Hoare logic and Model checking

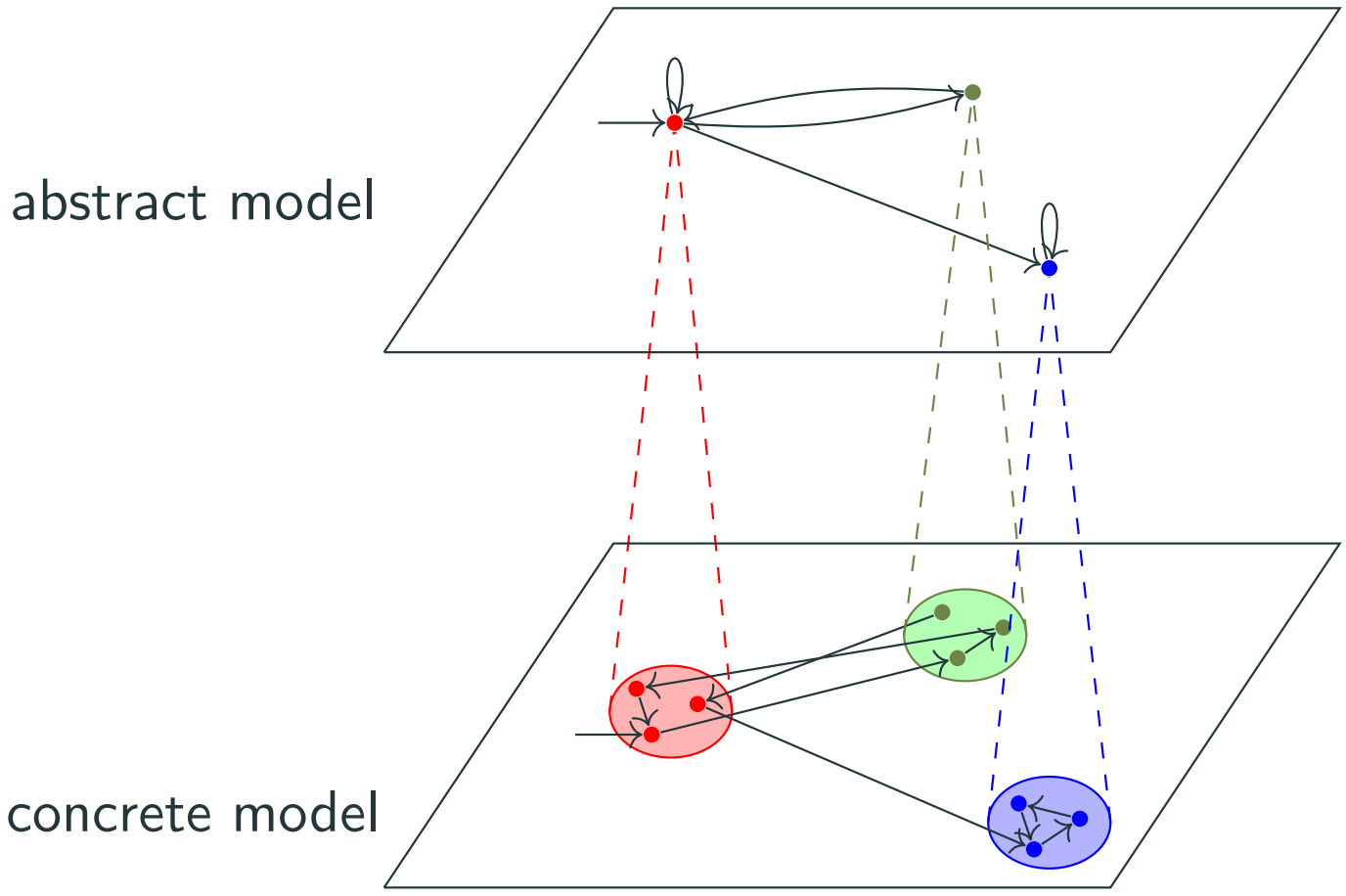
Part II: Model checking

Lecture 10: Relating temporal models

Jean Pichon-Pharabod
University of Cambridge

CST Part II – 2020/21

Relating temporal models



Relating temporal models

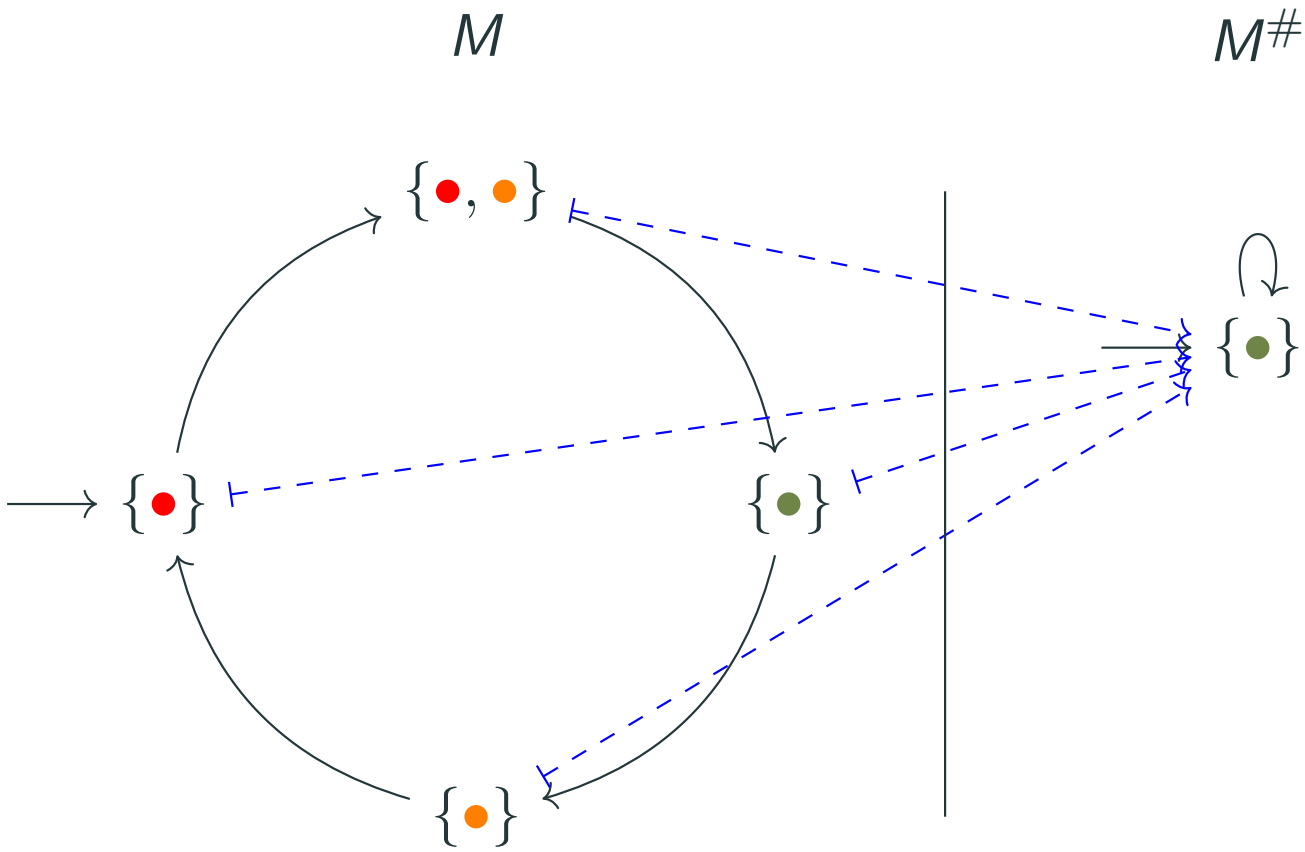
The premise of model checking is that checking the model translates to confidence in the modelled artefact.

If we can express the artefact as a temporal model too, and if the abstract model can **simulate** the concrete model, then we can check some classes of properties on the abstract model and know that they hold of the concrete model.

However, discarding the unimportant aspects the the artefact is also a crucial aspect of modelling.

Abstraction of traffic lights by some Cambridge taxi drivers

$$AP ::= \bullet \mid \bullet \mid \bullet$$



...still, another crucial aspect of modelling is to not discard the crucial aspects of the artefact.

Temporal model simulation 1/2

R is a **temporal model simulation** of M by M':

$$① \preccurlyeq^{③} ② \in \; (M \in \mathrm{TModel}) \to (M' \in \mathrm{TModel}) \to (M.S \to M'.S \to \mathrm{Prop}) \to \mathrm{Prop}$$

$$M \preccurlyeq^{R} M' \stackrel{def}{=}$$

(1) R is consistent with labels:

$$\left(\begin{array}{l} \forall s \in M.S, s' \in M'.S. \\ \quad s \; R \; s' \to \forall p \in AP. \; M'.\ell \; s' \; p \to M.\ell \; s \; p \end{array} \right) \wedge$$

(2) R relates initial states of M to initial states in M':

$$(\forall s \in M.S. \; M.S_0 \; s \to \exists s' \in M'.S. \; M'.S_0 \; s' \wedge s \; R \; s') \wedge$$

(continued on the next slide)

Temporal model simulation 2/2

(3) any step in M can be matched by a step in M' from any R-related start state to some R-related end state:

$$\left(\begin{array}{l} \forall s_0, s_1 \in M.S, s_0' \in M'.S. \\ \quad s_0\ M.T\ s_1 \wedge s_0\ R\ s_0' \rightarrow \\ \quad\quad \exists s_1' \in M'.S. \\ \quad\quad\quad s_0'\ M'.T\ s_1' \wedge s_1\ R\ s_1' \end{array}\right)$$

$$\begin{array}{ccc} s_0 & \overset{R}{\dashrightarrow} & s_0' \\ {\scriptstyle M.T}\downarrow & & \\ s_1 & & \end{array} \quad \rightarrow \quad \exists s_1'. \quad \begin{array}{ccc} s_0 & \overset{R}{\dashrightarrow} & s_0' \\ {\scriptstyle M.T}\downarrow & & \downarrow{\scriptstyle M'.T} \\ s_1 & \underset{R}{\dashrightarrow} & s_1' \end{array}$$

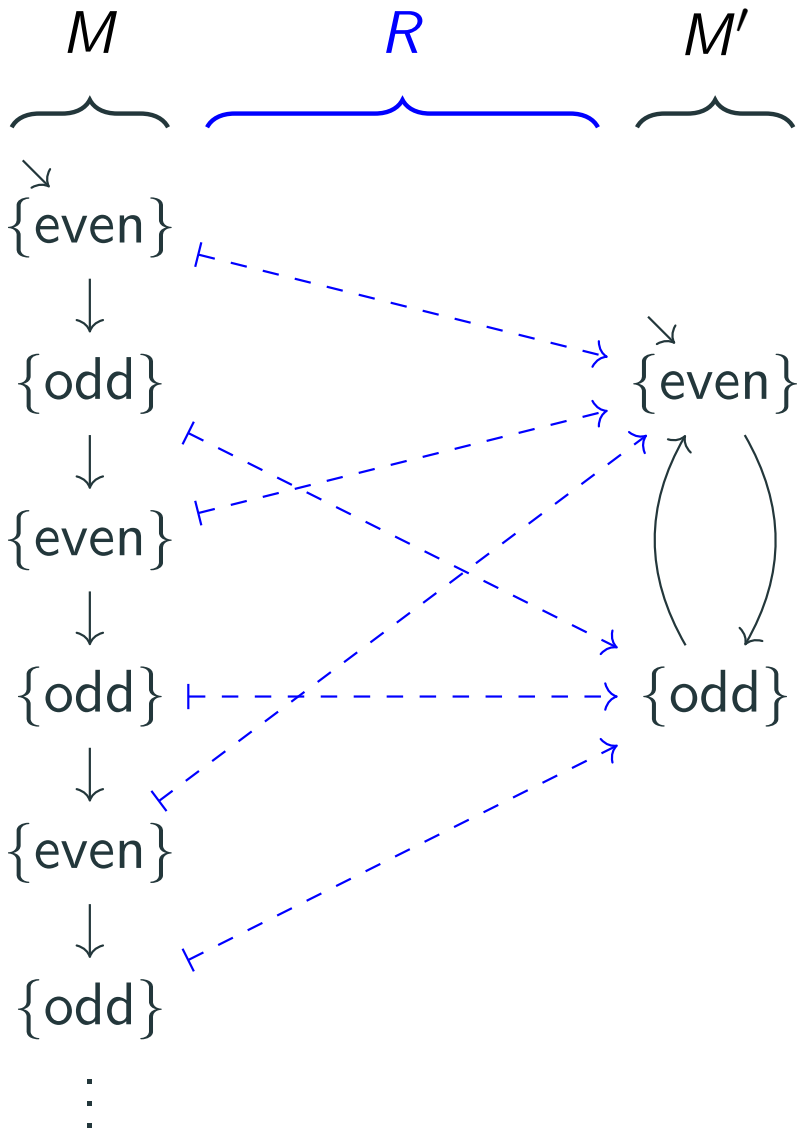
Examples of simulations

The identity relation is a simulation:

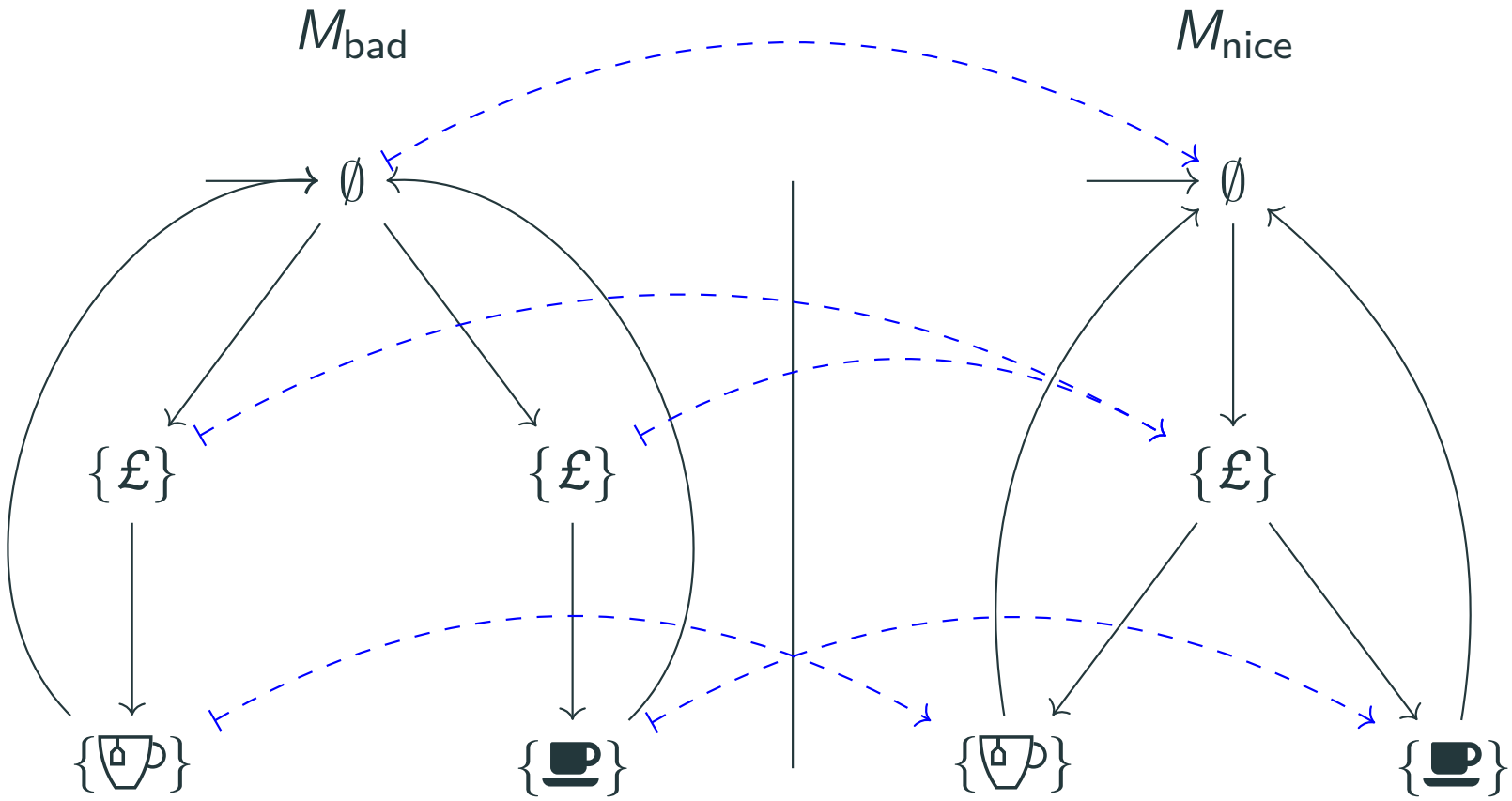
$$\begin{array}{l} \forall M \in \mathsf{TModel}. \\ \quad \text{let } R = (s \mapsto s) \text{ in} \\ \quad M \preccurlyeq^{R} M \end{array}$$

The terrible punter (lecture 1) can simulate the good punter (lecture 3) by, when it has a choice of things, doing a good thing.

Examples of simulations



Milner's tea & coffee machines



Temporal model simulation

Often, the details of the simulation are not so important, what matters is the existence of a simulation:

$$① \preccurlyeq ② \in \mathsf{TModel} \to \mathsf{TModel} \to \mathsf{Prop}$$
$$(M \preccurlyeq M') \stackrel{def}{=} \exists R.\, M \preccurlyeq^{R} M'$$

It means that M' is "more abstract" than M: it may have more behaviour, making it less precise, but that allows it to have possibly fewer states and transitions.

Simulation preserves ACTL*

The universal, implication-free fragment of CTL*, ACTL$^{*\mathsf{IF}}$, is compatible with the simulation preorder:

$$\forall M \in \mathsf{TModel}, M' \in \mathsf{TModel}, \psi \in \mathsf{StateProp}^{\mathsf{ACTL}^{*}\mathsf{IF}}.$$
$$(M \preccurlyeq M' \wedge \mathsf{us}\ \psi \wedge M' \models \psi) \rightarrow M \models \psi$$

(where us ψ means ψ is a universal state property)

It suffices to show the property holds of the more abstract model to know it holds of the more concrete model.

This property can seem strange, because F ϕ has an existential feel to it. In fact, it is very fragile, and really depends on left-totality!

Temporal model bisimulation

R is a **temporal model bisimulation** of M by M':

$$\begin{aligned} ① \approx^{③} ② \in\ & (M \in \mathsf{TModel}) \to (M' \in \mathsf{TModel}) \to \\ & (M.S \to M'.S \to \mathsf{Prop}) \to \mathsf{Prop} \\ M \approx^{R} M' \stackrel{def}{=}\ & M \preccurlyeq^{R} M' \wedge M' \preccurlyeq^{R} M \end{aligned}$$

As for simulations, the details of the bisimulation are not so important, often what matters is the existence of a bisimulation:

$$\begin{aligned} & ① \approx ② \in \mathsf{TModel} \to \mathsf{TModel} \to \mathsf{Prop} \\ & (M \approx M') \stackrel{def}{=} \exists R.\, M \approx^{R} M' \end{aligned}$$

Bisimulation preserves CTL*

All of CTL* is compatible with bisimulation equivalence:

$$\forall M \in \mathsf{TModel}, M' \in \mathsf{TModel}, \psi \in \mathsf{StateProp}^{\mathsf{WI}}.$$
$$M \approx M' \to (M \models \psi \leftrightarrow M' \models \psi)$$

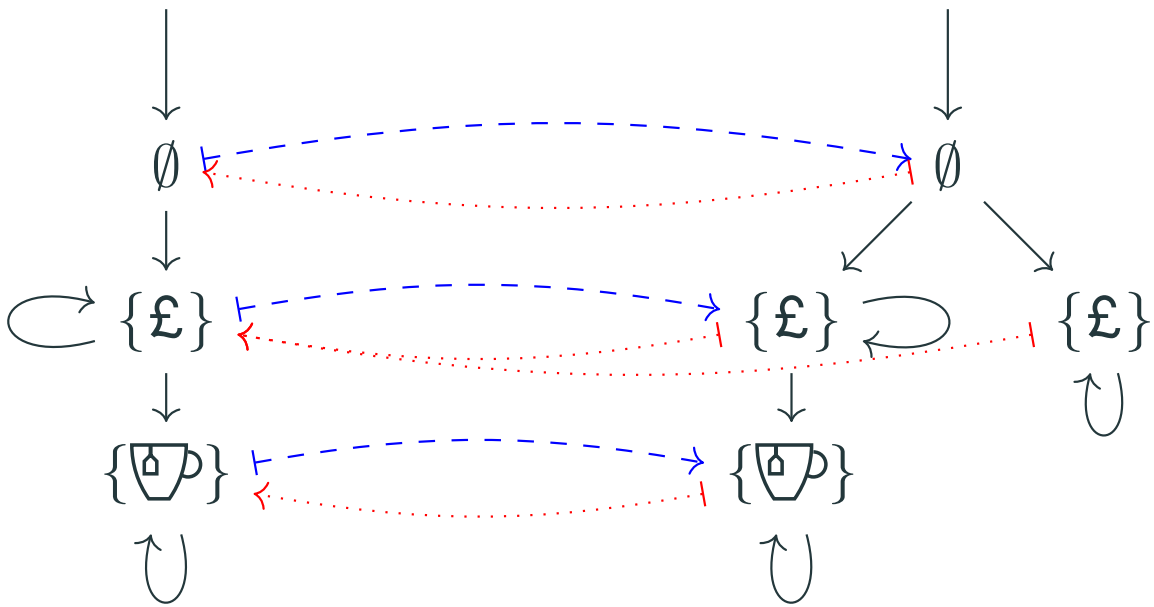
Bisimulation and simulations

Bisimulation implies simulations in both directions

$$M \approx M' \to (M \preccurlyeq M' \wedge M' \preccurlyeq M)$$

⚠ but in general not the other way around!

For example, on a variation of the tea & coffee machines example:



Revisiting stuttering

What if we want to abstract multiple steps of the concrete model with one step of the abstract model?

$\rightsquigarrow$ We can change our notion of path to allow staying any finite number of times in any state (in addition to allowing forever on states with self-loops).

We can then adapt most of the notions we have seen so far. However, in this setting, we do not want to use the X temporal operator.

This is the approach taken by TLA+.

Summary

We saw how abstraction can be used to relate temporal models in a way that makes checking some classes of properties sound.

...but remember an important part of modelling is judicious under-approximation! $\rightsquigarrow$ domain knowledge is crucial.

In the next lecture, we will look at how to implement model checking.