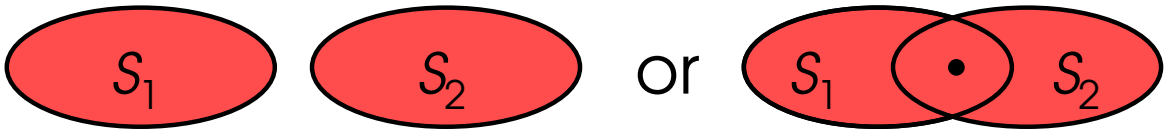
EXPTIME-complete Decision Problems for Modal and Mixed Specifications

Adam Antonik, Imperial College, London
Michael Huth, Imperial College, London
Kim G. Larsen, Aalborg University
Ulrik Nyman, Aalborg University
Andrzej Wąsowski, IT University of Copenhagen

EXPRESS 2008 Toronto, Canada

We Ask Complexity Questions For

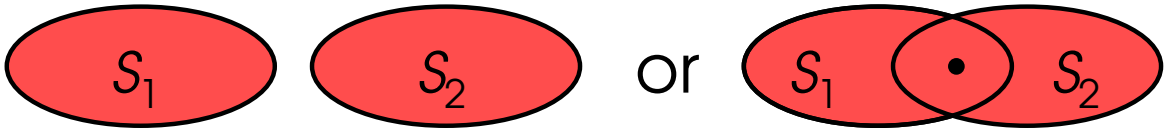
CI Common Implementation



?

We Ask Complexity Questions For

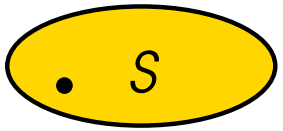
CI Common Implementation



?

C Consistency

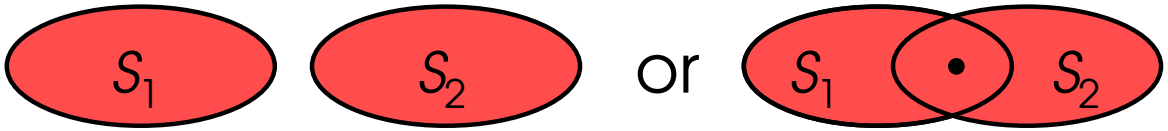
$S = \varnothing$ or



?

We Ask Complexity Questions For

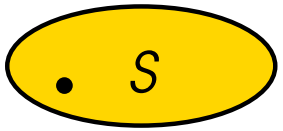
CI Common Implementation



?

C Consistency

$S = \varnothing$ or



?

TR Thorough Refinement

?

Agenda

- Modal and Mixed **Specifications** in a Nutshell
- The Problems and Our **Claims**
- Some **Proof** Sketches
- Open Issues & **Summary**

Part I

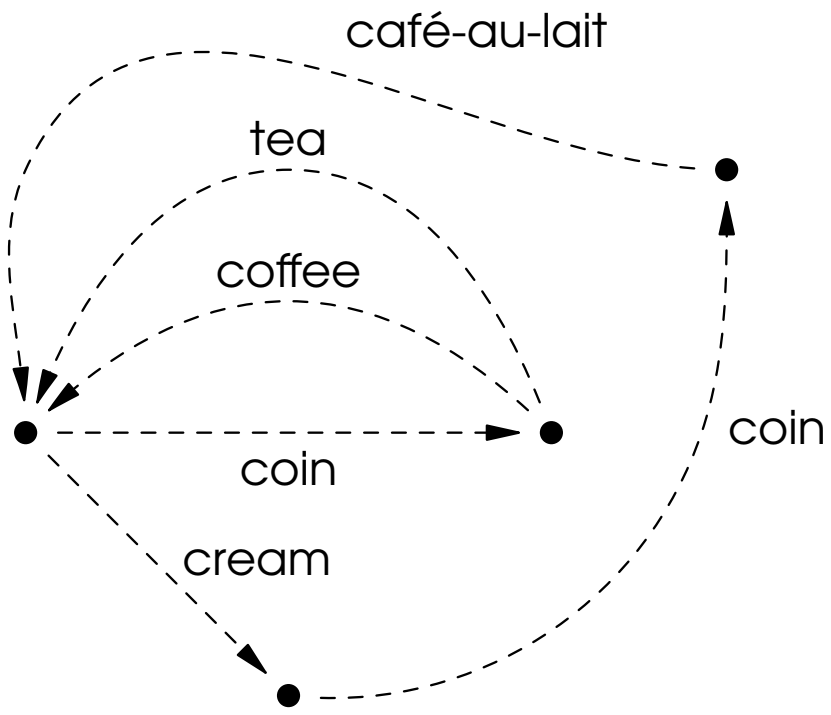
Modal & Mixed Specifications in A Nutshell

Labeled Transition Systems

A Coffeemaker Example

Some traces of the coffeemaker:

- insert coin, get coffee
- insert coin, get tea
- press cream, insert coin, get café au lait

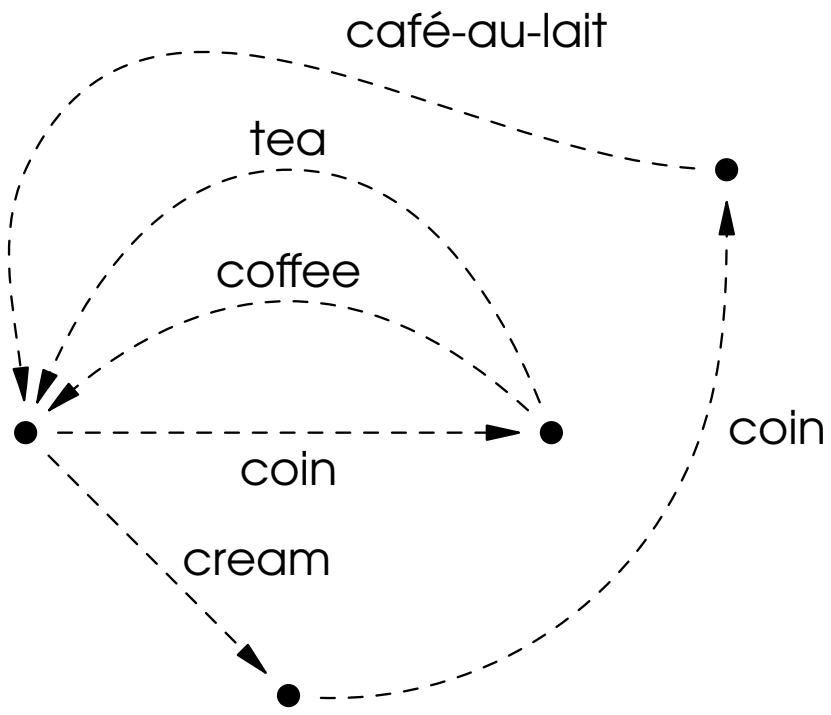


Labeled Transition Systems

A Coffeemaker Example

An LTS + simulation refinement

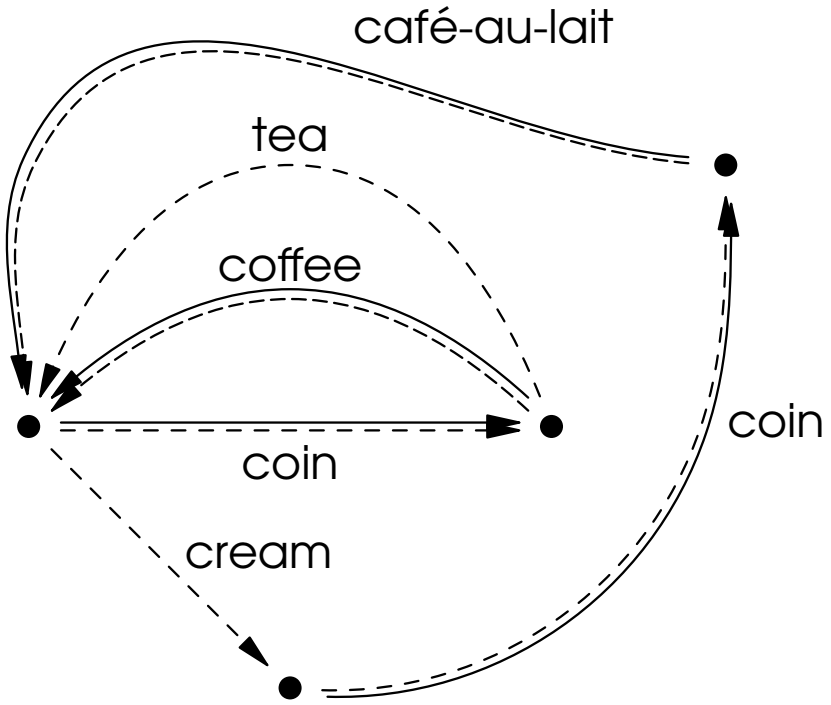
- Overapproximate possible behaviors in each state
- An empty LTS "•" is a perfect refinement.



Modal Specifications

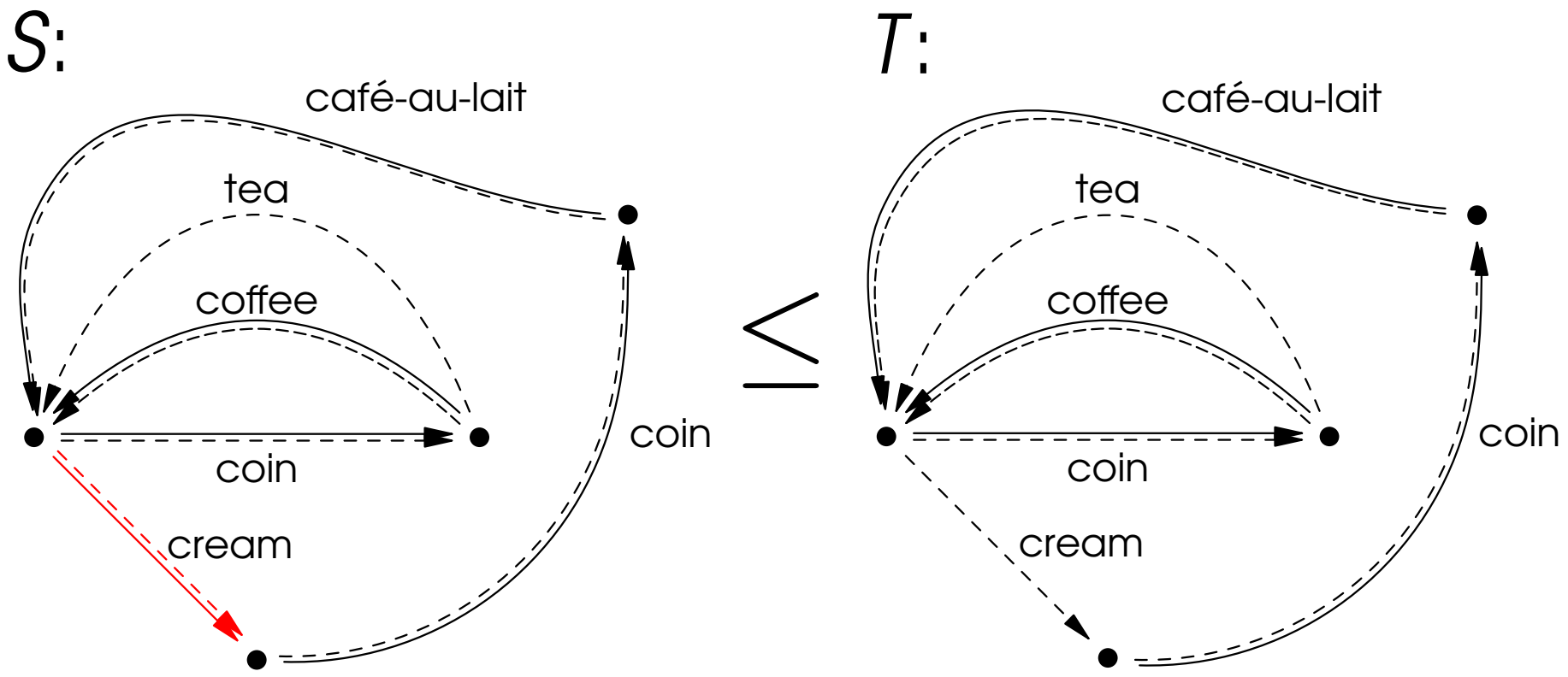
Larsen & Thomsen, LICS'88

- Under- and over-approximate behavior
- Each implementation **must** accept coins and produce coffee
- Cream or tea optional
- If cream offered then caffe-au-lait must be delivered



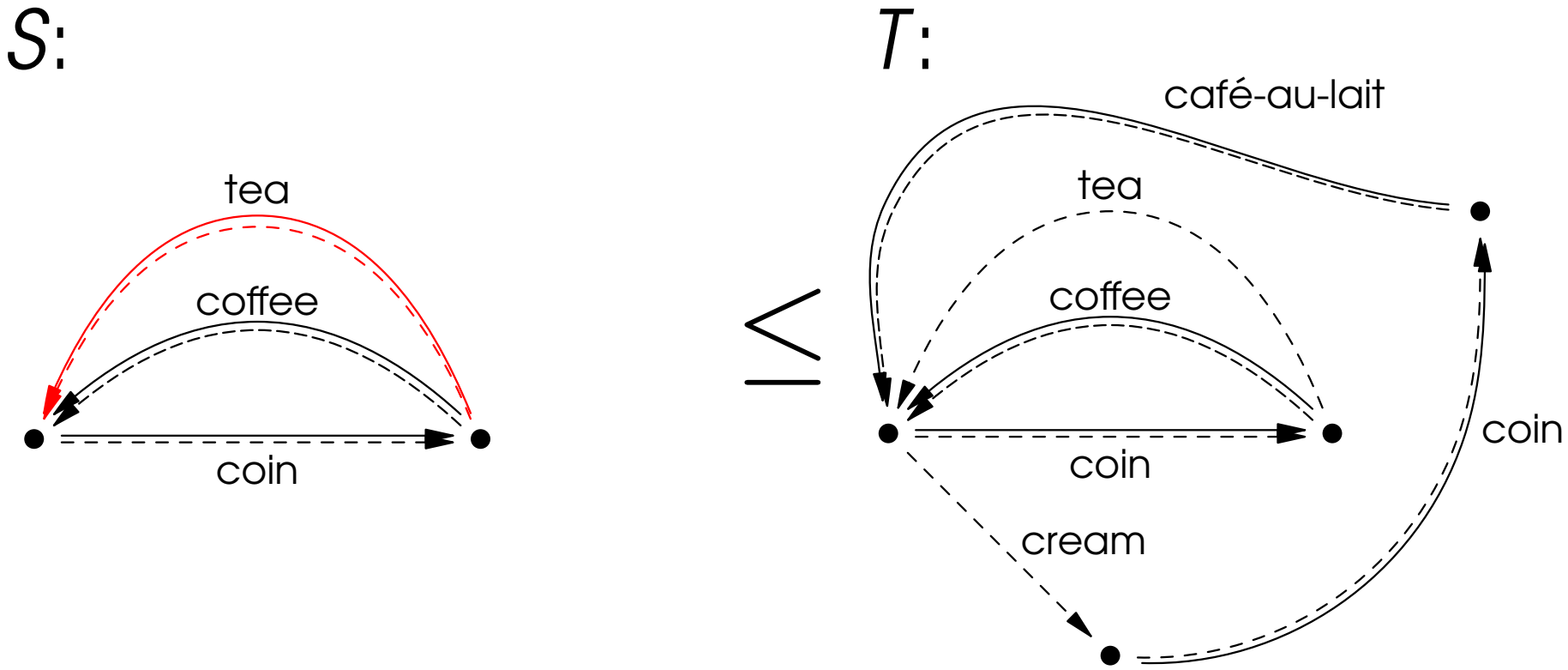
All required behavior (**must**) is allowed (**may**).

Refinement



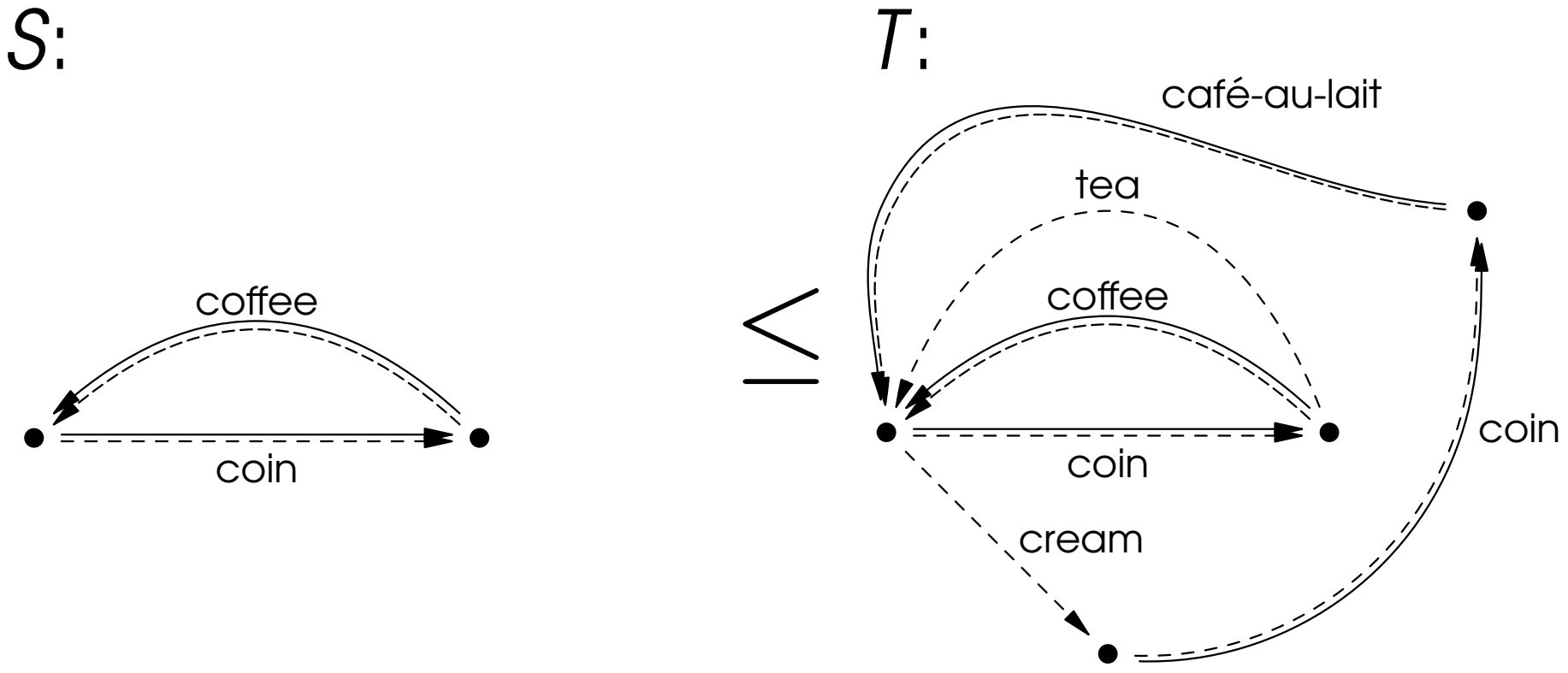
May refines to must, may or nothing. Must refines to must.

Refinement



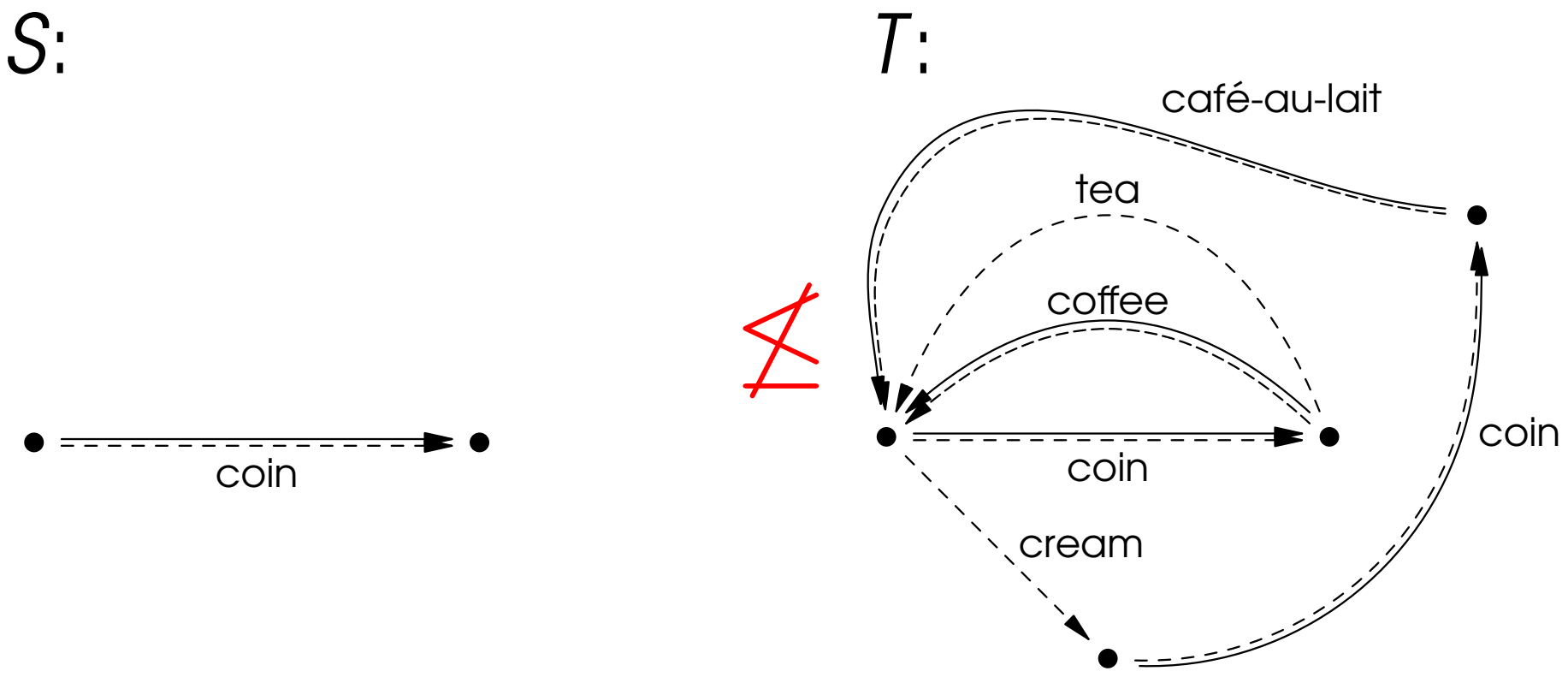
May refines to must, may or nothing. Must refines to must.

Refinement



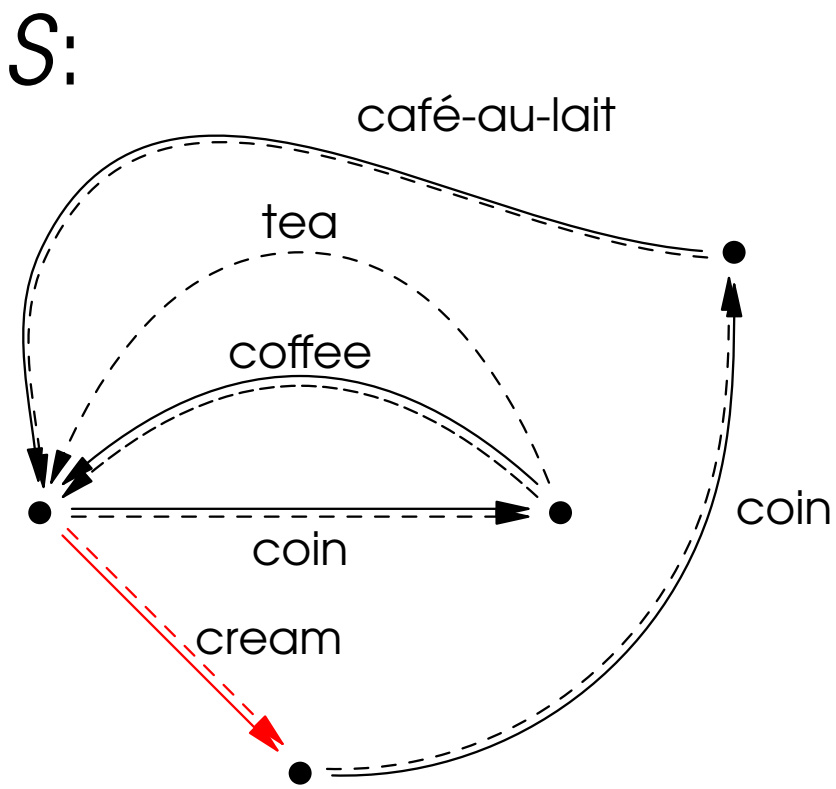
Infinitely many more refinements exist!!!

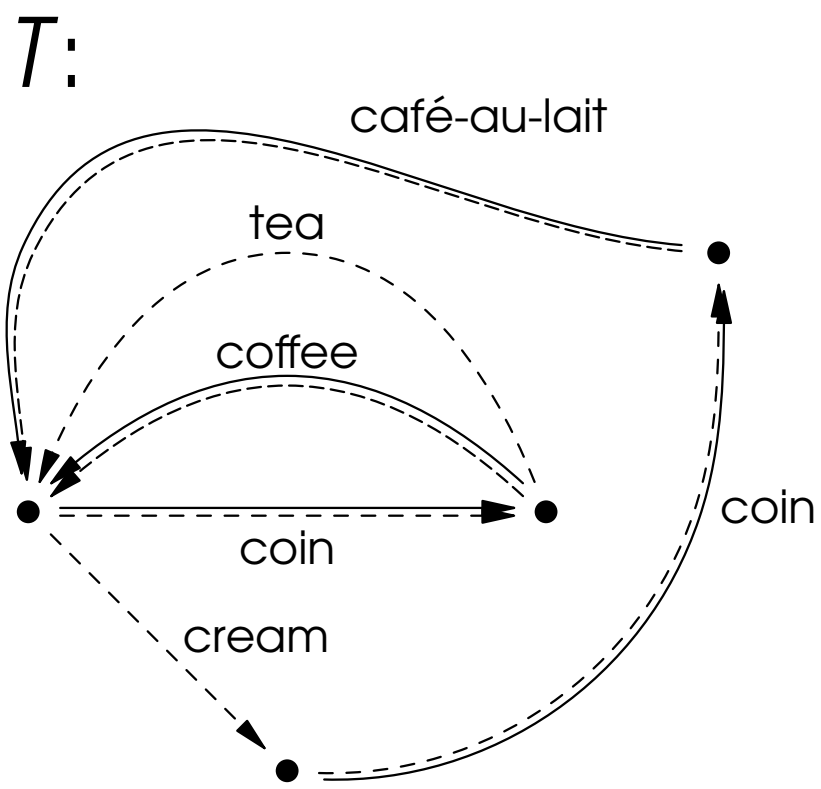
Refinement



But this is not a refinement!

Refinement



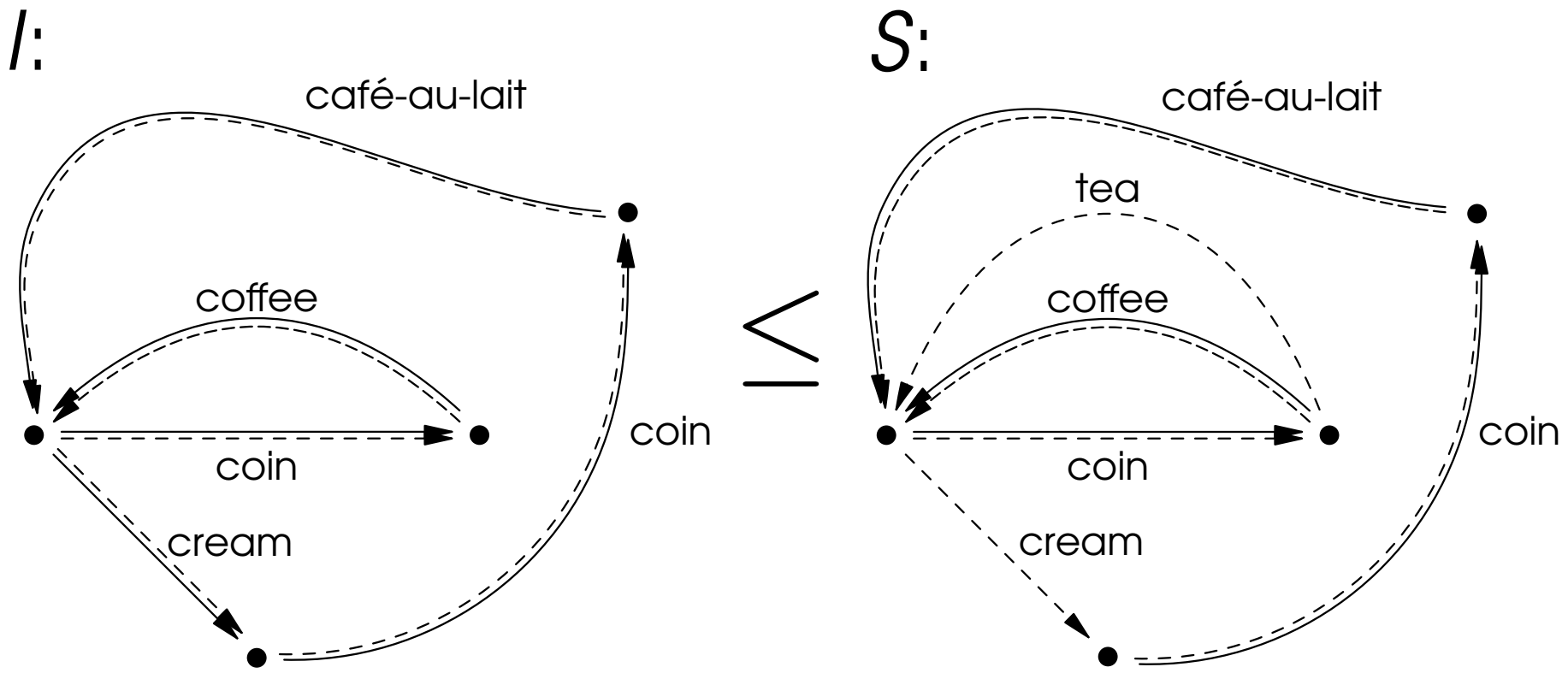


A relation $\leq$ is refinement iff for every $s \leq t$ it holds that

whenever $s \dashrightarrow^{a} s'$ then also $t \dashrightarrow^{a} t'$ for some t' and $s' \leq t'$

whenever $t \xrightarrow{a} t'$ then also $s \xrightarrow{a} s'$ for some s' and $s' \leq t'$

Implementations

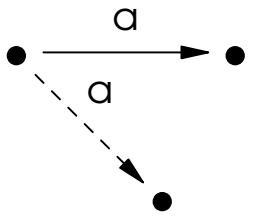


I is an implementation of S iff

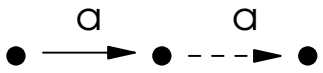
$$I \leq S \text{ and } \longrightarrow_I \; = \; \dashrightarrow_I$$

Mixed vs Modal Specifications

- **Modal** specifications: $\longrightarrow \subseteq \dashrightarrow$
  - $\rightarrow$ Always have implementations (consistent)
- **Mixed** specifications: possibly $\longrightarrow \not\subseteq \dashrightarrow$
  - $\rightarrow$ Larsen'89, Dams'96
- A **consistent** mixed specification:



- An **inconsistent** mixed specification:



Why Modal & Mixed Specifications ?

- **Semantic foundation** for specification & verification
- Same spec **combines** under- & over-approximations
  $\rightarrow$ existential and universal properties in static analysis
- Refinement is the **mid-way** between simulation (too weak) & bisimulation (too strong)
- See **recent survey** by the authors for more applications and more results
  $\rightarrow$ Bulleting of EATCS, June 2008

Part II

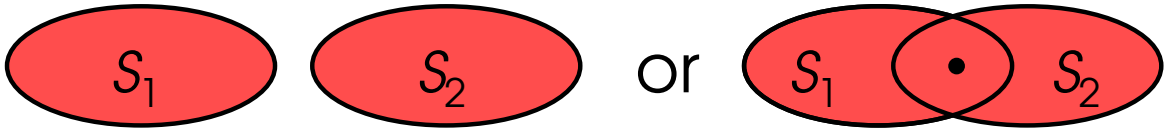
The Problems
&
Our Claims

Common Implementation

Problem CI

For modal (mixed) specifications S_1 and S_2 decide if

$$\exists \text{ implementation } I.\ I \leq S_1 \text{ and } I \leq S_2$$



?

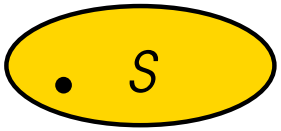
Claim: EXPTIME-complete

Consistency

Problem C

For a **mixed** specification S decide if

$$\exists \text{ implementation } I.\ I \leq S$$

$S = \varnothing$ or  **?**

Claim: EXPTIME-complete

Remark: this problem is trivial for **modal** specifications.

Thorough Refinement

Problem TR

For a **mixed** specifications S_1 and S_2 decide if

$$\forall \text{ implementations } I.\ I \leq S_1 \text{ implies } I \leq S_2$$

?

Claim: EXPTIME-complete

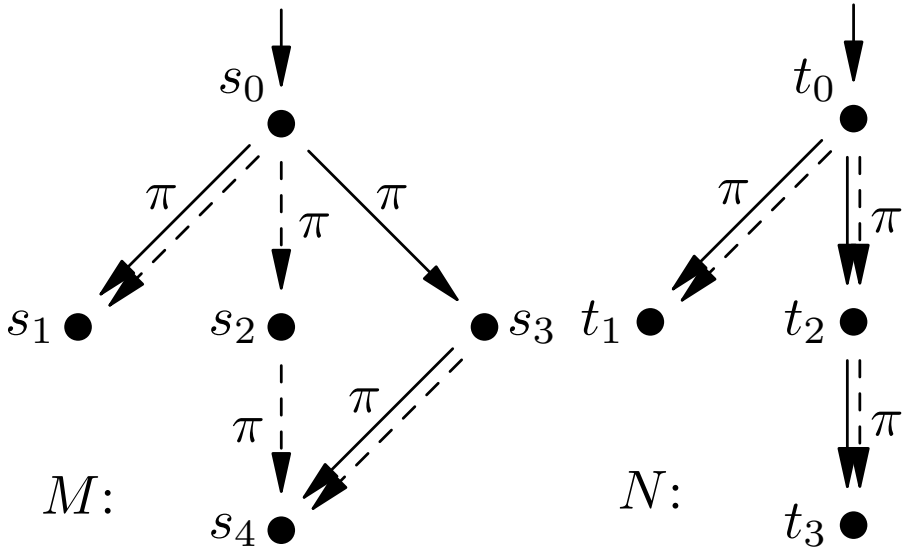
Remark: this problem is open for **modal** specifications.

Refinement vs Thorough Refinement

Note that refinement is in P, while TR is EXPTIME-complete.

So Refinement and TR **do not coincide**.

(Hüttel'88) proves this using a counterexample in this spirit:



Implementations sets of M and N are equal, but $M \not\leq N$.
Similar examples exist for properly modal specifications.

Part III

Proof Sketches

Bounds Before This Work

Antonik et al. FOSSACS'08

	Modal spec.	**Mixed spec.**
CI	PSPACE-hard, EXPTIME	PSPACE-hard, EXPTIME
C	trivial	PSPACE-hard, EXPTIME
TR	PSPACE-hard, EXPTIME	PSPACE-hard, EXPTIME

FOSSACS'08:

- Two complicated reductions showing the red !'s.
- A chain of reductions along the red arrows.

Bounds Before This Work

Antonik et al. FOSSACS'08

	Modal spec.	**Mixed spec.**
CI	PSPACE-hard, EXPTIME	PSPACE-hard, EXPTIME
C	trivial	PSPACE-hard, EXPTIME
TR	PSPACE-hard, EXPTIME	PSPACE-hard, EXPTIME

FOSSACS'08:

- Two complicated reductions showing the red !'s.
- A chain of reductions along the red arrows.

Bounds Before This Work

Antonik et al. FOSSACS'08

	Modal spec.	**Mixed spec.**
CI	PSPACE-hard, EXPTIME	PSPACE-hard, EXPTIME
C	trivial	PSPACE-hard, EXPTIME
TR	PSPACE-hard, EXPTIME	PSPACE-hard, EXPTIME

FOSSACS'08:

- Two complicated reductions showing the red !'s.
- A chain of reductions along the red arrows.

New Bounds — The Proof Structure

	Modal spec.	**Mixed spec.**
CI	PSPACE-hard, EXPTIME	PSPACE-hard, EXPTIME
C	trivial	PSPACE-hard, EXPTIME
TR	PSPACE-hard, EXPTIME	PSPACE-hard, EXPTIME

- Prove hardness of CI for modal specifications
- By the know sequence of reductions arrive at the remaining results
- So far failed to reduce TR in the modal case

New Bounds — The Proof Structure

	Modal spec.	Mixed spec.
CI	EXPTIME-hard, EXPTIME	PSPACE-hard, EXPTIME
C	trivial	PSPACE-hard, EXPTIME
TR	PSPACE-hard, EXPTIME	PSPACE-hard, EXPTIME

- Prove hardness of CI for modal specifications
- By the know sequence of reductions arrive at the remaining results
- So far failed to reduce TR in the modal case

New Bounds — The Proof Structure

	Modal spec.	Mixed spec.
CI	EXPTIME-hard, EXPTIME	PSPACE-hard, EXPTIME
C	trivial	PSPACE-hard, EXPTIME
TR	PSPACE-hard, EXPTIME	PSPACE-hard, EXPTIME

- Prove hardness of CI for modal specifications
- By the know sequence of reductions arrive at the remaining results
- So far failed to reduce TR in the modal case

New Bounds — The Proof Structure

	Modal spec.	Mixed spec.
CI	EXPTIME-hard, EXPTIME	EXPTIME-hard, EXPTIME
C	trivial	EXPTIME-hard, EXPTIME
TR	PSPACE-hard, EXPTIME	EXPTIME-hard, EXPTIME

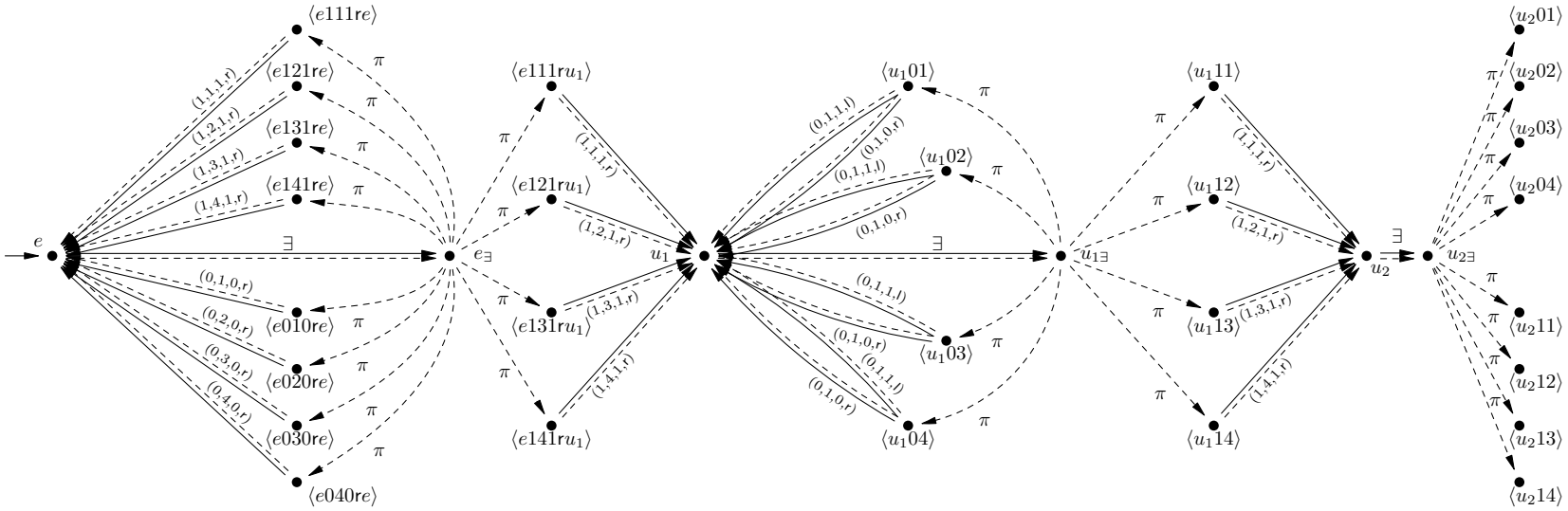
- Prove hardness of CI for modal specifications
- By the know sequence of reductions arrive at the remaining results
- So far failed to reduce TR in the modal case

CI for Modal Specs is EXPTIME-complete

Most of the paper is devoted to EXPTIME-completeness of CI for Modal Specifications

The proof is by reduction from the acceptance problem for linearly bounded alternating Turing machines.

A teaser:



More in the paper.

Part IV

Closing

Summary

	Modal specifications	Mixed specifications
CI	**EXPTIME-complete**	**EXPTIME-complete**
C	trivial	**EXPTIME-complete**
TR	PSPACE-hard, EXPTIME	**EXPTIME-complete**

New results in **bold**.
The remaining gap in red.