Refinement of Kripke Models for Dynamics

Francien Dechesne[1], Simona Orzan[1], and Yanjing Wang[2]

[1] Department of Computer Science, Eindhoven University of Technology, P.O. Box 513, NL-5600MB, Eindhoven, The Netherlands
[2] Centrum voor Wiskunde en Informatica, P.O. Box 94079, NL-1090 GB Amsterdam, The Netherlands

Abstract. We propose a property-preserving refinement/abstraction theory for Kripke Modal Labelled Transition Systems incorporating not only state mapping but also label and proposition lumping, in order to have a compact but informative abstraction. We develop a 3-valued version of Public Announcement Logic (PAL) which has a dynamic operator that changes the model in spirit of public broadcasting. It is proven that the refinement relation of *static* models assures us to safely check any *dynamic* properties in terms of PAL-formulas on the abstraction of a model. The theory is in particular interesting and applicable for an epistemic setting as the example of the Muddy Children puzzle shows, especially in the view of the growing interest for epistemic modelling and (automatic) verification of communication protocols.

1 Introduction

Epistemic logics are modal logics for reasoning about knowledge, traditionally used to describe the distribution of information between parties in communication acts. Recently, these logics have become interesting also from a more practical perspective, i.e. for modelling knowledge development during communication protocols, by the addition of dynamics: mathematical constructions that enable to reason about knowledge and information *change* [8, 1, 2]. Methods based on epistemic logics have been developed for the analysis of complex communication protocols: e.g. BAN logic [4], the theory of function views [13] and interpreted systems [8, 10, 19]. These approaches are also more and more tool-supported, and interesting protocol properties are assessed or discarded by (automatic) model checking [11, 19, 22].

The structures on which epistemic formulas can be evaluated are Kripke models as in usual modal logic, but often with many labels representing different agents' uncertainties. Inevitably, when epistemic modelling is applied to complex situations, very large epistemic models can be expected. One way to deal with it is to import the refinement and abstraction techniques developed for labelled transition systems (LTS), e.g. [16, 15, 20], where two types of approximations of the transitions are introduced in the model in order to have an informative abstraction of the original model. The 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 labelled differently that might be similar to each other — for instance if they express uncertainties of agents playing similar roles in an multi-agent system. Another specific characteristic of epistemic Kripke models is that in modelling practical situations, numerous different basic propositions might be used. We may expect to lump some of those transitions with different labels or combine states with different propositional valuations to obtain a more compact abstraction. However, the traditional LTS abstraction techniques do not perform this type of reductions, so an adaptation is needed. Moreover, when we include the dynamic modalities, which essentially change the model, into the language (e.g the announcements or actions see [8, 1, 12, 7]), it is a challenge to adapt the LTS abstraction theory such that a suitable abstraction relation on the concrete model will make sure that it is safe to check dynamic formulas on the abstract model.

In this paper, based on *Kripke Modal Labelled Transition Systems* (KMLTSs), we propose a refinement theory incorporating not only state mapping but also label and proposition lumping, in order to have a compact but informative abstraction. We develop a 3-valued Public Announcement Logic (PAL) and prove that the refinement relation of *static* models *can* assure us to safely check any *dynamic* properties in terms of PAL-formulas on the abstractions of a KMLTS model. Thus the theory can be used to abstract Kripke models, since Kripke models can be regarded as a special case of KMLTS. This theory is in particular applicable for an epistemic setting as the example of the Muddy Children shows.

In the flourishing field of abstraction techniques there is so far, to the best of our knowledge, no work on the abstraction of Kripke models that can reduce both the number of labels and basic propositions. The closest related literature to the current paper is a work on abstraction of LTSs [20] in which the labels could be grouped. Since both temporal and knowledge properties can be expressed using box- and diamond modalities of modal languages, model checkers on LTSs are sometimes employed to verify epistemic properties [11, 19, 22]. However, LTS abstractions were never used in this context. A complementary technique for escaping the epistemic explosion problem is symbolic model checking discussed in [17].

Section 2 introduces Kripke Modal Labelled Transition Systems, together with a 3-valued interpretation of PAL. In Section 3, the notions of refinement and abstraction are introduced and the preservation results are proven. Section 4 contains two examples of applying abstraction to some real epistemic models. We conclude in Section 5.

2 Preliminaries

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

2.1 Kripke Modal Labelled Transition System

A standard Kripke model consists of a set of states S, the labelled relations R among them and a 2-valued valuation V which assigns the truth value for each basic proposition on each state[3]. 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 $\perp$ 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* [16], where *must* transitions are under-approximations (the relations are necessarily there in the concrete model) and *may* for over-approximations (there are possibly such relations). Since necessarily existent relations should be at least possible, we require that the *must* relations are included in the *may* relations.

Formally, similar to the definition of Kripke Modal Transition Systems in [14, 9], we have:

Definition 1 (Kripke Modal Labelled Transition System). *A Kripke Modal Labelled Transition System (KMLTS) is a tuple* $\mathcal{M} = (I, P; S, \rightarrow_{\diamond}, \rightarrow_{\Box}, V)$ *where:*

- I *is a non-empty set of labels;*
- P *is a set of basic propositions;*
- S *is a non-empty set of states;*
- $\rightarrow_{\diamond}$ *is a set of transitions of the form* $s \xrightarrow{i}_{\diamond} s'$ *where* $i \in I$*;*
- $\rightarrow_{\Box}$ *is a set of transitions of the form* $s \xrightarrow{i}_{\Box} s'$ *where* $i \in I$*;*
- V *is a valuation function:* $V : S \rightarrow \{true, false, \perp\}^P$.

We require that $\rightarrow_{\Box} \subseteq \rightarrow_{\diamond}$ *. We call* (I, P) *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 signature (I, P) in the specifications of models since in the following we will use models of different signatures.

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

Definition 2 (Concrete model). *A KMLTS* $\mathcal{M} = (I, P; S, \rightarrow_{\diamond}, \rightarrow_{\Box}, V)$ *is a concrete model if:*

- $\rightarrow_{\diamond} = \rightarrow_{\Box}$;
- *for all* $s \in S$*, all* $p \in P : V(s)(p) \neq \perp$.

[3] In an epistemic setting, the states (also called "possible worlds") are interpreted as states of affairs that may be considered possible by agents: an i-relation from one state to other means that at the first state agent i considers the second possible.

2.2 Public announcement Logic

Public Announcement Logic initiated in [18] is a convenient language to describe announcements and their informational consequences for (a group of) agents. Based on the standard language of epistemic logic (logic of knowledge), a new modality $[\psi]$ is introduced into the language, with $[\psi]\phi$ intended to express "*if ψ is true then after the announcement of ψ, ϕ is true.*". Various case studies showed 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 (we refer interested readers to [21] for detailed explanations).

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

$$\varphi ::= p \mid \varphi \wedge \varphi \mid \neg\varphi \mid \Box_i\varphi \mid [\chi]\phi$$

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

As usual, we define $\phi \vee \psi$, $\phi \to \psi$ and $\Diamond_i\phi$ as the abbreviations of $\neg(\neg\phi \wedge \neg\psi)$, $\neg\phi \vee \psi$ and $\neg\Box_i\neg\phi$ respectively.

Here we do not fix the interpretation of $\Box$ to be "knowledge", since our approach does not require the model to be $S5$.[4] As we will see in the next section, the overall approach is not constrained to be used only in epistemic settings (reasoning about knowledge).

2.3 Semantics

The semantics for 2-valued public announcement logic is the extension of standard modal logic with $[\psi]$ as a "*relativization operator*", meaning: $\mathcal{M}, s \vDash [\psi]\phi \iff [\mathcal{M}, s \vDash \psi$ implies $\mathcal{M}|_\psi, s \vDash \phi]$, where $\mathcal{M}|_\psi$ is the restriction of $\mathcal{M}$ on the states where ψ holds. We extend such relativization to the 3-valued case and take the usual semantics for $\Box$ as in the logics on Modal Transition Systems:

Definition 3 (3-valued Semantics). *The truth value of a $\mathcal{L}_{I,P}$ formula ϕ in a state s of a KMLTS $\mathcal{M} = (I, P; S \to_\Diamond, \to_\Box, V)$, written $[\![\phi]\!]^{\mathcal{M},s}$, is defined as follows:*

[4] $S5$ is a set of axioms characterizing models in which the relations are equivalence relations. Not constrained within $S5$ models, we will have more freedom to find the most suitable abstractions as we will see in the Muddy Children example.

$$
\begin{array}{rcl}
[\![p]\!]^{\mathcal{M},s} & = & V(s)(p) \\
[\![\neg\psi]\!]^{\mathcal{M},s} & = & \neg_3 [\![\psi]\!]^{\mathcal{M},s} \\
[\![\psi_1 \wedge \psi_2]\!]^{\mathcal{M},s} & = & [\![\psi_1]\!]^{\mathcal{M},s} \wedge_3 [\![\psi_2]\!]^{\mathcal{M},s} \\
[\![\Box_i\psi]\!]^{\mathcal{M},s} & = & \begin{cases} \mathit{true} & \mathit{if}\ \forall s' : s \xrightarrow{i}_{\Diamond} s' \implies [\![\psi]\!]^{\mathcal{M},s'} = \mathit{true} \\ \mathit{false} & \mathit{if}\ \exists s' : s \xrightarrow{i}_{\Box} s'\ \mathit{and}\ [\![\psi]\!]^{\mathcal{M},s'} = \mathit{false} \\ \bot & \mathit{otherwise} \end{cases} \\
[\![[\phi]\psi]\!]^{\mathcal{M},s} & = & \begin{cases} \mathit{true} & \mathit{if}\ [\![\phi]\!]^{\mathcal{M},s} = \mathit{false}\ \mathit{or}\ [\![\psi]\!]^{\mathcal{M}|_\phi,s} = \mathit{true} \\ \mathit{false} & \mathit{if}\ [\![\phi]\!]^{\mathcal{M},s} = \mathit{true}\ \mathit{and}\ [\![\psi]\!]^{\mathcal{M}|_\phi,s} = \mathit{false} \\ \bot & \mathit{otherwise} \end{cases}
\end{array}
$$

where:

- $\neg_3(\mathit{true}) = \mathit{false}, \neg_3(\mathit{false}) = \mathit{true}$ *and* $\neg_3(\bot) = \bot$, *and for any* $x, y \in \{\mathit{true}, \mathit{false}, \bot\}$: $x \wedge_3 y = \mathit{min}(x, y)$ *w.r.t.* $\leq_v$: $\mathit{false} \leq_v \bot \leq_v \mathit{true}$.
- $\mathcal{M}|_\phi = (I, P; S' \rightarrow'_\Diamond, \rightarrow'_\Box, V')$ *is defined as follows:*
  - $S' = \{s \in S \mid [\![\phi]\!]^{\mathcal{M},s} \neq \mathit{false}\}$;
  - $\rightarrow'_\Diamond = \rightarrow_\Diamond |_{S' \times S'}$;
  - $\rightarrow'_\Box = \rightarrow_\Box \cap (S' \times \{s \in S' \mid [\![\phi]\!]^{\mathcal{M},s} = \mathit{true}\})$;
  - $V'(s) = V(s)$ *for* $s \in S'$.

The intuitive idea behind the semantics of $\Box$ is that $\Box\phi$ is true if all the possible (*may*) relations lead to ϕ-true states, and is false if there exists a necessary (*must*) relation leading to a ϕ-false state. The relativization w.r.t. ϕ keeps all ϕ-*not-false* states and all the relations among them, except for the *must* relations directed at a ϕ-*not-true* state.

Although our concern in this paper is primarily to develop the theory of epistemic abstrcations, 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 KLMTSs, 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 [3], it is to expect that such a model checking algorithm will not be more complex than the ones for checking (2-valued) PAL on KMs or LTSs.

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

$$[\![\phi]\!]^{\mathcal{M},s} = \mathit{true} \iff \mathcal{M}', s \vDash \phi \qquad [\![\phi]\!]^{\mathcal{M},s} = \mathit{false} \iff \mathcal{M}', s \nvDash \phi$$

where $\mathcal{M}'$ is the standard Kripke model converted from $\mathcal{M}$ by lumping *may* and *must* relations together. For 2-valued Public Announcement Logic the following reduction axioms hold:

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

In the 3-valued case, there are a few cases where the left hand side of $\leftrightarrow$ gives *false* while the right hand side gives $\perp$, all involving the valuation of ϕ to be $\perp$. So if we only consider concrete models then the evaluation of ϕ is either *true* or *false* and the above equivalences hold.

3 Refinement and Logical Characterization

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

3.1 Refinement and Abstraction

As observed in [20], one can use abstraction to reduce the number of labels in infinitely-labelled systems, and obtain a model checkable abstract model. It is also intuitive to lump similar transitions with different labels together to a unified one. In epistemic modelling, the labels denote the corresponding agents' uncertainties and in many cases several agents play a similar role. We aim for an abstraction method that can reduce the labels even if there are finitely many of them. On the other hand, different propositions may also have a similar role on different states. A compact abstraction may combine propositions together as well. In the following, we use two mappings from one signature to the other to capture the above intuitions of lumping labels and propositions. It is crucial to note that the abstraction of a model may have a different signature.

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

Definition 4 (Refinement and Abstraction). *Given two KMLTSs $\mathcal{M} = (I, P; S, \rightarrow_\Diamond, \rightarrow_\Box, V)$ and $\mathcal{N} = (I', P'; T, \rightarrow'_\Diamond, \rightarrow'_\Box, V')$ 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 $p \in P : V(s)(p) \neq \perp$ 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 $R(t', s')$;*
- *$s \xrightarrow{i}_\Box s'$ implies $\forall i' \in f^{-1}[i] : \exists t' \in T$ such that $t \xrightarrow{i'}_\Box t'$ and $R(t', s')$.*

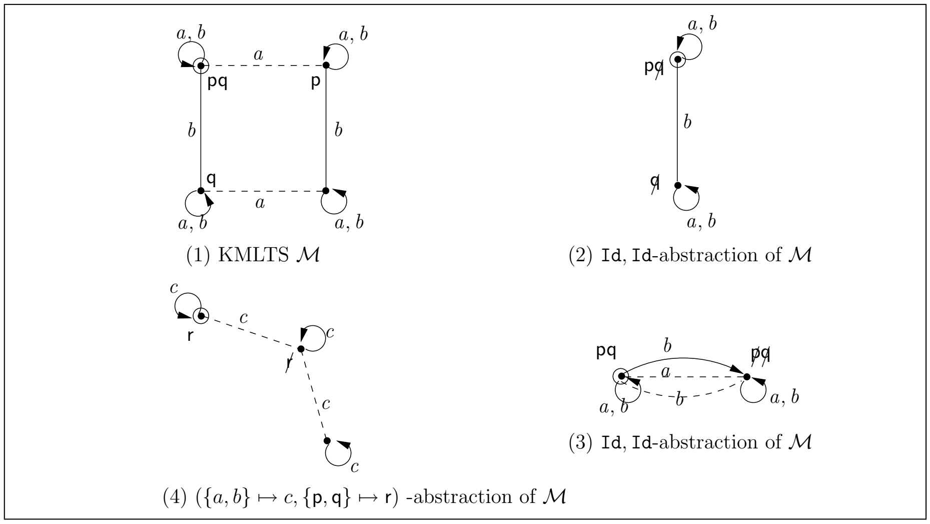

Fig. 1. A pointed KMLTS and three possible abstractions of it. Dot lines are for *may* relations and solid lines for *must*. *May* relations that coincide with corresponding *must* ones are omitted. If there is no arrow on a relation then it is bidirectional. $\not p$ is to mean the value of p is $\bot$ at current state. In (2), the mappings are the identity functions, and the valuation of proposition q is mapped to $\bot$ for all worlds. In (3), the abstraction is given by the identity functions as well, but collapsing different worlds. In (4), there's an abstraction obtained by collapsing both agents and both propositions.

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

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

The first condition says that the valuation in the more abstract model can be less informative in terms of making some proposition $\bot$ but never unfaithful. The intuition behind the requirement of *must* is that i-*must* relation in the more abstract model is more like an "intersection" of corresponding i'-*must* for $i' \in f^{-1}[i]$. For *may*, an $f(i')$-*may* relation in the more abstract model is like a "union" of those i''-*may* relations in the more refined model where $f(i'') = f(i')$.

Note that for two 2-valued Kripke models with the same signature (I, P), $\mathcal{N}$ is a refinement of $\mathcal{M}$ in the classical sense of [15] iff $\mathcal{N}$ is an $(Id_I, Id_P)-$refinement of $\mathcal{M}$ where Id_X is identity function on the domain X.

Fig. 1 shows an example of a KMLTS $\mathcal{M}$ and some abstractions of it.

Since $\rightarrow_\Box \subseteq \rightarrow'_\Diamond$, we can turn a KMLTS into a concrete refinement of itself by deleting all the $\rightarrow_\Diamond$ relations that does not have a $\rightarrow_\Box$ counterpart and by adapting the valuation to become two-valued (e.g. by defining $V'(s)(p) = \mathit{false}$ whenever $V(s)(p) = \bot$ and $V'(s)(p) = V(s)(p)$ otherwise). Therefore:

Proposition 1. *A KMLTS $\mathcal{M}$ always has a concrete refinement.*

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 refinement relation, we need to check different formulas on these two models. Given two pointed models $(\mathcal{M}, s)$ and $(\mathcal{N}, t)$, two formulas ϕ and ψ we say $[\![\psi]\!]^{\mathcal{M},s} \leq [\![\phi]\!]^{\mathcal{N},t}$ if the following hold:

1. $[\![\psi]\!]^{\mathcal{M},s} = \mathit{true} \implies [\![\phi]\!]^{\mathcal{N},t} = \mathit{true}$;
2. $[\![\psi]\!]^{\mathcal{M},s} = \mathit{false} \implies [\![\phi]\!]^{\mathcal{N},t} = \mathit{false}$.

Then our goal is to check whether $\mathcal{N}, t \Subset_{f,g} \mathcal{M}, s$ implies for all ϕ:$[\![\ulcorner\phi\urcorner]\!]^{\mathcal{M},s} \leq [\![\phi]\!]^{\mathcal{N},t}$ where $\ulcorner\phi\urcorner$ is the corresponding formula of ϕ. To pinpoint the right formulas to check, we introduce the following translation:

Definition 5 (Translation of formulas). *Given signatures $(I', P'), (I, P)$, and surjective functions $f : I' \to I$ and $g : P' \to P$, we define the translation of an $\mathcal{L}_{I',P'}$-formula ϕ into an $\mathcal{L}_{I,P}$-formula $\ulcorner\phi\urcorner_{f,g}$ inductively as follows:*

$$\begin{array}{lcl}
\ulcorner p'\urcorner_{f,g} & = & g(p') \\
\ulcorner\neg\psi\urcorner_{f,g} & = & \neg\ulcorner\psi\urcorner_{f,g} \\
\ulcorner\psi_1 \wedge \psi_2\urcorner_{f,g} & = & \ulcorner\psi_1\urcorner_{f,g} \wedge \ulcorner\psi_2\urcorner_{f,g} \\
\ulcorner\Box_{i'}\psi\urcorner_{f,g} & = & \Box_{f(i')}\ulcorner\psi\urcorner_{f,g} \\
\ulcorner[\chi]\psi\urcorner_{f,g} & = & [\ulcorner\chi\urcorner_{f,g}]\ulcorner\psi\urcorner_{f,g}
\end{array}$$

Before proving the main result of this paper, we first prove a result establishing the refinement relation between the updated models $\mathcal{N}|_\chi, t$ and $\mathcal{M}|_\chi, s$ if $\mathcal{N}, t \Subset_{f,g} \mathcal{M}, s$ where χ is a $\mathcal{L}_{I,P}$-formula.

Lemma 1. *Suppose $(\mathcal{N}, t), (\mathcal{M}, s)$ are two pointed KMLTSs with signatures (I', P') and (I, P) and set of states T and S respectively. For any $\mathcal{L}_{I',P'}$ formula χ such that $t \in \mathcal{N}|\chi$ and $s \in \mathcal{M}|_{\ulcorner\chi\urcorner_{f,g}}$ we have $\mathcal{N}|_\chi, t \Subset_{f,g} \mathcal{M}|_{\ulcorner\chi\urcorner_{f,g}}, s$ if for each $t' \in T, s' \in S$ the following condition holds:*

$$\mathcal{N}, t' \Subset_{f,g} \mathcal{M}, s' \implies [\![\ulcorner\chi\urcorner_{f,g}]\!]^{\mathcal{M},s'} \leq [\![\chi]\!]^{\mathcal{N},t'} \qquad (\star)$$

Proof. Suppose $\mathcal{N}, t \Subset_{f,g} \mathcal{M}, s$ then there is a relation R which constitutes an f, g-refinement between $\mathcal{N}$ and $\mathcal{M}$ with $(t, s) \in R$. We claim that $R' = R \cap (\mathcal{N}|_\chi \times \mathcal{M}|_{\ulcorner\chi\urcorner_{f,g}})$ is an f, g-refinement 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 refinement relation:

- for the condition on p: follows from this property of R and the fact that the update does not change valuations of the propositions.
- Suppose $t \xrightarrow{i'}_{\Diamond} t'$ in $\mathcal{N}|_{\chi}$, then according to the definition of the update $t \xrightarrow{i'}_{\Diamond} t'$ in $\mathcal{N}$. Since $\mathcal{N}, t \Subset_{f,g} \mathcal{M}, s$, there exists $s' \in \mathcal{M}$: $s \xrightarrow{f(i')}_{\Diamond} s'$ and $(t', s') \in R$. We only need to show that $s' \in \mathcal{M}|_{\ulcorner\chi\urcorner_{f,g}}$. Suppose not, then $[\![\ulcorner\chi\urcorner_{f,g}]\!]^{\mathcal{M},s'} = \textit{false}$. Due to condition $(\star)$, $[\![\chi]\!]^{\mathcal{N},t'} = \textit{false}$, but then $t' \notin \mathcal{N}|_{\chi}$, contradiction.
- Suppose $s \xrightarrow{i}_{\Box} s'$ in $\mathcal{M}|_{\ulcorner\chi\urcorner_{f,g}}$, then $[\![\ulcorner\chi\urcorner_{f,g}]\!]^{\mathcal{M},s'} = \textit{true}$ and $s \xrightarrow{i'}_{\Box} s'$ in $\mathcal{M}$. Since $\mathcal{N}, t \Subset_{f,g} \mathcal{M}, s$, for any $i' \in f^{-1}[i]$ there exists $t' \in \mathcal{N}$ such that $t \xrightarrow{i'}_{\Box} t'$ and $(t', s') \in R$. We only need to show that for each such $t' : t' \in \mathcal{N}|_{\chi}$. Since $[\![\ulcorner\chi\urcorner_{f,g}]\!]^{\mathcal{M},s'} = \textit{true}$, by condition $(\star)$ $[\![\chi]\!]^{\mathcal{N},t'} = \textit{true}$. Therefore, $t' \in \mathcal{N}|_{\chi}$ by the definition of $\mathcal{N}|_{\chi}$.

Theorem 1. *Suppose $\mathcal{N}, \mathcal{M}$ are KMLTSs w.r.t. I', P' and I, P respectively. s and t are two worlds in $\mathcal{M}$ and $\mathcal{N}$ respectively. Then $\mathcal{N}, t \Subset_{f,g} \mathcal{M}, s$ implies for all $\phi \in \mathcal{L}_{I',P'} : [\![\ulcorner\phi\urcorner_{f,g}]\!]^{\mathcal{M},s} \leq [\![\phi]\!]^{\mathcal{N},t}$.*

Proof. We prove the theorem by induction on the structure of ϕ :

- $\phi = p'$: trivial, follows from the first condition of the definition of refinement.
- $\phi = \neg\psi$: suppose $[\![\ulcorner\phi\urcorner_{f,g}]\!]^{\mathcal{M},s} = \textit{true}$ then according to the semantics $[\![\ulcorner\psi\urcorner_{f,g}]\!]^{\mathcal{M},s} = \textit{false}$. Thus by induction hypothesis $[\![\psi]\!]^{\mathcal{N},t} = \textit{false}$. Therefore $[\![\phi]\!]^{\mathcal{N},t} = \textit{true}$. For the case $[\![\ulcorner\phi\urcorner_{f,g}]\!]^{\mathcal{M},s} = \textit{false}$, similar.
- $\phi = \psi_1 \wedge \psi_2$:
  - suppose $[\![\ulcorner\phi\urcorner_{f,g}]\!]^{\mathcal{M},s} = \textit{true}$ then according to the semantics $[\![\ulcorner\psi_1\urcorner_{f,g}]\!]^{\mathcal{M},s} = \textit{true}$ and $[\![\ulcorner\psi_2\urcorner_{f,g}]\!]^{\mathcal{M},s} = \textit{true}$. Thus by induction hypothesis $[\![\psi_1]\!]^{\mathcal{N},t} = \textit{true}$ and $[\![\psi_2]\!]^{\mathcal{N},t} = \textit{true}$. Therefore $[\![\phi]\!]^{\mathcal{N},t} = \textit{true}$.
  - suppose $[\![\ulcorner\phi\urcorner_{f,g}]\!]^{\mathcal{M},s} = \textit{false}$ then according to the semantics either $[\![\ulcorner\psi_1\urcorner_{f,g}]\!]^{\mathcal{M},s} = \textit{false}$ or $[\![\ulcorner\psi_2\urcorner_{f,g}]\!]^{\mathcal{M},s} = \textit{false}$. Without loss of generality, suppose the latter. Thus by induction hypothesis $[\![\psi_2]\!]^{\mathcal{N},t} = \textit{false}$. Therefore $[\![\phi]\!]^{\mathcal{N},t} = \textit{false}$.
- $\phi = \Box_{i'}\psi$: then $\ulcorner\phi\urcorner_{f,g} = \Box_{f(i')}\ulcorner\psi\urcorner_{f,g}$.
  - suppose $[\![\ulcorner\phi\urcorner_{f,g}]\!]^{\mathcal{M},s} = \textit{true}$ then according to the semantics for all s' with $s \xrightarrow{f(i')}_{\Diamond} s'$ we have $[\![\ulcorner\psi\urcorner_{f,g}]\!]^{\mathcal{M},s'} = \textit{true}$. Suppose in $\mathcal{N}$ there is a world t' such that $t \xrightarrow{i'}_{\Diamond} t'$ then according to the definition of refinement, there is a $s'' \in \mathcal{M}$ such that $s \xrightarrow{f(i')}_{\Diamond} s''$ and $\mathcal{N}, t' \Subset_{f,g} \mathcal{M}, s''$. Thus $[\![\ulcorner\psi\urcorner_{f,g}]\!]^{\mathcal{M},s''} = \textit{true}$. By induction hypothesis, $[\![\psi]\!]^{\mathcal{N},t'} = \textit{true}$. Therefore $[\![\Box_{i'}\psi]\!]^{\mathcal{N},t} = \textit{true}$.
  - suppose $[\![\ulcorner\phi\urcorner_{f,g}]\!]^{\mathcal{M},s} = \textit{false}$ then according to the semantics, there is s' with $s \xrightarrow{f(i')}_{\Box} s'$ such that $[\![\ulcorner\psi\urcorner_{f,g}]\!]^{\mathcal{M},s} = \textit{false}$. By definition of refinement, for any $i'' \in f^{-1}[f(i')]$ there is a $t' \in \mathcal{N}$ such that $t \xrightarrow{i''}_{\Box} t'$ and $\mathcal{N}, t' \Subset_{f,g} \mathcal{M}, s'$. By induction hypothesis, for all such $t' : [\![\psi]\!]^{\mathcal{N},t'} = \textit{false}$. Thus for all $i'' \in f^{-1}[f(i')] : [\![\Box_{i''}\psi]\!]^{\mathcal{N},t} = \textit{false}$. In particular: $[\![\Box_{i'}\psi]\!]^{\mathcal{N},t} = \textit{false}$.

- $\phi = [\chi]\psi$
  - suppose $[\![\ulcorner\phi\urcorner_{f,g}]\!]^{\mathcal{M},s} = \mathit{true}$ then $[\![\ulcorner\chi\urcorner_{f,g}]\!]^{\mathcal{M},s} = \mathit{false}$ or $[\![\ulcorner\psi\urcorner_{f,g}]\!]^{\mathcal{M}|_{\ulcorner\chi\urcorner_{f,g}},s} = \mathit{true}$. If $[\![\ulcorner\chi\urcorner_{f,g}]\!]^{\mathcal{M},s} = \mathit{false}$ then $[\![\chi]\!]^{\mathcal{N},t} = \mathit{false}$ according to induction hypothesis. Thus $[\![\phi]\!]^{\mathcal{N},t} = \mathit{true}$. If $[\![\ulcorner\chi\urcorner_{f,g}]\!]^{\mathcal{M},s} \neq \mathit{false}$ and $[\![\ulcorner\psi\urcorner_{f,g}]\!]^{\mathcal{M}|_{\ulcorner\chi\urcorner_{f,g}},s} = \mathit{true}$ then $s \in \mathcal{M}|_{\ulcorner\chi\urcorner_{f,g}}$. Now suppose $[\![\chi]\!]^{\mathcal{N},t} \neq \mathit{false}$ then $t \in \mathcal{N}|_\chi$. We need to show that $[\![\psi]\!]^{\mathcal{N}|_\chi,t} = \mathit{true}$. By induction hypothesis $\mathcal{N},t' \Subset_{f,g} \mathcal{M},s' \implies [\![\ulcorner\chi\urcorner_{f,g}]\!]^{\mathcal{M},s'} \leq [\![\chi]\!]^{\mathcal{N},t'}$ for each $s' \in S, t' \in T$. Therefore from Lemma 1 we have $\mathcal{N}|_\chi, t \Subset_{f,g} \mathcal{M}|_{\ulcorner\chi\urcorner_{f,g}}, s$. By induction hypothesis, $[\![\psi]\!]^{\mathcal{N}|_\chi,t} = \mathit{true}$. Thus $[\![\phi]\!]^{\mathcal{N},t} = \mathit{true}$.
  - suppose $[\![\ulcorner\phi\urcorner_{f,g}]\!]^{\mathcal{M},s} = \mathit{false}$ then $[\![\ulcorner\chi\urcorner_{f,g}]\!]^{\mathcal{M},s} = \mathit{true}$ and $[\![\ulcorner\psi\urcorner_{f,g}]\!]^{\mathcal{M}|_{\ulcorner\chi\urcorner_{f,g}},s} = \mathit{false}$. Since $[\![\ulcorner\chi\urcorner_{f,g}]\!]^{\mathcal{M},s} = \mathit{true}$ then $[\![\chi]\!]^{\mathcal{N},t} = \mathit{true}$ by induction hypothesis. We only need to show $[\![\psi]\!]^{\mathcal{N}|_\chi,s} = \mathit{false}$. It is clear that $t \in \mathcal{N}|_\chi$ and $s \in \mathcal{M}|_{\ulcorner\chi\urcorner_{f,g}}$, then from induction hypothesis the condition of Lemma 1 holds, it follows that $\mathcal{N}|_\chi, t \Subset_{f,g} \mathcal{M}|_{\ulcorner\chi\urcorner_{f,g}}, s$. Thus from induction hypothesis we have $[\![\psi]\!]^{N|_\chi,t} = \mathit{false}$. Therefore according to the semantics, $[\![\phi]\!]^{\mathcal{N},t} = \mathit{false}$.

Corollary 1. *Suppose $(\mathcal{N},t),(\mathcal{M},s)$ are two pointed KMLTSs w.r.t. (I',P') and (I,P) respectively. If $\mathcal{N},t \Subset_{f,g} \mathcal{M},s$ and $\mathcal{N}$ is a Kripke model converted from a concrete KMLTS then for any formula $\phi \in \mathcal{L}_{I',P'}$:*

- $[\![\ulcorner\phi\urcorner_{f,g}]\!]^{\mathcal{M},s} = \mathit{true} \implies \mathcal{N},t \vDash \phi$
- $[\![\ulcorner\phi\urcorner_{f,g}]\!]^{\mathcal{M},s} = \mathit{false} \implies \mathcal{N},t \vDash \neg\phi$

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

To justify the logical characterization, we prove the converse of Theorem 1.

Theorem 2. *Suppose $(\mathcal{N},t)$ and $(\mathcal{M},s)$ are two pointed KMLTS models w.r.t. I',P' and I,P respectively that enjoy image finiteness, that is there are at most finitely many successors of a certain state w.r.t to transitions labelled the same. If for every formula $\phi \in \mathcal{L}_{I',P'}$: $[\![\ulcorner\phi\urcorner_{f,g}]\!]^{\mathcal{M},s} \leq [\![\phi]\!]^{\mathcal{N},t}$ then $\mathcal{N},t \Subset_{f,g} \mathcal{M},s$.*

Proof. Let $R = \{(t',s') \mid \text{for every } \phi : [\![\ulcorner\phi\urcorner_{f,g}]\!]^{\mathcal{M},s'} \leq [\![\phi]\!]^{\mathcal{N},t'}\}$. We claim that R is a refinement relation between $\mathcal{M}$ and $\mathcal{N}$. Clearly $(t,s) \in R$. Now we check the 3 conditions of refinement relations:

- for the condition on valuations of s and t: obvious, since $[\![\ulcorner p\urcorner_{f,g}]\!]^{\mathcal{M},s} \leq [\![p]\!]^{\mathcal{N},t}$.
- suppose towards contradiction that $\exists t' : t \xrightarrow{i'}_\diamond t'$ in $\mathcal{N}$ but for any $s' \in S$: $s \xrightarrow{f(i')}_\diamond s'$ 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'_i, since $(t',s'_i) \notin R$ then there is a formula $\psi_{s'_i}$ such that $[\![\ulcorner\psi_{s'_i}\urcorner_{f,g}]\!]^{\mathcal{M},s'_i} = \mathit{true}$ but $[\![\psi_{s'_i}]\!]^{\mathcal{N},t'} \neq \mathit{true}$[5].Note that $\Box_{f(i')}(\bigvee_0^n \ulcorner\psi_{s'_i}\urcorner_{f,g})$ is *true* at s but $\Box_{i'}(\bigvee_0^n \psi_{s'_i})$ is not *true* at t, contradictory to the assumption that $(t,s) \in R$.

[5] If $[\![\ulcorner\psi_{s'_i}\urcorner_{f,g}]\!]^{\mathcal{M},s'} = \mathit{false}$ but $[\![\psi_{s'_i}]\!]^{\mathcal{N},t'} \neq \mathit{false}$ then $[\![\ulcorner\neg\psi_{s'_i}\urcorner_{f,g}]\!]^{\mathcal{M},s'} = \mathit{true}$ but $[\![\neg\psi_{s'_i}]\!]^{\mathcal{N},t'} \neq \mathit{true}$.

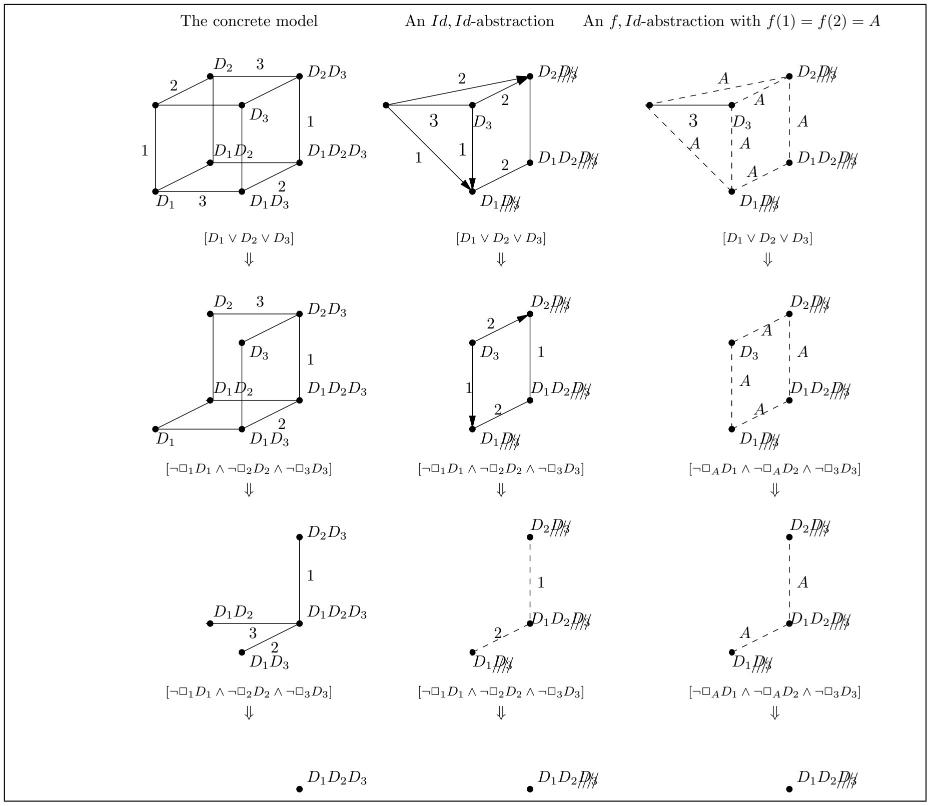

Fig. 2. Abstraction of the Muddy Children for $n = 3$ children. Each world has reflexive *may*-relations for each $i \in I$, some have reflexive *must*-relations, but for simplicity of presentation, all reflexive relations are omitted; $\not{D_3}$ means proposition D_3 has valuation $\perp$ in the current state.

- suppose towards contradiction that $\exists s' : s \xrightarrow{f(i')}_\Box s'$ in $\mathcal{M}$ but for some $i'' \in f^{-1}[f(i')]$ any $t' \in T$: $t \xrightarrow{i''}_\Box t'$ implies $(t', s') \notin R$. According to image finiteness, we have only finitely many such t', call them $t'_0 \dots t'_n$. For each t'_i, since $(t', s'_i) \notin R$ then there is a formula $\psi_{t'_i}$ such that $[\![\ulcorner \psi_{t'_i} \urcorner_{f,g}]\!]^{\mathcal{M},s'} =$ *false* but $[\![\psi_{t'_i}]\!]^{\mathcal{N},t'_i} \neq$ *false*. Note that $\Box_{f(i')}(\bigvee_0^n \ulcorner \psi_{t'_i} \urcorner_{f,g})$ is *false* at s but $\Box_{i''}(\bigvee_0^n \psi_{t_i})$ is not *false* at t, contradictory to the assumption that $(t, s) \in R$.

4 Examples

4.1 The Muddy Children

A standard example demonstrating the effect of updates on the knowledge within a group of agents, is the epistemic modelling of the Muddy Children Puzzle (cf. the seminal work on reasoning about knowledge [8]). The setting is as follows: out of n children, $k > 1$ 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, you should step forward." If nobody steps forward, he orders again: "If you now know you are dirty, step forward." After exactly k requests to step forward, the k dirty children suddenly do so (because they are honest and perfect reasoners).

The left column of Fig. 2 shows the standard epistemic model for this setting with three children. Proposition D_i signifies "child i is dirty". After the first update formula ("At least one of you is dirty"), all updates are of the form "nobody knows (yet) he is dirty" (by showing no move). One can check that if only one child is dirty, it will know after the first update. In that case a world satisfying only one D_i is the actual world; from this world in the updated model, child i considers no other worlds possible anymore. If nobody steps forward after the first request (implying nobody knows yet whether he is dirty), and a child sees only one other muddy child, it will know that he himself must be dirty as well (otherwise this other child would have known previously). This is modelled by the fact that after the second update the worlds with only one dirty child disappear in the updated model (they are no longer considered possible by anybody). If then nothing happens (third update), it must be the case that all three are dirty (and everybody knows this).

The middle and right columns of Fig. 2 show abstracted versions of the concrete model on the left. The refinement relation underlying both abstractions relates three pairs of states in the concrete model to three single states in the abstraction (for example, the world with D_2 true and the world with D_2, D_3 true in the concrete model are related to the one world in the abstracted model where D_2 is true and D_3 undefined). 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 D be the abbreviation of the first update $(D_1 \vee D_2 \vee D_3)$ and K be the abbreviation of the next ones $(\neg\Box_1 D_1 \wedge \neg\Box_2 D_2 \wedge \neg\Box_3 D_3)$. Notice the following significant properties can be verified to be true in the two abstractions: (1) In the case all three children are dirty, children 1 and 2 (resp. abstract child A in right-hand side abstraction) will know they are dirty after three updates. Namely $\ulcorner[D][K][K](\Box_1 D_1 \wedge \Box_2 D_2)\urcorner_{f,g}$ is true at the worlds in both abstractions that are corresponding to the world which makes D_1, D_2 and D_3 true in the original model. Thus $[D][K][K](\Box_1 D_1 \wedge \Box_2 D_2)$ is true in that world in the original model. (2) In the case children 1 and 3 are dirty, child 1 will know he is dirty after 2 updates (resp. child A will know child 1 is dirty), and in the case 2 and 3 are dirty, child 2 will know he is dirty after 2 updates (resp. child A will know child 2 is dirty). (3) In the case only child 3 is dirty, he will know after the first announcement. All the above properties in (2) and (3) can be checked in the abstractions. Similar abstractions could be generalized to n children case.

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). [6]

4.2 Encoded broadcast

Consider the following simple situation: a television sender wants to broadcast its programs (i.e., streams of bits) only to paying viewers. Therefore, it distributes a key c to the registered clients indexed $1 \dots n$. Some other unregistered parties, indexed $n+1 \dots n+m$ do not get the key, so they should not get access to the programs. A model of this situation can be seen in Figure 3 (up). b represents the bit currently waiting to be broadcasted, and $\mathsf{b_1} \dots \mathsf{b_{n+m}}$ are the bits located at the sites of the $n+m$ viewers, currently waiting to be set to b's value. In the actual worlds, let us consider that $\mathsf{c} = \mathit{true}$ and $\mathsf{b} = \mathit{true}$. We are interested in

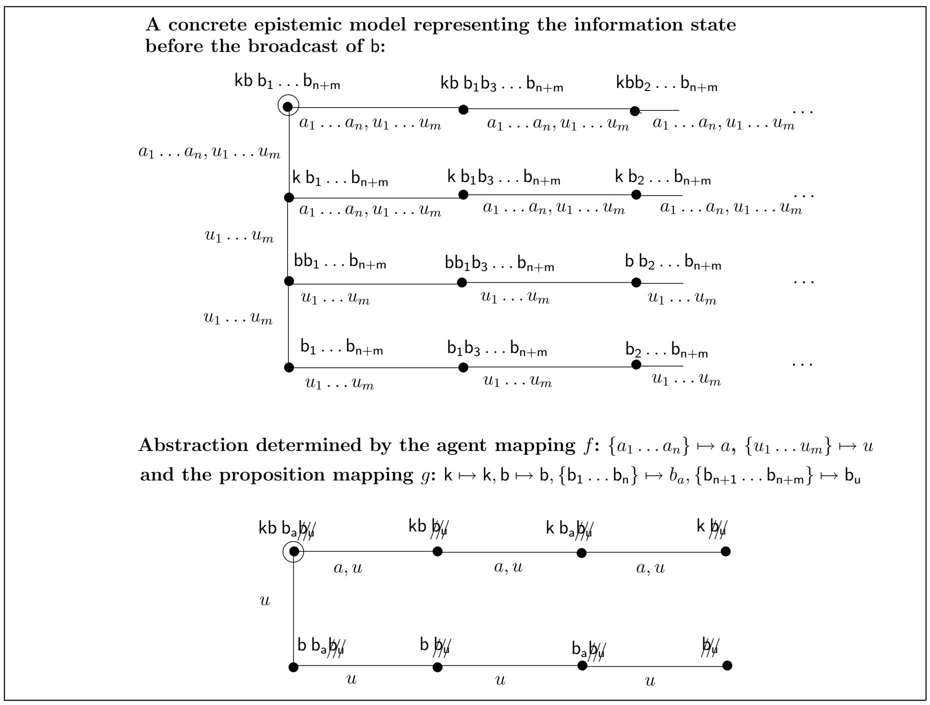

Fig. 3. Epistemic modelling of encoded broadcasting. To keep a clear overview, only a minimal numbers of arrows was drawn; the transitive and reflexive closure of the arrow relation forms the intended equivalence. (up): on each row, the dots stand for a continuation of the sequence of worlds with indistinguishable worlds where the valuations range through all the subsets of $\{b_1 \dots b_{n+m}\}$.

[6] It means some of the axioms for $S5$ are undefined in the non-S5 abstractions of this example.

checking that, after bit b has been broadcasted, (only) the authorized users have received it correctly.

The size of this epistemic model varies obviously with m and n and can be huge, but it is also very regular. The uncertainty relation for every unauthorized agent u_i is the complete graph. Intuitively, this is because such an agent does not hold any information on the value of the key c, of the broadcast bit b or of any of the waiting bits $\mathsf{b_1} \dots \mathsf{b_{n+m}}$. So u_i considers all the valuations as possible. The authorized agents only see as possible the worlds where $\mathsf{c} = \mathit{true}$, since this is the correct value for c and they know it. For the rest of the factual variables, authorized agents do not have any information, so they cannot distinguished further between the worlds with $\mathsf{c} = \mathit{true}$.

A straightforward abstraction of this concrete model can be seen in Figure 3 (down). Broadcasting bit b to the key-holders can be modelled by the public announcement of the formula

$$\beta \equiv \bigwedge_{i \in \{1 \dots n+m\}} \Box_i \mathsf{c} \rightarrow (\mathsf{b} \leftrightarrow \mathsf{b_i}).$$

Translated according to Definition 5 and the two mappings from Figure 3 (down), β becomes $\ulcorner \beta \urcorner_{f,g} \equiv \Box_a \mathsf{c} \rightarrow (\mathsf{b} \leftrightarrow \mathsf{b_a}) \wedge \Box_u \mathsf{k} \rightarrow (\mathsf{b} = \mathsf{b_u})$.

The correct receive property by authorized viewers might be formalized as: forall $i \in \{1 \dots n\}$, $[\beta]\Box_i \mathsf{b_i}$ (since the transmitted bit was *true*). Its translation to the abstract context is $[\ulcorner \beta \urcorner_{f,g}]\Box_a \mathsf{b_a}$, which turns out to be true on the model in Figure 3 (down), therefore, according to Theorem 1, all original formulas are true.

The other desired property is, of course, that unauthorized users will not receive b: forall $i \in \{n+1 \dots n+m\}$, $[\ulcorner \beta \urcorner_{f,g}]\neg\Box_i \mathsf{b_i}$. Due to the globally undefined valuation of $\mathsf{b_u}$, the translation of this formula cannot be established to hold in the abstract model. However, we can verify another convincing formula, $[\ulcorner \beta \urcorner_{f,g}]\neg\Box_u \mathsf{b}$, meaning, again via Theorem 1, that the value of b doesn't leak to the unauthorized agents. Note that *must* relations are needed in order to establish satisfiability of such negative knowledge properties. An interesting observation is that, due to the enormous density of arrows in an epistemic model, *must* relations will occur often enough in abstracted models. This is quite different than the case of LTSs, where by far most relations in abstracted models are of the *may* type.

5 Conclusion

We proposed a refinement/abstraction framework for KMLTSs, which allows reasoning on small coarse abstract models and transfer the results on refined detailed models. In particular, if the concrete Kripke models are epistemic models, interesting knowledge properties are preserved by refinements and abstractions as shown by the Muddy children example.

The theoretical novelty of this work is the extension of traditional abstraction techniques to both the label and proposition mapping, and to a logic containing a dynamic *public announcement* modality. Both features are of fundamental importance in (epistemic) modelling and verification, which constitutes the main motivation of our work. In order to incorporate the full power of dynamic epistemic modelling, more research is needed to integrate general update constructions as formalized by action models [1]. The abstraction of action models is also of our interests, as it is shown in [6]that action models can be of huge size when modelling protocols. It would also be interesting to adapt the framework for Interpreted Systems [8, 19], which combine both epistemic and temporal characteristics.

On a practical side, our framework opens the way to automatic epistemic verification of large or even infinite models. Future research should be dedicated to practical problems like generating abstract models directly from textual or formal, but compact, protocol specifications. A possible starting point is the process algebra language of [5].

Acknowledgement We thank the anonymous referees for their detailed comments. The first and the third authors are supported by Dutch NWO project VEMPS(612.000.528).

References

1. A. Baltag and L.S.Moss. Logics for epistemic programs. *Synthese*, 139(2):165–224, 2004.
2. J. van Benthem, J. van Eijck, and B. Kooi. Logics of communication and change. *Information and Computation*, 2006.
3. G. Bruns and P. Godefroid. Model checking with multi-valued logics. In *ICALP*, volume 3142 of *LNCS*, 2004.
4. M. Burrows, M. Abadi, and R. Needham. A logic of authentication. In *Practical Cryptography for Data Internetworks*. IEEE Computer Society Press, 1996.
5. F. Dechesne, M. Mousavi, and S.M. Orzan. Operational and epistemic approaches to protocol analysis: Bridging the gap. In *Proceedings LPAR'07*, volume 4790 of *LNCS*, 2007.
6. F. Dechesne and Y. Wang. Dynamic epistemic verification of security protocols: framework and case study. In *A Meeting of the minds: Proceedings LORI workshop*, Texts in Computer Science, pages 129–144, 2007.
7. J. van Eijck. DEMO program and documentation, 2005. Available from `http://www.cwi.nl/~jve/demo/`.
8. R. Fagin, J. Y. Halpern, Y. Moses, and M.Y. Vardi. *Reasoning About Knowledge*. MIT Press, 1995.
9. P. Godefroid and R. Jagadeesan. Automatic abstraction using generalized model checking. In *Proceedings CAV '02*, pages 137–150, 2002.
10. J.Y. Halpern and K.R. O'Neill. Anonymity and information hiding in multiagent systems. *Journal of Computer Security*, pages 483–514, 2005.
11. W. van der Hoek and M. Wooldridge. Model checking knowledge and time. In *Proceedings SPIN'02*, volume 2318 of *LNCS*, pages 95–111, 2002.
12. A. Hommersom, J.-J. Meyer, and E.P. de Vink. Update semantics of security protocols. *Synthese*, 142:229–267, 2004. Knowledge, Rationality and Action subseries.

13. D. Hughes and V. Shmatikov. Information hiding, anonymity and privacy: A modular approach. *Journal of Computer Security*, 12(1):3–36, 2004.
14. M. Huth, R. Jagadeesan, and D. Schmidt. Modal transition systems: A foundation for three-valued program analysis. *LNCS*, 2028, 2001.
15. K.G. Larsen. Modal specifications. In *Automatic Verification Methods for Finite State Systems*, pages 232–246, 1989.
16. K.G. Larsen and B. Thomsen. A modal process logic. In *Proceedings LICS*, pages 203–210, 1988.
17. R. van der Meyden and Kaile Su. Symbolic model checking the knowledge of the dining cryptographers. In *Proc. CSFW 2004*, pages 280–291. IEEE, 2004.
18. J.A. Plaza. Logics of public communications. In *Proceedings ISMIS'89*, pages 201–216, 1989.
19. F. Raimondi and A. Lomuscio. Automatic verification of deontic interpreted systems by model checking via OBDD's. *Journal of Applied Logic*, 2006.
20. J.C. van de Pol and M. Valero Espada. Modal abstractions in μCRL*. In *AMAST*, pages 409–425, 2004.
21. H. van Ditmarsch, W. van der Hoek, and B. Kooi. *Dynamnic Epistemic Logic*, volume 337 of *Synthese Library.* Springer, 2008.
22. J. van Eijck and S.M. Orzan. Epistemic verification of anonymity. *ENTCS*, 168, 2007.