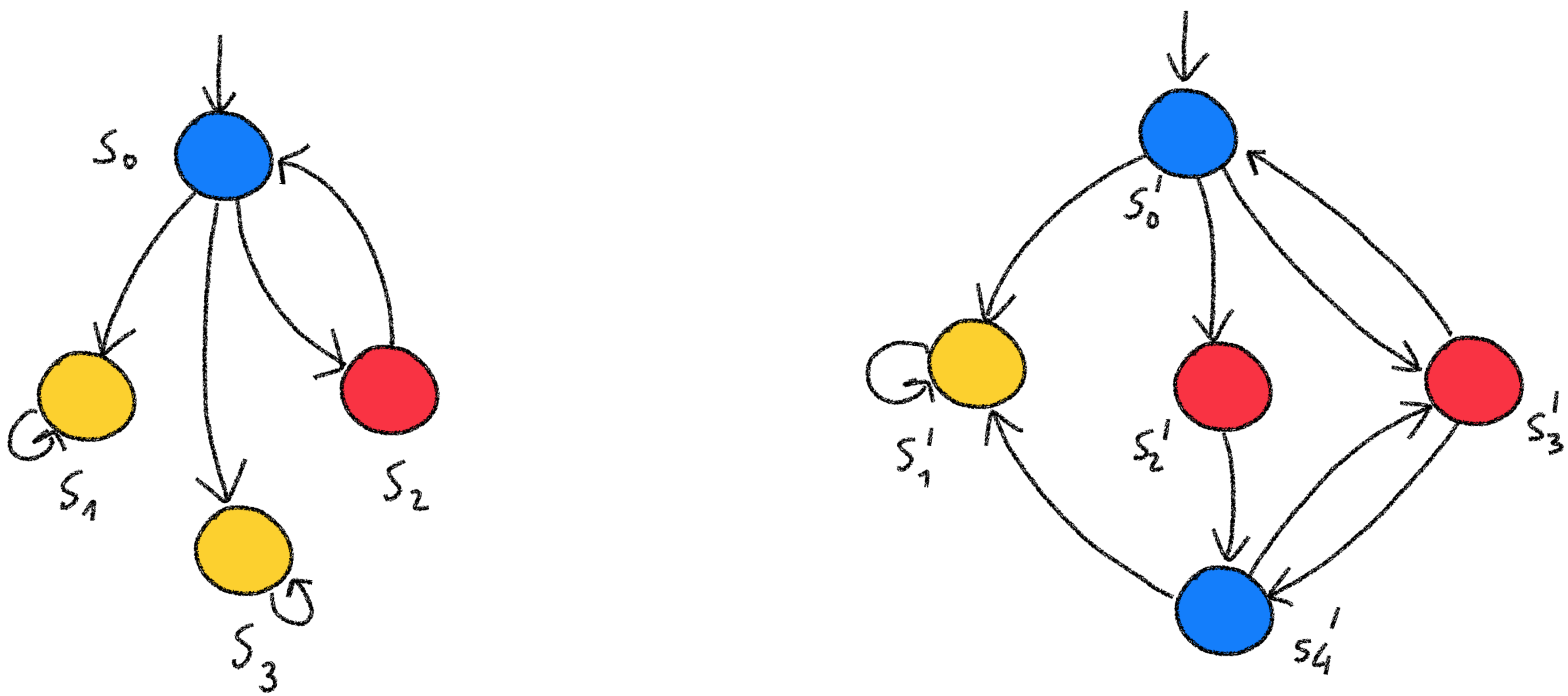


How can we fix the left transition system to achieve bisimulation equivalence?

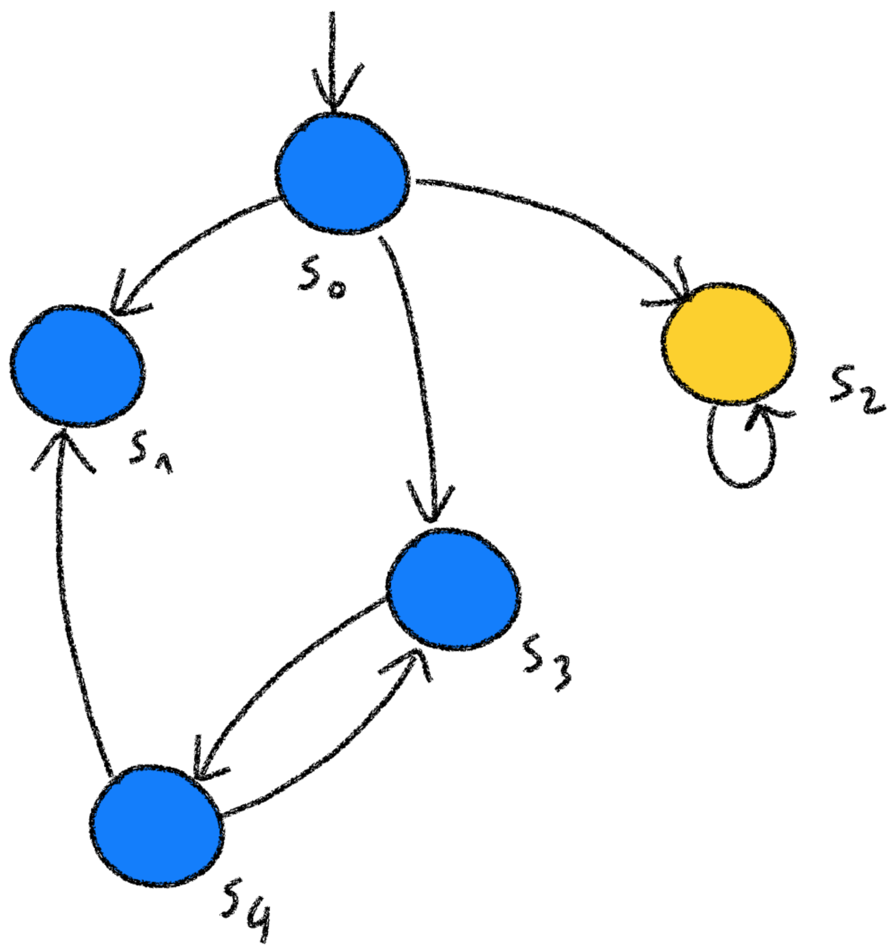
Bisimilar or not?

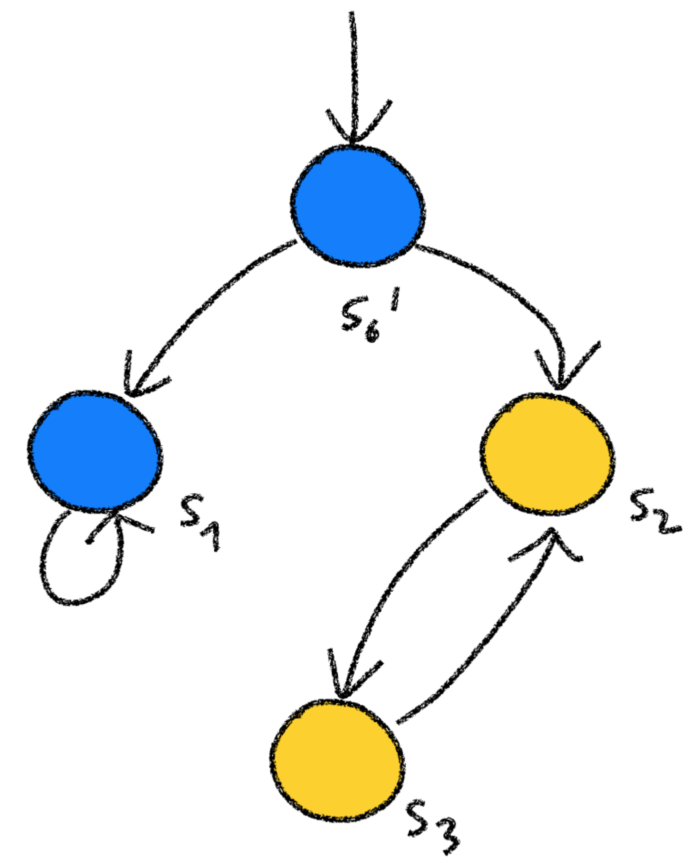


Bisimilar or not?

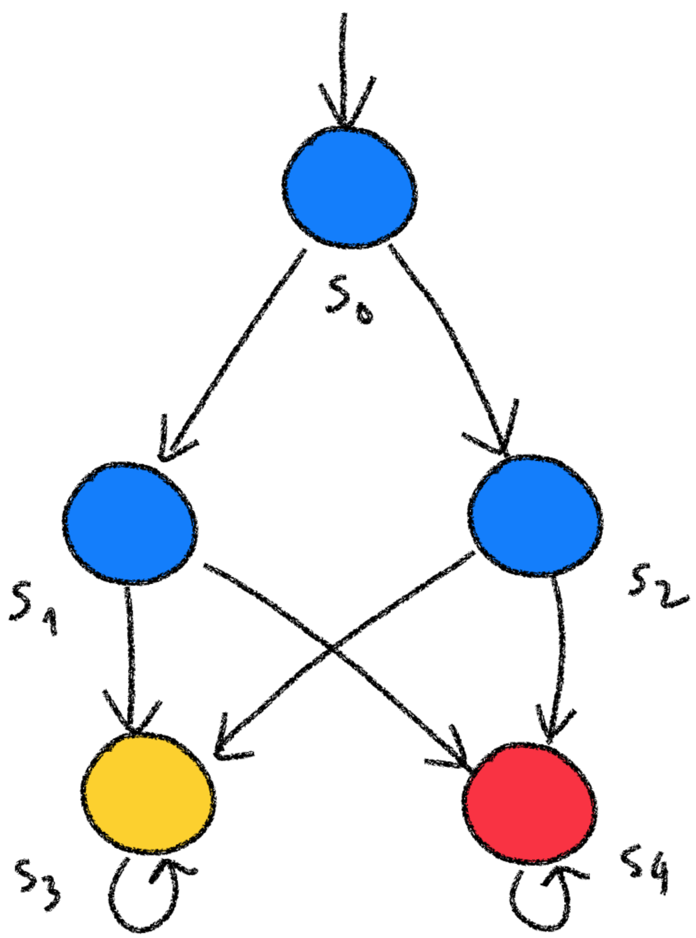


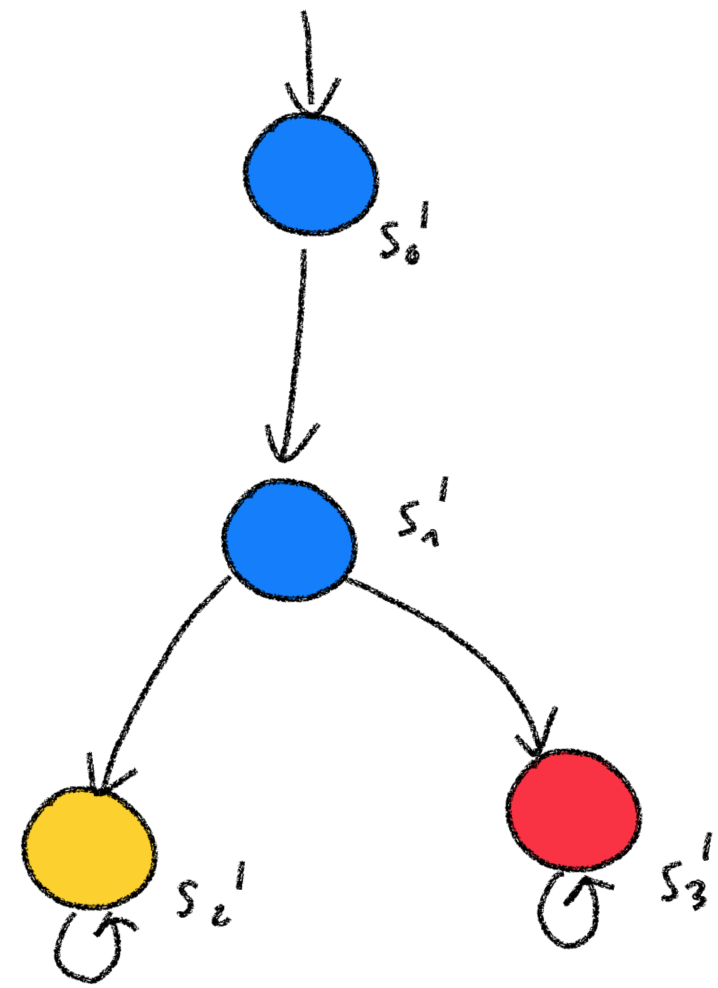
Bisimilar or not?





Bisimilar or not?





Properties of bisimilarity

Bisimilarity is **reflexive** (for one transition system)

$$T \sim T$$

Bisimilarity is **symmetric**

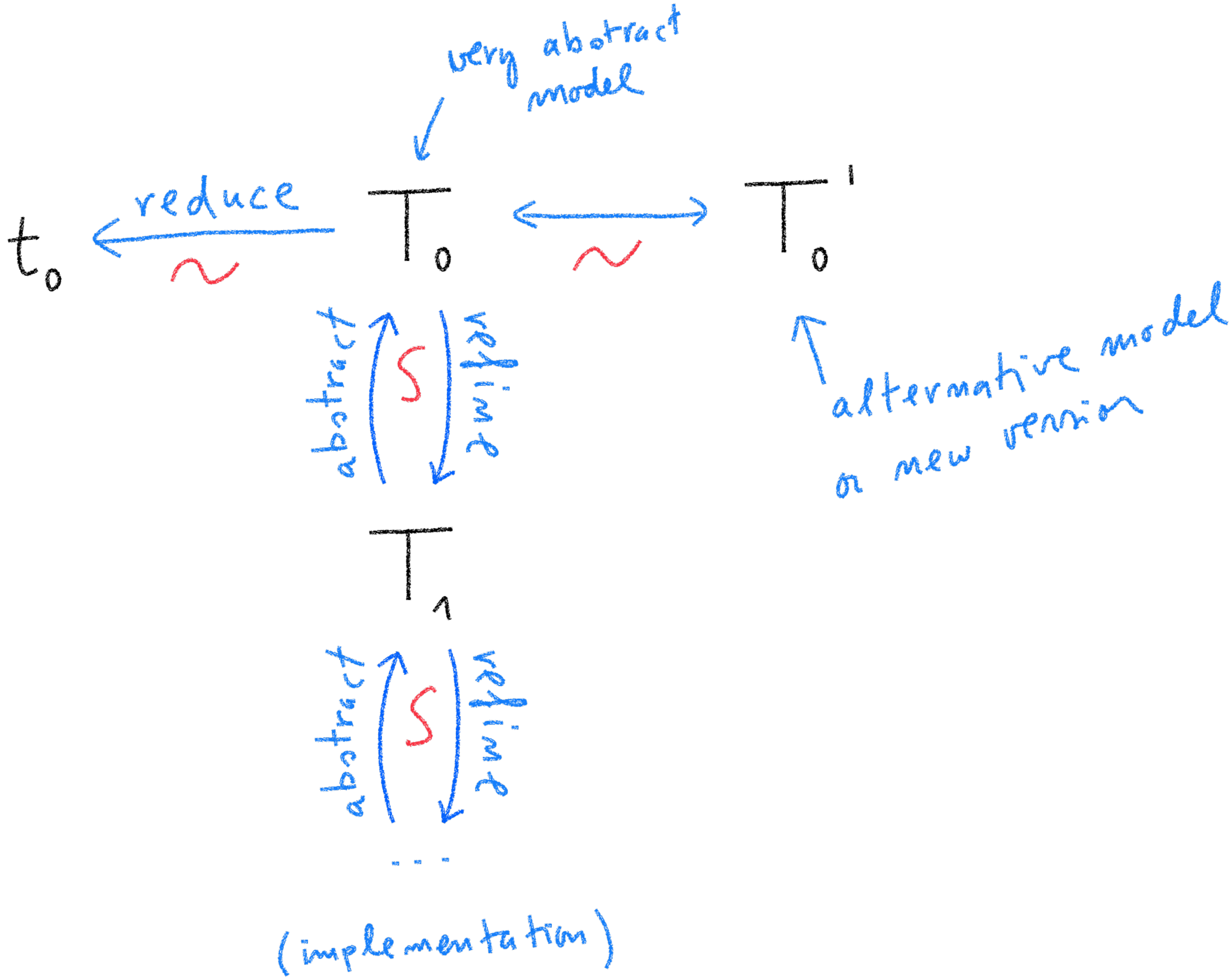
$T \sim T'$ implies $T' \sim T$

Bisimilarity is **transitive**

$T \sim T'$ and $T' \sim T''$ implies $T \sim T''$

In other words, bisimilarity is an **equivalence relation**.

Ideal situation



Properties of bisimulations for single transition systems

Let R be a bisimulation for T. Then…

- R is **reflexive**

  $(s, s) \in R$

- R is **symmetric**

  $(s, s') \in R$ implies $(s', s) \in R$

- R is **transitive**

  $(s, s') \in R$ and $(s', s'') \in R$ implies $(s, s'') \in R$

In other words, R is an equivalence relation.

Hence, we can work with the **equivalence classes of R**, as a more compact way of representing R, i.e. as a partition of S with blocks being equivalence classes.

Bisimulations

- Reading material
- Bisimulation relations and bisimulation equivalence
- Computing bisimulations and reducing systems
- Bisimulations equivalence vs other equivalences
- Exercises & Homework

Why compute bisimulations? And how?

hopefully small

very abstract model

$$t_0 \underset{\sim}{\xleftarrow{\text{reduce}}} T_0$$

model check this

potentially large

$t_0 \models \phi$ iff $T_0 \models \phi$

Partition refinement algorithm for one transition system

Rough sketch of the main idea:

Step 1:

Start optimistically guessing that **all states can be put together in the same equivalence class**. This gives you one single partition of the states.

Step 2:

Split the equivalence classes into one block for each different way of labelling states (i.e. each different subset of AP).

Step 3:

For all blocks B in the current partition

check if the states in B satisfy condition (2) of bisimulation, i.e. that states in the same block can mimic each other. If that is not true, split B to make the condition hold and restart the loop (step 3).

If you reach this point the **current partition** is the **bisimilarity relation**!

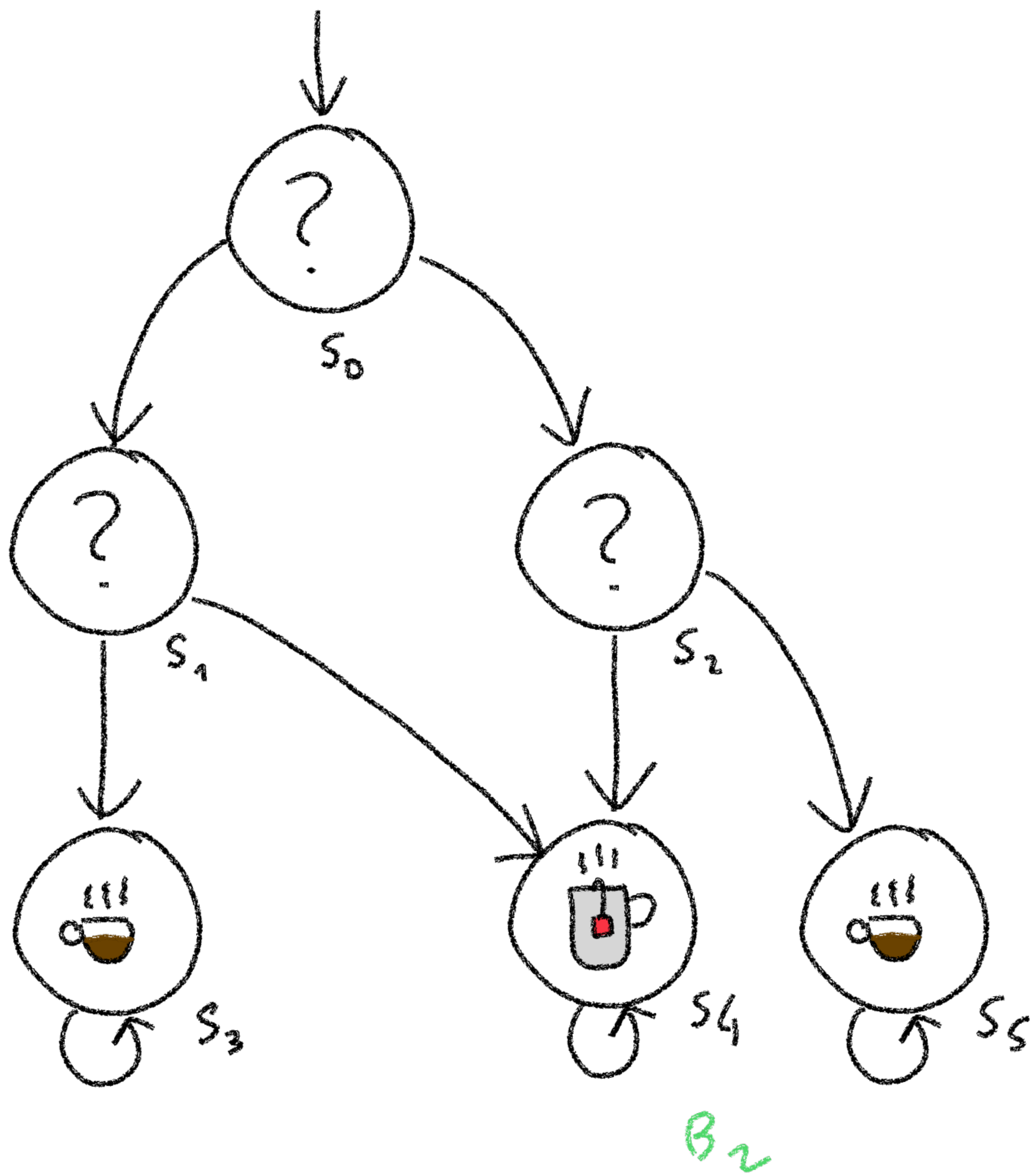
NOTE: efficient algorithms exist, which follow this idea but are smart in the refinement loop, to avoid duplicate checks.

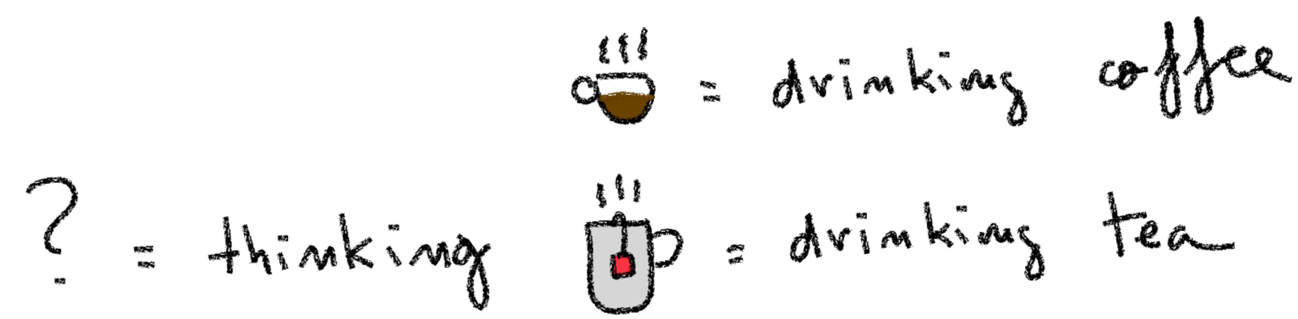
Partition refinement algorithm for one transition system

Now in pseudo-code

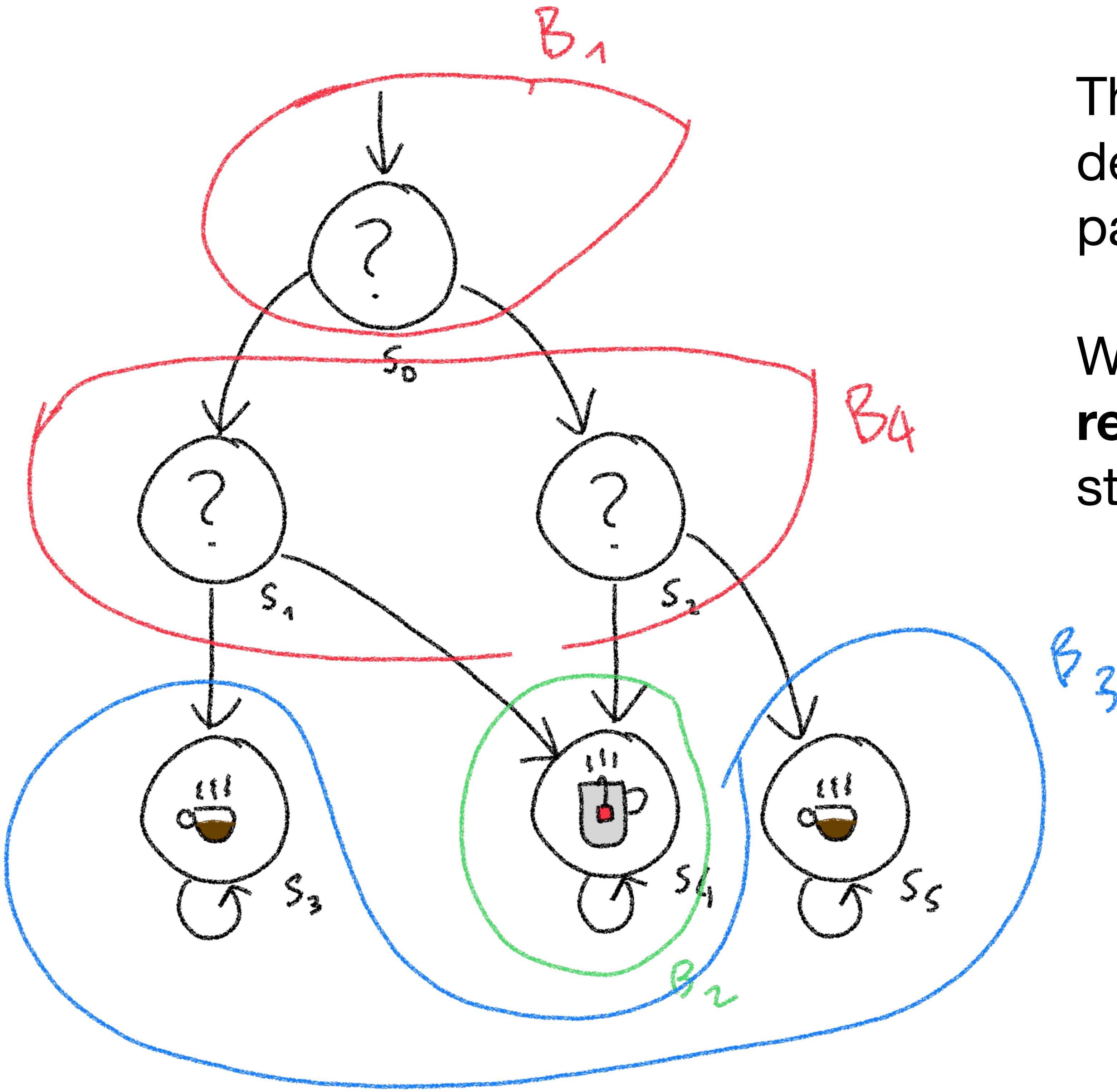
```
// Start by creating a partition where each block corresponds
// to a subset of AP
T:= { { s in S s.t. L(s) = K } | K is a subset of AP }

// Partition refinement loop
do
  fixpoint := true
  // Try to use each block to split other blocks
  for each block B in T do
   // Blocks to be potentially split
   for each block B' in T
    for each pair of states s, s' from B'
     // Check if condition (2) of bisimulation is violated
     if s has a transition to B and s' does not have a transition to B then
      B0 := states in B' that have a transition to B
      B1 := states in B' that don't have a transition to B
      remove B' from T
      add B0,B1 to T
      fixpoint := false
until fixpoint // break the loop if you reach a fix point
```

Partition refinement at work



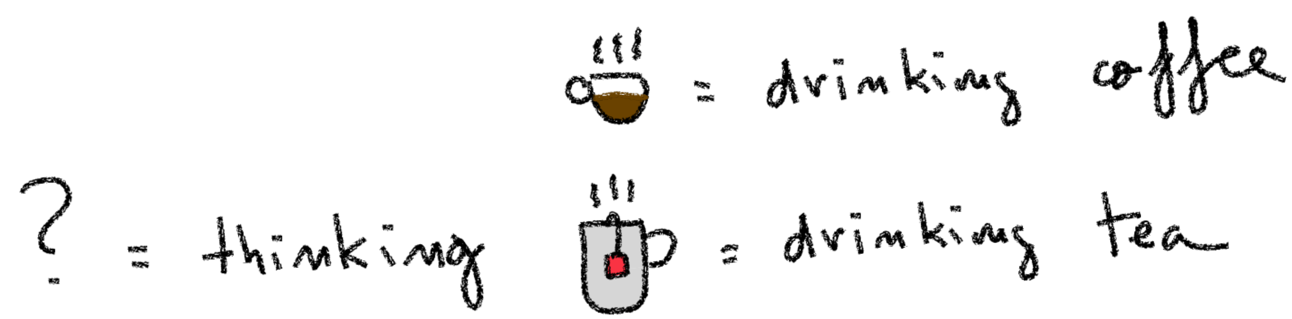


Partition refinement at work

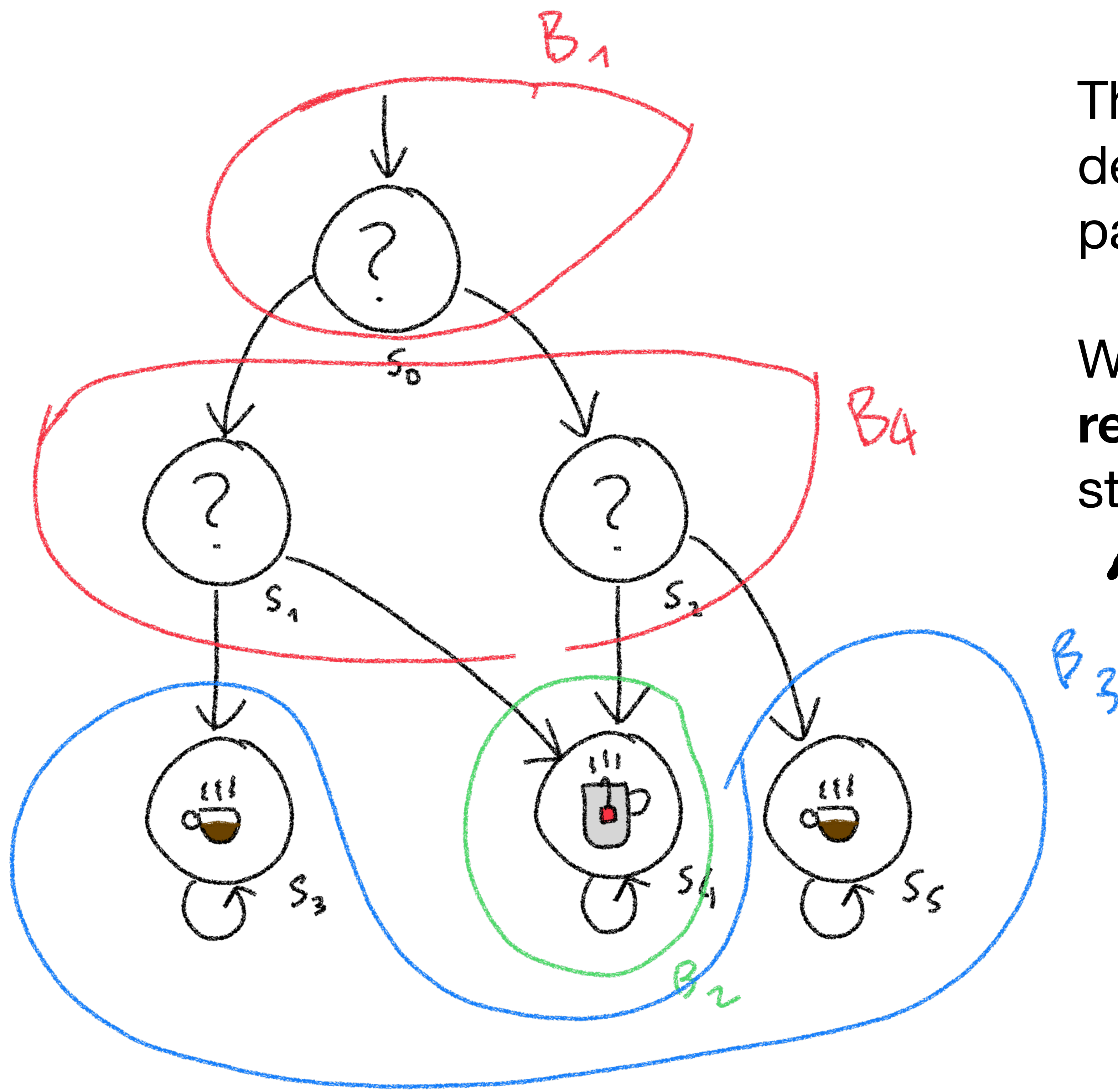


This is a **bisimulation relation** defined by the blocks of the partition.

We get also a **bisimilarity relation** (there are as many states as possible)!



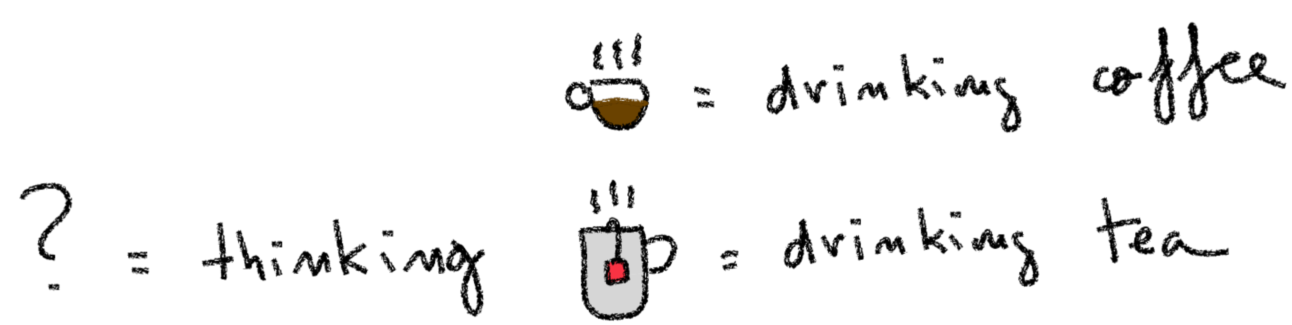
Partition refinement at work



This is a **bisimulation relation** defined by the blocks of the partition.

We get also a **bisimilarity relation** (there are as many states as possible)!

Why?
Because we have been “deconstructing” our relation starting from the maximum one



Bisimulation quotient, minimising transition systems

Let T = (S,→,I,AP,L) be a transition system (with no actions).

Assume you have bisimulation R (typically ~) for T. You can now exploit R to compute the **R-quotient** of T as a new transition system T/R = (S',→,I',AP,L').

The set of states S' is the set of equivalence classes

$$S' = S/R$$

The labelling function L' just takes the label of any state in the equivalence class

$$L'([s]) = L(s)$$

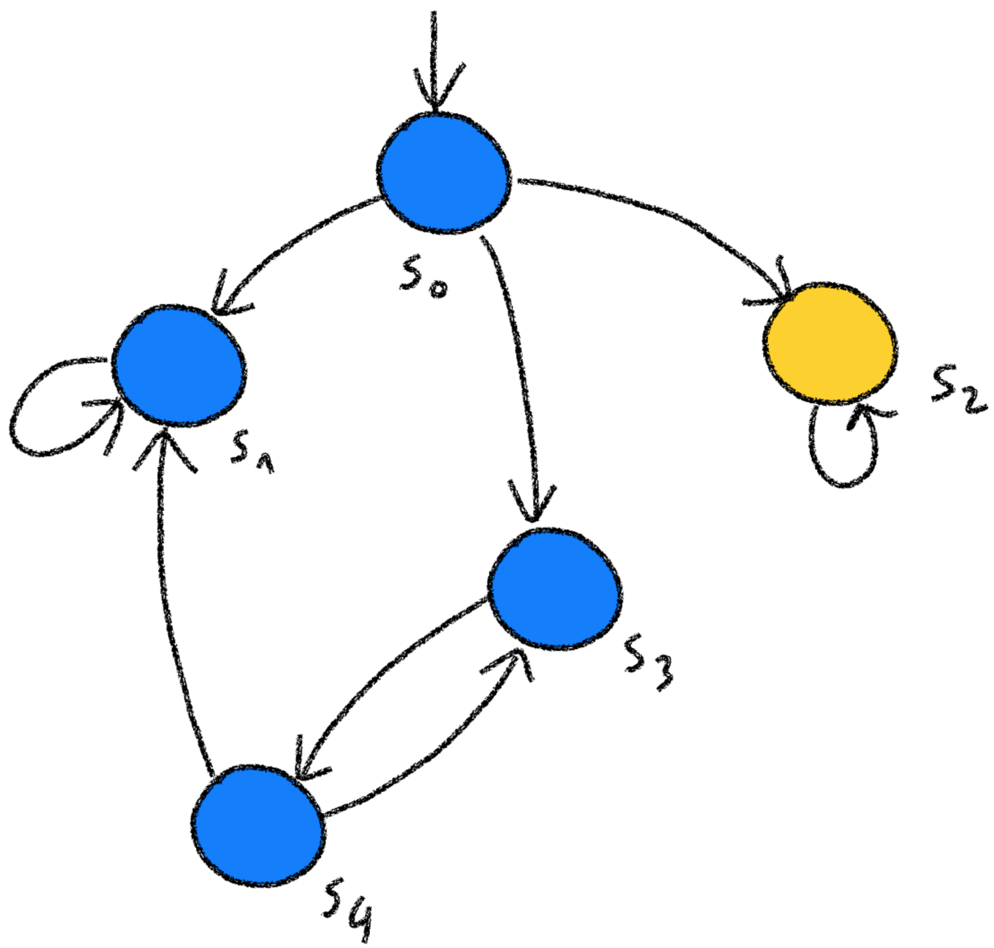
Transitions are lifted to equivalence classes

$$\frac{s \rightarrow s'}{[s] \rightarrow' [s']}$$

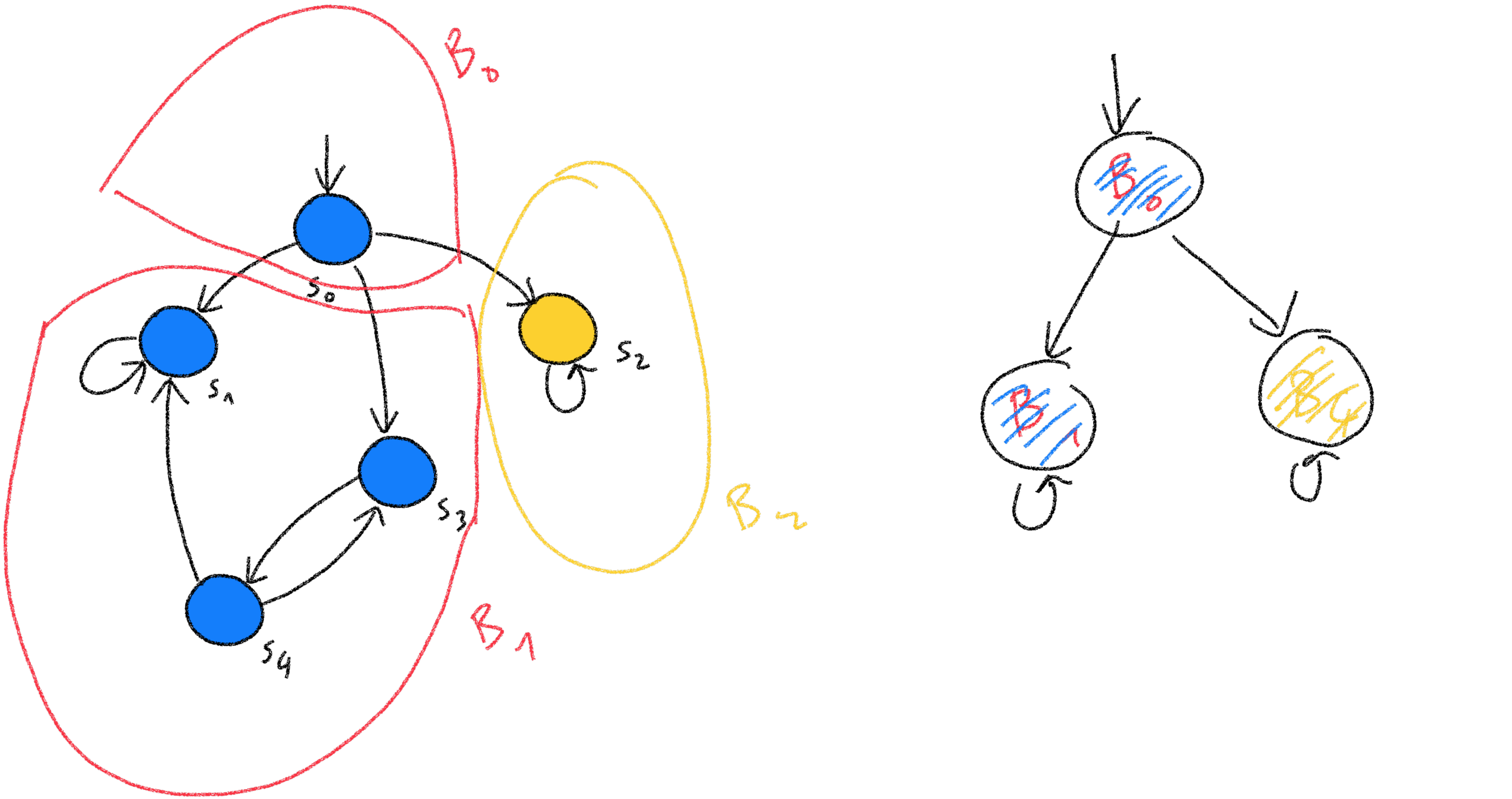
The set of initial states is the set of equivalence classes with at least one initial state.

$$I' = \{[s] \mid s' \in I \text{ and } s' \in [s]\}$$

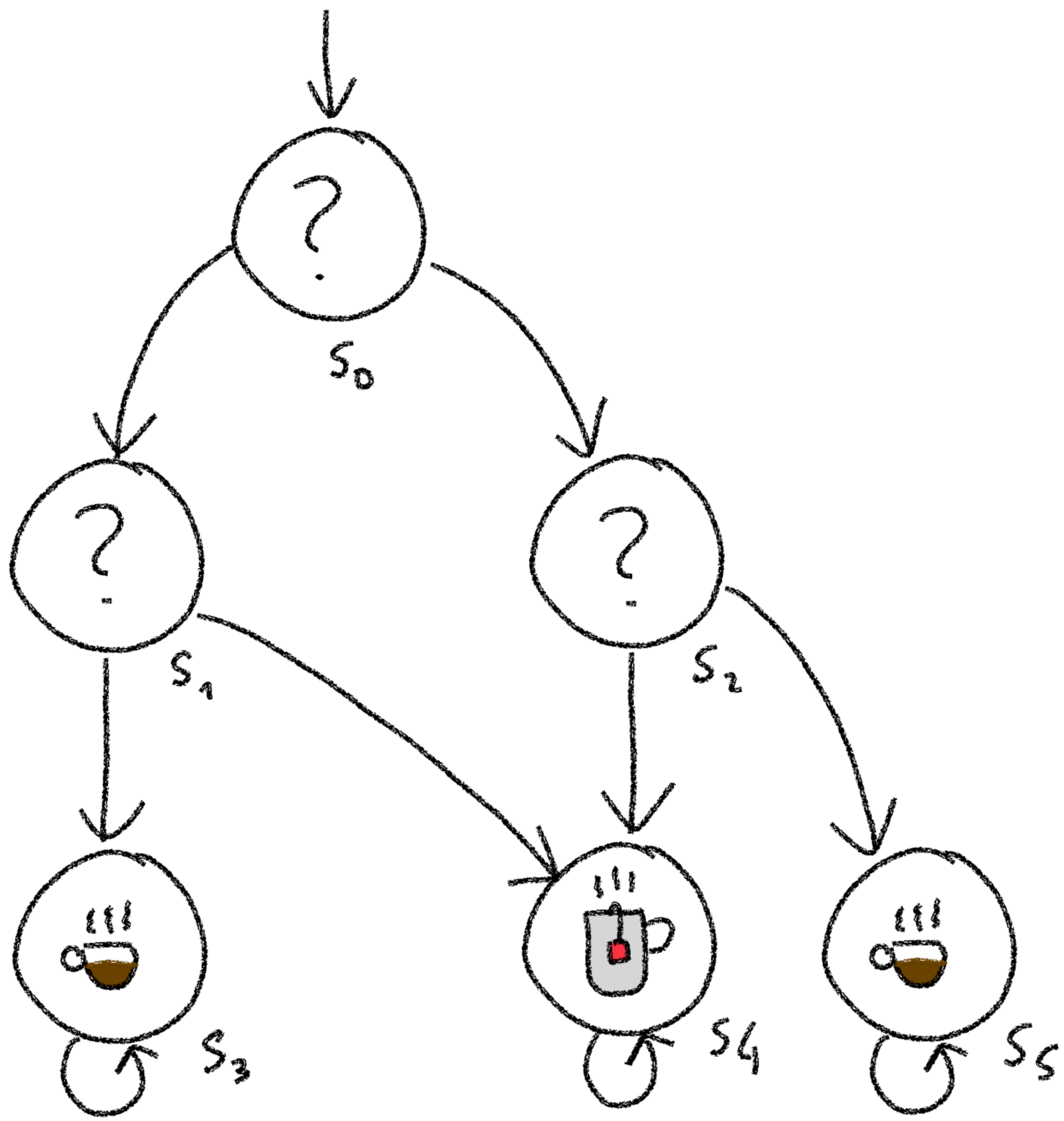
Building the R-quotient

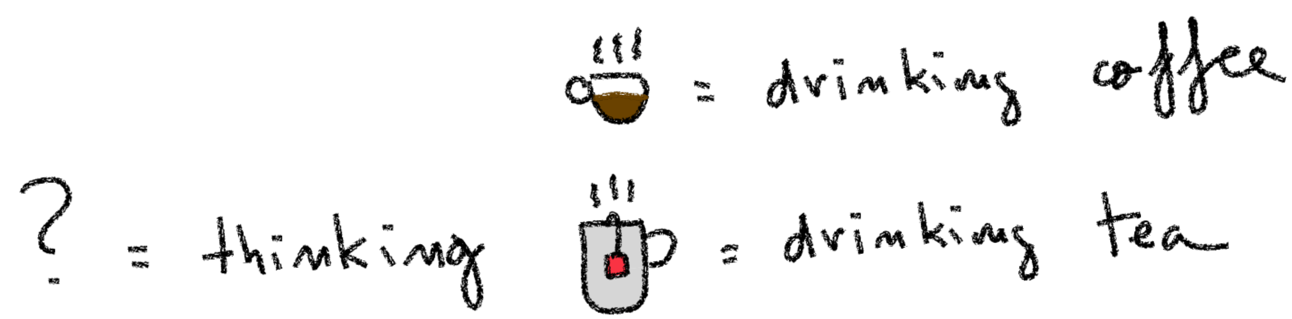


Building the R-quotient

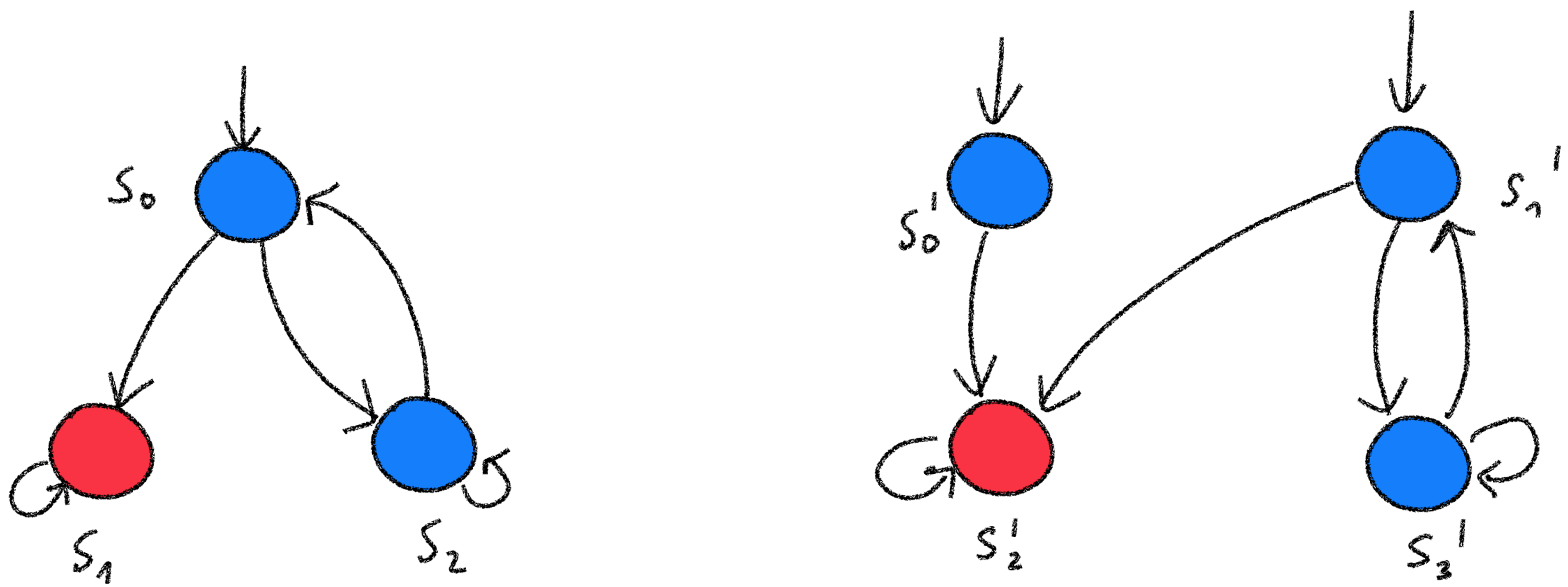


Bisimulation quotient at work





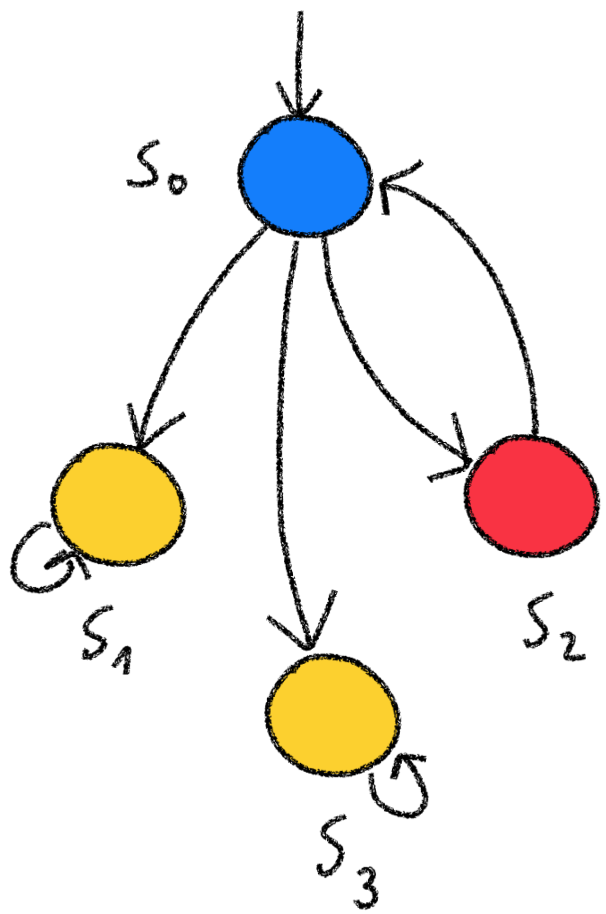
More examples for partition refinement and minimisation

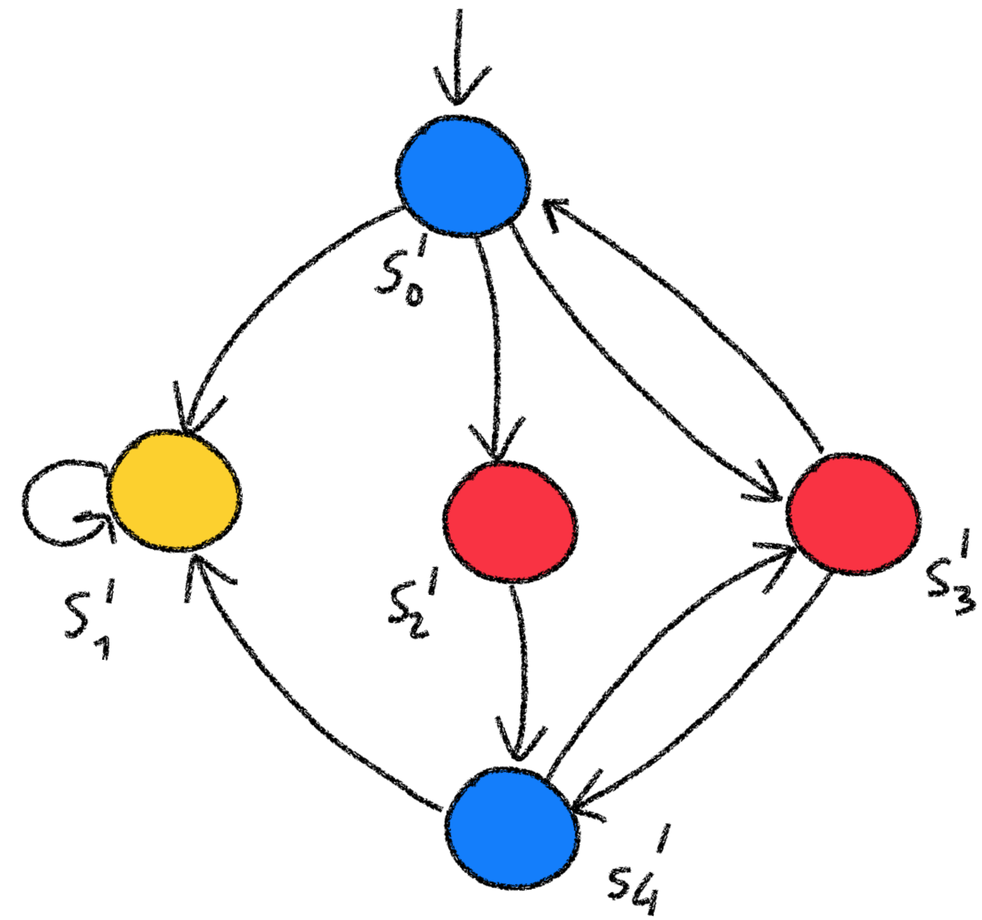


Idea on **partition refinement for bisimilarity checking**:

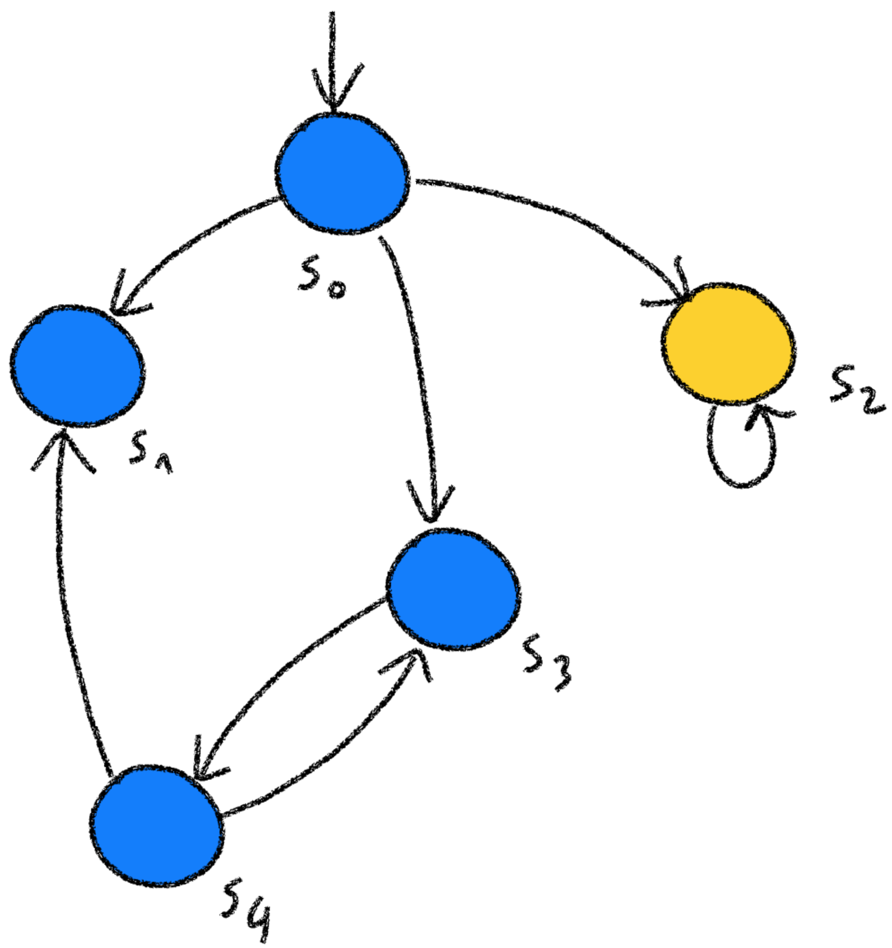
- Consider T1 and T2 as one transition system
- Run partition refinement. If there is one isolated block with states from one TS only, then **not bisimilar!**

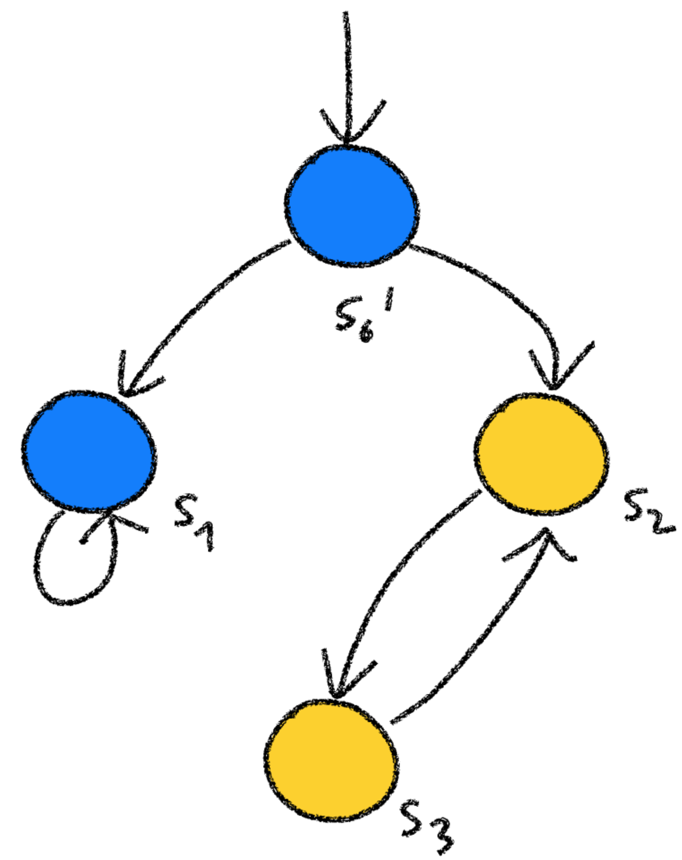
More examples for partition refinement and minimisation



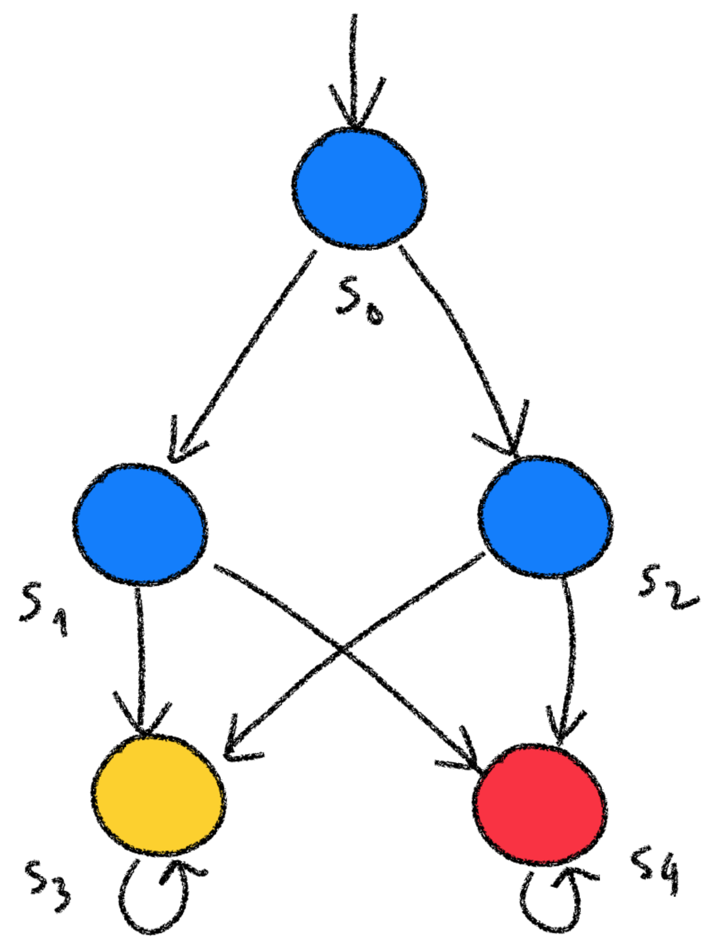


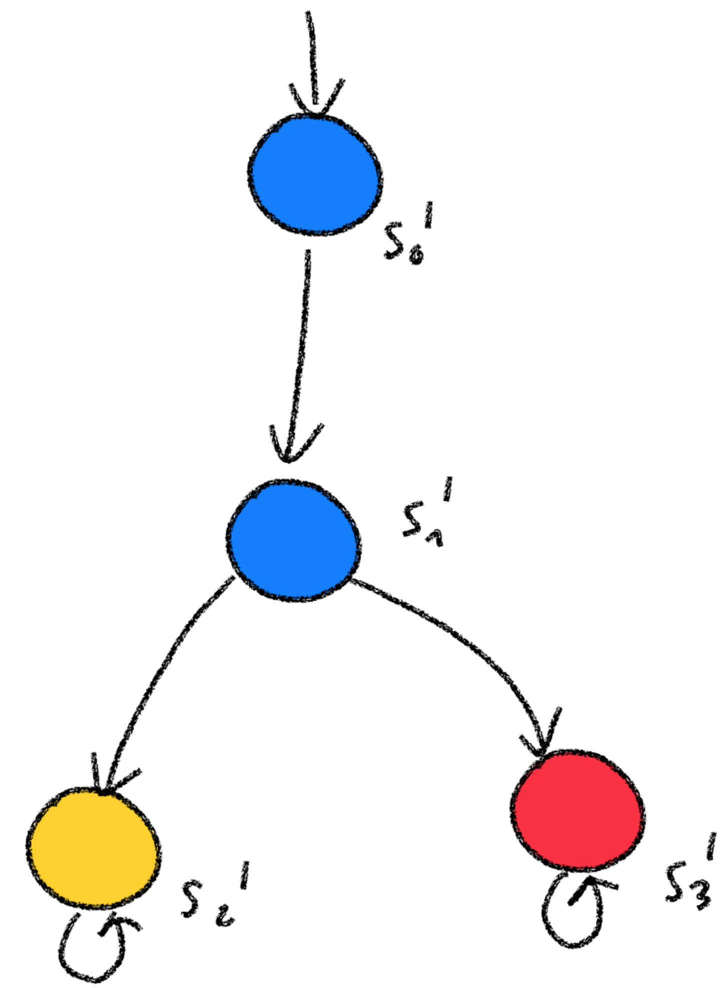
More examples for partition refinement and minimisation





More examples for partition refinement and minimisation





Bisimulations

- Reading material
- Bisimulation relations and bisimulation equivalence
- Computing bisimulations and reducing systems
- Bisimulations equivalence vs other equivalences
- Exercises & Homework

Bisimilarity implies trace equivalence

We have seen that if s~s' then s' can mimic s **step-wise**

$$\begin{tikzcd} s_0 \arrow[r] \arrow[d, phantom, "R"] & s_1 \arrow[d, phantom, "R"] \\ s'_0 \arrow[r] & s'_1 \end{tikzcd}$$

Bisimilarity implies trace equivalence

We have seen that if s~s' then s' can mimic s **step-wise**

$$\begin{tikzcd} s_0 \arrow[r] \arrow[d, phantom, "R"] & s_1 \arrow[d, phantom, "R"] \\ s'_0 \arrow[r] & s'_1 \end{tikzcd}$$

But, actually, s' can mimic s also **path-wise**

$$\begin{tikzcd} s_0 \arrow[r] \arrow[d, phantom, "R"] & s_1 \arrow[r] & s_2 \arrow[r] & \cdots \\ s'_0 & & & \end{tikzcd}$$

Bisimilarity implies trace equivalence

We have seen that if s~s' then s' can mimic s **step-wise**

$$\begin{array}{ccc} s_0 & \longrightarrow & s_1 \\ R & & R \\ s'_0 & \longrightarrow & s'_1 \end{array}$$

But, actually, s' can mimic s also **path-wise**

$$\begin{array}{ccccccc} s_0 & \longrightarrow & s_1 & \longrightarrow & s_2 & \longrightarrow & \cdots \\ R & & R & & & & \\ s'_0 & \longrightarrow & s'_1 & & & & \end{array}$$

Bisimilarity implies trace equivalence

We have seen that if s~s' then s' can mimic s **step-wise**

$$\begin{array}{ccc} s_0 & \longrightarrow & s_1 \\ R & & R \\ s'_0 & \longrightarrow & s'_1 \end{array}$$

But, actually, s' can mimic s also **path-wise**

$$\begin{array}{ccccccc} s_0 & \longrightarrow & s_1 & \longrightarrow & s_2 & \longrightarrow & \cdots \\ R & & R & & R & & \\ s'_0 & \longrightarrow & s'_1 & \longrightarrow & s'_2 & \longrightarrow & \cdots \end{array}$$

Given an execution, we can obtain a **bisimilar** execution!

As a consequence, two **bisimilar transition system have the same traces!**

Trace equivalence does not imply bisimilarity

The converse doesn't hold!

If T and T' are trace equivalent (i.e. have the same traces) then it is not necessarily the case that T and T' are bisimulation equivalent.

Which example seen in the class shows this?

Bisimulations equivalences vs other CTL*, CTL equivalence

Recall, for a temporal logic L we say that two transition systems (resp. states) are L-equivalent if they satisfy the same properties

$T \equiv_L T'$ iff $\forall \phi \in L\,.\, T \vDash \phi \;\Leftrightarrow T' \vDash \phi$ $\qquad$ $s \equiv_L s'$ iff $\forall \phi \in L\,.\, s \vDash \phi \;\Leftrightarrow s' \vDash \phi$

Bisimulations equivalences vs other CTL*, CTL equivalence

Recall, for a temporal logic L we say that two transition systems (resp. states) are L-equivalent if they satisfy the same properties

$$T \equiv_L T' \text{ iff } \forall \phi \in L \,.\, T \vDash \phi \;\Leftrightarrow T' \vDash \phi \qquad\qquad s \equiv_L s' \text{ iff } \forall \phi \in L \,.\, s \vDash \phi \;\Leftrightarrow s' \vDash \phi$$

It holds that Bisimulation equivalence, CTL* equivalence and CTL equivalence coincide.

$$T \sim T' \text{ iff } T \equiv_{\text{CTL}^*} T' \text{ iff } T \equiv_{\text{CTL}} T' \qquad\qquad s \sim s' \text{ iff } s \equiv_{\text{CTL}^*} s' \text{ iff } s \equiv_{\text{CTL}} s'$$

This means that equivalent transition systems (resp. states) satisfy the same CTL* formulas, and hence also the same CTL formulas!

Bisimulations equivalences vs other CTL*, CTL equivalence

Recall, for a temporal logic L we say that two transition systems (resp. states) are L-equivalent if they satisfy the same properties

$$T \equiv_L T' \text{ iff } \forall \phi \in L \,.\, T \models \phi \;\Leftrightarrow T' \models \phi \qquad\qquad s \equiv_L s' \text{ iff } \forall \phi \in L \,.\, s \models \phi \;\Leftrightarrow s' \models \phi$$

It holds that Bisimulation equivalence, CTL* equivalence and CTL equivalence coincide.

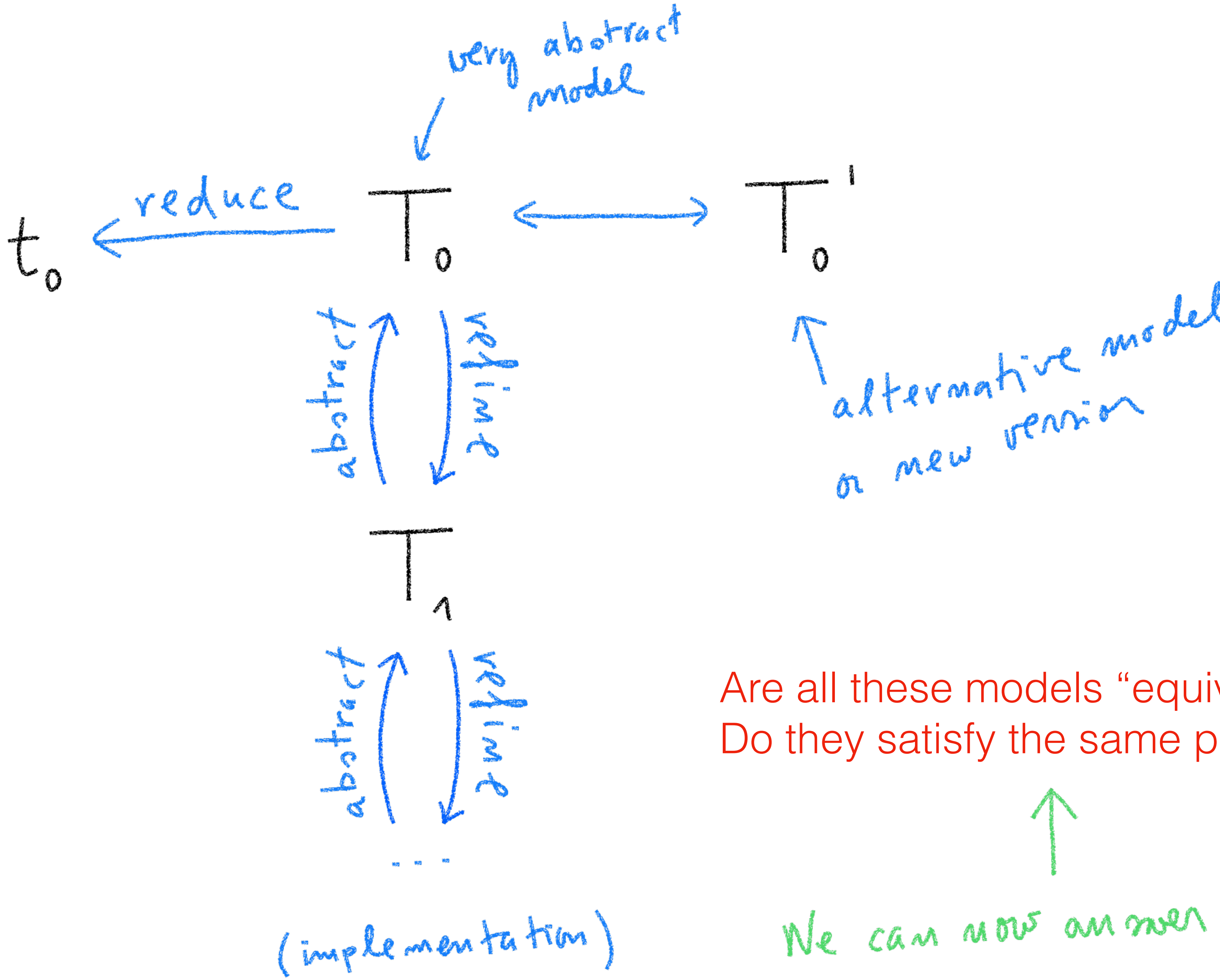
$$T \sim T' \text{ iff } T \equiv_{\mathrm{CTL}^*} T' \text{ iff } T \equiv_{\mathrm{CTL}} T' \qquad\qquad s \sim s' \text{ iff } s \equiv_{\mathrm{CTL}^*} s' \text{ iff } s \equiv_{\mathrm{CTL}} s'$$

This means that equivalent transition systems (resp. states) satisfy the same CTL* formulas, and hence also the same CTL formulas!

Another consequence is that if two transition systems are not bisimilar then we can find a CTL formula to distinguish them.

See proof in Katoen's lecture on Youtube: https://youtu.be/XNmazTIsOaw?t=2013

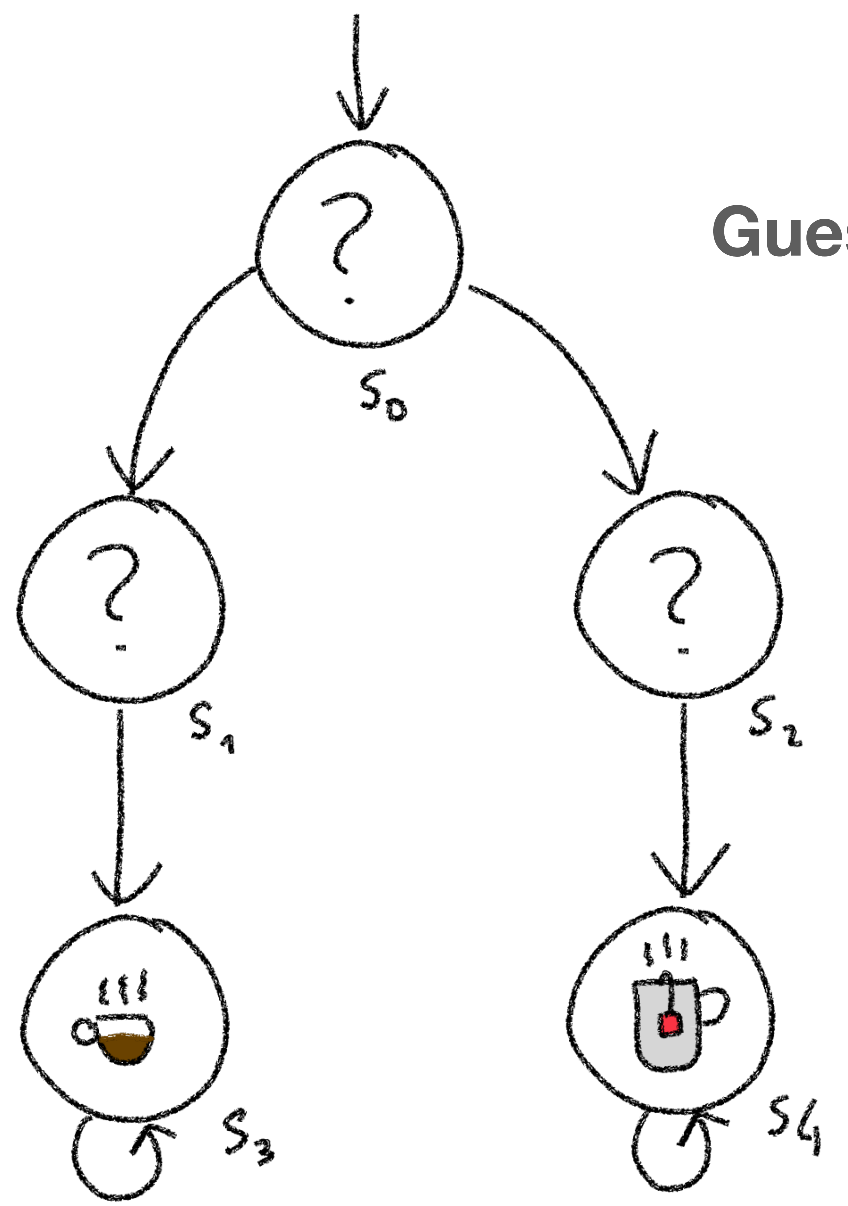
Relating models



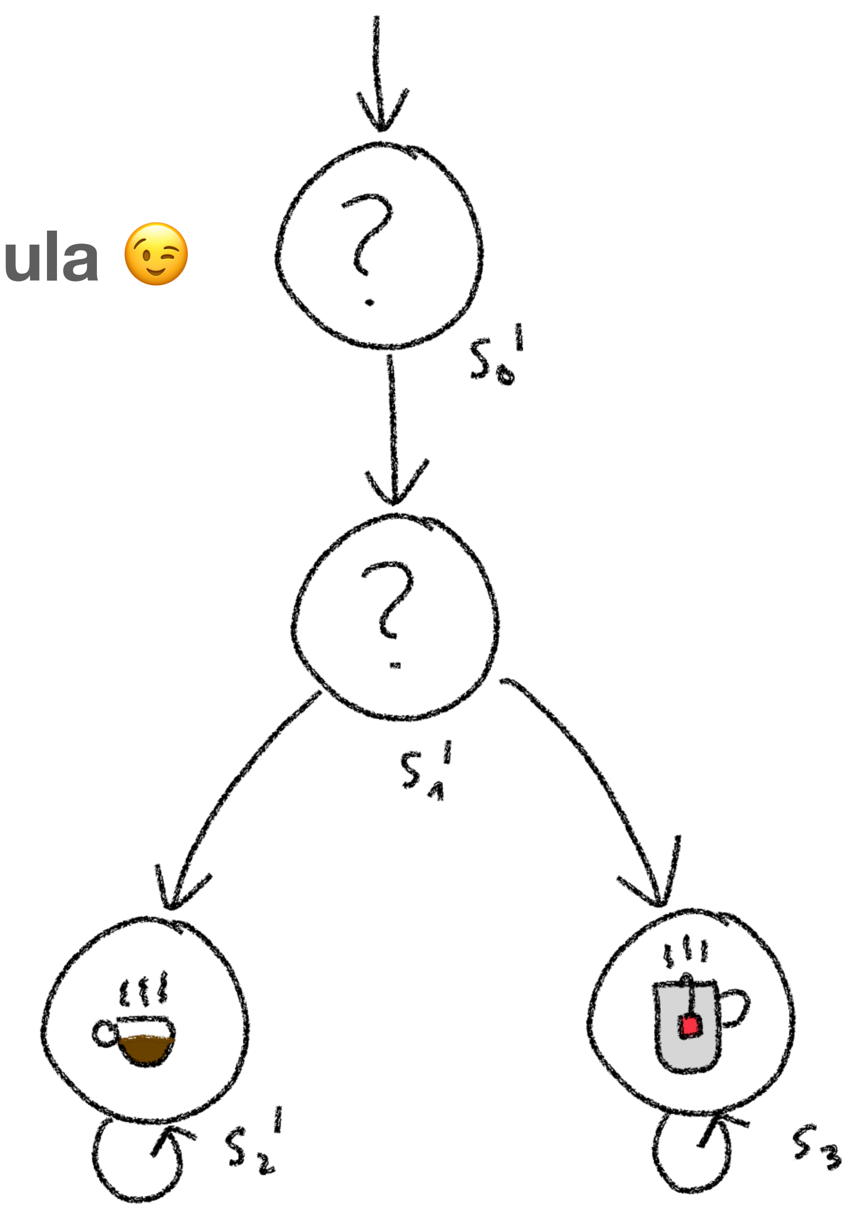
Are all these models "equivalent"?
Do they satisfy the same properties?

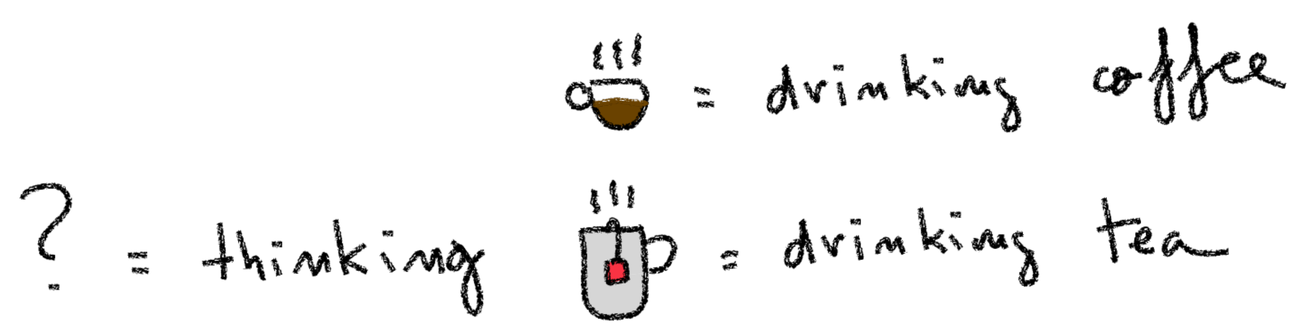
We can now answer to this!

A CTL formula distinguishing these two transition systems



Guess the formula 😉





And finally…

Key points of this lecture

Definition of bisimulation relation, a formal way to relate transition systems and states that have the same properties.

Definition of bisimulation equivalence, the most precise bisimulation relation.

Definition of bisimulation quotient, the smallest “reduced” transition system equivalent to a given one.

Bisimulation equivalence and CTL equivalence coincide! This means bisimilar transition systems satisfy the same CTL properties.

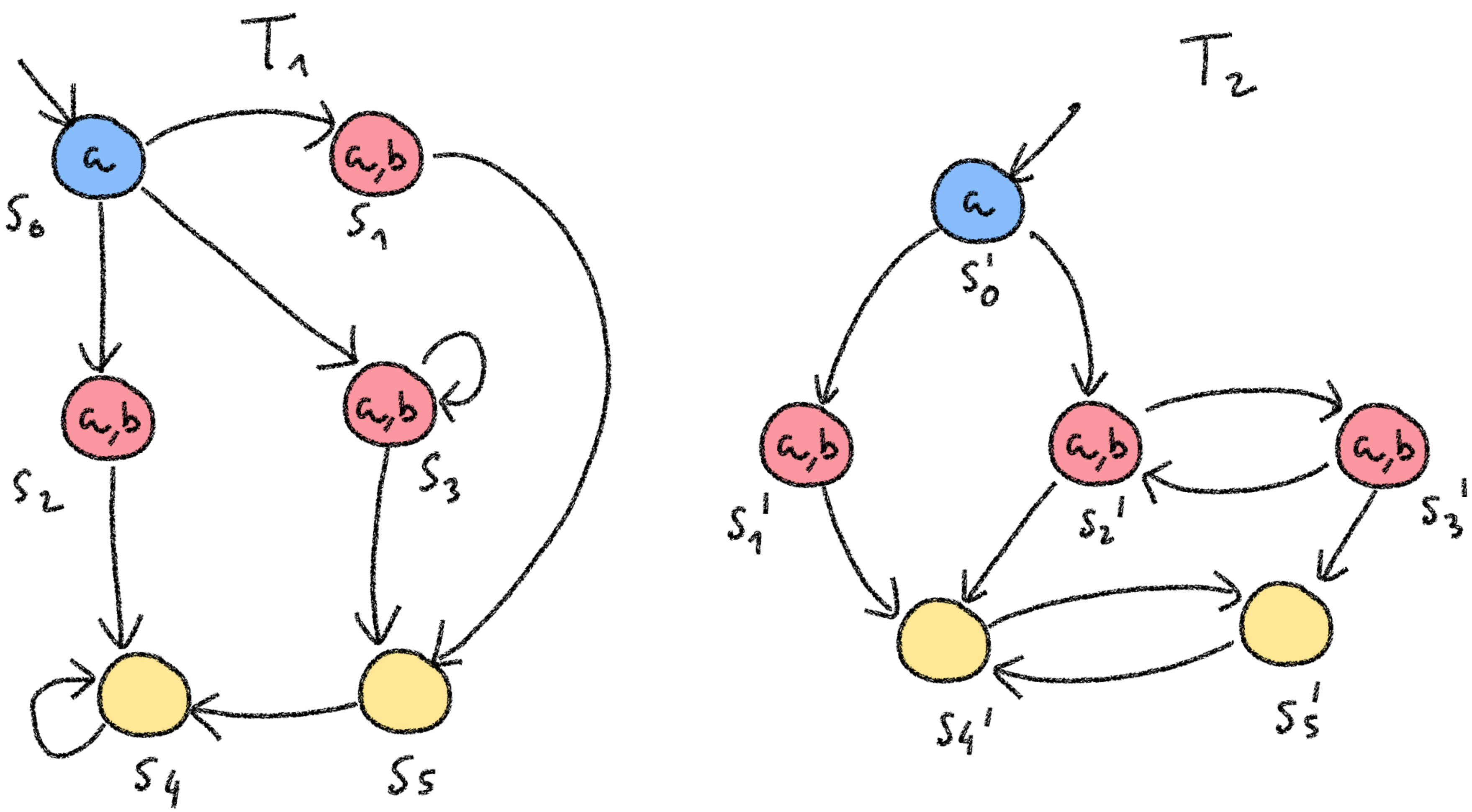
Bisimulations

- Reading material
- Bisimulation relations and bisimulation equivalence
- Computing bisimulations and reducing systems
- Bisimulations equivalence vs other equivalences
- Exercises & Homework

APPENDIX: Exercises

Exercise 05.1

Consider the two transition systems below. Are they bisimulation-equivalent?

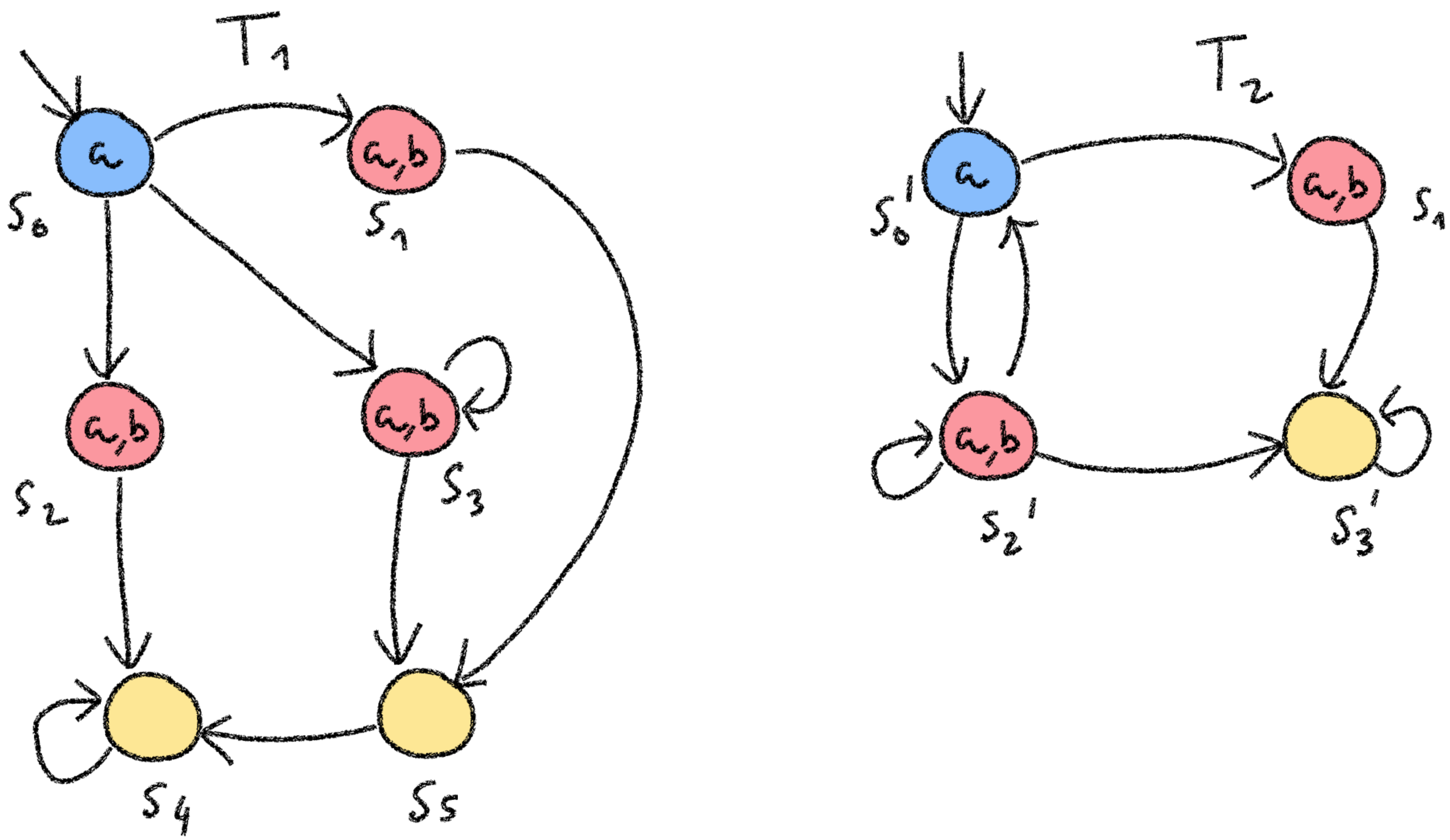


If yes, provide a bisimulation relation, if no provide an example of a CTL formula that is satisfied by one transition system and not by the other.

NOTE: you can check T1 against T2 directly, or you can minimise T1 into T1' and T2 into T2' first, and then check T1' against T2'. You can also try both approaches :)

Exercise 05.2

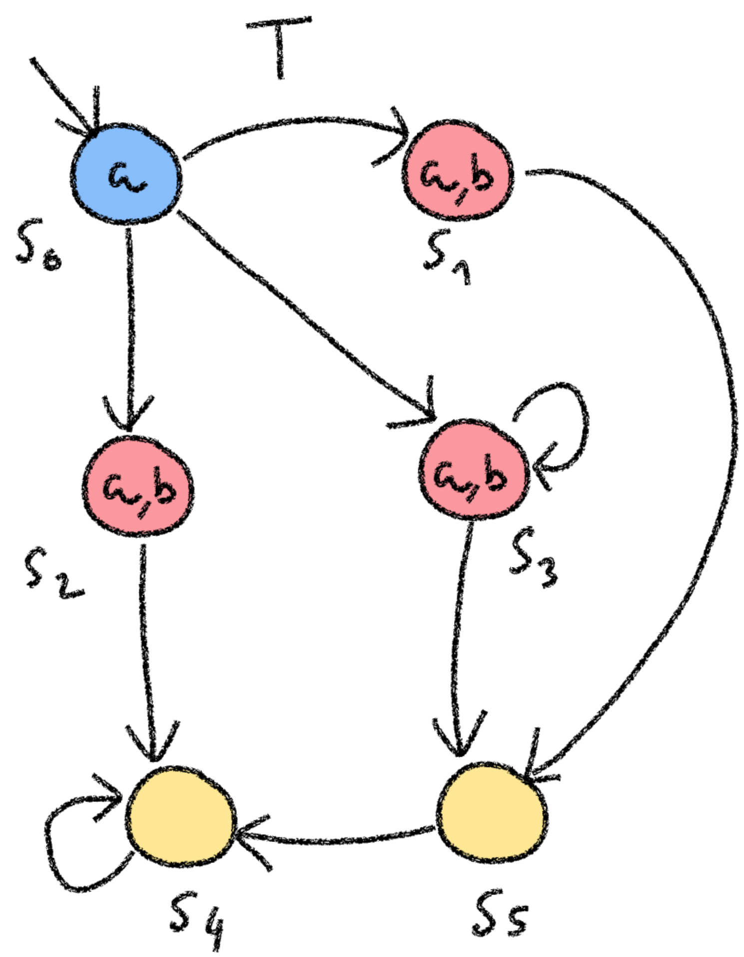
Consider the two transition systems below. Are they bisimulation-equivalent?



If yes, provide a bisimulation relation, if no provide an example of a CTL formula that is satisfied by one transition system and not by the other.

Exercise 05.3

Consider the transition system below



Compute the largest bisimulation relation (~) for it and build the bisimulation quotient.