



## UvA-DARE (Digital Academic Repository)

### Epistemic modelling and protocol dynamics

Wang, Y.

**Publication date**  
2010

[Link to publication](#)

#### **Citation for published version (APA):**

Wang, Y. (2010). *Epistemic modelling and protocol dynamics*. [Thesis, fully internal, Universiteit van Amsterdam]. Institute for Logic, Language and Computation.

#### **General rights**

It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

#### **Disclaimer/Complaints regulations**

If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: <https://uba.uva.nl/en/contact>, or a letter to: Library of the University of Amsterdam, Secretariat, P.O. Box 19185, 1000 GD Amsterdam, The Netherlands. You will be contacted as soon as possible.

### 7.1 Introduction

In this chapter, we import the 3-valued abstraction-refinement techniques developed for temporal logics to DEL model checking (see, e.g., [BG99, GHJ01]), with new features particularly relevant for a multi-agent epistemic setting. The abstraction-refinement method intuitively relates a detailed model (refined model) with a coarser one (abstract model) in which some information may be lost, but the information kept is faithful to the detailed model. In the Kripke models of the epistemic setting, there are often transitions with different labels that might be similar to each other, for instance, if they express uncertainties of agents playing similar roles in a multi-agent system. Another specific characteristic of epistemic Kripke models is that in modelling practical situations numerous different basic propositions might be used as we have seen in the Russian Cards or Muddy Children examples in the previous chapters. We may expect to lump together some of those transitions with different labels or combine states with different propositional valuations to obtain a more compact abstraction. However, the traditional abstraction techniques do not perform these types of reductions, therefore an adaptation is needed. Moreover, to apply the abstraction on DEL, it is a challenge to design a reasonable 3-valued semantics of DEL which facilitates faithful reasoning on abstract models.

Specifically, in this chapter, we extend the abstraction-refinement theory for *Kripke Modal Labelled Transition Systems* (KMLTSs) [HJS01], incorporating not only state mapping but also label and proposition lumping, in order to obtain compact but informative abstractions. We develop a 3-valued Public Announcement Logic (PAL) and prove that the abstraction relation on *static* models *can* assure us to safely verify any *dynamic* properties in terms of PAL-formulas on the abstractions of a KMLTS. Thus the theory can be used to abstract Kripke models, since Kripke models can be regarded as a special case of KMLTSs. This theory is in particular applicable for an epistemic setting as the example of the Muddy Children shows. We shall also see that under certain conditions, the components as in Chapter 5 can be viewed as abstractions of the composed model.

**Related work** In the flourishing field of abstraction techniques, to the best of our knowledge, no work on the abstraction of Kripke models exists yet with reducing both the number of labels and of basic propositions. The literature related most closely to the current chapter is the work on abstraction of LTSs [vdPE04] in which the labels could be grouped. In the related field of Epistemic Temporal Logic, although the computational complexity of ETL model checking has been well-addressed in the literature (see e.g., [vdMS99, SG02, vdMS04] and the survey on page 157 of this thesis), the state space reduction techniques, such as symmetry reductions and abstractions, have not been used until recently [CDLR09, CLDQ09]. The multi-valued semantics of model logic has been discussed in [Fit91, Fit92] in a very general setting while we focus on the 3-valued semantics of PAL based on KMLTSs.

**Structure of the chapter** Section 7.2 introduces Kripke Modal Labelled Transition Systems, together with a 3-valued interpretation of PAL. In Section 7.3, the notions of refinement and abstraction are introduced and the preservation results are proven. Section 7.4 contains two examples of applying abstraction to some real epistemic models. We conclude in Section 7.5.

## 7.2 Preliminaries

In this section we introduce the 3-valued Public Announcement Logic interpreted on 3-valued Kripke Modal Labelled Transition Systems.

### 7.2.1 Kripke Modal Labelled Transition System

In order to define abstractions of Kripke models the standard definition is extended in the following sense:

- To incorporate the approximation of propositional information in the abstract model, we use 3-valued valuations instead of 2-valued ones. Besides *true* and *false*, atomic propositions can now have a third truth value  $\uparrow$  which is intended to mean *unknown*.
- To incorporate the approximation of relations, two types of relations *must* and *may* are introduced as in *Modal Transition Systems* [LT88]<sup>1</sup>, where *must*-relations are under-approximations (the relations are necessarily there in the concrete model) and *may*-relations are over-approximations (there are possibly such relations). Since necessarily existing relations should be at least possible, we require that the *must*-relations are included in the *may*-relations. Essentially, *may*- and *must*-relations together also assign “truth values” to the relations in the model: a relation from  $s$  to  $s'$  is “true” if there is a *must*-relation between  $s$  and  $s'$ , it is “false” if there is no *may*-relation between the states, and it is “unknown”

<sup>1</sup>See also [AHL<sup>+</sup>08] for a survey on such systems.

when there is a *may*-relation between  $s$  and  $s'$  without a corresponding *must*-relation.

Formally, similar to the definition of Kripke Modal Transition Systems in [HJS01, GJ02], we have:

**7.2.1. DEFINITION. (Kripke Modal Labelled Transition System)** A *Kripke Modal Labelled Transition System* (KMLTS) is a tuple  $\mathcal{M} = (S, \mathbf{P}, \Sigma, \dashrightarrow, \rightarrow, V)$  where:

- $S, \mathbf{P}, \Sigma$  are as usual;
- $\dashrightarrow$  is a set of transitions of the form  $s \dashrightarrow^i s'$  where  $i \in \Sigma$ ;
- $\rightarrow$  is a set of transitions of the form  $s \rightarrow^i s'$  where  $i \in \Sigma$ ;
- $V$  is a valuation function:  $V : S \rightarrow \{\text{true}, \text{false}, \uparrow\}^{\mathbf{P}}$ .

We require that  $\rightarrow \subseteq \dashrightarrow$ . We call  $(\mathbf{P}, \Sigma)$  the signature of  $\mathcal{M}$ . A *pointed KMLTS*  $(\mathcal{M}, s)$  is a pair of a KMLTS  $\mathcal{M}$  and a distinguished state  $s$  in it. □

We include the signature  $(\mathbf{P}, \Sigma)$  in the specification of the models as, in general, the signatures of a model and its abstractions will be different.

A standard Kripke model can be regarded as a special kind of KMLTS, where *must* and *may* coincide and the valuation is essentially 2-valued:

**7.2.2. DEFINITION. (Concrete model)** A KMLTS  $\mathcal{M} = (S, \mathbf{P}, \Sigma, \dashrightarrow, \rightarrow, V)$  is a concrete model if:

- $\dashrightarrow = \rightarrow$ ;
- for all  $s \in S$ , all  $p \in \mathbf{P} : V(s)(p) \neq \uparrow$ .

□

## 7.2.2 Three-valued Public Announcement Logic

Public Announcement Logic (PAL), initiated in [Pla89, GG97], is a convenient language for describing announcements and their informational consequences for (a group of) agents. Based on the standard language of epistemic logic (logic of knowledge), a new modality  $[\!|\phi]$  is introduced into the language, with  $[\!|\phi]\psi$  intended to express “if  $\phi$  is true then after the announcement of  $\phi$ ,  $\psi$  is true.” (see page 16 of this thesis). Various case studies show this logic to be powerful in helping to understand complicated higher order reasoning about knowledge and announcements such as in the cases of Muddy Children, Sum and Product and the protocol of Dining Cryptographers.<sup>2</sup>

<sup>2</sup>we refer interested readers to [vDvdHK07] for detailed explanations

Formally, given a signature  $(\mathbf{P}, \Sigma)$ , the formulas of the *Public Announcement Logic*  $\text{PAL}_{\Sigma, \mathbf{P}}$  are defined by

$$\phi ::= p \mid \phi \wedge \psi \mid \neg\phi \mid \Box_i\phi \mid [!\phi]\phi$$

where  $p \in \mathbf{P}$ ,  $i \in \Sigma$ . As usual, we define  $\phi \vee \psi$ ,  $\phi \rightarrow \psi$  and  $\Diamond_i\phi$  as abbreviations of  $\neg(\neg\phi \wedge \neg\psi)$ ,  $\neg\phi \vee \psi$  and  $\neg\Box_i\neg\phi$  respectively.

As we will see in the next section, our overall approach is not constrained to be used only in epistemic settings, as it does not require the model to be S5.<sup>3</sup> Not constrained within S5 models, we have more freedom to find suitable abstractions, as we will see in the Muddy Children example.

The semantics for 2-valued public announcement logic is the extension of standard modal logic with relativization operators  $[!\phi]$ :  $\mathcal{M}, s \models [!\phi]\psi \iff [\mathcal{M}, s \models \phi \text{ implies } \mathcal{M}|_{\phi}, s \models \psi]$ , where the relativized model  $\mathcal{M}|_{\phi}$  is the restriction of  $\mathcal{M}$  to the states where  $\phi$  holds. We extend such relativization, which we call “update” in the context of PAL, to the 3-valued case and take the usual semantics for  $\Box$  as in the logics on Modal Transition Systems:

**7.2.3. DEFINITION. (3-valued Semantics of PAL)** The truth value of a  $\text{PAL}_{\Sigma, \mathbf{P}}$  formula  $\phi$  in a state  $s$  of a KMLTS  $\mathcal{M} = (S, \mathbf{P}, \Sigma, \dashrightarrow, \rightarrow, V)$ , written  $\llbracket \phi \rrbracket^{\mathcal{M}, s}$ , is defined by:

$$\begin{aligned} \llbracket p \rrbracket^{\mathcal{M}, s} &= V(s)(p) \\ \llbracket \neg\phi \rrbracket^{\mathcal{M}, s} &= \neg_3 \llbracket \phi \rrbracket^{\mathcal{M}, s} \\ \llbracket \phi \wedge \psi \rrbracket^{\mathcal{M}, s} &= \llbracket \phi \rrbracket^{\mathcal{M}, s} \wedge_3 \llbracket \psi \rrbracket^{\mathcal{M}, s} \\ \llbracket \Box_i\phi \rrbracket^{\mathcal{M}, s} &= \begin{cases} true & \text{if } \forall s' : s \dashrightarrow_i s' \implies \llbracket \phi \rrbracket^{\mathcal{M}, s'} = true \\ false & \text{if } \exists s' : s \dashrightarrow_i s' \text{ and } \llbracket \phi \rrbracket^{\mathcal{M}, s'} = false \\ \uparrow & \text{otherwise} \end{cases} \\ \llbracket [!\phi]\psi \rrbracket^{\mathcal{M}, s} &= \begin{cases} true & \text{if } \llbracket \phi \rrbracket^{\mathcal{M}, s} = false \text{ or } \llbracket \psi \rrbracket^{\mathcal{M}|_{\phi}, s} = true \\ false & \text{if } \llbracket \phi \rrbracket^{\mathcal{M}, s} = true \text{ and } \llbracket \psi \rrbracket^{\mathcal{M}|_{\phi}, s} = false \\ \uparrow & \text{otherwise} \end{cases} \end{aligned}$$

where:

- $\neg_3(true) = false$ ,  $\neg_3(false) = true$  and  $\neg_3(\uparrow) = \uparrow$ , and for any  $x, y \in \{true, false, \uparrow\}$ :  
 $x \wedge_3 y = \min(x, y)$  w.r.t.  $\leq_v$ :  $false \leq_v \uparrow \leq_v true$ .
- $\mathcal{M}|_{\phi} = (\Sigma, \mathbf{P}, S', \dashrightarrow', \rightarrow', V')$  is defined as follows:
  - $S' = \{s \in S \mid \llbracket \phi \rrbracket^{\mathcal{M}, s} \neq false\}$ ;
  - $\dashrightarrow' = \dashrightarrow \cap (S' \times \Sigma \times S')$ ;
  - $\rightarrow' = \rightarrow \cap (S' \times \Sigma \times \{s \in S' \mid \llbracket \phi \rrbracket^{\mathcal{M}, s} = true\})$ ;
  - $V'(s) = V(s)$  for  $s \in S'$ .

<sup>3</sup>S5 is a set of formulas axiomatizing the reading of  $\Box$  as knowledge. S5 characterizes models in which the relations are equivalence relations.

Note that the above 3-valued semantics for the propositional fragment of PAL is essentially Kleene's *strong* 3-valued logic [Kle50] which is the strongest 3-valued propositional logic satisfying the following property:

**[monotonicity]** the behaviour of  $\uparrow$  is compatible with any increase in information, i.e. if the truth value of a basic proposition appearing in  $\phi$  is changed from  $\uparrow$  to *true* or *false* then the truth value of  $\phi$  should not be inherently changed from *false* to *true* or from *true* to *false*.

From the perspective of abstraction, monotonicity guarantees that if we have a definite truth value (*true* or *false*) of a formula in the 3-valued valuation (abstract model) then this truth value should be the same w.r.t any 2-valued valuation (concrete model) obtained by turning  $\uparrow$  values into either *true* or *false*. Thus we can *correctly* reason about the concrete model by looking at the abstract model<sup>4</sup>.

The semantics of  $\Box_i\phi$  is given as in [HJS01]<sup>5</sup>. The intuitive idea behind the semantics of  $\Box_i$  is that  $\Box_i\phi$  is true if all the possible (*may*) *i*-relations lead to  $\phi$ -true states, and is false if there exists a necessary (*must*) *i*-relation leading to a  $\phi$ -false state. A moment of reflection should confirm that this semantics for modal formulas also complies with the above monotonicity in spirit: turning the *3rd* truth value of propositions and transitions into definite truth values in a model will not change the definite truth value of any modal formula.

The semantics of  $[\!\!\uparrow\!\!\phi]\psi$  is given with the similar concern of monotonicity. The updated model  $\mathcal{M}|_\phi$  defined above keeps all the  $\phi$ -*not-false* states and all the relations among them, except for the *must*-relations that lead to  $\phi$ -unknown states in  $\mathcal{M}$ . Recall that the *must*-relations signify *necessary* relations. However, a  $\phi$ -unknown state  $s$  is not necessarily there in the updated model, as  $\uparrow$  leaves the possibility open that  $\phi$  could 'actually' be *false*. A relation directed at a possibly but not necessarily existent state, cannot be a necessary relation, so *must*-relations to  $\phi$ -unknown states are removed.

Note that  $\mathcal{M}|_\phi$  is still a KMLTS since  $\rightarrow' \subseteq \rightarrow$  by definition. It is not hard to check that this 3-valued semantics "coincides" with the standard 2-valued semantics on concrete models. Formally, for any  $\text{PAL}_{\Sigma, P}$  formula  $\phi$ , any concrete model  $\mathcal{M}$ :

$$\llbracket \phi \rrbracket^{\mathcal{M}, s} = \text{true} \iff \mathcal{M}', s \vDash \phi \quad \llbracket \phi \rrbracket^{\mathcal{M}, s} = \text{false} \iff \mathcal{M}', s \not\vDash \phi$$

where  $\mathcal{M}'$  is the standard Kripke model converted from  $\mathcal{M}$  by lumping *may* and *must* relations together and  $\vDash$  is the satisfaction relation for the standard 2-valued semantics of PAL.

<sup>4</sup> Although Kleene's strong 3-valued logic is the *strongest* one satisfying monotonicity, it does *not* mean we can get all the possible definite truth values w.r.t. the concrete model by looking at the abstract ones, e.g., the truth value of  $p \vee \neg p$  is  $\uparrow$  if the truth value of  $p$  is  $\uparrow$ , although  $p \vee \neg p$  is valid under 2-valued valuation.

<sup>5</sup> [HJS01] presented the 3-valued semantics in an equivalent form by assigning each formula a pair of sets of states:  $\llbracket \phi \rrbracket^{\text{true}}$  (the states where  $\phi$  is *necessarily* true) and  $\llbracket \phi \rrbracket^{\text{pos}}$  (the states where  $\phi$  is *possibly* true). See [GJ03] for discussions on these two forms.

For 2-valued PAL the following reduction axioms hold:

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

A natural question to ask is, in the above axioms, whether the formula at the left hand side of  $\leftrightarrow$  always has the same truth value as the right hand side formula given an arbitrary KMLTS? The answer is “No.” For example, consider the axiom PF and an KMLTS  $\mathcal{M}_1$  with a single state  $s$  where  $p$  is  $\uparrow$  and  $q$  is *false*, then  $\llbracket [!p]\neg q \rrbracket^{\mathcal{M}_1, s} = \text{true}$  but  $\llbracket p \rightarrow \neg[!p]q \rrbracket^{\mathcal{M}_1, s} = \uparrow$ .

Moreover, we can show that any other reasonable 3-valued semantics of PAL can not reduce the left hand side of  $\leftrightarrow$  to the right hand side. First note that an *informative* 3-valued semantics should indeed make  $\llbracket [!p]\neg q \rrbracket^{\mathcal{M}_1, s} = \text{true}$ , since changing the valuation of  $p$  in  $\mathcal{M}_1$  to *true* or *false* will only make  $[!p]\neg q$  true. We call a 3-valued semantics of PAL on KMLTSs *reasonable* if:

1. it coincides with strong Kleene 3-valued logic on its propositional fragment;
2. it coincides with the standard 2-valued semantics of PAL on concrete KMLTSs;
3. it is monotonic with respect to basic propositions.

Now we can show:

**7.2.4. PROPOSITION.** *There is no reasonable 3-valued semantics for PAL such that  $\llbracket p \rightarrow \neg[!p]q \rrbracket^{\mathcal{M}_1, s} = \text{true}$ .*

**PROOF** Suppose towards a contradiction that  $\llbracket p \rightarrow \neg[!p]q \rrbracket^{\mathcal{M}_1, s} = \text{true}$  w.r.t to a reasonable 3-valued semantics of PAL. Note that  $\llbracket p \rrbracket^{\mathcal{M}_1, s} = \uparrow$ , then according to the strong Kleene semantics, we have  $\llbracket \neg[!p]q \rrbracket^{\mathcal{M}_1, s} = \text{true}$ , thus  $\llbracket [!p]q \rrbracket^{\mathcal{M}_1, s} = \text{false}$ . However if we change the valuation of  $p$  in  $\mathcal{M}_1$  to *false* then  $[!p]q$  would be *true* according to the standard 2-valued semantics of PAL, which contradicts monotonicity.  $\times$

The above result also shows that we can not translate the 3-valued PAL back to its modal logic fragment by just applying the reduction axioms of the 2-valued PAL.

Although our concern in this chapter is primarily to develop the theory of epistemic abstractions, the ultimate goal is to enable automatic verification of large epistemic models. Designing efficient algorithms for checking the satisfaction of 3-valued PAL formulae on KMLTSs, based on the definition above, is an interesting topic in itself and we leave it as further work. We now only note that, looking at similar results in the literature [BG04], we expect that such a model checking algorithm will not be more complex than the ones for checking (2-valued) PAL on Kripke models.

## 7.3 Abstraction and Logical Characterization

In this section we extend the classic definition of abstraction with label and proposition mappings in order to reduce the number of labels and possibly achieve smaller abstraction models. We show that we can reason about properties of the more refined model by model checking the more abstract model.

### 7.3.1 Abstraction

As observed in [vdPE04], to do model checking on infinitely-labelled systems, one needs abstraction to obtain a model with a reduced finite number of labels. We aim for an abstraction method that reduces the labels also in the finite case, by lumping similar transitions with different labels together into a unified one. This is often applicable in the epistemic case, as several agents may play a similar role and therefore have similar uncertainties. On the other hand, different propositions may also have a similar role on different states, in which case abstractions may combine propositions together as well. In the following, we use two mappings between signatures to capture the above intuitions of lumping labels and propositions. It is important to note that these abstractions produce models with a different signature than the original one.

**Notation** For a function  $h$  and  $x$  in its range, we use  $h^{-1}[x]$  to denote the pre-image of  $x$ .

**7.3.1. DEFINITION. (Abstraction and Refinement)** Let  $\mathcal{M} = (S, \Sigma, \mathbf{P}, \dashrightarrow, \rightarrow, V)$  and  $\mathcal{N} = (T, \Sigma', \mathbf{P}', \dashrightarrow', \rightarrow', V')$  be two KMLTSs. Given two surjective functions  $f : \Sigma' \rightarrow \Sigma$  and  $g : \mathbf{P}' \rightarrow \mathbf{P}$ , a binary relation  $R \subseteq T \times S$  is called an  $f, g$ -abstraction 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  $p \in \mathbf{P} : V(s)(p) \neq \uparrow$  implies  $\forall p' \in g^{-1}[p] : V'(t)(p') = V(s)(p)$ ;
- $t \dashrightarrow^{i'} t'$  implies  $\exists s' \in S : s \dashrightarrow^{f(i')} s'$  and  $R(t', s')$ ;
- $s \xrightarrow{i} s'$  implies  $\forall i' \in f^{-1}[i] : \exists t' \in T$  such that  $t \xrightarrow{i'} t'$  and  $R(t', s')$ .

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

Correspondingly,  $(\mathcal{N}, t)$  is called an  $f, g$ -refinement of  $(\mathcal{M}, s)$  iff  $(\mathcal{M}, s)$  is an  $f, g$ -abstraction of  $(\mathcal{N}, t)$ . □

The first condition says that the valuation in the more abstract model can be less informative by making some propositions *unknown* ( $\uparrow$ ), but never unfaithful. The second condition requires that if an  $i'$ -may-transition in the more refined model then

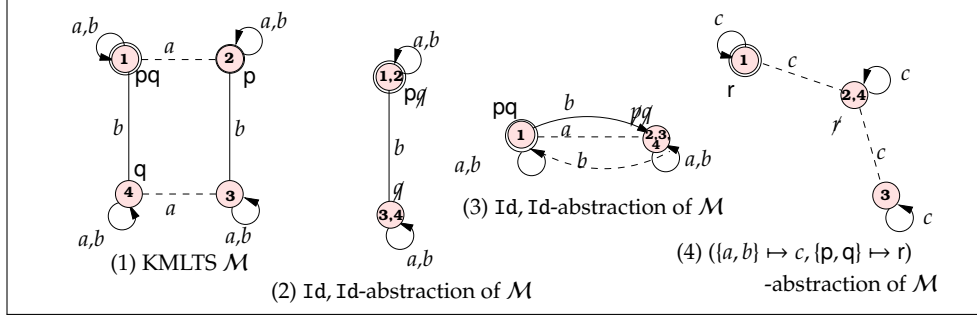


Figure 7.1: A pointed KMLTS and three possible abstractions of it. Dotted lines are for *may*-relations and solid lines for *must*. *May*-relations that coincide with corresponding *must* ones are omitted. If there is no arrow on a relation then it is bidirectional.

there is a matching transition in the more abstract model w.r.t the label mapping. The last condition says if there is an  $i$ -*must*-transition in the more abstract model then there is a corresponding  $i'$ -*must*-transition in the more refined model for *each*  $i'$  such that  $f(i') = i$ .

Note that for two 2-valued Kripke models with the same signature  $(\mathbf{P}, \Sigma)$ ,  $\mathcal{N}$  is a refinement of  $\mathcal{M}$  in the classical sense of [Lar90] iff  $\mathcal{N}$  is an  $(Id_{\Sigma}, Id_{\mathbf{P}})$ -refinement of  $\mathcal{M}$  where  $Id_X$  is identity function on the domain  $X$ .

Fig. 7.1 shows an example of a KMLTS  $\mathcal{M}$  and several abstractions of it. In the picture,  $\uparrow$  is to mean the value of  $p$  is *unknown* ( $\uparrow$ ) at the current state while the absence of a proposition at a state means it is *false* there. For clarity, the states of  $\mathcal{M}$  are numbered and the numbers on the states of the abstracted models indicate which original states they represent. In (2), the mappings are the identity functions, and the valuation of proposition  $q$  is mapped to  $\uparrow$  for all worlds. In (3), the abstraction is given by the identity functions as well, but collapsing different worlds. In (4), there is an abstraction obtained by lumping both agents and both propositions.

Since  $\rightarrow \subseteq \dashrightarrow$ , we can make a concrete refinement of any KMLTS by dropping *may* relations that do not have a *must* counterpart (i.e.  $\dashrightarrow'$ ,  $\rightarrow' := \rightarrow$ ) and by adapting the valuation to become two-valued (e.g., by defining  $V'(s)(p) = \text{false}$  whenever  $V(s)(p) = \uparrow$  and  $V'(s)(p) = V(s)(p)$  otherwise). Therefore:

**7.3.2. PROPOSITION.** *A KMLTS  $\mathcal{M}$  always has a concrete refinement.*

### 7.3.2 Logical Characterization

We will prove a preservation result of satisfaction of formulas between a pointed model  $(\mathcal{N}, t)$  and its abstraction  $(\mathcal{M}, s)$ . Intuitively we want a formula to be true/false at  $\mathcal{N}$  if it is true/false at  $\mathcal{M}$  respectively, such that we can safely model check the more abstract model to get the information of the more refined one. However, as

these models may have different signatures due to the  $f, g$  mappings attached to the abstraction relation, we need to check different formulas on these two models. 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.  $\llbracket \psi \rrbracket^{\mathcal{M}, s} = \text{false} \implies \llbracket \phi \rrbracket^{\mathcal{N}, t} = \text{false}.$

Then our goal is to check whether  $(\mathcal{N}, t) \in_{f, g} (\mathcal{M}, s)$  implies for all  $\phi$ :  $\llbracket \ulcorner \phi \urcorner \rrbracket^{\mathcal{M}, s} \leq \llbracket \phi \rrbracket^{\mathcal{N}, t}$  where  $\ulcorner \phi \urcorner$  is a formula in the signature of  $\mathcal{M}$  corresponding to  $\phi$ . To pinpoint the right formulas to check, we introduce the following translation:

**7.3.3. DEFINITION. (Translation of formulas)** Given signatures  $(\mathbf{P}', \Sigma'), (\mathbf{P}, \Sigma)$ , and surjective functions  $f : \Sigma' \rightarrow \Sigma, g : \mathbf{P}' \rightarrow \mathbf{P}$ , we define the translation of an  $\text{PAL}_{\mathbf{P}', \Sigma'}$ -formula  $\phi$  into an  $\text{PAL}_{\mathbf{P}, \Sigma}$ -formula  $\ulcorner \phi \urcorner_{f, g}$  inductively as follows:

$$\begin{aligned} \ulcorner p' \urcorner_{f, g} &= g(p') \\ \ulcorner \neg \psi \urcorner_{f, g} &= \neg \ulcorner \psi \urcorner_{f, g} \\ \ulcorner \psi_1 \wedge \psi_2 \urcorner_{f, g} &= \ulcorner \psi_1 \urcorner_{f, g} \wedge \ulcorner \psi_2 \urcorner_{f, g} \\ \ulcorner \square_i \psi \urcorner_{f, g} &= \square_{f(i)} \ulcorner \psi \urcorner_{f, g} \\ \ulcorner [! \chi] \psi \urcorner_{f, g} &= [! \ulcorner \chi \urcorner_{f, g}] \ulcorner \psi \urcorner_{f, g} \end{aligned}$$

□

Before proving the main result of this chapter, we first prove a result establishing the abstraction relation between the updated models  $(\mathcal{N}|_\chi, t)$  and  $(\mathcal{M}|_{\ulcorner \chi \urcorner_{f, g}}, s)$  for some  $\mathcal{L}_{\mathbf{P}, \Sigma}$ -formula  $\chi$ , given that  $(\mathcal{N}, t) \in_{f, g} (\mathcal{M}, s)$

**7.3.4. LEMMA.** *Suppose  $(\mathcal{N}, t), (\mathcal{M}, s)$  are pointed KMLTSs with signatures  $(\mathbf{P}', \Sigma')$  and  $(\mathbf{P}, \Sigma)$  and sets of states  $T$  and  $S$  respectively, such that  $(\mathcal{N}, t) \in_{f, g} (\mathcal{M}, s)$ . Then for any  $\text{PAL}_{\Sigma', \mathbf{P}'}$  formula  $\chi$  such that  $t$  is in  $\mathcal{N}|_\chi$  and  $s$  is in  $\mathcal{M}|_{\ulcorner \chi \urcorner_{f, g}}$ , the following (1) implies (2):*

1. *for each  $t' \in T, s' \in S : (\mathcal{N}, t') \in_{f, g} (\mathcal{M}, s') \implies \llbracket \ulcorner \chi \urcorner_{f, g} \rrbracket^{\mathcal{M}, s'} \leq \llbracket \chi \rrbracket^{\mathcal{N}, t'}$  (★)*
2.  $(\mathcal{N}|_\chi, t) \in_{f, g} (\mathcal{M}|_{\ulcorner \chi \urcorner_{f, g}}, s)$

**PROOF** Suppose  $(\mathcal{N}, t) \in_{f, g} (\mathcal{M}, s)$  then there is a relation  $R$  which constitutes an  $f, g$ -refinement between  $\mathcal{N}$  and  $\mathcal{M}$  with  $(t, s) \in R$ . Now given a  $\text{PAL}_{\Sigma', \mathbf{P}'}$  formula  $\chi$  such that  $t$  is in  $\mathcal{N}|_\chi$  and  $s$  is in  $\mathcal{M}|_{\ulcorner \chi \urcorner_{f, g}}$ , let  $T|_\chi$  and  $S|_{\ulcorner \chi \urcorner_{f, g}}$  be the sets of states of  $\mathcal{N}|_\chi$  and  $\mathcal{M}|_{\ulcorner \chi \urcorner_{f, g}}$ . We claim that  $R' = R \cap (T|_\chi \times S|_{\ulcorner \chi \urcorner_{f, g}})$  is an  $f, g$ -abstraction relation between  $\mathcal{N}|_\chi$  and  $\mathcal{M}|_{\ulcorner \chi \urcorner_{f, g}}$ . Note that  $(t, s) \in R'$  since  $t \in \mathcal{N}|_\chi$  and  $s \in \mathcal{M}|_{\ulcorner \chi \urcorner_{f, g}}$ . Now we check the three conditions of the abstraction relation:

- for the condition on  $p$ : follows from the first item in the definition of  $R$  and the fact that the valuation of an updated model is just the restriction of the original valuation to the remaining states.

- suppose  $t \xrightarrow{i'} t'$  in  $\mathcal{N}|_{\chi}$ , then  $t \xrightarrow{i'} t'$  in  $\mathcal{N}$  according to the definition of the update. Since  $(t, s) \in R$  and  $R$  is an abstraction relation, there exists  $s' \in \mathcal{M}$ :  $s \xrightarrow{f(i')} s'$  and  $(t', s') \in R$ . We must still show that  $s' \in \mathcal{M}|_{\chi \uparrow_{f,g}}$ . Suppose not, then  $\llbracket \ulcorner \chi \urcorner_{f,g} \rrbracket^{\mathcal{M}, s'} = false$ . Because  $(t', s') \in R$  ensures  $(\mathcal{N}, t') \in_{f,g} (\mathcal{M}, s')$ , it then follows from  $(\star)$  that  $\llbracket \ulcorner \chi \urcorner \rrbracket^{\mathcal{N}, t'} = false$ . But then  $t' \notin \mathcal{N}|_{\chi}$ , contradiction.
- suppose  $s \xrightarrow{i} s'$  in  $\mathcal{M}|_{\chi \uparrow_{f,g}}$ , then  $\llbracket \ulcorner \chi \urcorner_{f,g} \rrbracket^{\mathcal{M}, s'} = true$  and  $s \xrightarrow{i} s'$  in  $\mathcal{M}$ . Because  $R$  is an  $f, g$ -abstraction relation and  $(t, s) \in R$ , for any  $i' \in f^{-1}[i]$  there exists  $t' \in \mathcal{N}$  such that  $t \xrightarrow{i'} t'$  and  $(t', s') \in R$ . To show that  $(t', s') \in R'$  for such  $t'$ , it remains to show that  $t' \in \mathcal{N}|_{\chi}$ . Since  $\llbracket \ulcorner \chi \urcorner_{f,g} \rrbracket^{\mathcal{M}, s'} = true$  and  $(t', s') \in R$ , it then follows from condition  $(\star)$  that  $\llbracket \ulcorner \chi \urcorner \rrbracket^{\mathcal{N}, t'} = true$ . Hence,  $t' \in \mathcal{N}|_{\chi}$ .

✱

Now come our main results (Theorem 7.3.5 and Theorem 7.3.7) based on the above lemma.

**7.3.5. THEOREM.** *Suppose  $\mathcal{N}, \mathcal{M}$  are two KMLTSs w.r.t.  $\mathbf{Y}, \mathbf{P}'$  and  $\mathbf{I}, \mathbf{P}$  respectively.  $s$  and  $t$  are two states in  $\mathcal{M}$  and  $\mathcal{N}$  respectively. Then:*

$$(\mathcal{N}, t) \in_{f,g} (\mathcal{M}, s) \text{ implies that for all } \phi \in \text{PAL}_{\Sigma', \mathbf{P}'} : \llbracket \ulcorner \phi \urcorner_{f,g} \rrbracket^{\mathcal{M}, s} \leq \llbracket \ulcorner \phi \urcorner \rrbracket^{\mathcal{N}, t}.$$

**PROOF** We prove the theorem by induction on the structure of  $\phi$  :

- $\phi = p'$  : trivial, follows from the first condition of the definition of  $\in_{f,g}$ .
- $\phi = \neg\psi$  : suppose  $\llbracket \ulcorner \phi \urcorner_{f,g} \rrbracket^{\mathcal{M}, s} = true$  then according to the semantics  $\llbracket \ulcorner \psi \urcorner_{f,g} \rrbracket^{\mathcal{M}, s} = false$ . Thus by induction hypothesis  $\llbracket \ulcorner \psi \urcorner \rrbracket^{\mathcal{N}, t} = false$ . Therefore  $\llbracket \ulcorner \phi \urcorner \rrbracket^{\mathcal{N}, t} = true$ . For the case  $\llbracket \ulcorner \phi \urcorner_{f,g} \rrbracket^{\mathcal{M}, s} = false$ , similar.
- $\phi = \psi_1 \wedge \psi_2$  :
  - suppose  $\llbracket \ulcorner \phi \urcorner_{f,g} \rrbracket^{\mathcal{M}, s} = true$  then by the semantics:  $\llbracket \ulcorner \psi_1 \urcorner_{f,g} \rrbracket^{\mathcal{M}, s} = true$  and  $\llbracket \ulcorner \psi_2 \urcorner_{f,g} \rrbracket^{\mathcal{M}, s} = true$ . Thus by induction hypothesis  $\llbracket \ulcorner \psi_1 \urcorner \rrbracket^{\mathcal{N}, t} = true$  and  $\llbracket \ulcorner \psi_2 \urcorner \rrbracket^{\mathcal{N}, t} = true$ . Therefore  $\llbracket \ulcorner \phi \urcorner \rrbracket^{\mathcal{N}, t} = true$ .
  - suppose  $\llbracket \ulcorner \phi \urcorner_{f,g} \rrbracket^{\mathcal{M}, s} = false$  then by the semantics either  $\llbracket \ulcorner \psi_1 \urcorner_{f,g} \rrbracket^{\mathcal{M}, s} = false$  or  $\llbracket \ulcorner \psi_2 \urcorner_{f,g} \rrbracket^{\mathcal{M}, s} = false$ . Without loss of generality, suppose the latter. Thus by induction hypothesis  $\llbracket \ulcorner \psi_2 \urcorner \rrbracket^{\mathcal{N}, t} = false$ . Therefore  $\llbracket \ulcorner \phi \urcorner \rrbracket^{\mathcal{N}, t} = false$ .
- $\phi = \square_{i'}\psi$  : then  $\ulcorner \phi \urcorner_{f,g} = \square_{f(i')} \ulcorner \psi \urcorner_{f,g}$ .
  - suppose  $\llbracket \ulcorner \phi \urcorner_{f,g} \rrbracket^{\mathcal{M}, s} = true$  then according to the semantics for all  $s'$  with  $s \xrightarrow{f(i')} s'$  we have  $\llbracket \ulcorner \psi \urcorner_{f,g} \rrbracket^{\mathcal{M}, s'} = true$ . Suppose in  $\mathcal{N}$  there is a world  $t'$  such

that  $t \xrightarrow{i'} t'$  then according to the definition of refinement, there is a  $s'' \in \mathcal{M}$  such that  $s \xrightarrow{f(i')} s''$  and  $(\mathcal{N}, t') \in_{f,g} (\mathcal{M}, s'')$ . Thus  $\llbracket \Gamma \psi \neg_{f,g} \rrbracket^{\mathcal{M}, s''} = true$ . By induction hypothesis,  $\llbracket \psi \rrbracket^{\mathcal{N}, t'} = true$ . Therefore  $\llbracket \square_{i'} \psi \rrbracket^{\mathcal{N}, t} = true$ .

- suppose  $\llbracket \Gamma \phi \neg_{f,g} \rrbracket^{\mathcal{M}, s} = false$  then according to the semantics, there is  $s'$  with  $s \xrightarrow{f(i')} s'$  such that  $\llbracket \Gamma \psi \neg_{f,g} \rrbracket^{\mathcal{M}, s'} = false$ . By definition of refinement, for any  $i'' \in f^{-1}[f(i')]$  there is a  $t' \in \mathcal{N}$  such that  $t \xrightarrow{i''} t'$  and  $(\mathcal{N}, t') \in_{f,g} (\mathcal{M}, s')$ . By induction hypothesis, for all such  $t' : \llbracket \psi \rrbracket^{\mathcal{N}, t'} = false$ . Thus for all  $i'' \in f^{-1}[f(i')]$  :  $\llbracket \square_{i''} \psi \rrbracket^{\mathcal{N}, t} = false$ . In particular:  $\llbracket \square_{i'} \psi \rrbracket^{\mathcal{N}, t} = false$ .

- $\phi = [!\chi]\psi$

- if  $\llbracket \Gamma \phi \neg_{f,g} \rrbracket^{\mathcal{M}, s} = true$  then  $\llbracket \Gamma \chi \neg_{f,g} \rrbracket^{\mathcal{M}, s} = false$  or  $\llbracket \Gamma \psi \neg_{f,g} \rrbracket^{\mathcal{M}|_{\chi \neg_{f,g} s}} = true$ . If  $\llbracket \Gamma \chi \neg_{f,g} \rrbracket^{\mathcal{M}, s} = false$  then  $\llbracket \chi \rrbracket^{\mathcal{N}, t} = false$  by induction hypothesis, hence  $\llbracket \phi \rrbracket^{\mathcal{N}, t} = true$ . Otherwise,  $\llbracket \Gamma \psi \neg_{f,g} \rrbracket^{\mathcal{M}|_{\chi \neg_{f,g} s}} = true$  and  $\llbracket \Gamma \chi \neg_{f,g} \rrbracket^{\mathcal{M}, s} \neq false$ , then  $s \in \mathcal{M}|_{\chi \neg_{f,g}}$ . Now suppose  $\llbracket \chi \rrbracket^{\mathcal{N}, t} \neq false$ , so:  $t \in \mathcal{N}|_{\chi}$ . We need to show that  $\llbracket \psi \rrbracket^{\mathcal{N}|_{\chi}, t} = true$ . By induction hypothesis  $(\mathcal{N}, t') \in_{f,g} (\mathcal{M}, s') \implies \llbracket \Gamma \chi \neg_{f,g} \rrbracket^{\mathcal{M}, s'} \leq \llbracket \chi \rrbracket^{\mathcal{N}, t'}$  for each  $s' \in S, t' \in T$ . Therefore from Lemma 7.3.4 we have  $(\mathcal{N}|_{\chi}, t) \in_{f,g} (\mathcal{M}|_{\chi \neg_{f,g}}, s)$ . By induction hypothesis,  $\llbracket \psi \rrbracket^{\mathcal{N}|_{\chi}, t} = true$ . Thus  $\llbracket \phi \rrbracket^{\mathcal{N}, t} = true$ .
- if  $\llbracket \Gamma \phi \neg_{f,g} \rrbracket^{\mathcal{M}, s} = false$  then  $\llbracket \Gamma \chi \neg_{f,g} \rrbracket^{\mathcal{M}, s} = true$  and  $\llbracket \Gamma \psi \neg_{f,g} \rrbracket^{\mathcal{M}|_{\chi \neg_{f,g} s}} = false$ . Since  $\llbracket \Gamma \chi \neg_{f,g} \rrbracket^{\mathcal{M}, s} = true$  then  $\llbracket \chi \rrbracket^{\mathcal{N}, t} = true$  by induction hypothesis. We only need to show  $\llbracket \psi \rrbracket^{\mathcal{N}|_{\chi}, t} = false$ . It is clear that  $t \in \mathcal{N}|_{\chi}$  and  $s \in \mathcal{M}|_{\chi \neg_{f,g}}$ , then by induction hypothesis the condition of Lemma 7.3.4 holds, and it follows that  $(\mathcal{N}|_{\chi}, t) \in_{f,g} (\mathcal{M}|_{\chi \neg_{f,g}}, s)$ . Thus by the induction hypothesis we have  $\llbracket \psi \rrbracket^{\mathcal{N}|_{\chi}, t} = false$ . Therefore:  $\llbracket \phi \rrbracket^{\mathcal{N}, t} = false$ .

✱

**7.3.6. COROLLARY.** *Suppose  $(\mathcal{N}, t), (\mathcal{M}, s)$  are two pointed KMLTSs w.r.t.  $(\mathbf{I}, \mathbf{P}')$  and  $(\mathbf{I}, \mathbf{P})$  respectively. If  $(\mathcal{N}, t) \in_{f,g} (\mathcal{M}, s)$  and  $\mathcal{N}$  is a Kripke model converted from a concrete KMLTS then for any formula  $\phi \in \text{PAL}_{\Sigma, \mathbf{P}'}$  :*

- $\llbracket \Gamma \phi \neg_{f,g} \rrbracket^{\mathcal{M}, s} = true \implies \mathcal{N}, t \vDash \phi$
- $\llbracket \Gamma \phi \neg_{f,g} \rrbracket^{\mathcal{M}, s} = false \implies \mathcal{N}, t \vDash \neg \phi$

By the above corollary, to know whether  $\phi$  is satisfied at a pointed Kripke model, we can instead model check  $\Gamma \phi \neg_{f,g}$  on its  $f, g$ -abstraction.

To justify the logical characterization, we prove the converse of Theorem 7.3.5.

**7.3.7. THEOREM.** *Suppose  $(\mathcal{N}, t)$  and  $(\mathcal{M}, s)$  are pointed KMLTSs with signatures  $(\mathbf{P}', \Sigma')$  and  $(\mathbf{P}, \Sigma)$ , and suppose they enjoy image finiteness (see page 11). Then:*

*If for every  $\phi \in \text{PAL}_{\mathbf{P}', \Sigma'} : \llbracket \ulcorner \phi \urcorner_{f,g} \rrbracket^{\mathcal{M}, s} \leq \llbracket \phi \rrbracket^{\mathcal{N}, t}$  then  $(\mathcal{N}, t) \in_{f,g} (\mathcal{M}, s)$ .*

**PROOF** Assume that for every formula  $\phi \in \text{PAL}_{\Sigma', \mathbf{P}'}$ :  $\llbracket \ulcorner \phi \urcorner_{f,g} \rrbracket^{\mathcal{M}, s} \leq \llbracket \phi \rrbracket^{\mathcal{N}, t}$ , and let  $R = \{(t', s') \mid \text{for every } \phi : \llbracket \ulcorner \phi \urcorner_{f,g} \rrbracket^{\mathcal{M}, s'} \leq \llbracket \phi \rrbracket^{\mathcal{N}, t'}\}$ . Then  $(t, s) \in R$ , and we check the three conditions of definition 7.3.1 for  $R$ . Suppose  $(t', s') \in R$ , then:

- The first condition follows from  $\llbracket \ulcorner p' \urcorner_{f,g} \rrbracket^{\mathcal{M}, s'} \leq \llbracket p' \rrbracket^{\mathcal{N}, t'}$  for  $p' \in \mathbf{P}'$ .
- Suppose towards contradiction that  $\exists t'' : t' \xrightarrow{i'} t''$  in  $\mathcal{N}$  but for any  $s'' \in S$ :  $s' \xrightarrow{f(i')} s''$  implies  $(t'', s'') \notin R$ . According to image finiteness, we have only finitely many such  $s''$  (call them  $s''_0 \dots s''_n$ ). For each  $s''_k$ , since  $(t'', s''_k) \notin R$ , there must be a formula  $\psi_{s''_k}$  such that  $\llbracket \ulcorner \psi_{s''_k} \urcorner_{f,g} \rrbracket^{\mathcal{M}, s''_k} = \text{true}$  but  $\llbracket \psi_{s''_k} \rrbracket^{\mathcal{N}, t''} \neq \text{true}$ .<sup>6</sup> Now  $\Box_{f(i')} (\bigvee_{k=0}^n \ulcorner \psi_{s''_k} \urcorner_{f,g})$  is *true* at  $s'$  but  $\Box_{i'} (\bigvee_{k=0}^n \psi_{s''_k})$  is not *true* at  $t'$ , contradicting the assumption that  $(t', s') \in R$ .
- Suppose towards contradiction that  $s' \xrightarrow{f(i')} s''$  in  $\mathcal{M}$ , but there exists  $i'' \in f^{-1}[f(i')]$  such that  $\forall t'' \in T$ :  $t' \xrightarrow{i''} t''$  implies  $(t'', s'') \notin R$ . According to image finiteness, there are only finitely many such  $t''$  (call them  $t''_0 \dots t''_n$ ). For each  $t''_k$ , since  $(t''_k, s'') \notin R$ , there must be a formula  $\psi_{t''_k}$  such that  $\llbracket \ulcorner \psi_{t''_k} \urcorner_{f,g} \rrbracket^{\mathcal{M}, s''} = \text{false}$  but  $\llbracket \psi_{t''_k} \rrbracket^{\mathcal{N}, t''_k} \neq \text{false}$ . Note that  $\Box_{f(i')} (\bigvee_{k=0}^n \ulcorner \psi_{t''_k} \urcorner_{f,g})$  is *false* at  $s'$  but  $\Box_{i''} (\bigvee_{k=0}^n \psi_{t''_k})$  is not *false* at  $t'$ , contradicting the assumption that  $(t', s') \in R$ .

✕

## 7.4 The Muddy Children and Abstraction

Recall the discussions we had in Section 5.2 of Chapter 5: we can decompose the model for  $n$ -Muddy Children (see Example 1.1.2) into  $n$  two-world models (with disjoint vocabularies)  $\mathcal{M}_1, \mathcal{M}_2, \dots, \mathcal{M}_n$  where each  $\mathcal{M}_i$  represents the children's observation about whether child  $i$  is dirty:

$$m_i \text{ --- } i \text{ --- } \overline{m}_i$$

It is clear that we can view each  $\mathcal{M}_i$  as a KMLTS with signatures  $\mathbf{P} = \{m_1, m_2, \dots, m_n\}$  and  $\Sigma = \{1, 2, \dots, n\}$ , where may- and must-relations coincide but propositions in  $\mathbf{P} - \{m_i\}$  are assigned the third truth value  $\uparrow$ . It is not hard to see that each  $\mathcal{M}_i$  is an (id, id)-abstraction of the composed model  $\mathcal{M}$ . Thus we can verify the properties

<sup>6</sup>If  $\llbracket \ulcorner \psi_{s''_k} \urcorner_{f,g} \rrbracket^{\mathcal{M}, s''_k} = \text{false}$  but  $\llbracket \psi_{s''_k} \rrbracket^{\mathcal{N}, t''} \neq \text{false}$  then  $\llbracket \ulcorner \neg \psi_{s''_k} \urcorner_{f,g} \rrbracket^{\mathcal{M}, s''_k} = \text{true}$  but  $\llbracket \neg \psi_{s''_k} \rrbracket^{\mathcal{N}, t''} \neq \text{true}$ .

about the composed model by looking at its components. For example, let  $\phi$  be the common knowledge formula  $C(\neg K_i m_i \wedge \neg K_i \neg m_i)$ , universally verifying  $\phi$  against  $\mathcal{M}$  (checking  $\mathcal{M} \models \phi$ ) is then reduced to checking  $\mathcal{M}_i \models \phi$ , which is obviously true.

More generally, we can prove Theorem 5.2.13 in Chapter 5 as an easy application of our Theorem 7.3.5:

**7.4.1. THEOREM.** *If a pointed S5 model  $(\mathcal{M}, s)$  is decomposable (w.r.t  $\oplus$ ) into S5 models  $(\mathcal{M}_0, s_0), (\mathcal{M}_1, s_1), \dots, (\mathcal{M}_n, s_n)$  with disjoint vocabularies  $\mathbf{P}_0, \mathbf{P}_1, \dots, \mathbf{P}_n$ , then for any epistemic formula  $\phi$  based on  $\mathbf{P}_i$ :  $\mathcal{M}_i, s_i \models \phi \iff \mathcal{M}, s \models \phi$ .*

**PROOF** Again we consider the models  $\mathcal{M}_i$  and  $\mathcal{M}$  as KMLTSs where may- and must-relations coincide as above. We let  $R$  be the relation linking a world  $s$  in  $\mathcal{M}$  with a world  $t$  in  $\mathcal{M}_i$  iff  $s$  is composed by  $t$  and other worlds from other models. We need to show that  $R$  is indeed an (id, id)-abstraction relation. The first and second conditions of Definition 7.3.1 are trivial, according to the definition of  $\oplus$  in Section 5.2.

Now suppose  $t \xrightarrow{i} t'$  in  $\mathcal{M}_i$  and  $sRt$ . Since  $sRt$  then we can assume that  $s$  is a tuple  $\langle t_0, \dots, t_i, \dots, t_n \rangle$  where  $t_i = t$  and each  $t_j$  is from the model  $\mathcal{M}_j$ . Since  $\mathbf{P}_i$  are disjoint from each other, then there must be a state  $s' = \langle t_0, \dots, t', \dots, t_n \rangle$  in  $\mathcal{M}$  differing from  $s$  only in the  $i$ th place in the tuple. Since all the  $\mathcal{M}_i$  are S5 models,  $t_j \xrightarrow{i} t_j$  in  $\mathcal{M}_j$  for  $j \neq i$ . Because  $t_i \xrightarrow{i} t'$  then by the definition of the composed model,  $s \xrightarrow{i} s'$  in  $\mathcal{M}$ .  $\times$

Note that the above abstraction of the model of  $n$ -Muddy Children by decomposition with two-world models is somehow too coarse, since it does not reflect the dynamics of the story. For example, on a two-world abstraction of  $n$ -Muddy Children, the announcement of  $m_1 \vee m_2 \vee m_3$  (one of you is muddy) simply does not change anything since the truth value of  $m_1 \vee m_2 \vee m_3$  on these two-world abstractions is either *true* or  $\uparrow$ . In the sequel, let us consider more sophisticated abstractions of the model of Muddy Children which reflect the dynamics of announcements. We will focus on the 3-children case from now on.

The left column of Fig. 7.2 shows the standard epistemic model and its dynamics for 3-Muddy Children. The middle and right columns of Fig. 7.2 show abstracted versions of the concrete model on the left. The abstraction relation underlying both abstractions relates three pairs of worlds in the concrete model to three single worlds in the abstraction, while the world with all propositions *false* and the world with only  $m_3$  *true* are kept (for example, the world with  $m_2$  *true* and the world with  $m_2, m_3$  *true* in the concrete model are related to the one world in the abstracted model where  $m_2$  is *true* and  $m_3$  *unknown*). In the middle column, the parameters  $f, g$  for the refinement are identities, in the right column  $f$  maps both 1 and 2 to abstract label  $A$ . Let  $\phi_m$  be the abbreviation of the first announcement ( $m_1 \vee m_2 \vee m_3$ ) and  $\phi_K$  be the abbreviation of the next ones ( $\neg \Box_1 m_1 \wedge \neg \Box_2 m_2 \wedge \neg \Box_3 m_3$ ). Notice the following significant properties can be verified to be *true* in the two abstractions: (1) In both abstractions,  $\lceil [!\phi_m][!\phi_K][!\phi_K](\Box_1 m_1 \wedge \Box_2 m_2) \rceil_{f,g}$  is *true* at the worlds that correspond to the world which makes  $m_1, m_2$  and  $m_3$  *true* in the original model. Thus by Theorem 7.3.5,  $[!\phi_m][!\phi_K][!\phi_K](\Box_1 m_1 \wedge \Box_2 m_2)$  is *true* in that world in the

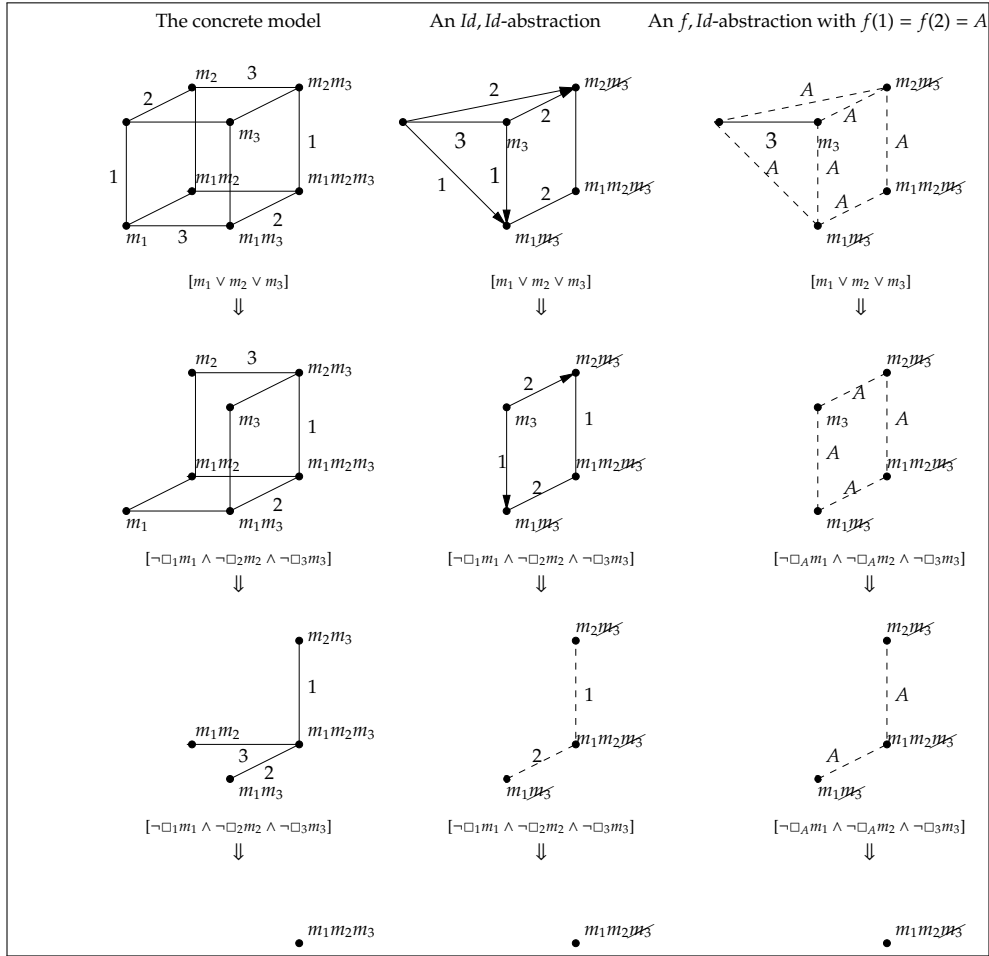


Figure 7.2: Abstractions of the Muddy Children for  $n = 3$  children. Each world has reflexive *may*-relations for each  $i \in \Sigma = \{1, 2, 3\}$ , some have reflexive *must*-relations, but for simplicity of presentation, all reflexive relations are omitted as usual.

original model. Namely, in the case all three children are muddy, children 1 and 2 will know they are muddy after three announcements. (2) In both abstractions,  $\lceil [! \phi_m][! \phi_k] \Box_1 m_1 \rceil_{f,g}$  is *true* at the worlds that correspond to the original world where only  $m_1$  and  $m_3$  are *true*. Namely in the case children 1 and 3 are muddy, child 1 will know he is muddy after 2 updates. (3)  $\lceil [! \phi_m] \Box_3 m_3 \rceil_{f,g}$  is *true* at the worlds with only  $m_3$  *true*. Namely when child 3 is the only muddy child, he will know after the first announcement. For the generalization to the  $n$  children case, similar abstractions can be made.

Note that whereas all relations in the concrete model are equivalence relations (S5), this is no longer the case for the abstractions: in the middle abstraction, the *must* relations can be seen to be non-symmetric, and in the right abstraction, the relation labelled  $A$  is no longer transitive (in general the union of two equivalence relations is not necessarily transitive)<sup>7</sup>.

## 7.5 Conclusion and Future work

We have developed an abstraction framework for KMLTSs, which allows us to verify properties that involves public announcements on smaller abstract models instead of on big concrete models. We demonstrate the use of our framework by looking at the example of Muddy Children. Another example of abstracting a model for encoded broadcast can be found in [DOW08].

The theoretical novelty of this chapter is the extension of traditional abstraction techniques to both the label and proposition mappings and to a logic containing dynamic modalities (*public announcements*) which change the models. Both features are of fundamental importance in (epistemic) modelling and verification, which is the main motivation of our work. In order to incorporate the full power of dynamic epistemic modelling, more research is needed on integrating general update constructions as formalized by action models [BM04]. The abstraction of action models is also useful, as it is shown in [DW07] that the action models can be quite large when modelling protocols. Another goal is to adapt this framework to Interpreted Systems [FHMV95], which combines both epistemic and temporal characteristics.

On a practical side, our framework opens a way to dynamic epistemic verification of large or even infinite models. Future research should be dedicated to practical problems like generating abstract models automatically from formal, but compact, model specifications [CG]<sup>+</sup>03].

---

<sup>7</sup>From Theorem 7.3.5, the truth values of some S5 axioms are  $\uparrow$  rather than *true* in the non-S5 abstractions of this example.