

# Refinement of Kripke Models for Dynamics

Francien Dechesne, Yanjing Wang and Simona Orzan

Prose, Oct. 29 2008



- 1 Introduction
- 2 Abstraction/Refinement and Logical Characterization
- 3 An Example
- 4 Conclusions

# Context

VEMPS-project (NWO Open Competitie):

*Verification and Epistemics of Multiparty Protocol Security*

Many security properties are intended to ensure that the right agents get to *know* the right thing, while the enemies should not get to *know* certain things.

Our project aims to find useful applications for logics of *knowledge* in verification of security protocols.

# Epistemic logic

Epistemic Logics: Propositional *modal logics* with modalities interpreted as *to Know* ( $K_a\phi$ ) on Kripke models where the relations are equivalence relations.

# Epistemic logic

Epistemic Logics: Propositional *modal logics* with modalities interpreted as *to Know* ( $K_a\phi$ ) on Kripke models where the relations are equivalence relations.

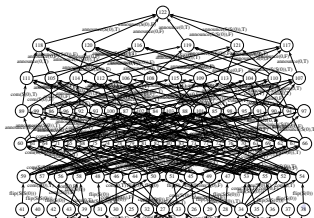
Dynamic Epistemic Logic adds *dynamic modalities*. E.g. Public Announcement logic:  $[\phi]K_a\psi$  expresses after the true announcement of  $\phi$ ,  $\psi$  is true [Plaza 89].

# Epistemic logic

Epistemic Logics: Propositional *modal logics* with modalities interpreted as *to Know* ( $K_a\phi$ ) on Kripke models where the relations are equivalence relations.

Dynamic Epistemic Logic adds *dynamic modalities*. E.g. Public Announcement logic:  $[\phi]K_a\psi$  expresses after the true announcement of  $\phi$ ,  $\psi$  is true [Plaza 89].

Epistemic verification: checking an epistemic formula on an epistemic Kripke model. These epistemic models can also be HUGE, especially when we model realistic situations.

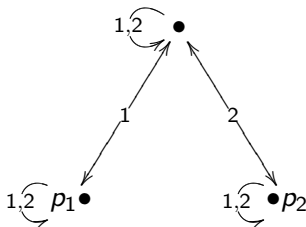


# Motivation

- Use Epistemic Logics for practical reasoning.

# Motivation

- Use Epistemic Logics for practical reasoning.
- (Dynamic) Epistemic Modelling of real life cases can produce huge Kripke models, but often the relations and basic propositions in multi-agent epistemic models are somehow 'similar'.



# Motivation

- Use Epistemic Logics for practical reasoning.
- (Dynamic) Epistemic Modelling of real life cases can produce huge Kripke models, but often the relations and basic propositions in multi-agent epistemic models are somehow 'similar'.



We try to use such similarities to reduce models.

# Motivation

- Use Epistemic Logics for practical reasoning.
- (Dynamic) Epistemic Modelling of real life cases can produce huge Kripke models, but often the relations and basic propositions in multi-agent epistemic models are somehow 'similar'.
- We apply abstraction techniques for LTSs [van de Pol & Valero Espada 04] to the Kripke models for a dynamic epistemic logic.

# Motivation

- Use Epistemic Logics for practical reasoning.
- (Dynamic) Epistemic Modelling of real life cases can produce huge Kripke models, but often the relations and basic propositions in multi-agent epistemic models are somehow 'similar'.
- We apply abstraction techniques for LTSs [van de Pol & Valero Espada 04] to the Kripke models for a dynamic epistemic logic.
- Preservation result for 3-valued public announcement logic

# Kripke Modal Labelled Transition System

A *Kripke Modal Labelled Transition System* (KMLTS) is a tuple  $\mathcal{M} = (I, P; S, \rightarrow_{\diamond}, \rightarrow_{\square}, V)$  where:

# Kripke Modal Labelled Transition System

A *Kripke Modal Labelled Transition System* (KMLTS) is a tuple

$\mathcal{M} = (I, P; S, \rightarrow_{\diamond}, \rightarrow_{\square}, V)$  where:

- $I$  is a non-empty set of labels;

# Kripke Modal Labelled Transition System

A *Kripke Modal Labelled Transition System* (KMLTS) is a tuple

$\mathcal{M} = (I, P; S, \rightarrow_{\diamond}, \rightarrow_{\square}, V)$  where:

- $I$  is a non-empty set of labels;
- $P$  is a set of basic propositions;

# Kripke Modal Labelled Transition System

A *Kripke Modal Labelled Transition System* (KMLTS) is a tuple  $\mathcal{M} = (I, P; S, \rightarrow_{\diamond}, \rightarrow_{\square}, V)$  where:

- $I$  is a non-empty set of labels;
- $P$  is a set of basic propositions;
- $S$  is a non-empty set of states;

# Kripke Modal Labelled Transition System

A *Kripke Modal Labelled Transition System* (KMLTS) is a tuple

$\mathcal{M} = (I, P; S, \rightarrow_{\diamond}, \rightarrow_{\square}, V)$  where:

- $I$  is a non-empty set of labels;
- $P$  is a set of basic propositions;
- $S$  is a non-empty set of states;
- $V$  is a valuation function:  $V : S \rightarrow \{true, false, ?\}^P$   
(3-valued!).

# Kripke Modal Labelled Transition System

A *Kripke Modal Labelled Transition System* (KMLTS) is a tuple

$\mathcal{M} = (I, P; S, \rightarrow_{\diamond}, \rightarrow_{\square}, V)$  where:

- $I$  is a non-empty set of labels;
- $P$  is a set of basic propositions;
- $S$  is a non-empty set of states;
- $V$  is a valuation function:  $V : S \rightarrow \{true, false, ?\}^P$   
(3-valued!).
- $\rightarrow_{\diamond}$  is a set of *may*-transitions  $s \xrightarrow{i}_{\diamond} s'$  where  $i \in I$ ;

# Kripke Modal Labelled Transition System

A *Kripke Modal Labelled Transition System* (KMLTS) is a tuple

$\mathcal{M} = (I, P; S, \rightarrow_{\diamond}, \rightarrow_{\square}, V)$  where:

- $I$  is a non-empty set of labels;
- $P$  is a set of basic propositions;
- $S$  is a non-empty set of states;
- $V$  is a valuation function:  $V : S \rightarrow \{true, false, ?\}^P$   
(3-valued!).
- $\rightarrow_{\diamond}$  is a set of *may*-transitions  $s \xrightarrow{i}_{\diamond} s'$  where  $i \in I$ ;
- $\rightarrow_{\square}$  is a set of *must*-transitions  $s \xrightarrow{i}_{\square} s'$  where  $i \in I$ ;

# Kripke Modal Labelled Transition System

A *Kripke Modal Labelled Transition System* (KMLTS) is a tuple  $\mathcal{M} = (I, P; S, \rightarrow_{\diamond}, \rightarrow_{\square}, V)$  where:

- $I$  is a non-empty set of labels;
- $P$  is a set of basic propositions;
- $S$  is a non-empty set of states;
- $V$  is a valuation function:  $V : S \rightarrow \{true, false, ?\}^P$  (3-valued!).
- $\rightarrow_{\diamond}$  is a set of *may*-transitions  $s \xrightarrow{i}_{\diamond} s'$  where  $i \in I$ ;
- $\rightarrow_{\square}$  is a set of *must*-transitions  $s \xrightarrow{i}_{\square} s'$  where  $i \in I$ ;

Requirement:  $\rightarrow_{\square} \subseteq \rightarrow_{\diamond}$ . ('*necessary*' implies '*possible*')

$(I, P)$ : *signature* of  $\mathcal{M}$ .

*pointed KMLTS*: a pair  $(\mathcal{M}, s)$  with  $s \in S$

# Kripke Modal Labelled Transition System

A *Kripke Modal Labelled Transition System* (KMLTS) is a tuple  $\mathcal{M} = (I, P; S, \rightarrow_{\diamond}, \rightarrow_{\square}, V)$  where:

- $I$  is a non-empty set of labels;
- $P$  is a set of basic propositions;
- $S$  is a non-empty set of states;
- $V$  is a valuation function:  $V : S \rightarrow \{true, false, ?\}^P$  (3-valued!).
- $\rightarrow_{\diamond}$  is a set of *may*-transitions  $s \xrightarrow{i}_{\diamond} s'$  where  $i \in I$ ;
- $\rightarrow_{\square}$  is a set of *must*-transitions  $s \xrightarrow{i}_{\square} s'$  where  $i \in I$ ;

Requirement:  $\rightarrow_{\square} \subseteq \rightarrow_{\diamond}$ . ('*necessary*' implies '*possible*')

$(I, P)$ : *signature* of  $\mathcal{M}$ .

*pointed KMLTS*: a pair  $(\mathcal{M}, s)$  with  $s \in S$

**concrete Kripke model: KMLTS with  $\rightarrow_{\square} = \rightarrow_{\diamond}$  and  $V(s)(p) \neq ?$ .**

# Public Announcement Logic (PAL)

Formally, given a signature  $(I, P)$ , the formulas of the *Public Announcement Logic*  $\mathcal{L}_{I,P}$  are defined by

$$\phi, \psi ::= p \mid \phi \wedge \psi \mid \neg\phi \mid K_i\phi \mid [\phi]\psi$$

where  $p \in P, i \in I$ .

# Public Announcement Logic (PAL)

Formally, given a signature  $(I, P)$ , the formulas of the *Public Announcement Logic*  $\mathcal{L}_{I,P}$  are defined by

$$\phi, \psi ::= p \mid \phi \wedge \psi \mid \neg\phi \mid K_i\phi \mid [\phi]\psi$$

where  $p \in P, i \in I$ .

Intuition of  $[\phi]\psi$ : after announcing that  $\phi$  is true,  $\psi$  is true.  
 $[\phi]$  is a dynamic operator.

We define 3-valued semantics for PAL on KMLTSs.

## 3-valued Semantics (propositional part)

$\llbracket \phi \rrbracket^{\mathcal{M},s}$ : truth value of  $\mathcal{L}_{I,P}$  formula  $\phi$  in state  $s$  of a KMLTS  
 $\mathcal{M} = (I, P; S \rightarrow_{\diamond}, \rightarrow_{\square}, V)$

Defined inductively:

$$\begin{aligned} \llbracket p \rrbracket^{\mathcal{M},s} &= V(s)(p) \\ \llbracket \neg \phi \rrbracket^{\mathcal{M},s} &= \neg_3 \llbracket \phi \rrbracket^{\mathcal{M},s} \\ \llbracket \phi \wedge \psi \rrbracket^{\mathcal{M},s} &= \llbracket \phi \rrbracket^{\mathcal{M},s} \wedge_3 \llbracket \psi \rrbracket^{\mathcal{M},s} \end{aligned}$$

where:

$\neg_3(\text{true}) = \text{false}$ ,  $\neg_3(\text{false}) = \text{true}$  and  $\neg_3(?) = ?$   
 $x \wedge_3 y = \min(x, y)$  w.r.t.  $\leq_v$ :  $\text{false} \leq_v ? \leq_v \text{true}$ .

# 3-valued Semantics (epistemic, dynamic part)

$$\llbracket K_i \phi \rrbracket^{\mathcal{M}, s} = \begin{cases} \textit{true} & \text{if } \forall s' : s \xrightarrow{i}_{\diamond} s' \implies \llbracket \phi \rrbracket^{\mathcal{M}, s'} = \textit{true} \\ \textit{false} & \text{if } \exists s' : s \xrightarrow{i}_{\square} s' \text{ and } \llbracket \phi \rrbracket^{\mathcal{M}, s'} = \textit{false} \\ ? & \text{otherwise} \end{cases}$$

## 3-valued Semantics (epistemic, dynamic part)

$$\begin{aligned} \llbracket K_i \phi \rrbracket^{\mathcal{M}, s} &= \begin{cases} \textit{true} & \text{if } \forall s' : s \xrightarrow{i}_{\diamond} s' \implies \llbracket \phi \rrbracket^{\mathcal{M}, s'} = \textit{true} \\ \textit{false} & \text{if } \exists s' : s \xrightarrow{i}_{\square} s' \text{ and } \llbracket \phi \rrbracket^{\mathcal{M}, s'} = \textit{false} \\ ? & \text{otherwise} \end{cases} \\ \llbracket [\phi] \psi \rrbracket^{\mathcal{M}, s} &= \begin{cases} \textit{true} & \text{if } \llbracket \phi \rrbracket^{\mathcal{M}, s} = \textit{false} \text{ or } \llbracket \psi \rrbracket^{\mathcal{M}|_{\phi}, s} = \textit{true} \\ \textit{false} & \text{if } \llbracket \phi \rrbracket^{\mathcal{M}, s} = \textit{true} \text{ and } \llbracket \psi \rrbracket^{\mathcal{M}|_{\phi}, s} = \textit{false} \\ ? & \text{otherwise} \end{cases} \end{aligned}$$

where  $\mathcal{M}|_{\phi} = (I, P; S' \xrightarrow{i}_{\diamond}, \xrightarrow{i}_{\square}, V')$  is the relativization of  $\mathcal{M}$  to  $\phi$ : the model restricted to all worlds where  $\phi$  could be true.

## 3-valued Semantics (epistemic, dynamic part)

$$\begin{aligned} \llbracket K_i \phi \rrbracket^{\mathcal{M}, s} &= \begin{cases} \text{true} & \text{if } \forall s' : s \xrightarrow{i}_{\diamond} s' \implies \llbracket \phi \rrbracket^{\mathcal{M}, s'} = \text{true} \\ \text{false} & \text{if } \exists s' : s \xrightarrow{i}_{\square} s' \text{ and } \llbracket \phi \rrbracket^{\mathcal{M}, s'} = \text{false} \\ ? & \text{otherwise} \end{cases} \\ \llbracket [\phi] \psi \rrbracket^{\mathcal{M}, s} &= \begin{cases} \text{true} & \text{if } \llbracket \phi \rrbracket^{\mathcal{M}, s} = \text{false} \text{ or } \llbracket \psi \rrbracket^{\mathcal{M}|_{\phi}, s} = \text{true} \\ \text{false} & \text{if } \llbracket \phi \rrbracket^{\mathcal{M}, s} = \text{true} \text{ and } \llbracket \psi \rrbracket^{\mathcal{M}|_{\phi}, s} = \text{false} \\ ? & \text{otherwise} \end{cases} \end{aligned}$$

where  $\mathcal{M}|_{\phi} = (I, P; S' \xrightarrow{i}_{\diamond}, \xrightarrow{i}_{\square}, V')$  is defined as follows:

- $S' = \{s \in S \mid \llbracket \phi \rrbracket^{\mathcal{M}, s} \neq \text{false}\}$ ;
- $\xrightarrow{i}_{\diamond} = \xrightarrow{i}_{\diamond} \upharpoonright_{S' \times S'}$ ;
- $\xrightarrow{i}_{\square} = \xrightarrow{i}_{\square} \cap (S' \times \{s \in S' \mid \llbracket \phi \rrbracket^{\mathcal{M}, s} = \text{true}\})$ ;
- $V'(s) = V(s)$  for  $s \in S'$ .

# Coincide with 2-value PAL

For 2-valued Public Announcement Logic the following reduction axioms hold:

$$\begin{array}{lll}
 (\text{At}) & [\phi]p & \leftrightarrow \phi \rightarrow p \\
 (\text{PF}) & [\phi]\neg\psi & \leftrightarrow \phi \rightarrow \neg[\phi]\psi \\
 (\text{Dist}) & [\phi](\psi_1 \wedge \psi_2) & \leftrightarrow [\phi]\psi_1 \wedge [\phi]\psi_2 \\
 (\text{Seq}) & [\phi][\psi]\chi & \leftrightarrow [\phi \wedge [\phi]\psi]\chi \\
 (\text{KA}) & [\phi]K_i\psi & \leftrightarrow \phi \rightarrow K_i[\phi]\psi
 \end{array}$$

We chose our semantics of the modalities such that we got optimal preservation of these axioms for the 3-valued case. They all hold whenever  $\phi$  has definite truth value, so they are preserved on concrete models.

# Coincide with 2-value PAL

For 2-valued Public Announcement Logic the following reduction axioms hold:

$$\begin{array}{lll}
 (\text{At}) & [\phi]p & \leftrightarrow \phi \rightarrow p \\
 (\text{PF}) & [\phi]\neg\psi & \leftrightarrow \phi \rightarrow \neg[\phi]\psi \\
 (\text{Dist}) & [\phi](\psi_1 \wedge \psi_2) & \leftrightarrow [\phi]\psi_1 \wedge [\phi]\psi_2 \\
 (\text{Seq}) & [\phi][\psi]\chi & \leftrightarrow [\phi \wedge [\phi]\psi]\chi \\
 (\text{KA}) & [\phi]K_i\psi & \leftrightarrow \phi \rightarrow K_i[\phi]\psi
 \end{array}$$

We chose our semantics of the modalities such that we got optimal preservation of these axioms for the 3-valued case. They all hold whenever  $\phi$  has definite truth value, so they are preserved on concrete models.

(In three cases, if  $\phi$  is undefined, left gives *false* but right ?.)

# Refinement and Abstraction

Given two KMLTSs  $\mathcal{M} = (I, P; S, \rightarrow_{\diamond}, \rightarrow_{\square}, V)$  and  $\mathcal{N} = (I', P'; T, \rightarrow'_{\diamond}, \rightarrow'_{\square}, V')$

# Refinement and Abstraction

Given two KMLTSs  $\mathcal{M} = (I, P; S, \rightarrow_{\diamond}, \rightarrow_{\square}, V)$  and  $\mathcal{N} = (I', P'; T, \rightarrow'_{\diamond}, \rightarrow'_{\square}, V')$  and two surjective functions  $f : I' \rightarrow I$  and  $g : P' \rightarrow P$ ,

# Refinement and Abstraction

Given two KMLTSs  $\mathcal{M} = (I, P; S, \rightarrow_{\diamond}, \rightarrow_{\square}, V)$  and  $\mathcal{N} = (I', P'; T, \rightarrow'_{\diamond}, \rightarrow'_{\square}, V')$  and two surjective functions  $f : I' \rightarrow I$  and  $g : P' \rightarrow P$ , a binary relation  $R \subseteq T \times S$  is called an  $f, g$ -refinement relation between  $\mathcal{N}$  and  $\mathcal{M}$ , if for all  $t \in T, s \in S$  with  $(t, s) \in R$  the following hold:

# Refinement and Abstraction

Given two KMLTSs  $\mathcal{M} = (I, P; S, \rightarrow_{\diamond}, \rightarrow_{\square}, V)$  and  $\mathcal{N} = (I', P'; T, \rightarrow'_{\diamond}, \rightarrow'_{\square}, V')$  and two surjective functions  $f : I' \rightarrow I$  and  $g : P' \rightarrow P$ , a binary relation  $R \subseteq T \times S$  is called an  $f, g$ -refinement relation between  $\mathcal{N}$  and  $\mathcal{M}$ , if for all  $t \in T, s \in S$  with  $(t, s) \in R$  the following hold:

- for any  $p \in P : V(s)(p) \neq ?$  implies for all  $p' \in g^{-1}[p] : V'(t)(p') = V(s)(p)$ ;

# Refinement and Abstraction

Given two KMLTSs  $\mathcal{M} = (I, P; S, \rightarrow_{\diamond}, \rightarrow_{\square}, V)$  and  $\mathcal{N} = (I', P'; T, \rightarrow'_{\diamond}, \rightarrow'_{\square}, V')$  and two surjective functions  $f : I' \rightarrow I$  and  $g : P' \rightarrow P$ , a binary relation  $R \subseteq T \times S$  is called an  $f, g$ -refinement relation between  $\mathcal{N}$  and  $\mathcal{M}$ , if for all  $t \in T, s \in S$  with  $(t, s) \in R$  the following hold:

- for any  $p \in P : V(s)(p) \neq ?$  implies for all  $p' \in g^{-1}[p] : V'(t)(p') = V(s)(p)$ ;
- $t \xrightarrow{i'}_{\diamond} t'$  implies  $\exists s' \in S : s \xrightarrow{f(i')}_{\diamond} s'$  and  $R(t', s')$ ;

# Refinement and Abstraction

Given two KMLTSs  $\mathcal{M} = (I, P; S, \rightarrow_{\diamond}, \rightarrow_{\square}, V)$  and  $\mathcal{N} = (I', P'; T, \rightarrow'_{\diamond}, \rightarrow'_{\square}, V')$  and two surjective functions  $f : I' \rightarrow I$  and  $g : P' \rightarrow P$ , a binary relation  $R \subseteq T \times S$  is called an  $f, g$ -refinement relation between  $\mathcal{N}$  and  $\mathcal{M}$ , if for all  $t \in T, s \in S$  with  $(t, s) \in R$  the following hold:

- for any  $p \in P : V(s)(p) \neq ?$  implies for all  $p' \in g^{-1}[p] : V'(t)(p') = V(s)(p)$ ;
- $t \xrightarrow{\diamond} t'$  implies  $\exists s' \in S : s \xrightarrow{\diamond} s'$  and  $R(t', s')$ ;
- $s \xrightarrow{\square} s'$  implies  $\forall i' \in f^{-1}[i] : \exists t' \in T$  such that  $t \xrightarrow{\square} t'$  and  $R(t', s')$ .

# Refinement and Abstraction

Given two KMLTSs  $\mathcal{M} = (I, P; S, \rightarrow_{\diamond}, \rightarrow_{\square}, V)$  and  $\mathcal{N} = (I', P'; T, \rightarrow'_{\diamond}, \rightarrow'_{\square}, V')$  and two surjective functions  $f : I' \rightarrow I$  and  $g : P' \rightarrow P$ , a binary relation  $R \subseteq T \times S$  is called an  $f, g$ -refinement relation between  $\mathcal{N}$  and  $\mathcal{M}$ , if for all  $t \in T, s \in S$  with  $(t, s) \in R$  the following hold:

- for any  $p \in P : V(s)(p) \neq ?$  implies for all  $p' \in g^{-1}[p] : V'(t)(p') = V(s)(p)$ ;
- $t \xrightarrow{\diamond} t'$  implies  $\exists s' \in S : s \xrightarrow{\diamond} s'$  and  $R(t', s')$ ;
- $s \xrightarrow{\square} s'$  implies  $\forall i' \in f^{-1}[i] : \exists t' \in T$  such that  $t \xrightarrow{\square} t'$  and  $R(t', s')$ .

We say  $(\mathcal{N}, t)$  is an  $f, g$ -refinement of  $(\mathcal{M}, s)$  (notation:  $(\mathcal{N}, t) \in_{f,g} (\mathcal{M}, s)$ ) if there exists an  $f, g$ -refinement relation  $R$  between  $\mathcal{N}$  and  $\mathcal{M}$  such that  $(t, s) \in R$ .

## Intuition

$$\mathcal{N}, t : I', P' \quad \in_{f,g} \quad \mathcal{M}, s : I, P$$

## Intuition

 $\mathcal{N}, t : I', P'$ 

1, 2

 $\in_{f,g}$  $\mapsto_f$  $\mathcal{M}, s : I, P$ 

c

## Intuition

$\mathcal{N}, t : I', P'$	$\in_{f,g}$	$\mathcal{M}, s : I, P$
1, 2	$\mapsto_f$	$c$
$p_1, p_2$	$\mapsto_g$	$p_c$

## Intuition

 $\mathcal{N}, t : I', P'$ 

1, 2

 $p_1, p_2$ 

•

 $\in_{f,g}$  $\mapsto_f$  $\mapsto_g$  $\mathcal{M}, s : I, P$ 

c

 $p_c$ 

•

## Intuition

 $\mathcal{N}, t : I', P'$ 
 $1, 2$ 
 $p_1, p_2$ 

- 

 $\in_{f,g}$ 
 $\mapsto_f$ 
 $\mapsto_g$ 
 $\mathcal{M}, s : I, P$ 
 $c$ 
 $p_c$ 

- $p_c : true$

## Intuition

 $\mathcal{N}, t : I', P'$ 

1, 2

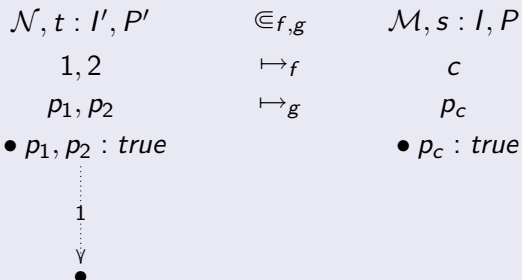
 $p_1, p_2$ 

- $p_1, p_2 : true$

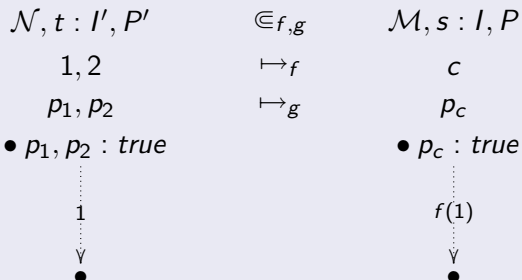
 $\in_{f,g}$  $\mapsto_f$  $\mapsto_g$  $\mathcal{M}, s : I, P$  $c$  $p_c$ 

- $p_c : true$

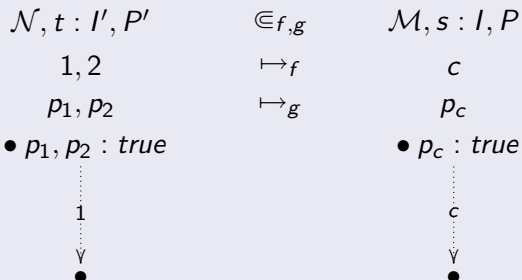
## Intuition



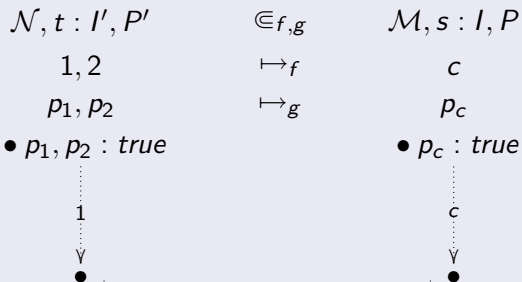
## Intuition



## Intuition



## Intuition



## Intuition

 $\mathcal{N}, t : I', P'$ 
 $1, 2$ 
 $p_1, p_2$ 

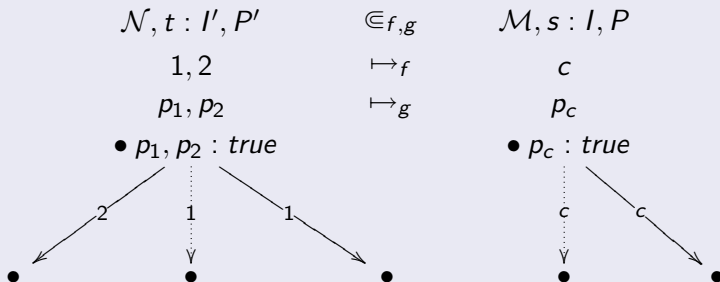
- $p_1, p_2 : true$

 $1$ 
 $\downarrow$ 
 $\in_{f,g}$ 
 $\mapsto_f$ 
 $\mapsto_g$ 
 $\mathcal{M}, s : I, P$ 
 $c$ 
 $p_c$ 

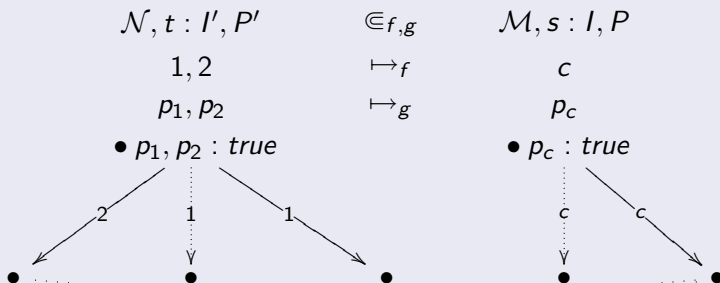
- $p_c : true$

 $c$ 
 $\downarrow$ 
 $c$

## Intuition



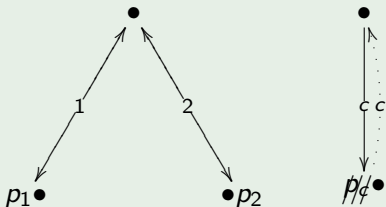
## Intuition



# Refinement and Abstraction

## Example

Example of a KMLTS  $\mathcal{M}$  and a  $f, g$ -abstraction of it where  $f(1) = f(2) = c$ ;  $g(p_1) = g(p_2) = p_c$ .



Dot lines are for *may* relations and solid lines for *must*. *May* relations that coincide with corresponding *must* ones are omitted.

# Desired Property

## Notation

Given two pointed models  $(\mathcal{M}, s)$ ,  $(\mathcal{N}, t)$ , and two formulas  $\phi, \psi$ , we say  $\llbracket \psi \rrbracket^{\mathcal{M}, s} \leq \llbracket \phi \rrbracket^{\mathcal{N}, t}$  if the following hold:

- 1  $\llbracket \psi \rrbracket^{\mathcal{M}, s} = \text{true} \implies \llbracket \phi \rrbracket^{\mathcal{N}, t} = \text{true};$
- 2  $\llbracket \psi \rrbracket^{\mathcal{M}, s} = \text{false} \implies \llbracket \phi \rrbracket^{\mathcal{N}, t} = \text{false}.$

# Desired Property

## Notation

Given two pointed models  $(\mathcal{M}, s)$ ,  $(\mathcal{N}, t)$ , and two formulas  $\phi, \psi$ , we say  $\llbracket \psi \rrbracket^{\mathcal{M}, s} \leq \llbracket \phi \rrbracket^{\mathcal{N}, t}$  if the following hold:

- 1  $\llbracket \psi \rrbracket^{\mathcal{M}, s} = \text{true} \implies \llbracket \phi \rrbracket^{\mathcal{N}, t} = \text{true};$
- 2  $\llbracket \psi \rrbracket^{\mathcal{M}, s} = \text{false} \implies \llbracket \phi \rrbracket^{\mathcal{N}, t} = \text{false}.$

## Safe reasoning

$(\mathcal{N}, t) \in_{f,g} (\mathcal{M}, s)$  implies for all  $\phi \in \mathcal{L}_{I', P'}$  :

$$\llbracket \lceil \phi \rceil_{f,g} \rrbracket^{\mathcal{M}, s} \leq \llbracket \phi \rrbracket^{\mathcal{N}, t}.$$

# Translation of the formulas

## Definition (Translation of formulas)

Given signatures  $(I', P')$ ,  $(I, P)$ , and surjective functions  $f : I' \rightarrow I$ ,  $g : P' \rightarrow P$ , we define the translation of an  $\mathcal{L}_{I', P'}$ -formula  $\phi$  into an  $\mathcal{L}_{I, P}$ -formula  $\lceil \phi \rceil_{f, g}$  inductively as follows:

$$\begin{aligned}
 \lceil p' \rceil_{f, g} &= g(p') \\
 \lceil \neg \psi \rceil_{f, g} &= \neg \lceil \psi \rceil_{f, g} \\
 \lceil \psi_1 \wedge \psi_2 \rceil_{f, g} &= \lceil \psi_1 \rceil_{f, g} \wedge \lceil \psi_2 \rceil_{f, g} \\
 \lceil K_{i'} \psi \rceil_{f, g} &= K_{f(i')} \lceil \psi \rceil_{f, g} \\
 \lceil [\chi] \psi \rceil_{f, g} &= \lceil \lceil \chi \rceil_{f, g} \rceil_{f, g} \lceil \psi \rceil_{f, g}
 \end{aligned}$$

# Translation of the formulas

## Definition (Translation of formulas)

Given signatures  $(I', P')$ ,  $(I, P)$ , and surjective functions  $f : I' \rightarrow I, g : P' \rightarrow P$ , we define the translation of an  $\mathcal{L}_{I', P'}$ -formula  $\phi$  into an  $\mathcal{L}_{I, P}$ -formula  $\lceil \phi \rceil_{f, g}$  inductively as follows:

$$\begin{aligned} \lceil p' \rceil_{f, g} &= g(p') \\ \lceil \neg \psi \rceil_{f, g} &= \neg \lceil \psi \rceil_{f, g} \\ \lceil \psi_1 \wedge \psi_2 \rceil_{f, g} &= \lceil \psi_1 \rceil_{f, g} \wedge \lceil \psi_2 \rceil_{f, g} \\ \lceil K_{i'} \psi \rceil_{f, g} &= K_{f(i')} \lceil \psi \rceil_{f, g} \\ \lceil [\chi] \psi \rceil_{f, g} &= \lceil \lceil \chi \rceil_{f, g} \rceil_{f, g} \lceil \psi \rceil_{f, g} \end{aligned}$$

## Example

$\lceil [p \wedge q \wedge r] K_1 p \vee K_2 q \rceil_{f, g} = [P \wedge R] K_A P$  with  $f(1) = f(2) = A$ ;  $g(p) = g(q) = P$  and  $g(r) = R$ .

# Logical Characterization

## Lemma (interaction between refinement and relativization)

For pointed KMLTSs  $(\mathcal{N}, t)$ ,  $(\mathcal{M}, s)$  and  $\mathcal{L}_{I', P'}$  formula  $\chi$ :  
 $(\mathcal{N}|_{\chi}, t) \in_{f,g} (\mathcal{M}|_{\neg\chi}, s)$  if the following conditions hold:

# Logical Characterization

## Lemma (interaction between refinement and relativization)

For pointed KMLTSs  $(\mathcal{N}, t)$ ,  $(\mathcal{M}, s)$  and  $\mathcal{L}_{I', P'}$  formula  $\chi$ :  
 $(\mathcal{N}|_{\chi}, t) \in_{f,g} (\mathcal{M}|_{\ulcorner \chi \urcorner_{f,g}}, s)$  if the following conditions hold:

- $(\mathcal{N}, t) \in_{f,g} (\mathcal{M}, s)$
- for each  $t' \in T, s' \in S$ :

$$(\mathcal{N}, t') \in_{f,g} (\mathcal{M}, s') \implies \llbracket \ulcorner \chi \urcorner_{f,g} \rrbracket^{\mathcal{M}, s'} \leq \llbracket \chi \rrbracket^{\mathcal{N}, t'}$$

# Logical Characterization

## Theorem

$(\mathcal{N}, t) \in_{f,g} (\mathcal{M}, s)$  implies for all  $\phi \in \mathcal{L}_{I',P'}$  :

$$\llbracket \Gamma \phi \Gamma_{f,g} \rrbracket^{\mathcal{M},s} \leq \llbracket \phi \rrbracket^{\mathcal{N},t}.$$

# Logical Characterization

## Theorem

$(\mathcal{N}, t) \in_{f,g} (\mathcal{M}, s)$  implies for all  $\phi \in \mathcal{L}_{I',P'}$  :

$$\llbracket \neg \phi \neg_{f,g} \rrbracket^{\mathcal{M},s} \leq \llbracket \phi \rrbracket^{\mathcal{N},t}.$$

## Theorem

If for every formula  $\phi \in \mathcal{L}_{I',P'}$ :  $\llbracket \neg \phi \neg_{f,g} \rrbracket^{\mathcal{M},s} \leq \llbracket \phi \rrbracket^{\mathcal{N},t}$  then  $(\mathcal{N}, t) \in_{f,g} (\mathcal{M}, s)$  (Image finiteness assumed).

## Muddy Children - the setting

- Out of  $n$  children,  $k \geq 1$  got mud on their foreheads while playing.

# Muddy Children - the setting

- Out of  $n$  children,  $k \geq 1$  got mud on their foreheads while playing.
- They can see whether other kids are dirty, but there is no mirror for them to discover whether they are dirty themselves.

# Muddy Children - the setting

- Out of  $n$  children,  $k \geq 1$  got mud on their foreheads while playing.
- They can see whether other kids are dirty, but there is no mirror for them to discover whether they are dirty themselves.
- Then father walks in and states: “At least one of you is dirty!” Then he requests “If you know you are dirty, step forward now.”

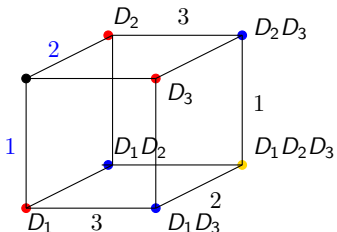
# Muddy Children - the setting

- Out of  $n$  children,  $k \geq 1$  got mud on their foreheads while playing.
- They can see whether other kids are dirty, but there is no mirror for them to discover whether they are dirty themselves.
- Then father walks in and states: “At least one of you is dirty!” Then he requests “If you know you are dirty, step forward now.”
- If nobody steps forward, he repeats his request: “If you now know you are dirty, step forward now.”

# Muddy Children - the setting

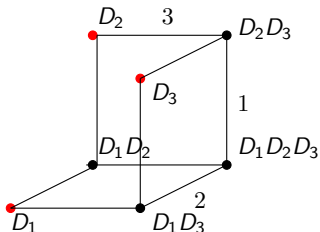
- Out of  $n$  children,  $k \geq 1$  got mud on their foreheads while playing.
- They can see whether other kids are dirty, but there is no mirror for them to discover whether they are dirty themselves.
- Then father walks in and states: “At least one of you is dirty!” Then he requests “If you know you are dirty, step forward now.”
- If nobody steps forward, he repeats his request: “If you now know you are dirty, step forward now.”
- After exactly  $k$  requests to step forward, the  $k$  dirty children suddenly do so (assuming they are honest and perfect reasoners).

# Muddy Children - the concrete model of $n = 3$ case



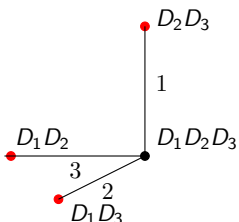
3 children may get mud on their foreheads while playing. Then father walks in and states: "At least one of you is dirty!" (Announcement:  $D_1 \vee D_2 \vee D_3$ ).

# Muddy Children - the concrete model of $n = 3$ case



If only one child is dirty then he should know now ( $K_x D_x$ ). If more than one child is dirty then no one steps forward at father's request.  
 (Announcement:  $\neg K_1 D_1 \wedge \neg K_2 D_2 \wedge \neg K_3 D_3$ )

# Muddy Children - the concrete model of $n = 3$ case



If only two children are dirty then they should know by now. If all the three children are dirty then no one steps forward at father's request.

(Announcement:  $\neg K_1 D_1 \wedge \neg K_2 D_2 \wedge \neg K_3 D_3$ ).

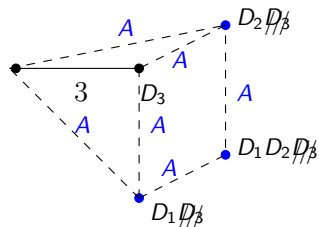
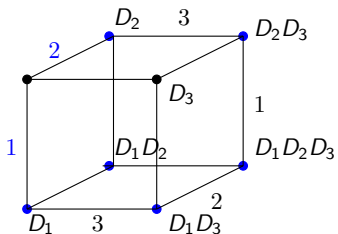
# Muddy Children - the concrete model of $n = 3$ case

$D_1 D_2 D_3$



Now everyone knows it:  $K_1 D_1 \wedge K_2 D_2 \wedge K_3 D_3$

# Muddy Children - Abstraction of $n=3$ case

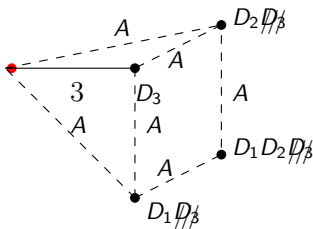


Abstractions of the Muddy Children for  $n = 3$  children.

$f(1) = f(2) = A$ ,  $f(3) = 3$  and  $g = Id$ .

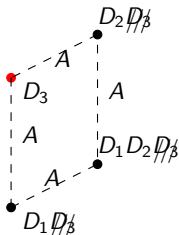
$D_3$  means proposition  $D_3$  has valuation ? in the current state.

# Muddy Children - Abstraction of $n=3$ case



First announcement:  $\lceil D_1 \vee D_2 \vee D_3 \rceil_{f,g} = D_1 \vee D_2 \vee D_3$ .

# Muddy Children - Abstraction of $n=3$ case

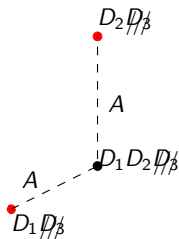


$\lceil K_3 D_3 \rceil_{f,g} = K_3 D_3$  holds at world  $D_3$ .

Announcement can be made if more than one child is dirty:

$\lceil \neg K_1 D_1 \wedge \neg K_2 D_2 \wedge \neg K_3 D_3 \rceil_{f,g} = \neg K_A D_1 \wedge \neg K_A D_2 \wedge \neg K_3 D_3$ .

# Muddy Children - Abstraction of $n=3$ case



$\vDash K_1 D_1 \neg_{f,g} = K_A D_1$  holds at world  $D_1 D_1/\beta$  and  $\vDash K_1 D_2 \neg_{f,g} = K_A D_2$  holds at  $D_2 D_1/\beta$ . If all the three children are dirty then announce:

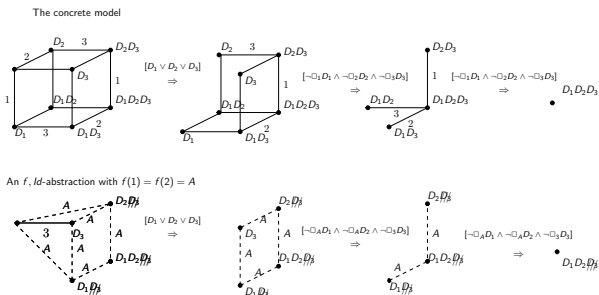
$\vDash \neg K_1 D_1 \wedge \neg K_2 D_2 \wedge \neg K_3 D_3 \neg_{f,g} = \neg K_A D_1 \wedge \neg K_A D_2 \wedge \neg K_3 D_3$ .

# Muddy Children - Abstraction of $n=3$ case

•  
 $D_1 D_2 \cancel{D_3}$

$\lceil K_1 D_1 \wedge K_2 D_2 \rceil_{f,g} = K_A D_1 \wedge K_A D_2$  holds at the only world.

# Muddy Children - Summary



Let  $D = D_1 \vee D_2 \vee D_3$  and  $E = \neg K_1 D_1 \wedge \neg K_2 D_2 \wedge \neg K_3 D_3$ .

- $\lceil [D][E][E](K_1 D_1 \wedge K_2 D_2) \rceil_{f,g}$  is true at  $D_1 D_2 D_3$ .
- $\lceil [D][E]K_1 D_1 \rceil_{f,g}$  is true at  $D_1 \not D_2 \not D_3$ .
- $\lceil [D]K_3 D_3 \rceil_{f,g}$  is true at  $D_3$ .

# Contributions

- Refinement/abstraction theory on Kripke models with proposition- and relation-lumping.
- A 3-valued version of Public Announcement Logic.
- Refinement relation on *static* models assures us to safely reason about any *dynamic* properties.

# Future works

- Extend the theory to more general DEL (with action models): abstraction of action models should be synchronized with abstraction of static models. (done)
- Extend  $f, g$ : the mappings from propositions/labels to boolean formulas and regular expressions. (almost done)
- Automatic abstraction?

Thank you very much for your attention!

# Muddy Children - the model of $n = 3$ case

