Dual-Priced Parametric Modal Transition Systems

Jiri Srba

Aalborg University, Denmark

Copenhagen Meeting on Variability Analysis, ITU, 18.11.2013

Joint work with Nikola Beneš, Jan Křetínský, Kim G. Larsen and Mikael H. Møller.

Motivation

Overall Aim

Need for a sound theory supporting a step-wise, component-based design of a software system.

- Components are specified in a formal way at a certain abstraction level.
- Specifications are gradually refined until a concrete system is produced.
- If the refinement steps preserve certain properties, the final system will as well.

Motivation

We focus on Modal Transition Systems (MTS), a specification formalism introduced by K.G. Larsen and B. Thomsen.

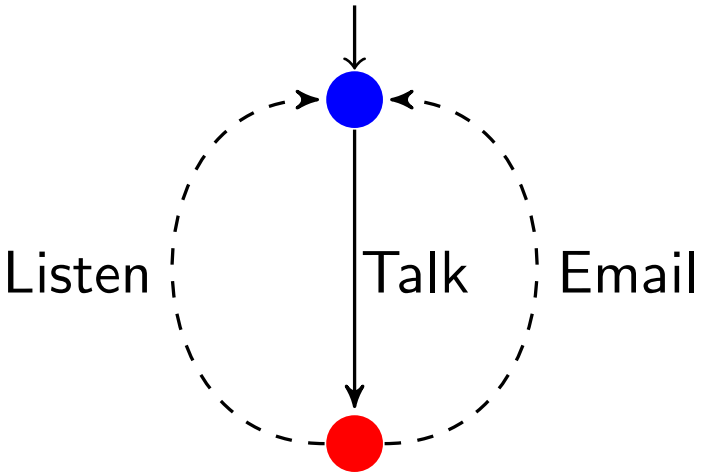
- MTS are automata-based specification formalism.
- MTS allow to express that certain actions must or may happen in their implementations.
- Recently many applications in component-based software development, interface theories, modal abstractions and program analysis.

Outline of the Talk

1. MTS definition, refinement relations, basic results.
2. Parametric MTS.
3. Dual-Priced MTS.

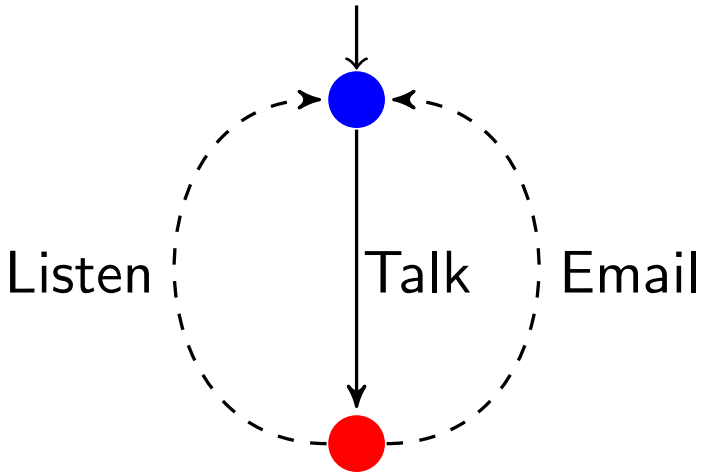
Example: ITU Meeting

Specification:

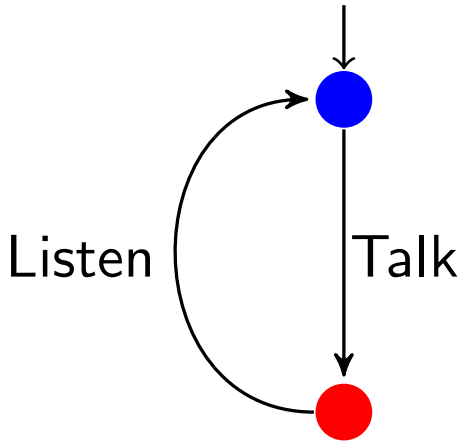


Example: ITU Meeting

Specification:

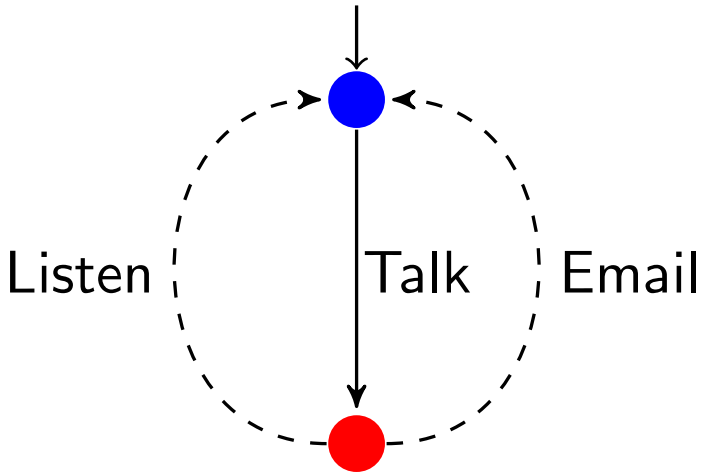


Implementations:

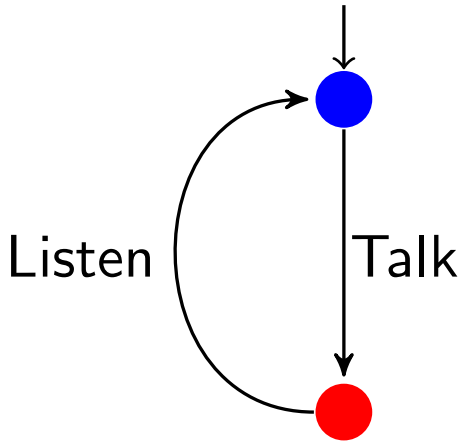


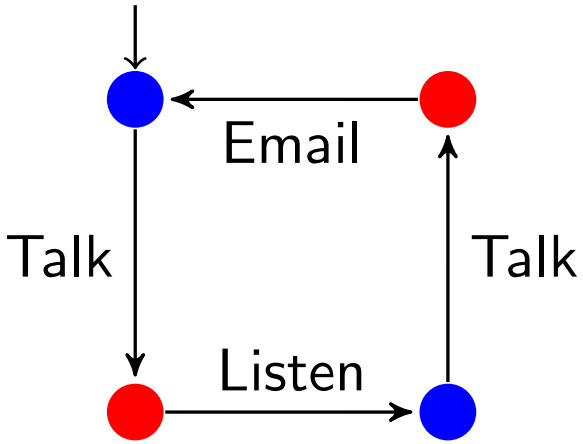
Example: ITU Meeting

Specification:



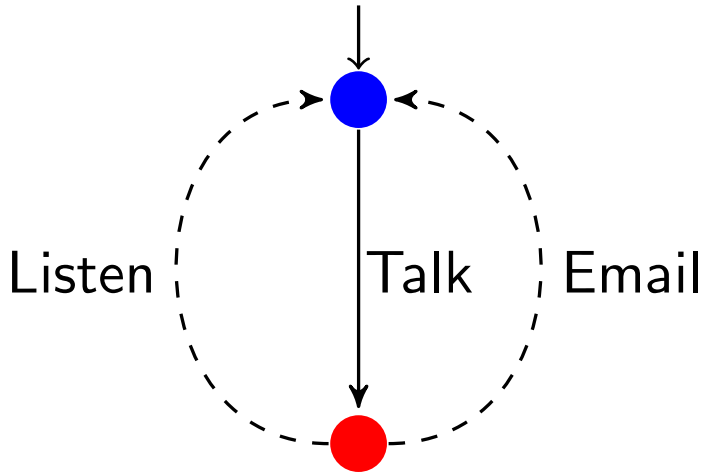
Implementations:



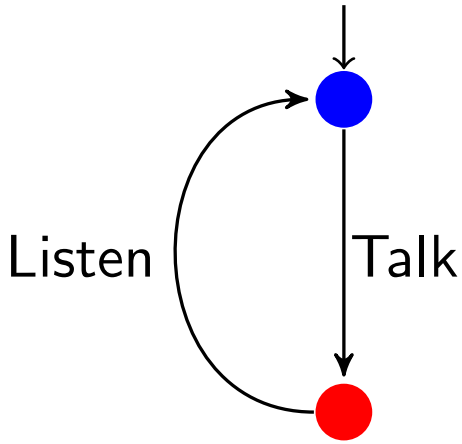


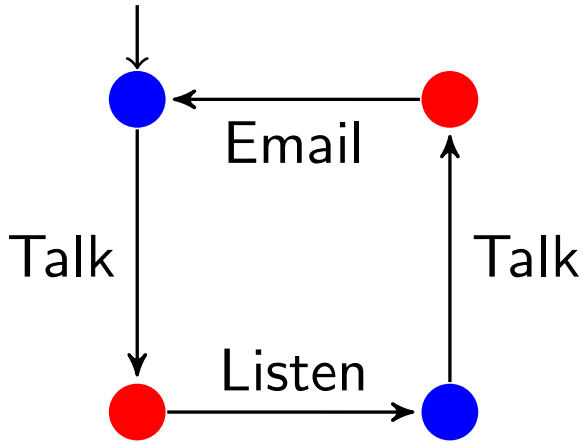
Example: ITU Meeting

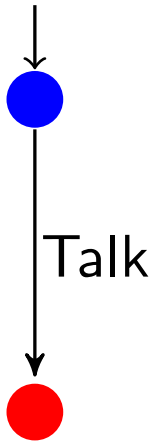
Specification:



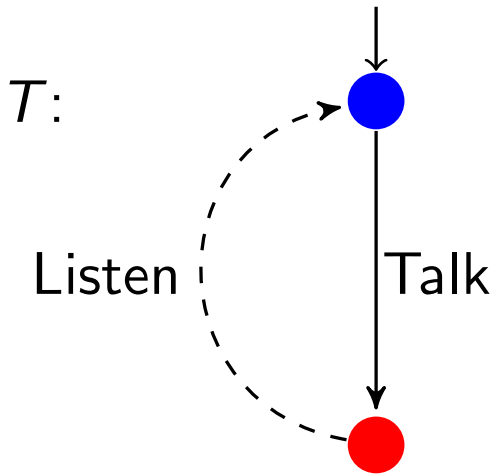
Implementations:

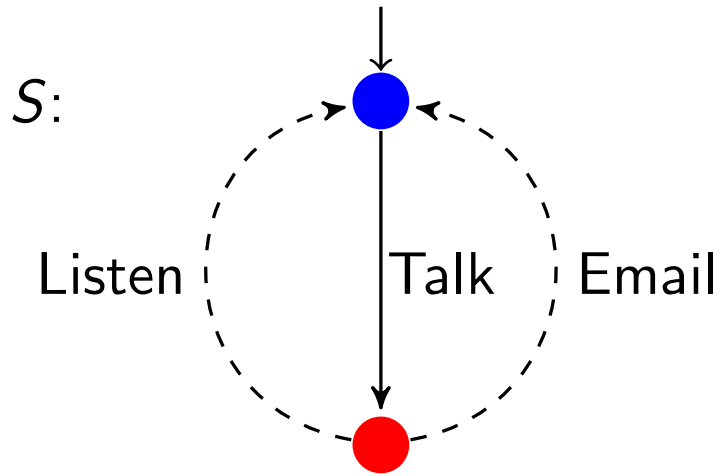




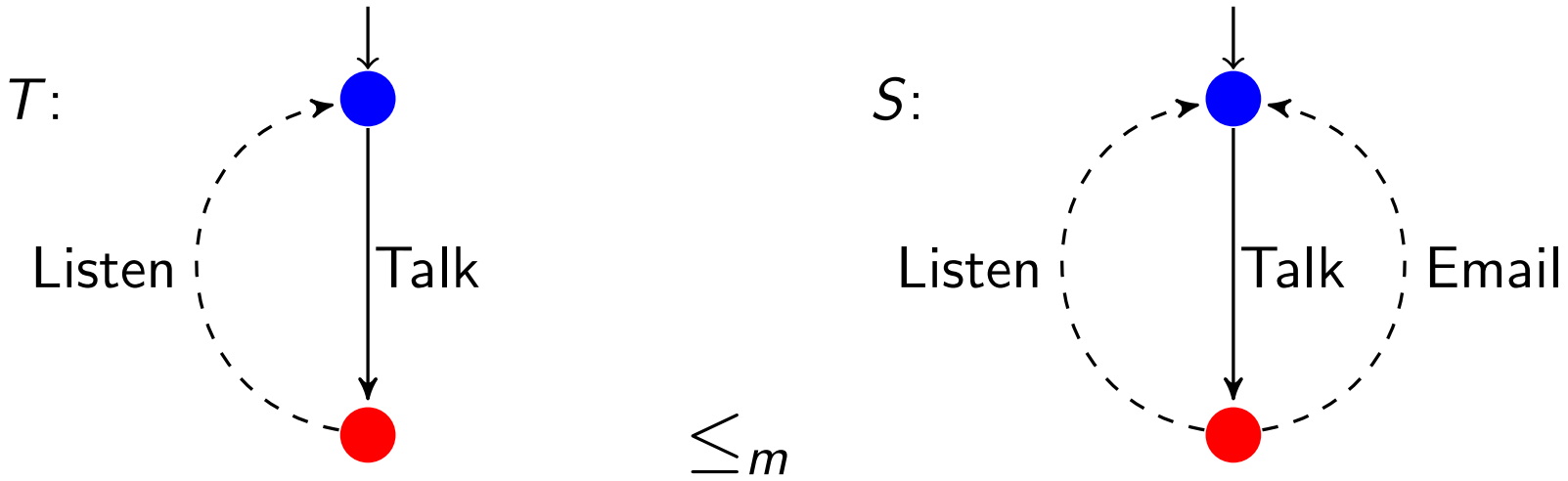


Modal Refinement

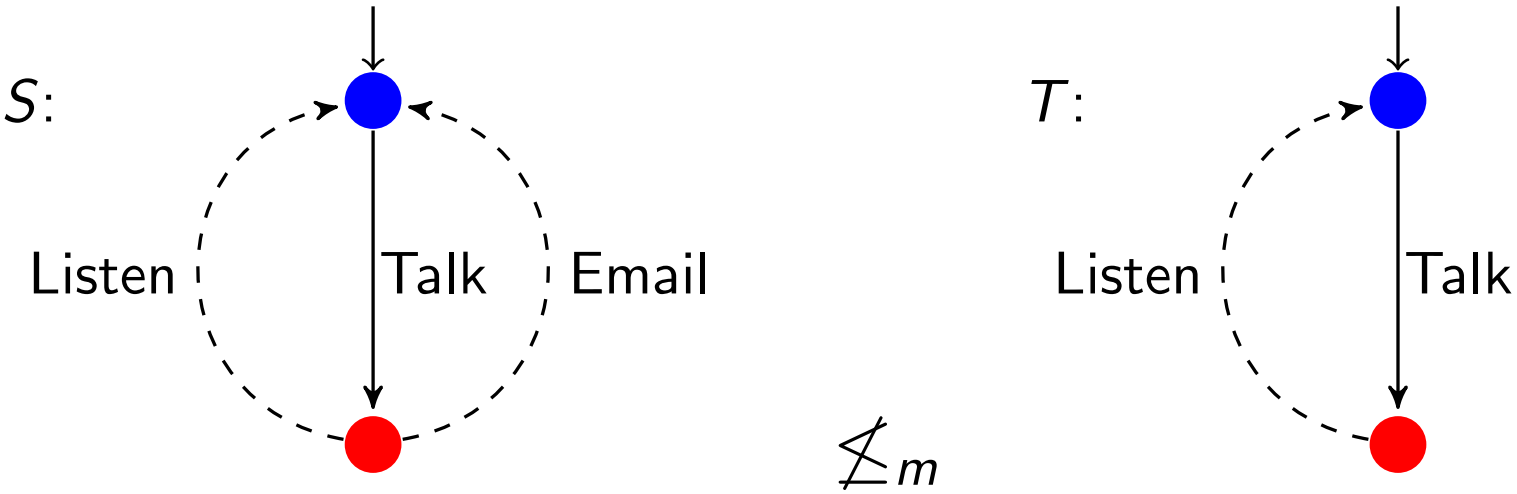




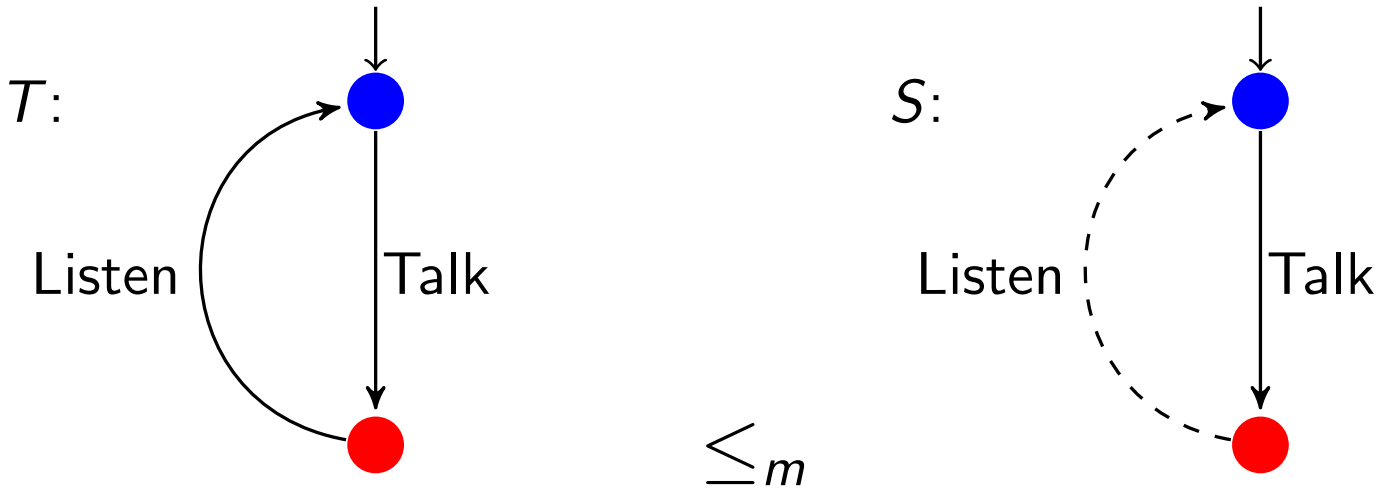
Modal Refinement



Modal Refinement



Modal Refinement



MTS Definition

Definition (Modal Transition System)

An MTS is a triple $(P, \dashrightarrow, \longrightarrow)$ where P is a set of states and $\longrightarrow \subseteq \dashrightarrow \subseteq P \times \Sigma \times P$.

If $S \xrightarrow{a} S'$ then also $S \overset{a}{\dashrightarrow} S'$; we draw only the must transition.

If $\longrightarrow = \dashrightarrow$ then the MTS is called an implementation.

MTS Definition

Definition (Modal Transition System)

An MTS is a triple $(P, \dashrightarrow, \longrightarrow)$ where P is a set of states and $\longrightarrow \subseteq \dashrightarrow \subseteq P \times \Sigma \times P$.

If $S \xrightarrow{a} S'$ then also $S \overset{a}{\dashrightarrow} S'$; we draw only the must transition.

If $\longrightarrow = \dashrightarrow$ then the MTS is called an implementation.

Definition (Modal Refinement $\leq_m$)

We write $T \leq_m S$ if there is a relation $\mathcal{R} \subseteq P \times P$ s.t. $(T, S) \in \mathcal{R}$ and for every $(A, B) \in \mathcal{R}$

- if $A \overset{a}{\dashrightarrow} A'$ then $B \overset{a}{\dashrightarrow} B'$ and $(A', B') \in \mathcal{R}$, and
- if $B \xrightarrow{a} B'$ then $A \xrightarrow{a} A'$ and $(A', B') \in \mathcal{R}$.

MTS Definition

Definition (Modal Transition System)

An MTS is a triple $(P, \dashrightarrow, \longrightarrow)$ where P is a set of states and $\longrightarrow \subseteq \dashrightarrow \subseteq P \times \Sigma \times P$.

If $S \xrightarrow{a} S'$ then also $S \overset{a}{\dashrightarrow} S'$; we draw only the must transition.

If $\longrightarrow = \dashrightarrow$ then the MTS is called an implementation.

Definition (Modal Refinement $\leq_m$)

We write $T \leq_m S$ if there is a relation $\mathcal{R} \subseteq P \times P$ s.t. $(T, S) \in \mathcal{R}$ and for every $(A, B) \in \mathcal{R}$

- if $A \overset{a}{\dashrightarrow} A'$ then $B \overset{a}{\dashrightarrow} B'$ and $(A', B') \in \mathcal{R}$, and
- if $B \xrightarrow{a} B'$ then $A \xrightarrow{a} A'$ and $(A', B') \in \mathcal{R}$.

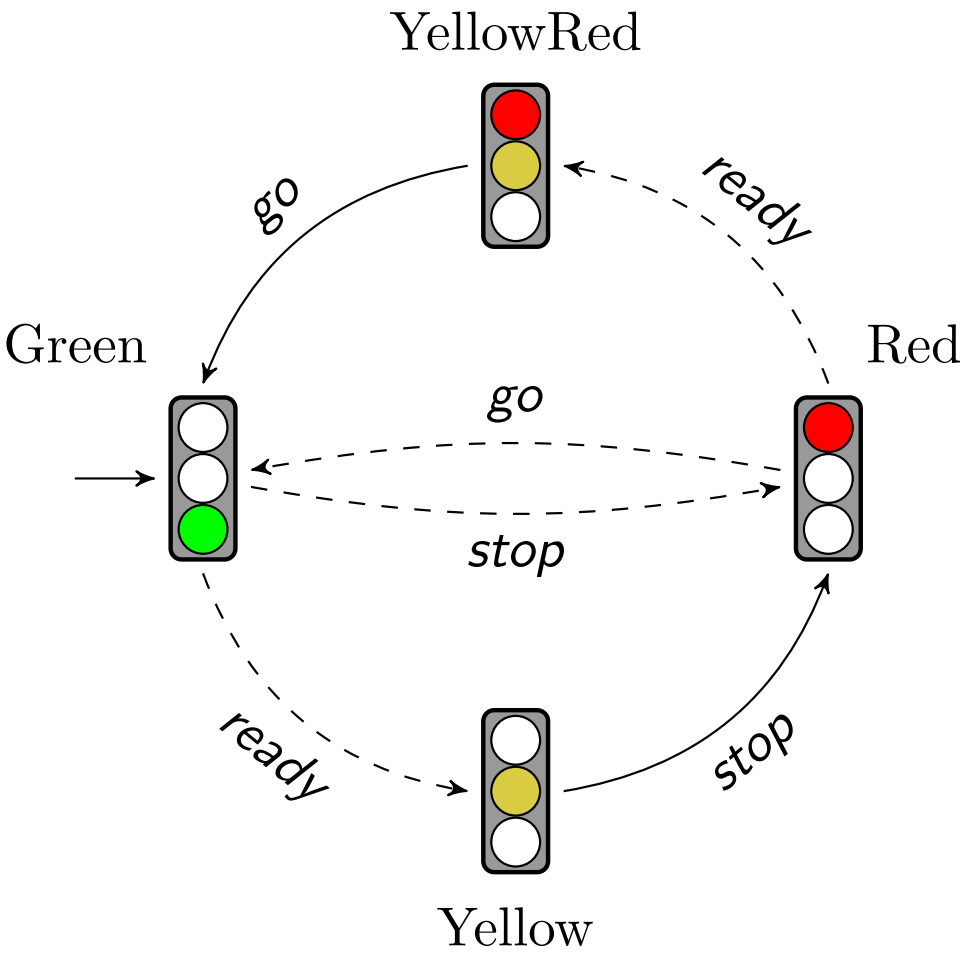
Note that on implementations $\leq_m$ coincides with bisimulation.

Parametric Modal Transition Systems [ATVA'11]

- MTS have many desirable properties but are a low level modelling formalism.
- Impossible to avoid deadlock states with outgoing may-transitions only.
- Impossible to define exclusive choices.
- Impossible to enforce persistent choices.

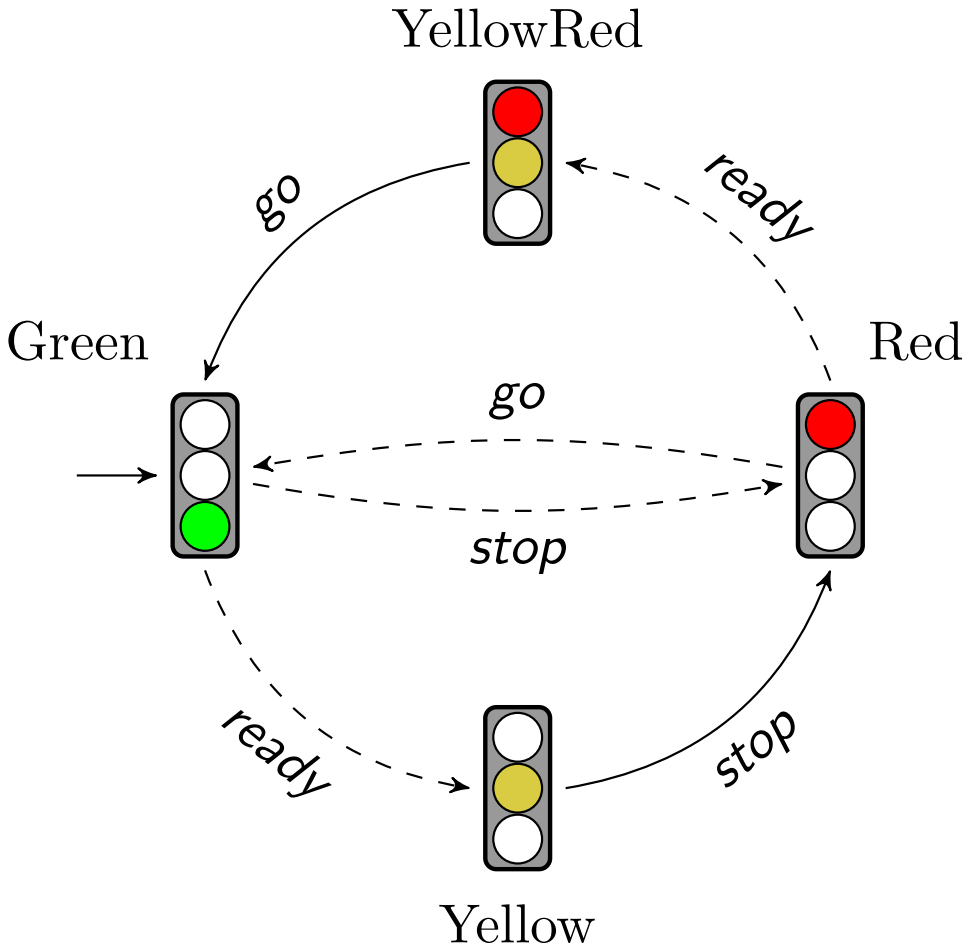
We suggest parametric MTS to deal with these issues.

Example: A Traffic Light

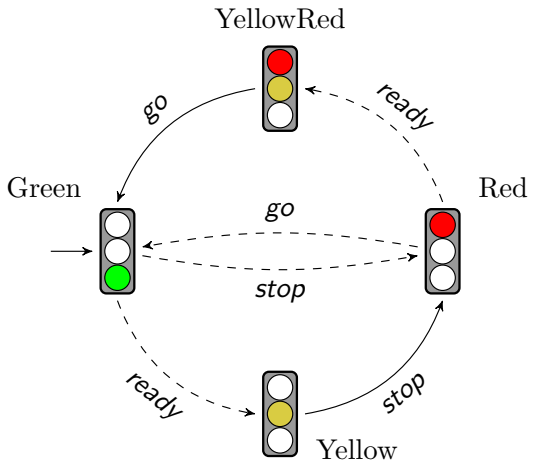


Example: A Traffic Light

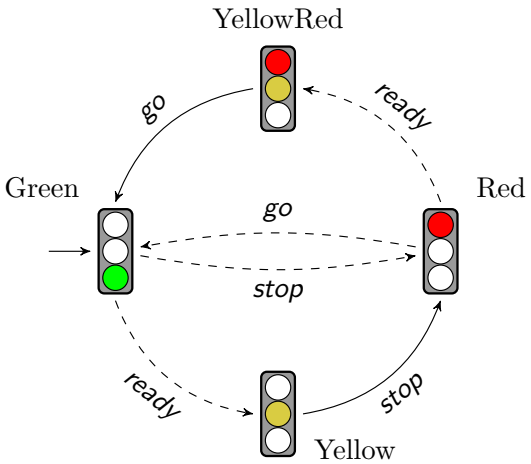
$\leq m$

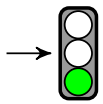


More Problematic Implementations

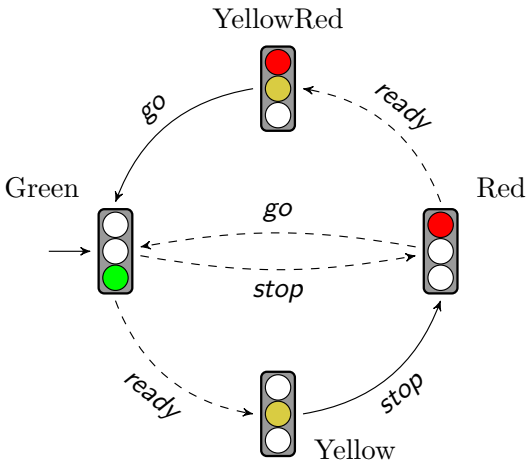


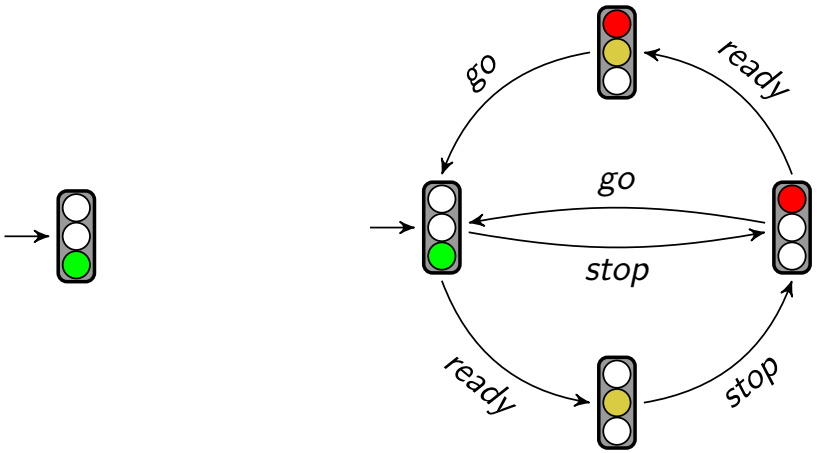
More Problematic Implementations



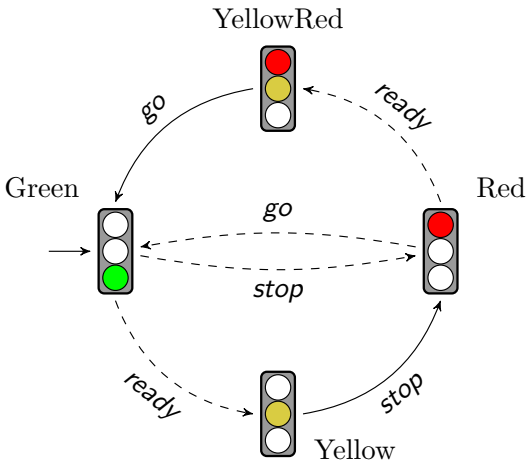


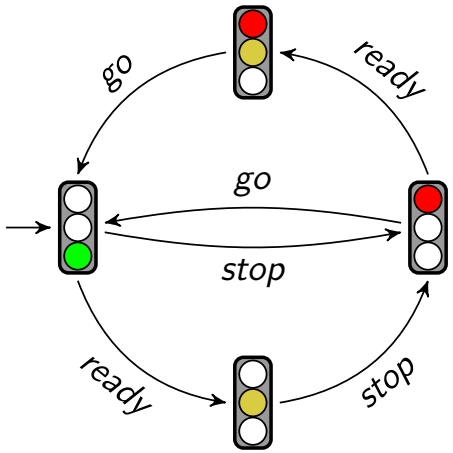
More Problematic Implementations

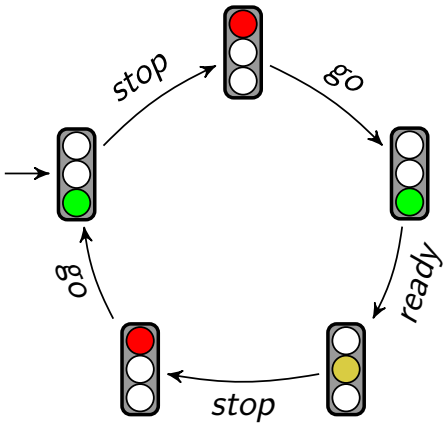




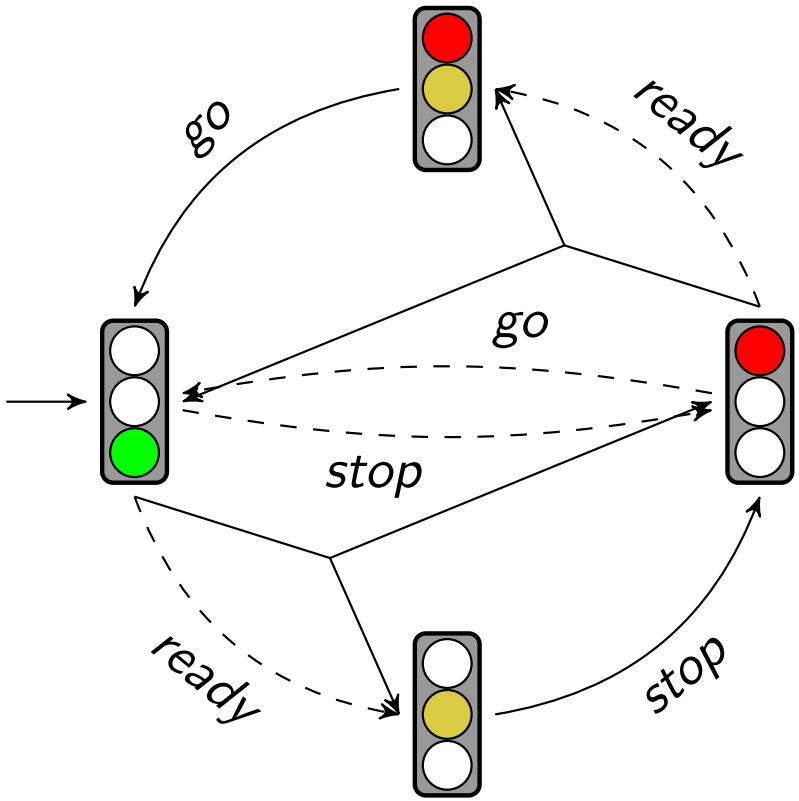
More Problematic Implementations



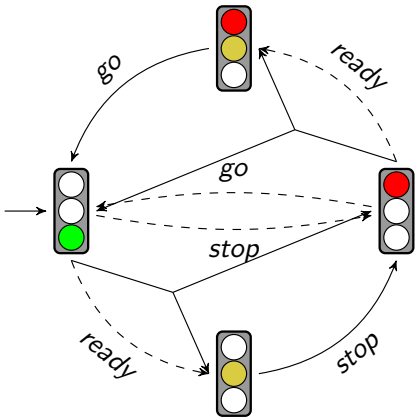


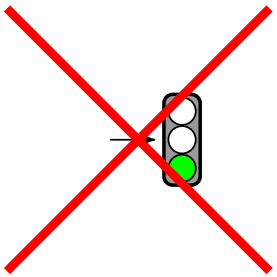


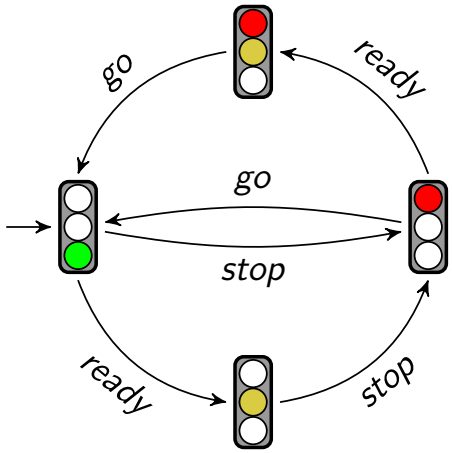
Disjunctive MTS

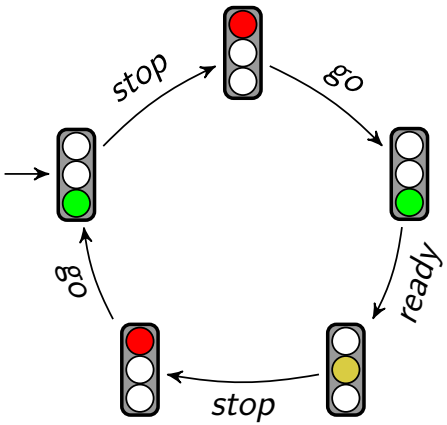


Disjunctive MTS

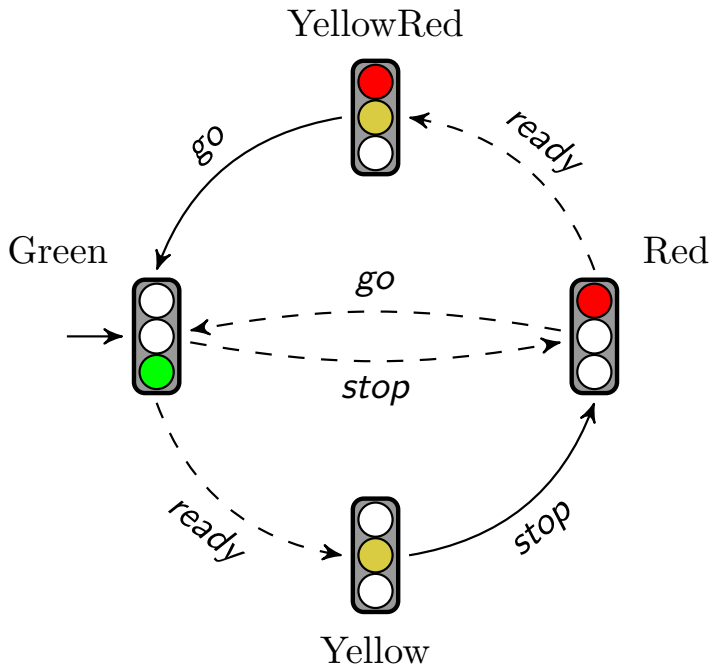








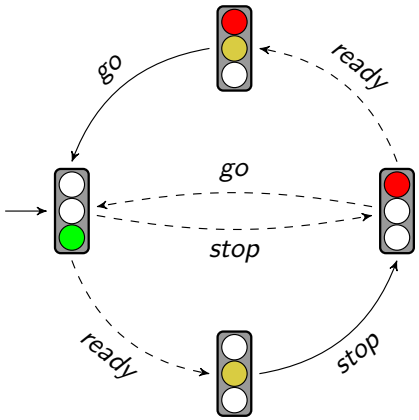
MTS with Obligations



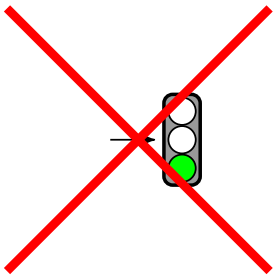
Obligation function $\Phi : \text{States} \to \mathcal{B}(\text{Transitions})$

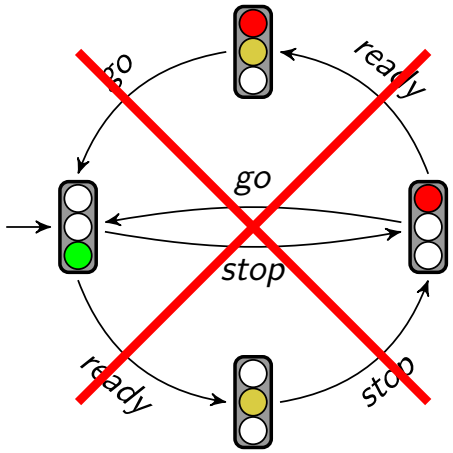
$$\begin{aligned}
\Phi(\text{Yellow}) &= \textit{stop} \\
\Phi(\text{YellowRed}) &= \textit{go} \\
\Phi(\text{Green}) &= \textit{stop} \oplus \textit{ready} \\
\Phi(\text{Red}) &= \textit{go} \oplus \textit{ready}
\end{aligned}$$

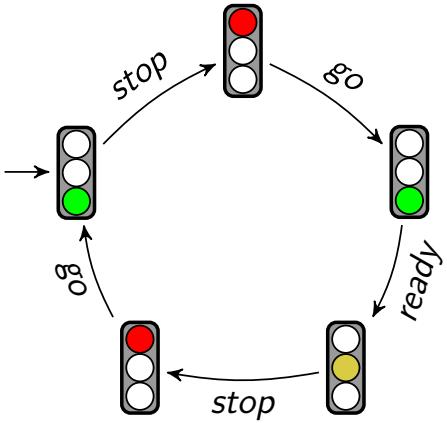
MTS with Obligations



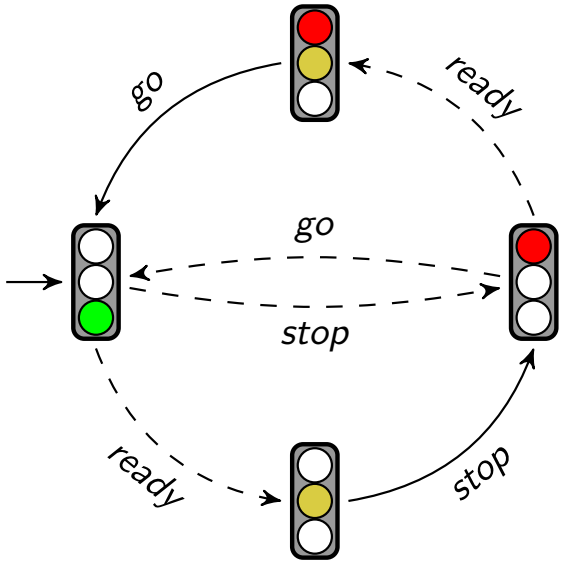
$$\begin{aligned}
\Phi(\text{Yellow}) &= \textit{stop} \\
\Phi(\text{YellowRed}) &= \textit{go} \\
\Phi(\text{Green}) &= \textit{stop} \oplus \textit{ready} \\
\Phi(\text{Red}) &= \textit{go} \oplus \textit{ready}
\end{aligned}$$







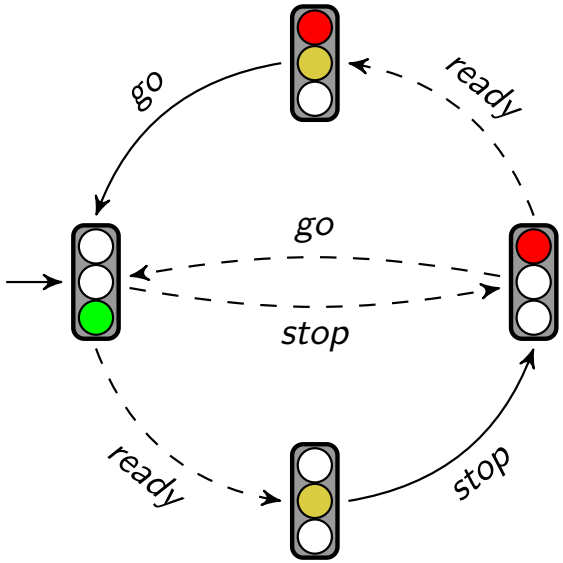
Parametric Modal Transition System



Obligation function $\Phi : \text{States} \rightarrow \mathcal{B}(\text{Transitions} \cup \text{Parameters})$

$\text{Parameters} = \{\mathit{RthenY}, \mathit{GthenY}\}$

Parametric Modal Transition System

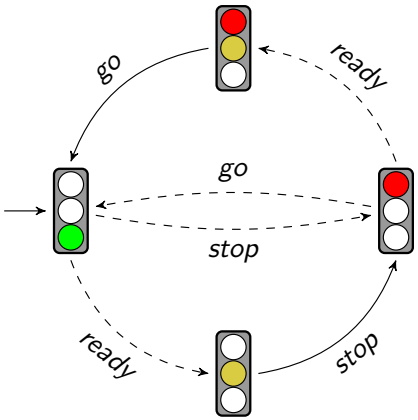


Obligation function $\Phi : \text{States} \rightarrow \mathcal{B}(\text{Transitions} \cup \text{Parameters})$

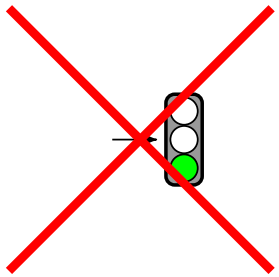
$\text{Parameters} = \{\mathit{RthenY}, \mathit{GthenY}\}$

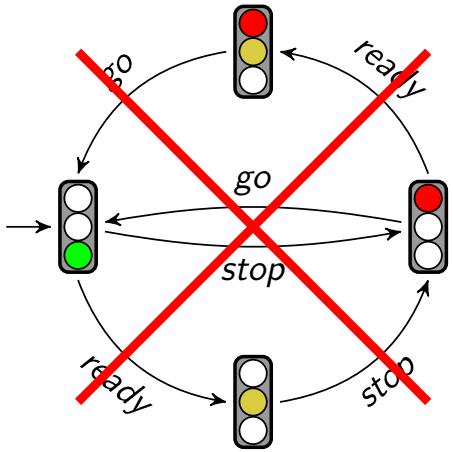
$$
\begin{aligned}
\Phi(\text{Yellow}) &= \mathit{stop} \\
\Phi(\text{YellowRed}) &= \mathit{go} \\
\Phi(\text{Green}) &= (\mathit{stop} \oplus \mathit{ready}) \wedge (\mathit{GthenY} \Leftrightarrow \mathit{ready}) \\
\Phi(\text{Red}) &= (\mathit{go} \oplus \mathit{ready}) \wedge (\mathit{RthenY} \Leftrightarrow \mathit{ready})
\end{aligned}
$$

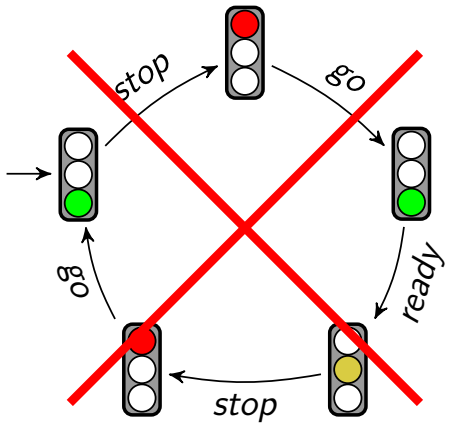
Parametric Modal Transition System



$$
\begin{aligned}
\Phi(\text{Yellow}) &= \mathit{stop} \\
\Phi(\text{YellowRed}) &= \mathit{go} \\
\Phi(\text{Green}) &= (\mathit{stop} \oplus \mathit{ready}) \wedge (\mathit{GthenY} \Leftrightarrow \mathit{ready}) \\
\Phi(\text{Red}) &= (\mathit{go} \oplus \mathit{ready}) \wedge (\mathit{RthenY} \Leftrightarrow \mathit{ready})
\end{aligned}
$$

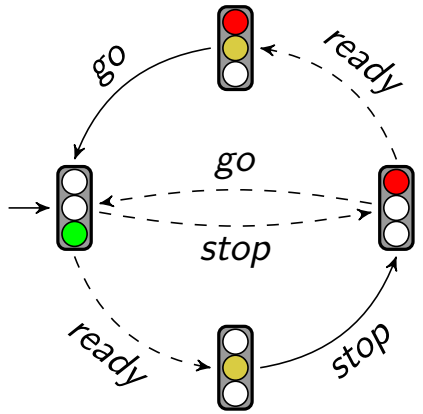






Modal Refinement

Parameters: $\{RthenY, GthenY\}$



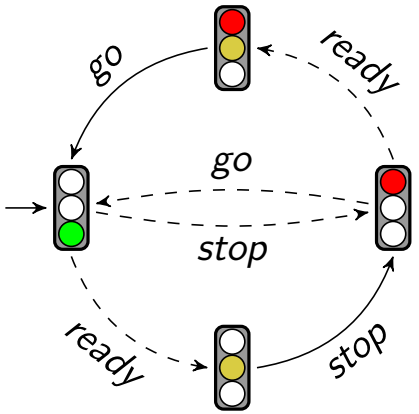
Obligation function:

$$\Phi(\mathrm{Green}) = (stop \oplus ready) \wedge (GthenY \Leftrightarrow ready)$$

$$\Phi(\mathrm{Red}) = (go \oplus ready) \wedge (RthenY \Leftrightarrow ready)$$

Modal Refinement

Parameters: $\{reqY\}$



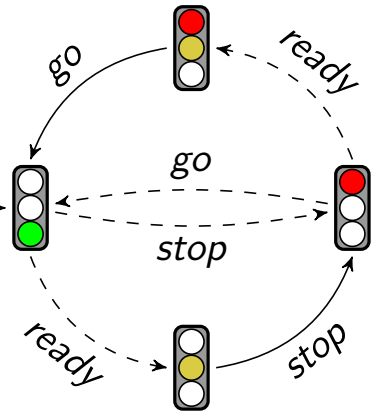
Obligation function:

$$\Phi(\mathrm{Green}) = (stop \oplus ready) \wedge (reqY \Leftrightarrow ready)$$

$$\Phi(\mathrm{Red}) = (go \oplus ready) \wedge (reqY \Leftrightarrow ready)$$

$\leq_m$

Parameters: $\{RthenY, GthenY\}$

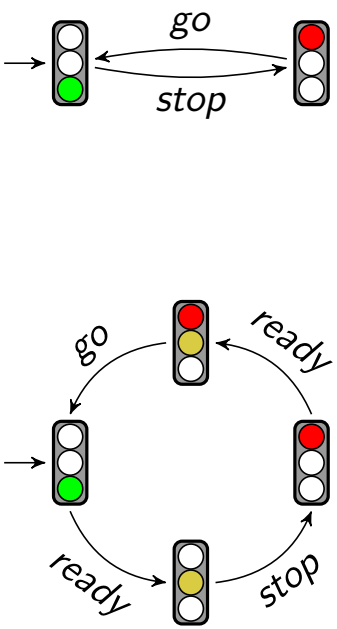


Obligation function:

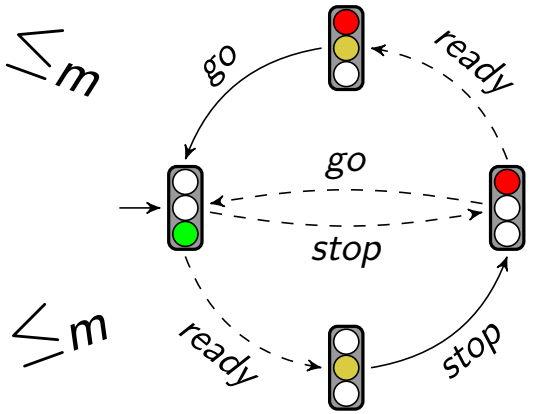
$$\Phi(\mathrm{Green}) = (stop \oplus ready) \wedge (GthenY \Leftrightarrow ready)$$

$$\Phi(\mathrm{Red}) = (go \oplus ready) \wedge (RthenY \Leftrightarrow ready)$$

Modal Refinement



Parameters: $\{reqY\}$

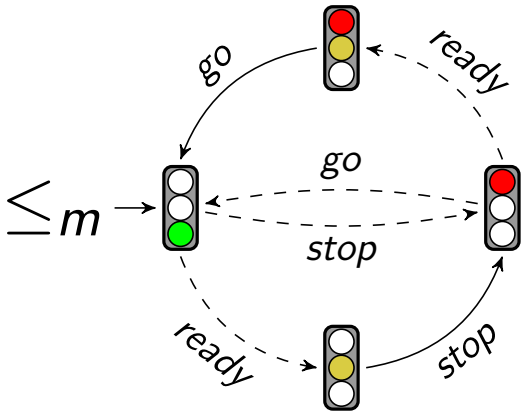


Obligation function:

$$\Phi(\mathrm{Green}) = (stop \oplus ready) \wedge (reqY \Leftrightarrow ready)$$

$$\Phi(\mathrm{Red}) = (go \oplus ready) \wedge (reqY \Leftrightarrow ready)$$

Parameters: $\{RthenY, GthenY\}$



Obligation function:

$$\Phi(\mathrm{Green}) = (stop \oplus ready) \wedge (GthenY \Leftrightarrow ready)$$

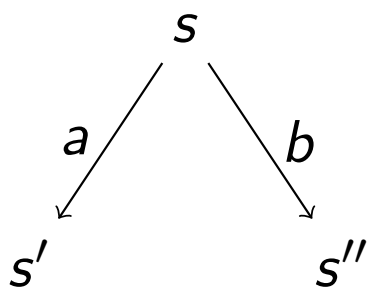
$$\Phi(\mathrm{Red}) = (go \oplus ready) \wedge (RthenY \Leftrightarrow ready)$$

Modal Refinement

For $s \in \text{States}$ and $\nu \subseteq \text{Parameters}$, let

$$\text{PossibleTransitions}_{\nu}(s) = \{T \subseteq \text{Transitions}(s) \mid T \cup \nu \models \Phi(s)\}$$

Example:



For $\Phi(s) = a \Leftrightarrow p$,

$$\text{PossibleTransitions}_{\{p\}}(s) = \Big\{\{a\}, \{a, b\}\Big\}$$

Modal Refinement

For $s \in \text{States}$ and $\nu \subseteq \text{Parameters}$, let

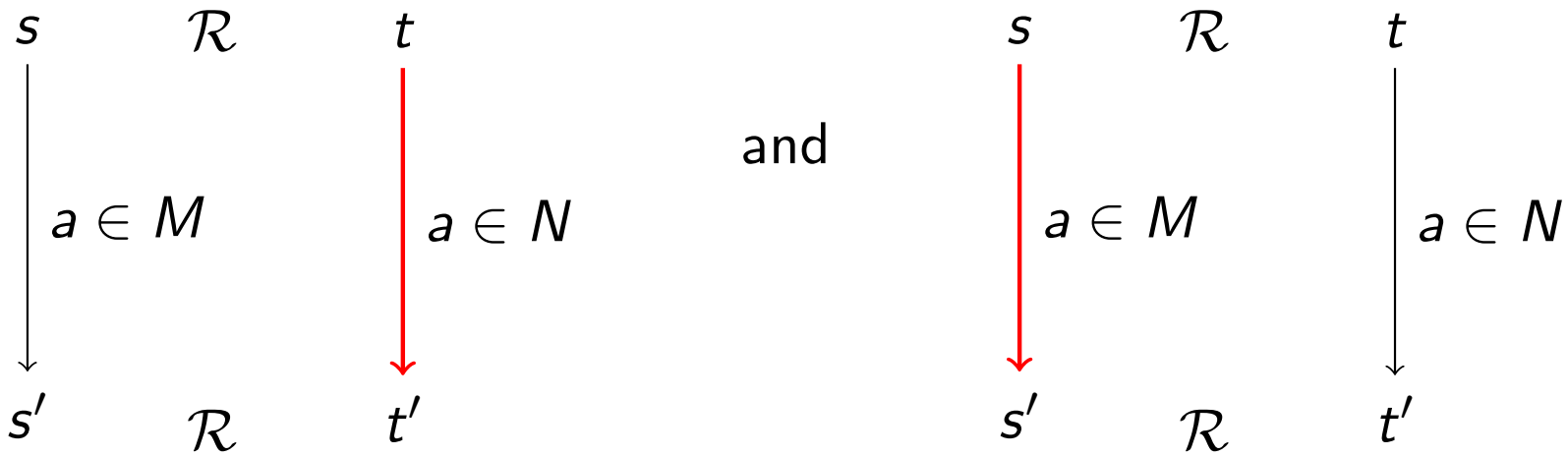
$$\text{PossibleTransitions}_\nu(s) = \{T \subseteq \text{Transitions}(s) \mid T \cup \nu \models \Phi(s)\}$$

Definition (Modal Refinement)

Binary relation $\mathcal{R}$ is a *modal refinement* if

$\forall \mu \subseteq \text{Parameters}_1 : \exists \nu \subseteq \text{Parameters}_2 :$ for every $(s,t) \in \mathcal{R}$:

$\forall M \in \text{PossibleTransitions}_\mu(s) : \exists N \in \text{PossibleTransitions}_\nu(t)$:



Complexity Results of Modal Refinement Checking

Parameter-free PMTS:

	Boolean	Positive	pCNF	pDNF	MTS
Boolean	Π_2^{p}-comp.	coNP-comp.	$\in$ coNP P-hard	coNP-comp.	$\in$ coNP P-hard
Positive	Π_2^{p}-comp.	coNP-comp.	P-comp.	coNP-comp.	P-comp.
pCNF	Π_2^{p}-comp.	coNP-comp.	P-comp.	coNP-comp.	P-comp.
pDNF	Π_2^{p}-comp.	P-comp.	P-comp.	P-comp.	P-comp.
MTS	Π_2^{p}-comp.	P-comp.	P-comp.	P-comp.	P-comp.
Impl	NP-comp.	P-comp.	P-comp.	P-comp.	P-comp.

Complexity Results of Modal Refinement Checking

Parameter-free PMTS:

	Boolean	Positive	pCNF	pDNF	MTS
Boolean	Π_2^{p}-comp.	coNP-comp.	$\in$ coNP P-hard	coNP-comp.	$\in$ coNP P-hard
Positive	Π_2^{p}-comp.	coNP-comp.	P-comp.	coNP-comp.	P-comp.
pCNF	Π_2^{p}-comp.	coNP-comp.	P-comp.	coNP-comp.	P-comp.
pDNF	Π_2^{p}-comp.	P-comp.	P-comp.	P-comp.	P-comp.
MTS	Π_2^{p}-comp.	P-comp.	P-comp.	P-comp.	P-comp.
Impl	NP-comp.	P-comp.	P-comp.	P-comp.	P-comp.

(General) PMTS:

	Boolean	positive	pCNF	pDNF
Boolean	Π_4^{p}-comp.	Π_3^{p}-comp.	$\in \Pi_3^{\mathrm{p}}$ Π_2^{p}-hard	Π_3^{p}-comp.
positive	Π_4^{p}-comp.	Π_3^{p}-comp.	Π_2^{p}-comp.	Π_3^{p}-comp.
pCNF	Π_4^{p}-comp.	Π_3^{p}-comp.	Π_2^{p}-comp.	Π_3^{p}-comp.
pDNF	Π_4^{p}-comp.	Π_2^{p}-comp.	Π_2^{p}-comp.	Π_2^{p}-comp.
MTS	Σ_3^{p}-comp.	NP-comp.	NP-comp.	NP-comp.
Impl	NP-comp.	NP-comp.	NP-comp.	NP-comp.

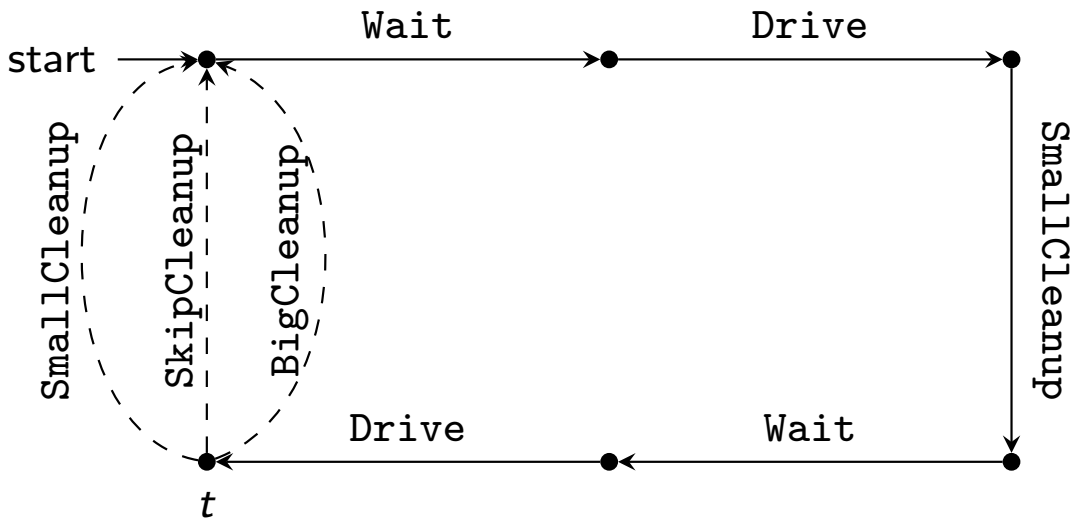
Cost and Duration [LPAR'12]

The cost of implemantations matters! (product lines)

- We suggest a quantitative extension of parametric MTS with cost and durations.
- Dual-priced scheme (investment cost plus the running cost).

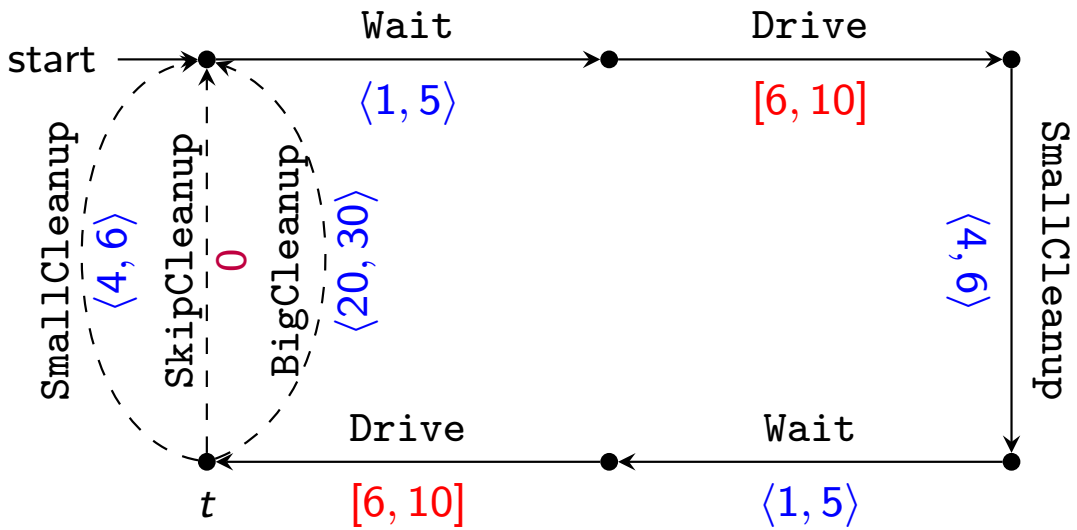
Modal Transition Systems with Durations

$$\Phi(t) = \begin{array}{l} \texttt{BigCleanup} \vee \\ \texttt{SkipCleanup} \vee \\ \texttt{SmallCleanup} \end{array}$$



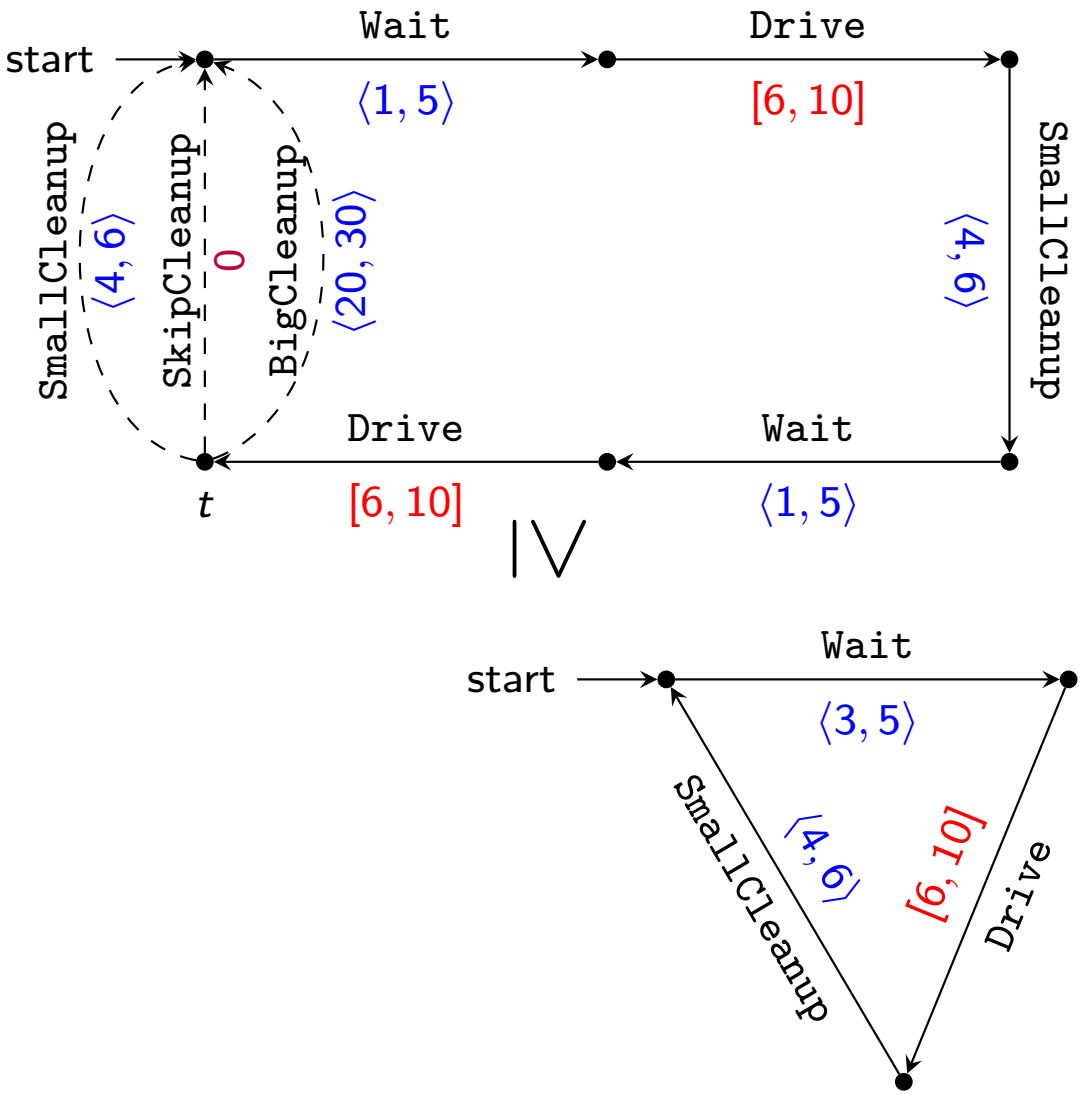
Modal Transition Systems with Durations

$$\Phi(t) = \begin{array}{l} \texttt{BigCleanup} \vee \\ \texttt{SkipCleanup} \vee \\ \texttt{SmallCleanup} \end{array}$$



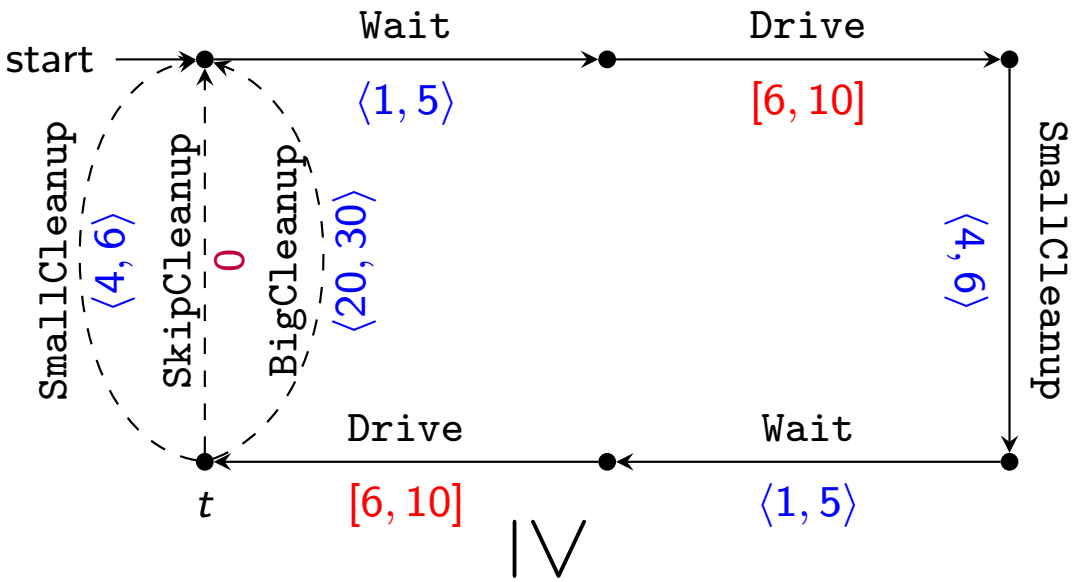
Modal Transition Systems with Durations

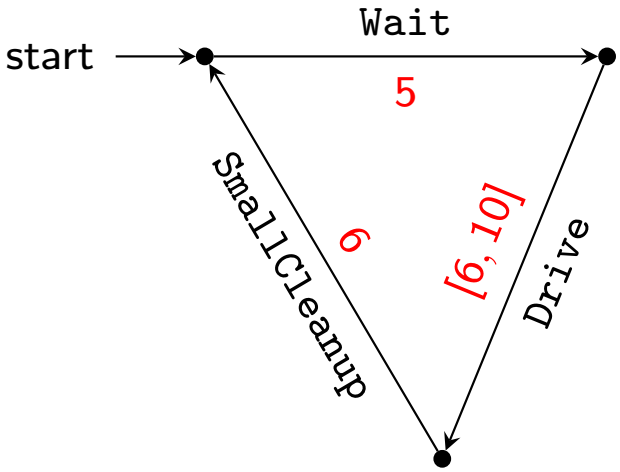
$$\Phi(t) = \begin{array}{l} \texttt{BigCleanup} \vee \\ \texttt{SkipCleanup} \vee \\ \texttt{SmallCleanup} \end{array}$$



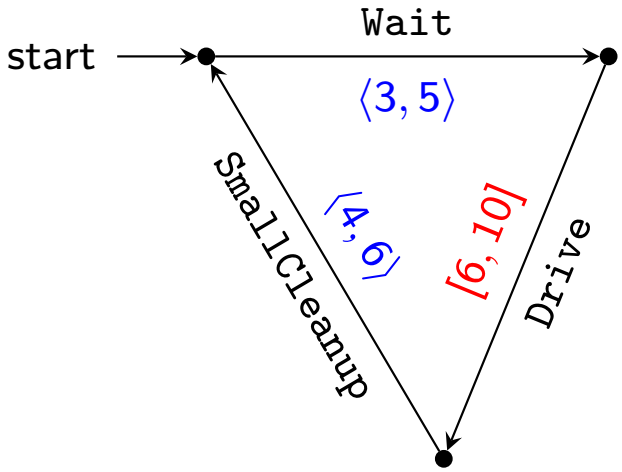
Modal Transition Systems with Durations

$$\Phi(t) = \texttt{BigCleanup} \vee \texttt{SkipCleanup} \vee \texttt{SmallCleanup}$$



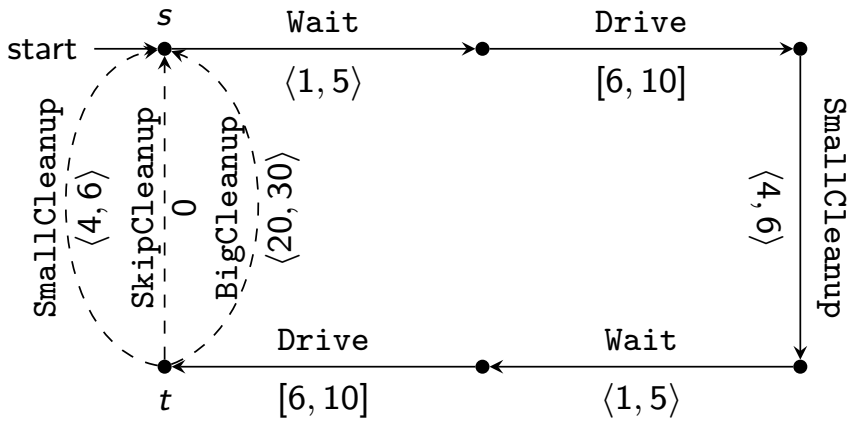


$\preceq_m$



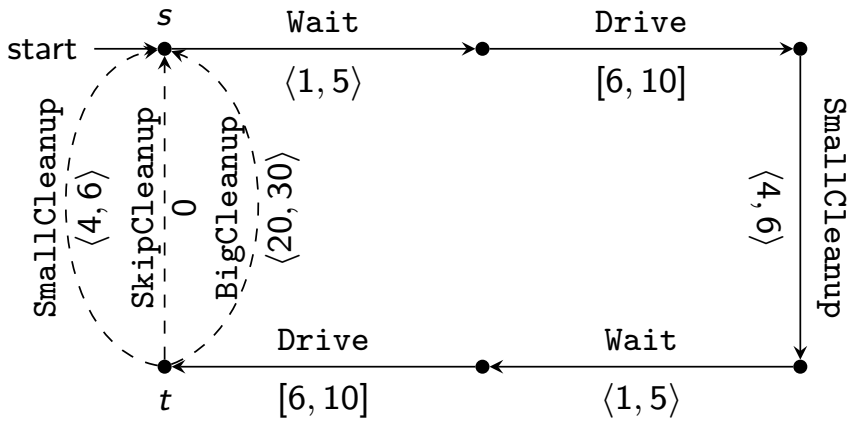
Dual-Price Scheme

$\Phi(t) =$ `BigCleanup` $\vee$
`SkipCleanup` $\vee$
`SmallCleanup`



Dual-Price Scheme

$\Phi(t) =$ BigCleanup $\vee$ SkipCleanup $\vee$ SmallCleanup

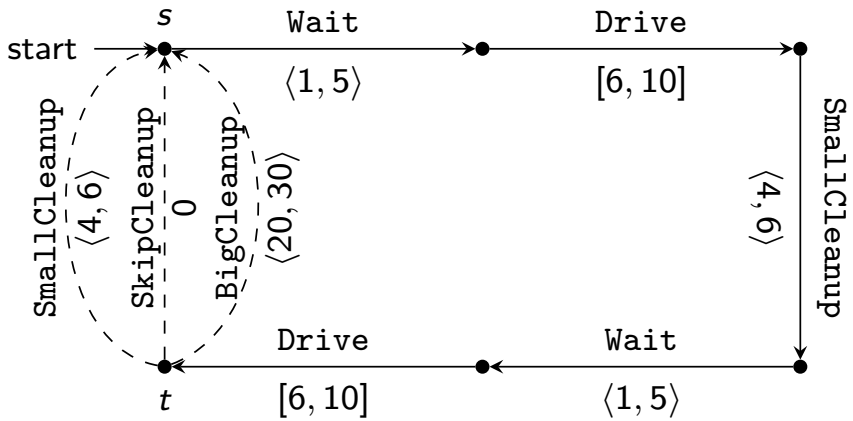


Hardware:
$H = \{\texttt{VacuumCleaner}, \texttt{Sponge}\}$

Requirements:
$\Psi(\texttt{BigCleanup}) = \texttt{VacuumCleaner}$
$\Psi(\texttt{SmallCleanup}) = \texttt{VacuumCleaner} \vee \texttt{Sponge}$

Dual-Price Scheme

$\Phi(t) =$ BigCleanup $\vee$ SkipCleanup $\vee$ SmallCleanup



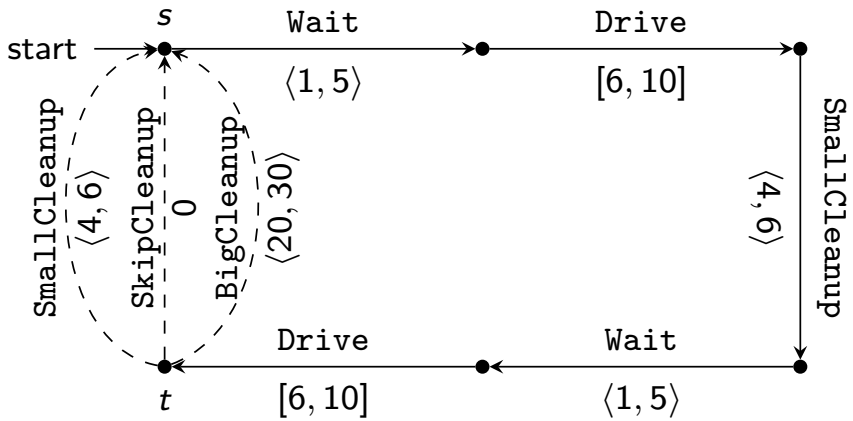
Hardware:
$H = \{\texttt{VacuumCleaner}, \texttt{Sponge}\}$

Requirements:
$\Psi(\texttt{BigCleanup}) = \texttt{VacuumCleaner}$
$\Psi(\texttt{SmallCleanup}) = \texttt{VacuumCleaner} \vee \texttt{Sponge}$

Investment:
$i(\texttt{VacuumCleaner}) = 100$
$i(\texttt{Sponge}) = 5$

Dual-Price Scheme

$\Phi(t) =$ BigCleanup $\vee$ SkipCleanup $\vee$ SmallCleanup



Hardware:
$H = \{\texttt{VacuumCleaner}, \texttt{Sponge}\}$

Requirements:
$\Psi(\texttt{BigCleanup}) = \texttt{VacuumCleaner}$
$\Psi(\texttt{SmallCleanup}) = \texttt{VacuumCleaner} \vee \texttt{Sponge}$

Investment:
$i(\texttt{VacuumCleaner}) = 100$
$i(\texttt{Sponge}) = 5$

Running Cost:

$a \in \Sigma$	$r(a)$
Wait	8
Drive	10
SmallCleanup	6
BigCleanup	7
SkipCleanup	0

Investment Cost

Definition (Investment Cost)

$$\mathrm{ic}(\mathcal{I}) = \min_{G \models \mathcal{I}} \sum_{g \in G} i(g)$$

Requirements:

$\Psi(\texttt{BigCleanup}) = \texttt{VacuumCleaner}$

$\Psi(\texttt{SmallCleanup}) = \texttt{VacuumCleaner} \vee \texttt{Sponge}$

Investment:

$i(\texttt{VacuumCleaner}) = 100$

$i(\texttt{Sponge}) = 5$

Investment Cost

Definition (Investment Cost)

$$\mathrm{ic}(\mathcal{I}) = \min_{G \models \mathcal{I}} \sum_{g \in G} i(g)$$

Requirements:

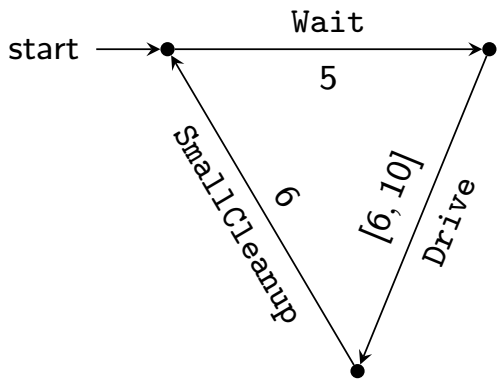
$\Psi(\texttt{BigCleanup}) = \texttt{VacuumCleaner}$

$\Psi(\texttt{SmallCleanup}) = \texttt{VacuumCleaner} \vee \texttt{Sponge}$

Investment:

$i(\texttt{VacuumCleaner}) = 100$

$i(\texttt{Sponge}) = 5$



$$\mathrm{ic}(\mathcal{I}_1) = 5$$

Investment Cost

Definition (Investment Cost)

$$\mathrm{ic}(\mathcal{I}) = \min_{G \models \mathcal{I}} \sum_{g \in G} i(g)$$

Requirements:

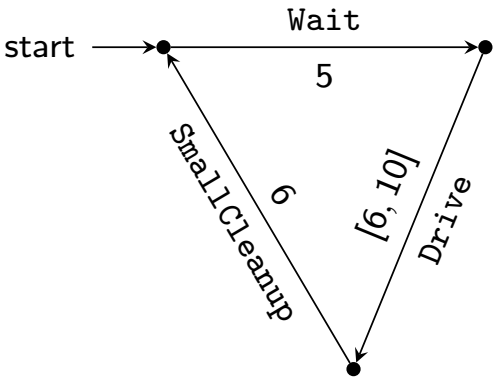
$\Psi(\texttt{BigCleanup}) = \texttt{VacuumCleaner}$

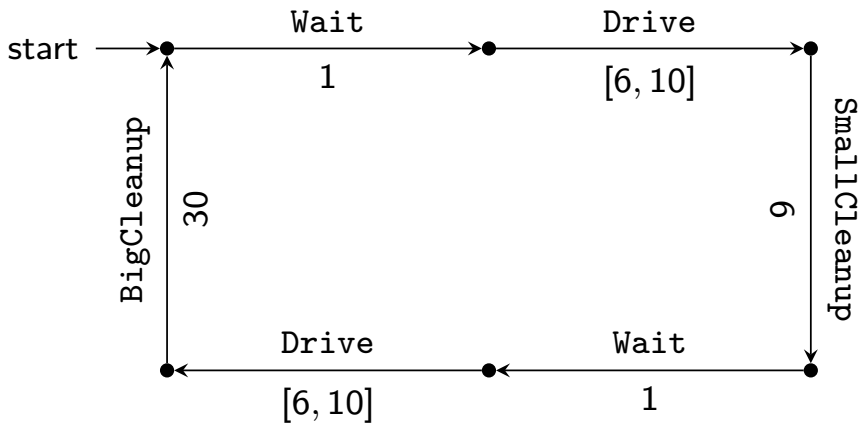
$\Psi(\texttt{SmallCleanup}) = \texttt{VacuumCleaner} \vee \texttt{Sponge}$

Investment:

$i(\texttt{VacuumCleaner}) = 100$

$i(\texttt{Sponge}) = 5$





$\mathrm{ic}(\mathcal{I}_1) = 5$

$\mathrm{ic}(\mathcal{I}_2) = 100$

Running Cost

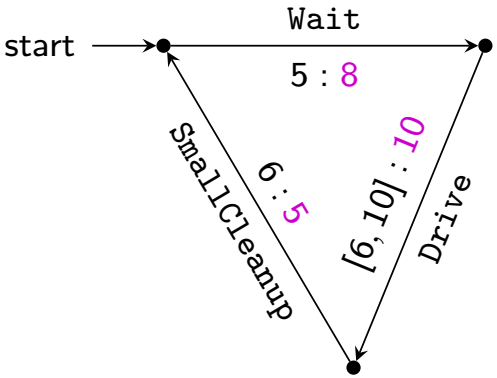
Definition (Running Cost)

$$\mathrm{rc}(\mathcal{I}) = \sup_{s_0 a_0 t_0 s_1 a_1 t_1 \cdots \in \mathcal{R}un(\mathcal{I})} \limsup_{n \to \infty} \frac{\sum_{i=0}^{n} r(a_i) \cdot t_i}{\sum_{i=0}^{n} t_i}$$

Running Cost

Definition (Running Cost)

$$\mathrm{rc}(\mathcal{I}) = \sup_{s_0 a_0 t_0 s_1 a_1 t_1 \cdots \in \mathcal{R}un(\mathcal{I})} \limsup_{n \to \infty} \frac{\sum_{i=0}^{n} r(a_i) \cdot t_i}{\sum_{i=0}^{n} t_i}$$



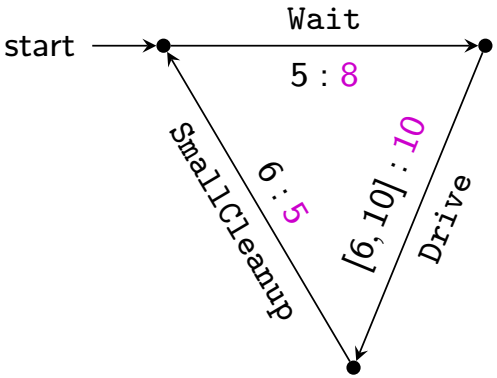
$$\frac{5 \cdot 8 + 10 \cdot 10 + 6 \cdot 5}{5 + 10 + 6}$$

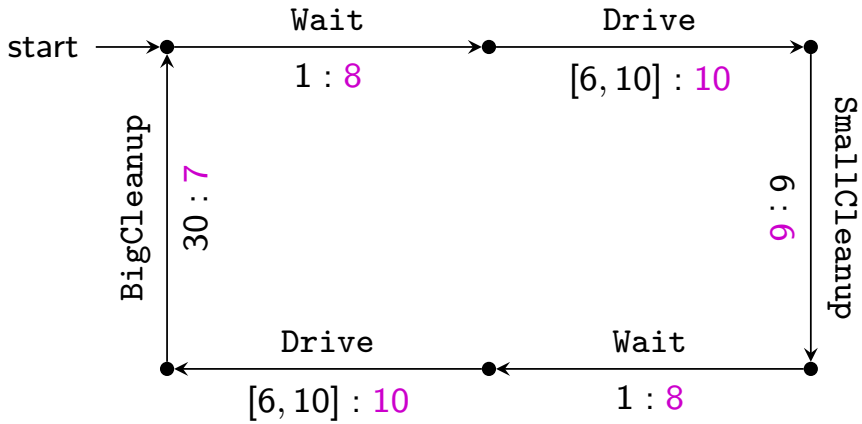
$$\approx 8.10$$

Running Cost

Definition (Running Cost)

$$\mathrm{rc}(\mathcal{I}) = \sup_{s_0 a_0 t_0 s_1 a_1 t_1 \cdots \in \mathcal{R}un(\mathcal{I})} \limsup_{n \to \infty} \frac{\sum_{i=0}^{n} r(a_i) \cdot t_i}{\sum_{i=0}^{n} t_i}$$





$$\frac{5 \cdot 8 + 10 \cdot 10 + 6 \cdot 5}{5 + 10 + 6}$$

$$\approx 8.10$$

$$\frac{1 \cdot 8 + 10 \cdot 10 + 6 \cdot 6 + 1 \cdot 8 + 10 \cdot 10 + 30 \cdot 7}{1 + 10 + 6 + 1 + 10 + 30}$$

$$\approx 7.97$$

Main Results

Problem (The Implementation Problem)

Given

- an MTSD specification $\mathcal{S}$,
- a dual-price scheme,
- an upper-bound max_{ic} for the investment cost and
- an upper bound max_{rc} on the running cost,

does there exist an implementation $\mathcal{I} \leq_m \mathcal{S}$ such that

- $\text{ic}(\mathcal{I}) \leq max_{\text{ic}}$ and
- $\text{rc}(\mathcal{I}) \leq max_{\text{rc}}$?

Main Results

Problem (The Implementation Problem)

Given

- an MTSD specification $\mathcal{S}$,
- a dual-price scheme,
- an upper-bound max_{ic} for the investment cost and
- an upper bound max_{rc} on the running cost,

does there exist an implementation $\mathcal{I} \leq_m \mathcal{S}$ such that

- $\text{ic}(\mathcal{I}) \leq max_{\text{ic}}$ and
- $\text{rc}(\mathcal{I}) \leq max_{\text{rc}}$?

Theorem

The implementation problem is NP-complete.

Main Results

Theorem

The implementation problem with

- positive obligation function Φ and
- a constant number of hardware components H

is polynomially equivalent to mean payoff games and thus it is in NP $\cap$ coNP and solvable in pseudo-polynomial time.

Conclusion

Modal transition systems are an elegant formalism for modelling of high-level specifications of reactive systems.

Our extension with parameters:

- specializes to refinements on the well-studied subclasses, and
- allows to model persistent choices.

Our dual-priced extension:

- shows how to deal with quantitative aspects,
- combines investment and running cost.

Future Work:

- Further generalization of the formalism to non-flat systems.
- Tool integration, case studies, application to product lines.