UNIVERSITY OF OSLO
Department of Informatics

Compositional Reasoning for Multi-Modal Logics

Research Report No. 419

Luca Aceto

Anna Ingólfsdóttir

Cristian Prisacariu

Joshua Sack

Isbn 82-7368-383-4
Issn 0806-3036

October 18, 2012

Compositional Reasoning for Epistemic Logics*

Luca Aceto† Anna Ingólfsdóttir‡ Cristian Prisacariu§
Joshua Sack¶

October 18, 2012

Abstract

We provide decomposition and quotienting results for multi-modal logic with respect to a composition operator, traditionally used for epistemic models, due to van Eijck et al. (Journal of Applied Non-Classical Logics 21(3–4):397–425, 2011), that involves sets of atomic propositions and valuation functions from Kripke models. While the composition operator was originally defined only for epistemic $S5^n$ models, our results apply to the composition of any pair of Kripke models. In particular, our quotienting result extends a specific result in the above mentioned paper by van Eijck et al. for the composition of epistemic models with disjoint sets of atomic propositions to compositions of any two Kripke models regardless of their sets of atomic propositions. We also explore the complexity of the formulas we construct in our decomposition result.

*Luca Aceto and Anna Ingólfsdóttir were partially supported by the project 'Processes and Modal Logics' (project nr. 100048021) of the Icelandic Research Fund.

†ICE-TCS, School of Computer Science, Reykjavik University, Reykjavik, Iceland. E-mail: luca@ru.is

‡ICE-TCS, School of Computer Science, Reykjavik University, Reykjavik, Iceland. E-mail: annai@ru.is

§Dept. of Informatics – Univ. of Oslo, P.O. Box 1080 Blindern, N-0316 Oslo, Norway. E-mail: cristi@ifi.uio.no

¶Dept. of Mathematics and Statistics – California State Univ. Long Beach. E-mail: joshua.sack@gmail.com

Contents

1 Introduction

Decomposition and quotienting techniques [1, 8, 14, 23] have been used for a wide variety of logics, such as Hennessy-Milner logic [9] or modal μ-calculus [12], and much attention has been given to extending and optimizing these [1, 13]. Compositional reasoning normally involves a parallel-like *composition operator* over the models of the logic in question. In the cases just cited, the main composition operator of interest is usually some form of parallel composition from process algebras [3, 10, 18, 19]. In these cases, one observes what is called the *state explosion problem*; when a system is built up by composing several processes/components, its state space grows exponentially with the number of components. This is the main drawback of doing model checking of such systems (even for algorithms that are linear in the size of the *model* and the formula). Compositional reasoning has proved useful in tackling the state space explosion problem in several applications.

Intuitively, considering some form of composition of models $M_1||M_2$ and a formula φ, to check on this composed model, the technique of compositional reasoning provides an alternative to checking $M_1||M_2 \models \varphi$, by instead checking two potentially simpler problems: $M_1 \models \phi_1$ and $M_2 \models \phi_2$. When the two new formulas are not much larger than the original, this method can be very useful. There are also heuristic techniques that aim at keeping the new formulas small [1].

The aim of this paper is to develop a theory of compositionality and quotienting for multi-modal logics with respect to a composition operator that has been recently introduced in [22] for epistemic models. This composition behaves similarly to the well-known synchronous composition; however, while the set of states in a parallel composition is generally the Cartesian product, the composition between epistemic models introduced in [22] eliminates states whose atomic valuation on the components are not, so to speak, compatible.

Arguably, the composition of [22] is the most natural that one would want on S5^n models. This composition behaves similarly to the well-known synchronous composition of labelled transition systems. It is easy to see (Th. A.2 and A.3 in Appendix) that the standard asynchronous composition that is normally studied in process algebras and concurrency theory does not preserve S5^n models, whereas the synchronous composition does. Another observation is that unlike other types of frames (i.e., transition systems without a valuation of propositional constants), the S5^n frames are trivial without propositional constants and a valuation attached to their states (i.e., they are bisimilar to a single reflexive point). Therefore, a composition of S5^n models should take valuations and propositional constants into consideration.

Although originally defined for $S5^n$ models, the composition of [22] is also well-defined on other classes of models. For example, the class of Kripke models is closed under it. An example of a class of models that is *not* closed with respect to the composition of [22] is that of KD45 models, often used to model belief. (See Remark 2.6.)

The involvement of valuations and propositional constants in compositions in general has received relatively little attention, and distinguishes the results in this paper from mainstream composition results [5,8,14,23]. There are, however, other compositions that use valuations and propositional constants, and there is work that employs related techniques. One composition that uses valuations is the concurrent program of [15], where two non-epistemic models are composed in such a way that the states of the composition may disagree with the components on the valuation. The composition we employ in this paper eliminates any state where there may be such disagreement between a composite state and its components. Another related composition is the update product from [4], though that composition is not between two Kripke models, but between a Kripke (or epistemic) model and an *action model*, a syntactic structure that differs from a Kripke model in that the valuation is replaced by a function assigning a formula to each point of the model. A composition result in the setting of transition systems that also involves pruning the global state space is that of [20]; however this result does not involve logic as we do. Furthermore, given that modal formulas characterize finite transition systems up to bisimulation, and synchronizing on common actions is similar to compatible states based on common valuations, there are connections between our techniques and the techniques for synchronizing up to bisimulation from [7].

Our most technically involved contribution is the proof strategy of a decomposition result (Th. 3.9) for the composition operator of [22]. This result follows naturally from the relationship between the primary composition of focus and an auxiliary composition (Th. 3.4). We also study the connections between the composition of models with overlapping sets of atomic propositions and compositions of models with disjoint sets of atomic propositions (Th. 5.5). Furthermore, we provide a quotienting theorem (Th. 4.3), which can be used to synthesize missing components in composite models. If we have a model N in the composition and want to construct M in order to achieve property φ for the composition of M and N, we can first compute the quotient formula of φ with respect to N and then synthesize a model for it, if one exists. We show in the proof of Corollary 5.6 that the quotienting result [22, Th. 16] involving only epistemic models with disjoint sets of atomic propositions is an instance of our quotienting result, and in Section 5.2, we discuss how to extend our primary decomposition result to one

involving an even more general composition operator. Finally, in Section 6, we provide an analysis of the complexity of the formulas we construct in our main decomposition result.

2 Preliminaries

In what follows we assume a fixed finite set I of *labels* or *agents*.

Definition 2.1 (Multi-modal logic) *The* multi-modal logic $\mathcal{L}(\mathsf{P})$*, over a set* P *of propositional constants, is defined by the grammar:*

$$\phi := p\,(p \in \mathsf{P}) \mid \bot \mid \phi \vee \phi \mid \neg\phi \mid \langle i\rangle\varphi\,(i \in I).$$

The set P *is called the* vocabulary *of the logic. The formulas* $\phi_1 \wedge \phi_2$*,* $\phi_1 \leftrightarrow \phi_2$*, and* $[i]\phi$ *for* $i \in I$ *are derived in the standard way from this grammar, empty disjunctions identified with* $\bot$*, and* $\top$ *with* $\neg\bot$*.*

We are especially interested here in epistemic logics where the modality $[i]\varphi$ is usually read as: *agent* i *"knows" formula* φ, and is written $K_i\varphi$. But our work is applicable more generally, to multi-modal logics with propositional constants. We also want our notation to be close to both the epistemic logic community and the works on decomposition techniques.

The logic $\mathcal{L}(\mathsf{P})$ is interpreted over *(multi-modal) Kripke models*.

Definition 2.2 (Multi-modal Kripke structure and model)

- *A* (multi-modal) Kripke structure *is a tuple* $K = (W, \rightarrow)$ *where* W *is the set of worlds (also called states), and* $\rightarrow$ *is a family of relations* $\xrightarrow{i} \subseteq W \times W$ *indexed by a fixed set* I*. A* pointed (multi-modal) Kripke structure *is a pair* (K, w)*, where* $K = (W, \rightarrow)$ *and* $w \in W$*.*

- *A* multi-modal Kripke model *is a tuple* $M = (W, \rightarrow, \mathsf{P}, V)$ *where* $(W, \rightarrow)$ *is a Kripke structure,* P *is the set of propositional constants (i.e., the vocabulary of the model), and* $V : W \rightarrow \mathcal{P}(\mathsf{P})$ *is a valuation function. A model is* finite *if* W *and* P *are both finite. A* pointed (multi-modal) Kripke model *is a pair* (M, w)*, where* $M = (W, \rightarrow, \mathsf{P}, V)$ *and* $w \in W$*.*

Definition 2.3 (Interpreting multi-modal logic) *The formulae in* $\mathcal{L}(\mathsf{P})$ *are interpreted in a Kripke model* $M = (W, \rightarrow, \mathsf{P}, V)$ *at some* $w \in W$ *as follows:*

- $(M, w) \models p$ *iff* $p \in V(w)$*,*

- $(M, w) \models \phi_1 \vee \phi_2$ *iff* $(M, w) \models \phi_1$ *or* $(M, w) \models \phi_2$,
- $(M, w) \models \neg\phi$ *iff it is not the case that* $(M, w) \models \phi$ *(abbreviated* $(M, w) \not\models \phi$*)*
- $(M, w) \models \langle i \rangle \phi$ *iff there exists a* $w' \in W$ *s.t.* $w \xrightarrow{i} w'$ *and* $(M, w') \models \phi$.

We read $(M, w) \models \varphi$ as: *"the formula* φ *holds/is true at state* w *in* M*"*. Sometimes we write $w \models \phi$ instead of $(M, w) \models \phi$ if the meaning is clear from the context.

2.1 Compositions of models

Our paper is mainly concerned with the study of the interplay of the logic $\mathcal{L}(\mathsf{P})$ and the composition operator introduced in [22], which we will denote $\oslash$ and formally define in Definition 2.5. Essentially this composition makes a *synchronous* composition of the relations of the two models, but the new set of states is only *a subset of the Cartesian product* of the two initial sets of states. For later use, we redefine the restriction on states from [22] in terms of the notion of *(in)consistent states*. Though in [22] the operation $\oslash$ is defined over $S5^n$ models, it can actually be applied to arbitrary multi-modal Kripke models. Since our decomposition technique does not use the restrictions of the $S5^n$ models, it can be readily used over any class of multi-modal Kripke models that is closed under the operation of Definition 2.5; $S5^n$ models form one such class.

Definition 2.4 (Consistent states) *For two models* $M = (W_M, \rightarrow_M, \mathsf{P}_M, V_M)$ *and* $N = (W_N, \rightarrow_N, \mathsf{P}_N, V_N)$*, where* P_M *and* P_N *may overlap, we say that two states* $w \in W_M$ *and* $v \in W_N$ *are* inconsistent*, written* $(M, w) \sharp (N, v)$*, iff*

$$\exists p \in \mathsf{P}_M \cap \mathsf{P}_N : (p \in V_M(w) \text{ and } p \notin V_N(v)) \text{ or } (p \notin V_M(w) \text{ and } p \in V_N(v)).$$

We say that w *and* v *are* consistent*, written* $(M, w) \diamond (N, v)$*, iff the two states are not inconsistent. We often write* $w \sharp v$ *for* $(M, w) \sharp (N, v)$ *and* $w \diamond v$ *for* $(M, w) \diamond (N, v)$ *when the models are clear from the context.*

Definition 2.5 (Composition of models [22]) *Let* $M = (W_M, \rightarrow_M, \mathsf{P}_M, V_M)$ *and* $N = (W_N, \rightarrow_N, \mathsf{P}_N, V_N)$ *be two finite models, with possibly overlapping vocabularies* P_M *and* P_N*. The composition of* M *and* N *is the finite model defined as* $M \oslash N = (W, \rightarrow, \mathsf{P}_M \cup \mathsf{P}_N, V)$ *with:*

- $W = \{(w, v) \mid w \in W_M, v \in W_N, \text{ and } w \diamond v\}$,

- $(w,v) \xrightarrow{i} (w',v')$ *iff* $w \xrightarrow{i}_M w'$ *and* $v \xrightarrow{i}_N v'$, *for* $(w,v),(w',v') \in W$ *and* $i \in I$, *and*
- $V((w,v)) = V_M(w) \cup V_N(v)$, *for* $(w,v) \in W$.

Note that, when the vocabularies are disjoint, the definition of $\diamond$ becomes vacuously true, whereas that of $\sharp$ is vacuously false. In this case, the above definition becomes the standard synchronous composition, where new states are from the full Cartesian product (as the requirement $w \diamond v$ can be ignored).

It was shown in [22, Th. 3] that the composition $\oslash$ endows the collection of epistemic $\mathrm{S5}^n$ with a commutative monoid structure, that is, up to total bisimilarity, the composition $\oslash$ is commutative, associative, and if E is the (epistemic $S5^n$) model with one point that is reflexive for every agent and has an empty set of atomic propositions, then E is a left and right unit for $\oslash$.

Remark 2.6 *It is folklore from model theory that a sentence of first order logic is preserved under restriction and product if and only if the sentence is universal Horn. A universal Horn sentence of first-order logic is the universal closure of a disjunction with at most one atom disjunct, and where the remaining disjuncts are negations of atoms (see, e.g., [16]). The classes of S5 models and S5^n models are universal Horn: the formulas for reflexivity, symmetry and transitivity can be written as Horn formulas. Hence the collection of epistemic models must be closed under the composition $\oslash$. However, the class of KD45 models, often used to model belief, is not universal Horn, for the seriality requirement cannot be expressed as a universal Horn sentence. Although a property that is not expressible by a universal Horn might be preserved under* some *products and restrictions, one can easily check that KD45 is indeed not preserved under $\oslash$ (Th. A.4 in Appendix).*

3 Compositional reasoning wrt. the $\oslash$ composition

This section presents our main result, a general decomposition for $\mathcal{L}(\mathsf{P})$ with respect to $\oslash$, and which we describe as follows. We consider two finite models $M = (W_M, \to_M, \mathsf{P}_M, V_M)$ and $N = (W_N, \to_N, \mathsf{P}_N, V_N)$ and a formula $\phi \in \mathcal{L}(\mathsf{P}_M \cup \mathsf{P}_N)$. Our aim is to find two formulas $\psi_1 \in \mathcal{L}(\mathsf{P}_M)$ and $\psi_2 \in \mathcal{L}(\mathsf{P}_N)$ such that

$$(M \oslash N, (w,v)) \models \phi \;\text{ iff }\; (M,w) \models \psi_1 \text{ and } (N,v) \models \psi_2.$$

We want ψ_1 and ψ_2 to depend only on φ, but for each φ there can actually be multiple candidate pairs of formulas (ψ_1, ψ_2). We thus follow the works on compositional reasoning for Hennessy-Milner logic [8], and reformulate the problem into finding a function $\chi : \mathcal{L}(\mathsf{P}_M \cup \mathsf{P}_N) \to \mathcal{P}(\mathcal{L}(\mathsf{P}_M) \times \mathcal{L}(\mathsf{P}_N))$ such that

$$(M \oslash N, (w, v)) \models \phi \quad \text{iff} \quad \exists (\psi_1, \psi_2) \in \chi(\phi) : (M, w) \models \psi_1 \text{ and } (N, v) \models \psi_2.$$

Note that this function χ returns a subset of $\mathcal{P}(\mathcal{L}(\mathsf{P}_M) \times \mathcal{L}(\mathsf{P}_N))$. This motivates the following definition, an auxiliary composition that we use to prove the main decomposition result of this section (Th. 3.9).

Definition 3.1 (Auxiliary composition) *Let $M = (W_M, \to_M, \mathsf{P}_M, V_M)$ and $N = (W_N, \to_N, \mathsf{P}_N, V_N)$ be two finite models. The* auxiliary composition *of M and N is defined as the model $M \odot N = (W, \to, \mathsf{P}, V)$ (also written $\binom{M}{N}$) with:*

- $W = W_M \times W_N$, *whose elements are also written* $\binom{w}{v}$ *for* $(w, v) \in W_M \times W_N$,
- $\binom{w}{v} \xrightarrow{i} \binom{w'}{v'}$ *iff* $w \xrightarrow{i}_M w'$ *and* $v \xrightarrow{i}_N v'$, *for* $\binom{w}{v}, \binom{w'}{v'} \in W$ *and* $i \in I$,
- $\mathsf{P} = \mathcal{L}(\mathsf{P}_M) \times \mathcal{L}(\mathsf{P}_N)$, *whose elements are also written* $\binom{\psi_1}{\psi_2}$ *for* (ψ_1, ψ_2),
- $V((w, v)) = \{(\varphi, \psi) \in \mathsf{P} \mid (M, w) \models \varphi \text{ and } (N, v) \models \psi\}$.

As before, we may subscript the components with the model (such as by writing $\mathsf{P}_{M \odot N}$ for the set atomic propositions in $M \odot N$). The usual laws of multi-modal logic apply when determining the truth of a formula $\Phi \in \mathcal{L}(\mathsf{P}_{M \odot N})$ in a pointed model. For example, from the definition of $V_{M \odot N}$, we have, for $(\phi, \psi) \in \mathsf{P}_{M \odot N}$, that

$$\binom{M}{N}, \binom{w}{v} \models \binom{\phi}{\psi} \quad \text{iff} \quad (M, w) \models \phi \text{ and } (N, v) \models \psi,$$

and, given $\Phi \in \mathcal{L}(\mathsf{P}_{M \odot N})$,

$$\binom{M}{N}, \binom{w}{v} \models \langle i \rangle \Phi \text{ iff } \binom{M}{N}, \binom{w'}{v'} \models \Phi \text{ for some } \binom{w'}{v'} \text{ with } \binom{w}{v} \xrightarrow{i} \binom{w'}{v'}.$$

We usually write $\binom{w}{v} \models \Phi$ for $\binom{M}{N}, \binom{w}{v} \models \Phi$ if the model is clear from context.

3.1 Relationship between ⊙ and ⊘

Our first step is to compare the compositions ⊙ and ⊘. A primary difference between these two is that ⊙ does not remove states that are considered inconsistent, while ⊘ does. We thus provide the following formulas in the language $\mathcal{L}(\mathsf{P}_{M\odot N})$ that characterize inconsistency and consistency:

$$\sharp_{M\odot N} = \bigvee_{p\in \mathsf{P}_M\cap \mathsf{P}_N} \left(\begin{pmatrix} p \\ \neg p \end{pmatrix} \vee \begin{pmatrix} \neg p \\ p \end{pmatrix} \right) \text{ and } \quad \diamond_{M\odot N} = \neg \sharp_{M\odot N}. \tag{1}$$

Lemma 3.2 *For two finite pointed models (M, w) and (N, v), we have*

$$\begin{pmatrix} M \\ N \end{pmatrix}, \begin{pmatrix} w \\ v \end{pmatrix} \models \sharp_{M\odot N} \quad \textit{iff} \quad (M, w) \sharp (N, v),$$

with the notation on the right taken from Definition 2.4.

Proof: This is immediate from the definitions. However, for completeness we expand it here. The following are equivalent:

- $\begin{pmatrix} M \\ N \end{pmatrix}, \begin{pmatrix} w \\ v \end{pmatrix} \models \sharp_{M\odot N}$
- $\begin{pmatrix} M \\ N \end{pmatrix}, \begin{pmatrix} w \\ v \end{pmatrix} \models \bigvee_{p\in \mathsf{P}_M\cap \mathsf{P}_N} \left(\begin{pmatrix} p \\ \neg p \end{pmatrix} \vee \begin{pmatrix} \neg p \\ p \end{pmatrix} \right)$
- For some $p \in \mathsf{P}_M \cap \mathsf{P}_N$, we have that $p \in V_M(w)$ but $p \notin V_N(v)$ or $p \notin V_M(w)$ but $p \in V_N(v)$.
- $(M, w) \sharp (N, v)$, cf. Def. 2.4. □

□

We now define a "meaning preserving" translation of formulas to be evaluated on models composed using ⊘ to those evaluated on models composed using ⊙. The correctness of this translation is given in Theorem 3.4.

Definition 3.3 (Translation function) *We define $Z : \mathcal{L}(\mathsf{P}_M \cup \mathsf{P}_N) \to \mathcal{L}(\mathsf{P}_{M\odot N})$ as follows:*

- $$Z(p) = \begin{cases} \begin{pmatrix} p \\ p \end{pmatrix} & \textit{if } p \in \mathsf{P}_M \cap \mathsf{P}_N, \\ \begin{pmatrix} p \\ \top \end{pmatrix} & \textit{if } p \in \mathsf{P}_M \setminus \mathsf{P}_N \\ \begin{pmatrix} \top \\ p \end{pmatrix} & \textit{if } p \in \mathsf{P}_N \setminus \mathsf{P}_M. \end{cases},$$

- $Z(\phi_1 \vee \phi_2) = Z(\phi_1) \vee Z(\phi_2)$,
- $Z(\neg\phi) = \neg Z(\phi)$,
- $Z(\langle i\rangle\phi) = \langle i\rangle(Z(\phi) \wedge \diamond)$.

Theorem 3.4 *Let $M = (W_M, \to_M, \mathsf{P}_M, V_M)$ and $N = (W_N, \to_N, \mathsf{P}_N, V_N)$ be finite models and $\phi \in \mathcal{L}(\mathsf{P}_M \cup \mathsf{P}_N)$. Then for all $(w, v) \in W_{M\oslash N}$ (i.e. such that $w \diamond v$)*

$$M \oslash N, (w, v) \models \phi \quad \textit{iff} \quad \binom{M}{N}, \binom{w}{v} \models Z(\phi).$$

Proof: In our simplified notation, we have to prove that

$$(w, v) \models \phi \text{ iff } \binom{w}{v} \models Z(\phi).$$

We prove the statement by structural induction on ϕ.

Base case: We only have to consider the case $\phi = p$ that follows directly from the definition of the satisfiability relation $\models$ for $M \oslash N$.

Inductive step: We consider the following cases:

$\phi = \phi_1 \vee \phi_2$: Now $Z(\phi_1 \vee \phi_2) = Z(\phi_1) \vee Z(\phi_2)$ and we proceed as follows:

$$(w, v) \models \phi_1 \vee \phi_2 \text{ iff } (w, v) \models \phi_1 \text{ or } (w, v) \models \phi_2 \text{ iff (by induction)}$$

$$\binom{w}{v} \models Z(\phi_1) \text{ or } \binom{w}{v} \models Z(\phi_2) \text{ iff}$$

$$\binom{w}{v} \models Z(\phi_1) \vee Z(\phi_2) \text{ iff } \binom{w}{v} \models Z(\phi_1 \vee \phi_2).$$

$\phi = \neg\phi_1$: Now $Z(\neg\phi_1) = \neg Z(\phi_1)$ and we get,

$$(w, v) \models \neg\phi_1 \text{ iff } (w, v) \not\models \phi_1 \text{ iff (by induction)}$$

$$\binom{w}{v} \not\models Z(\phi_1) \text{ iff } \binom{w}{v} \models \neg Z(\phi_1).$$

$\phi = \langle i \rangle \phi_1$: Now $Z(\langle i \rangle \phi_1) = \langle i \rangle (Z(\phi_1) \wedge \diamond)$. We proceed as follows:

$(w, v) \models \langle i \rangle \phi$ iff

$\exists (w', v') \in W_{M \oslash N}.(w, v) \xrightarrow{i} (w', v')$ and $(w', v') \models \phi$ iff (by induction)

$\exists w' \in W_M \exists v' \in W_N. \begin{pmatrix} w \\ v \end{pmatrix} \xrightarrow{i} \begin{pmatrix} w' \\ v' \end{pmatrix}, w' \diamond v'$ and $\begin{pmatrix} w' \\ v' \end{pmatrix} \models Z(\phi)$ iff

$\exists w' \in W_M \exists v' \in W_N. \begin{pmatrix} w \\ v \end{pmatrix} \xrightarrow{i} \begin{pmatrix} w' \\ v' \end{pmatrix}$ and $\begin{pmatrix} w' \\ v' \end{pmatrix} \models Z(\phi) \wedge \diamond$ iff

$\begin{pmatrix} w \\ v \end{pmatrix} \models \langle i \rangle (Z(\phi) \wedge \diamond)$.

□

□

3.2 Decomposing formulas

Recall from Theorem 3.4 that we relate the formula ϕ with a formula $Z(\phi)$ from $\mathcal{L}(\mathsf{P}_{M \odot N})$. We now proceed to show that any formula in $\mathcal{L}(\mathsf{P}_{M \odot N})$ is equivalent on $M \odot N$ to a disjunction of atomic propositions $\mathsf{P}_{M \odot N}$.

Definition 3.5 (Disjunctive Normal Form in $\mathcal{L}(\mathsf{P}_{M \odot N})$) *The set of Disjunctive Normal Forms in $\mathcal{L}(\mathsf{P}_{M \odot N})$, written $\mathbf{D}(\mathsf{P}_{M \odot N})$, is defined as the smallest set such that:*

- $\mathcal{L}(\mathsf{P}_M) \times \mathcal{L}(\mathsf{P}_N) \subseteq \mathbf{D}(\mathsf{P}_{M \odot N})$;
- *if* $\Phi_1, \Phi_2 \in \mathbf{D}(\mathsf{P}_{M \odot N})$ *then* $\Phi_1 \vee \Phi_2 \in \mathbf{D}(\mathsf{P}_{M \odot N})$.

Note the difference between this definition and the standard notion of disjunctive normal form (DNF). The conjuncts that normally appear in a DNF are, in our case, part of the pairs (elements of $\mathsf{P}_{M \odot N}$), and similarly for the negation. Moreover, this is a DNF for modal formulas, and similarly the modality is part of the atomic pairs.. These are possible because of the following result.

Lemma 3.6 (Equivalences) *The following are valid on $M \odot N$.*

$$\neg\begin{pmatrix}\phi\\ \psi\end{pmatrix} \leftrightarrow \begin{pmatrix}\neg\phi\\ \top\end{pmatrix} \vee \begin{pmatrix}\top\\ \neg\psi\end{pmatrix}$$

$$\begin{pmatrix}\phi_1\\ \psi_1\end{pmatrix} \wedge \begin{pmatrix}\phi_2\\ \psi_2\end{pmatrix} \leftrightarrow \begin{pmatrix}\phi_1 \wedge \phi_2\\ \psi_1 \wedge \psi_2\end{pmatrix},$$

$$\langle i\rangle\begin{pmatrix}\psi_1\\ \psi_2\end{pmatrix} \leftrightarrow \begin{pmatrix}\langle i\rangle\psi_1\\ \langle i\rangle\psi_2\end{pmatrix}.$$

Proof : All cases follow immediately from the definitions above. For completeness, we provide more explanation. For the first, each of the following are equivalent:

- $\begin{pmatrix}w\\ v\end{pmatrix} \models \neg\begin{pmatrix}\phi_1\\ \psi_1\end{pmatrix}$
- $w \models \neg\phi_1$ or $v \models \neg\psi_2$
- $\begin{pmatrix}w\\ v\end{pmatrix} \models \begin{pmatrix}\neg\phi_1\\ \top\end{pmatrix} \vee \begin{pmatrix}\top\\ \neg\phi_2\end{pmatrix}$

For the second, each of the following are equivalent:

- $\begin{pmatrix}w\\ v\end{pmatrix} \models \begin{pmatrix}\phi_1\\ \psi_1\end{pmatrix} \wedge \begin{pmatrix}\phi_2\\ \psi_2\end{pmatrix}$
- $w \models \phi_1 \wedge \phi_2$ and $v \models \psi_1 \wedge \psi_2$
- $\begin{pmatrix}w\\ v\end{pmatrix} \models \begin{pmatrix}\phi_1 \wedge \phi_2\\ \psi_1 \wedge \psi_2\end{pmatrix}$

For the third, each of the following are equivalent:

- $\begin{pmatrix}w\\ v\end{pmatrix} \models \langle i\rangle\begin{pmatrix}\psi_1\\ \psi_2\end{pmatrix}$
- $\begin{pmatrix}w'\\ v'\end{pmatrix} \models \begin{pmatrix}\psi_1\\ \psi_2\end{pmatrix}$, whenever $\begin{pmatrix}w\\ v\end{pmatrix} \xrightarrow{i} \begin{pmatrix}w'\\ v'\end{pmatrix}$
- $w' \models \psi_1$ whenever $w \xrightarrow{i} w'$ and $v' \models \psi_2$ whenever $v \xrightarrow{i} v'$
- $\begin{pmatrix}w\\ v\end{pmatrix} \models \begin{pmatrix}\langle i\rangle\psi_1\\ \langle i\rangle\psi_2\end{pmatrix}$ □

□

Definition 3.7 *We define a function* $\mathbf{d} : \mathcal{L}(\mathsf{P}_{M\odot N}) \to \mathbf{D}(\mathsf{P}_{M\odot N})$ *inductively as follows:*

- *If* $\Phi \in \mathsf{P}_{M\odot N}$, *then* $\mathbf{d}(\Phi) = \Phi$.
- *If* $\Phi_1, \Phi_2 \in \mathcal{L}(\mathsf{P}_{M\odot N})$, *then* $\mathbf{d}(\Phi_1 \vee \Phi_2) = \mathbf{d}(\Phi_1) \vee \mathbf{d}(\Phi_2)$.
- *If* $\Phi \in \mathcal{L}(\mathsf{P}_{M\odot N})$ *and* $\mathbf{d}(\Phi) = \bigvee_{k\in K} \binom{\phi_k}{\psi_k}$ *then*
  - $\mathbf{d}(\langle i\rangle\Phi) = \bigvee_{k\in K} \binom{\langle i\rangle\phi_k}{\langle i\rangle\psi_k}$,
  - $\mathbf{d}(\neg\Phi) = \bigvee \left\{ \binom{\neg \bigvee_{i\in I} \phi_i}{\neg \bigvee_{j\in K\setminus I} \psi_j} \mid I \subseteq K \right\}$.

The following result states that $\mathbf{d}$ preserves the semantics of the formulas.

Theorem 3.8 *For all* $\Phi \in \mathcal{L}(\mathsf{P}_{M\odot N})$, $w \in W_M$ *and* $v \in W_N$,

$$\binom{w}{v} \models \Phi \quad \textit{iff} \quad \binom{w}{v} \models \mathbf{d}(\Phi).$$

Proof : We prove the statement by structural induction on Φ, where the base case and the case for $\vee$ are easy. We treat the remaining two cases.

- For $\Phi = \neg\Phi_1$, we have by the inductive hypothesis that Φ_1 does not hold at $\binom{w}{v}$ iff $\mathbf{d}(\Phi_1)$ does not hold at $\binom{w}{v}$ in $M \odot N$, and hence it remains to show that (for $\mathbf{d}(\Phi_1) = \bigvee_{k\in K} \binom{\phi_k}{\psi_k}$)

$$\binom{w}{v} \models \neg \left(\bigvee_{k\in K} \binom{\phi_k}{\psi_k} \right) \text{ iff } \binom{w}{v} \models \bigvee \left\{ \binom{\bigwedge_{i\in I} \neg\phi_i}{\bigwedge_{j\in K\setminus I} \neg\psi_j} \mid I \in \mathcal{P}(K) \right\} \tag{2}$$

  By De Morgan's law and Lemma 3.6 (negation case), we have that the left-hand-side of (2) is equivalent to

$$\binom{w}{v} \models \bigwedge_{k\in K} \left(\binom{\neg\phi_k}{\top} \vee \binom{\top}{\neg\psi_k} \right) \tag{3}$$

  By the distributivity law and Lemma 3.6 (conjunction case), we have the equivalence of (3) with the right-hand-side of (2), after the $\top$ are contracted.

- The case where $\Phi = \langle i \rangle \Phi_1$ follows similar arguments, and makes use of the fact that in modal logics the diamond distributes over disjunction, and of Lemma 3.6 (diamond case). □

□ We are now ready for our main decomposition theorem.

Theorem 3.9 *Let* $\chi : \mathcal{L}(\mathsf{P}_M \cup \mathsf{P}_N) \to \mathcal{P}(\mathcal{L}(\mathsf{P}_M) \times \mathcal{L}(\mathsf{P}_N))$ *be defined by mapping* ϕ *to the set of disjuncts in* $\mathbf{d}(Z(\phi))$. *Then*

$$(M \oslash N, (w, v)) \models \phi \quad \textit{iff} \quad \exists (\psi_1, \psi_2) \in \chi(\phi) : (M, w) \models \psi_1 \textit{ and } (N, v) \models \psi_2.$$

Proof: This result immediately follows from Theorems 3.4 and 3.8, and the definition of the semantics of disjunction. □ □

4 Quotienting

In this section, we present our quotienting result, which we describe as follows. Having a composed pointed model $(M \oslash N, (w, v))$ and a formula $\varphi \in \mathcal{L}(\mathsf{P}_M \cup \mathsf{P}_N)$, build a new formula that depends explicitly only on one of the components, we denote this by $Q_{(N,v)}(\varphi)$, so that

$$(M \oslash N, (w, v)) \models \varphi \text{ iff } M, w \models Q_{(N,v)}(\varphi).$$

If for our logic and our composition operation $\oslash$, the resulting quotient formula is not significantly larger than the original formula and the component, then the model checking task is simplified [1].

We show how $Q_{(N,v)}(\varphi)$ can be derived, by beginning with the following formula for consistency.

Definition 4.1 (Consistent with v**)** *Given a finite model* $M = (W_M, \to_M, \mathsf{P}_M, V_M)$ *and a finite pointed model* $(N, v) = (W_N, \to_N, \mathsf{P}_N, V_N)$ *with* $v \in W_N$, *we define* $\diamond_v \in \mathcal{L}(\mathsf{P}_M \cap \mathsf{P}_N)$ *as:*

$$\diamond_v = \bigwedge \{p \mid p \in \mathsf{P}_M \cap \mathsf{P}_N,\ (N, v) \models p\} \\ \wedge \bigwedge \{\neg p \mid p \in \mathsf{P}_M \cap \mathsf{P}_N,\ (N, v) \models \neg p\}.$$

This definition essentially encodes the valuation of (N, v) over the common part of the vocabularies. Before, e.g. in Definition 5.2, $\diamond$ was encoding all possible valuations, because we did not know in advance the state v. The

intuition now is that if $M, w \models \diamond_v$ then w and v are consistent in the same sense as before. Again, we can observe that $\diamond_v$ is a tautology when P_M and P_N are disjoint.

One can already see how for quotienting, the knowledge of one component (N, v) is used to build the quotient formula $Q_{(N,v)}(\varphi)$; whereas before we were taking all possibilities into account in the pairs of formulas.

Definition 4.2 (Modal quotient function) *For some set of propositional constants P_M and a finite pointed model (N, v), we define the function $Q_{(N,v)} : \mathcal{L}(\mathsf{P}_M \cup \mathsf{P}_N) \to \mathcal{L}(\mathsf{P}_M)$ by*

- $Q_{(N,v)}(p) = \begin{cases} p \text{ iff } p \in \mathsf{P}_M \setminus \mathsf{P}_N, \text{ or both } p \in \mathsf{P}_M \cap \mathsf{P}_N \text{ and } N, v \models p \\ \top \text{ iff } p \in \mathsf{P}_N \setminus \mathsf{P}_M \text{ and } N, v \models p \\ \bot \text{ otherwise.} \end{cases}$,
- $Q_{(N,v)}(\phi_1 \vee \phi_2) = Q_{(N,v)}(\phi_1) \vee Q_{(N,v)}(\phi_2)$,
- $Q_{(N,v)}(\neg\phi) = \neg Q_{(N,v)}(\phi)$,
- $Q_{(N,v)}(\langle i \rangle \phi) = \langle i \rangle \bigvee_{v \xrightarrow{i} v'} (Q_{(N,v')}(\phi) \wedge \diamond_{v'})$.

Theorem 4.3 *For two finite models $M = (W_M, \to_M, \mathsf{P}_M, V_M)$ and $N = (W_N, \to_N, \mathsf{P}_N, V_N)$, a formula $\varphi \in \mathcal{L}(\mathsf{P}_M \cup \mathsf{P}_N)$, and two consistent states $w \diamond v$, we have*

$$M \oslash N, (w, v) \models \varphi \quad \textit{iff} \quad M, w \models Q_{(N,v)}(\varphi).$$

Proof: We prove the theorem by structural induction on φ.

Base case: $\varphi = p$ Follows directly from the definition.

Inductive step:

$\varphi = \phi_1 \vee \phi_2$

$M \oslash N, (w, v) \models \phi_1 \vee \phi_2$ iff
$M \oslash N, (w, v) \models \phi_1$ or $M \oslash N, (w, v) \models \phi_2$ iff
$M, w \models Q_{(N,v)}(\phi_1)$ or $M, w \models Q_{(N,v)}(\phi_2)$ iff (by induction)
$M, w \models Q_{(N,v)}(\phi_1) \vee Q_{(N,v)}(\phi_2)$ iff
$M, w \models Q_{(N,v)}(\phi_1 \vee \phi_2)$.

$\varphi = \neg\phi_1$:

$M \oslash N, (w, v) \models \neg\phi_1$ iff $M \oslash N, (w, v) \not\models \phi_1$ iff
$(M, w) \not\models Q_{(N,v)}(\phi_1)$ (by induction) iff
$(M, w) \models \neg Q_{(N,v)}(\phi_1)$ iff $(M, w) \models Q_{(N,v)}(\neg\phi_1)$.

$\varphi = \langle i \rangle \phi_1$: The following are equivalent

1. $M \oslash N, (w, v) \models \langle i \rangle \phi_1$
2. $\exists (w', v') \in W : (w, v) \xrightarrow{i} (w', v')$ and $M \oslash N, (w', v') \models \phi_1$
3. $\exists (w', v') \in W : (w, v) \xrightarrow{i} (w', v')$ and $M, w' \models Q_{(N,v')}(\phi_1)$
4. there exists w', such that $w \xrightarrow{i} w'$ and there exists v', such that $v \xrightarrow{i} v'$ and both $M, w' \models \Diamond_{v'}$ and $M, w' \models Q_{(N,v')}(\phi_1)$.
5. there exists w', such that $w \xrightarrow{i} w'$ and $M, w' \models \bigvee_{v \xrightarrow{i} v'} (Q_{(N,v')} \wedge \Diamond_{v'})$
6. $M, w \models \langle i \rangle (\bigvee_{v \xrightarrow{i} v'} (Q_{(N,v')} \wedge \Diamond_{v'}))$.

□

□

An interesting corollary of Theorem 4.3 is that checking whether a pointed model (M, w) satisfies a formula φ can always be reduced to an equivalent model-checking question over the pointed model (E, v), where E is the left and right unit for the composition operator $\oslash$ and v is the only state of E.

Corollary 4.4 *For each finite model $M = (W_M, \rightarrow_M, \mathsf{P}_M, V_M)$, state $w \in W_M$ and formula $\varphi \in \mathcal{L}(\mathsf{P}_M)$, there is some formula $\psi \in \mathcal{L}(\emptyset)$ such that*

$$M, w \models \varphi \quad \textit{iff} \quad E, v \models \psi \ .$$

Proof : Recall that, by Theorem 3 in [22], E is a left unit for $\oslash$ modulo total bisimilarity. In fact, each state (v, w) in $E \oslash M$ is bisimilar to the state w in M. This means that the pointed models $(E \oslash M, (v, w))$ and (M, w) satisfy the same formulas in $\mathcal{L}(\mathsf{P}_M)$. By Theorem 4.3, we now have that, for each formula $\varphi \in \mathcal{L}(\mathsf{P}_M)$,

$$M, w \models \varphi \ \text{ iff } \ E \oslash M, (v, w) \models \varphi \ \text{ iff } \ E, v \models Q_{(M,w)}(\varphi).$$

By the definition of quotienting, it is easy to see that $Q_{(M,w)}(\varphi) \in \mathcal{L}(\emptyset)$. We may therefore take that formula as the ψ mentioned in the statement of the theorem. □ □

5 Related results and relationships

5.1 Composing with disjoint vocabularies

The results of this section show that the problem of determining the truth value of a formula in the composition of models with arbitrary (overlapping) vocabularies can be equivalently formulated in terms of composition of models with *disjoint* vocabularies.

We first provide functions that transform the models.

Definition 5.1 *For some model $M = (W, \to, \mathsf{P}_M, V_M)$ and $i \in \{1, 2\}$, we define $g_i(M) = (W, \to, \mathsf{P}_M \times \{i\}, V)$, where $V(w) = V_M(w) \times \{i\}$.*

Given any two sets A and B, we define their disjoint union $A + B$ to be $(A \times \{1\}) \cup (B \times \{2\})$. We now define formulas in $\mathcal{L}(\mathsf{P}_M + \mathsf{P}_N)$ that characterize when two states are consistent or inconsistent.

Definition 5.2 *Let P_M and P_N be finite vocabularies. We define the Boolean formulas:*

- $\sharp(\mathsf{P}_M + \mathsf{P}_N) = \bigvee_{p \in \mathsf{P}_M \cap \mathsf{P}_N}(((p,1) \wedge \neg(p,2)) \vee (\neg(p,1) \wedge (p,2)))$.
- $\diamond(\mathsf{P}_M + \mathsf{P}_N) = \neg\sharp(\mathsf{P}_M + \mathsf{P}_N)$.

When M and N are understood from context, we simply write $\sharp$ and $\diamond$ for $\sharp(\mathsf{P}_M + \mathsf{P}_N)$ and $\diamond(\mathsf{P}_M + \mathsf{P}_N)$ respectively.

Note the similarity of the definition for $\sharp_{M \odot N}$ and $\sharp(P_M + P_N)$. Because of the pairing of models and of formulas in the valuation $V_{M \odot N}$, we did not need the change of the common propositions, as we are doing here for $\sharp(P_M + P_N)$. Otherwise the definitions are the same.

Proposition 5.3 *Let $M = (W_M, \to_M, \mathsf{P}_M, V_M)$ and $N = (W_N, \to_N, \mathsf{P}_N, V_N)$ be two finite models. For all $w \in W_M$ and $v \in W_N$, we have*

$$g_1(M) \oslash g_2(N),\ (w, v) \models \sharp(\mathsf{P}_M + \mathsf{P}_N) \quad \textit{iff} \quad (M, w)\,\sharp\,(N, v).$$

Proof: The proof is immediate from the definitions. But for completeness, we expand it here. The following are equivalent

1. $g_1(M) \oslash g_2(N)(w, v) \models \sharp$
2. $g_1(M) \oslash g_2(N)(w, v) \models \bigvee_{p \in \mathsf{P}_M \cap \mathsf{P}_N}(((p,1) \wedge \neg(p,2)) \vee (\neg(p,1) \wedge (p,2)))$

3. for some $p \in \mathsf{P}_M \cap \mathsf{P}_N$, $p \in V_M(w)$ but $p \notin V_N(v)$, or $p \notin V_M(w)$ but $p \in V_N(v)$
4. $(M, w) \sharp (N, v)$ $\square$

$\square$

Note that, by negating both sides of the above "iff", we have an equivalent formulation of the proposition with $\diamond$ in place of $\sharp$. We use the consistency Boolean formula $\diamond$ to rewrite a multi-modal formula that is defined over two possibly overlapping vocabularies, into a multi-modal formula over the two disjoint vocabularies of the corresponding models changed by the functions g_i from above.

Definition 5.4 (Function $f_{(\mathsf{P}_M,\mathsf{P}_N)}$) *For two sets of propositional constants $\mathsf{P}_M, \mathsf{P}_N$, we define a function $f_{(\mathsf{P}_M,\mathsf{P}_N)} : \mathcal{L}(\mathsf{P}_M \cup \mathsf{P}_N) \to \mathcal{L}(\mathsf{P}_M + \mathsf{P}_N)$ as follows:*

- $f_{(\mathsf{P}_M,\mathsf{P}_N)}(p) = \begin{cases} (p,1) \wedge (p,2) & p \in \mathsf{P}_M \cap \mathsf{P}_N, \\ (p,1) & p \in \mathsf{P}_M \setminus \mathsf{P}_N \\ (p,2) & p \in \mathsf{P}_N \setminus \mathsf{P}_M. \end{cases}$
- $f_{(\mathsf{P}_M,\mathsf{P}_N)}(\neg\phi) = \neg f_{(\mathsf{P}_M,\mathsf{P}_N)}(\phi)$.
- $f_{(\mathsf{P}_M,\mathsf{P}_N)}(\phi_1 \vee \phi_2) = f_{(\mathsf{P}_M,\mathsf{P}_N)}(\phi_1) \vee f_{(\mathsf{P}_M,\mathsf{P}_N)}(\phi_2)$.
- $f_{(\mathsf{P}_M,\mathsf{P}_N)}(\langle i \rangle \phi) = \langle i \rangle (f_{(\mathsf{P}_M,\mathsf{P}_N)}(\phi) \wedge \diamond)$.

The functions $g_1(M)$ and $g_2(N)$ produce models with the same structure but with disjoint vocabularies, thus the following is the result we are looking for.

Theorem 5.5 *Given any finite pointed models (M, w) and (N, v), such that $w \diamond v$, and any formula $\varphi \in \mathcal{L}(\mathsf{P}_M \cup \mathsf{P}_N)$,*

$$M \oslash N, (w, v) \models \varphi \quad \textit{iff} \quad g_1(M) \oslash g_2(N), (w, v) \models f_{(\mathsf{P}_M,\mathsf{P}_N)}(\varphi).$$

Proof sketch: We use induction on the structure of the formula φ.

Base case: We only have to consider the case $\phi = p$ that follows directly from the definition of the satisfiability relation $\models$, the definition of f, and the fact that $w \diamond v$.

Inductive step: We consider the following cases:

$\phi = \phi_1 \vee \phi_2$: Now $f(\phi_1 \vee \phi_2) = f(\phi_1) \vee f(\phi_2)$ and we proceed as follows:

$M \oslash N, (w, v) \models \phi_1 \vee \phi_2$ iff

$M \oslash N, (w, v) \models \phi_1$ or $M \oslash N, (w, v) \models \phi_2$ iff (by induction)

$g_1(M) \oslash g_2(N), (w, v) \models f(\phi_1)$ or $g_1(M) \oslash g_2(N), (w, v) \models f(\phi_2)$ iff

$g_1(M) \oslash g_2(N), (w, v) \models f(\phi_1) \vee f(\phi_2)$ iff

$g_1(M) \oslash g_2(N), (w, v) \models f(\phi_1 \vee \phi_2)$.

$\phi = \neg\phi_1$: Now $f(\neg\phi_1) = \neg f(\phi_1)$ and we get,

$M \oslash N, (w, v) \models \neg\phi_1$ iff $M \oslash N, (w, v) \not\models \phi_1$ iff (by induction)

$g_1(M) \oslash g_2(N), (w, v) \not\models f(\phi_1)$ iff $g_1(M) \oslash g_2(N), (w, v) \models \neg f(\phi_1)$.

$\phi = \langle i \rangle \phi$: Now $f(\langle i \rangle \phi) = \langle i \rangle (f(\phi) \wedge \diamond)$. We proceed as follows:

$M \oslash N, (w, v) \models \langle i \rangle \phi$ iff

$\exists (w', v') \in W_{M \oslash N}. (w, v) \xrightarrow{i}_{\oslash} (w', v')$ and $M \oslash N, (w', v') \models \phi$ iff (by induction)

$\exists w' \in W_M \exists v' \in W_N. (w, v) \xrightarrow{i}_{\oslash} (w', v'), w' \diamond v'$ and $g_1(M) \oslash g_2(N), (w', v') \models f(\phi)$ iff

$\exists w' \in W_M \exists v' \in W_N. (w, v) \xrightarrow{i} (w', v')$ and $g_1(M) \oslash g_2(N), (w', v') \models f(\phi) \wedge \diamond$ iff

$g_1(M) \oslash g_2(N), (w, v) \models \langle i \rangle (f(\phi) \wedge \diamond)$.

□ □

5.2 Special instances and extensions

In this section, we show that our quotienting result generalizes Theorem 16 from [22], and then we discuss how to extend our decomposition result (Th. 3.9) to one involving a more general composition operator described in [22, Remark 2].

Corollary 5.6 (for Th.16 of [22]) *Let (M_i, w_i), for $i \in \{1, \ldots, n\}$, be pointed models such that the P_{M_i} are pairwise disjoint. Then for any $\varphi \in \mathcal{L}(\mathsf{P}_{M_i})$, $i \in \{1, \ldots, n\}$, we have that*

$$(M_1 \oslash \cdots \oslash M_n), (w_1, \ldots, w_n) \models \varphi \quad \textit{iff} \quad M_i, w_i \models \varphi \ .$$

Proof sketch: This is an easy corollary of Theorem 4.3. Because $\oslash$ is commutative and associative, we can assume without loss of generality that $i = 1$. Let (N, v) be the pointed model $((M_2 \oslash \cdots \oslash M_n), (w_2, \ldots, w_n)$. Note that $\mathsf{P}_{M_1} \cap \mathsf{P}_N = \emptyset$. Now, $\varphi \in \mathcal{L}(\mathsf{P}_1)$, and hence $Q_{(N,v)}(p) = p$. The disjointness of the vocabularies ensures that $\diamond_v$ is always equivalent to $\top$. A simple induction on the structure of the input formula shows that $Q_{(N,v)}(\varphi)$ is equivalent to φ itself. The desired theorem then immediately results from Theorem 4.3. □ □

Compositional reasoning wrt. a generalized $\oslash$ composition: Our decomposition method (and the proofs) can be easily adapted to other settings. One is the application to compositional reasoning with respect to a generalization of the $\oslash$ operator, remarked in [22, Remark 2].

Definition 5.7 (Generalized $\oslash$ composition) *The* modal depth *of a formula φ is the maximum nesting of $\langle i \rangle$, $i \in I$, occurring in it. For each $n \geq 0$, and set of propositional constants P, we write $\mathcal{L}_n(\mathsf{P})$ for the collection of formulas in $\mathcal{L}(\mathsf{P})$ whose modal depth is at most n.*

Take the definition of $\diamond_0$ to be that of $\diamond$ from Definition 2.4. Define $\diamond_n$ to be the same as $\diamond$ only that instead of requiring agreement on the set of propositional constants $\mathsf{P}_M \cap \mathsf{P}_N$, we ask consistent states to satisfy the same formulas in $\mathcal{L}_n(\mathsf{P}_M \cap \mathsf{P}_N)$. Define the general composition operator $\oslash_n$ over finite models to be the same as $\oslash$ in Definition 2.5 but with $\diamond$ replaced by $\diamond_n$.

Note that $\oslash_0$ is the same as $\oslash$. All the proofs from Section 3 work for any of the generalized compositions $\oslash_n$. We only need to adapt the definitions of the $\diamond$ formulas to be in terms of the languages $\mathcal{L}_n(\mathsf{P}_M \cap \mathsf{P}_N)$. These languages are infinite. However, since $\mathsf{P}_M \cap \mathsf{P}_N$ is finite, if we quotient $\mathcal{L}_n(\mathsf{P}_M \cap \mathsf{P}_N)$ by the equivalence relation identifying every two formulas φ and ψ whenever $\varphi \leftrightarrow \psi$ is valid, then we are left with a finite language. Therefore the formula $\diamond_n$ can be expressed in $\mathcal{L}_n(\mathsf{P}_M \cap \mathsf{P}_N)$.

Another application of the decomposition method is to dynamic epistemic logic (DEL) [21]. One approach is to use reductions of DEL to the epistemic logic that we treated (see e.g. [21]) and then our Theorem 3.9. Another

interesting way is to use the logical language of DEL directly in our decomposition technique and use a result from [22, Th.18] (only for *propositionally differentiated* action models). We leave for future work the development of decomposition and quotienting results that apply directly to DEL.

6 Complexity issues

In this section, we investigate how the decomposition operator $\oslash$ affects size (which we call dimension) of the models being composed, and how the transformations Z and $\mathbf{d}$ affect the size (dimension) of the formulas. We also point out some techniques for optimizing these, though we leave the pursuit of these techniques for future work.

In what follows, for any finite set S, we denote the number of elements of S by $|S|$. Let the *dimension* of a finite model $M = (W, \to, \mathsf{P}, V)$ be $|W| + |P| + \sum_{i\in I} |\overset{i}{\to}| + \sum_{p\in\mathsf{P}} |V(p)|$. Given two models M and N, if P_M and P_N are disjoint, then the dimension of $M \oslash N$ is much larger than the sum of the dimensions of the components. In this case, the sizes of the components of the composed model $M \oslash N$ are as follows:

- $|W_{M\oslash N}| = |W_M| \times |W_N|$,
- $|\overset{i}{\to}_{M\oslash N}| = |\overset{i}{\to}_M| \times |\overset{i}{\to}_N|$,
- $|\mathsf{P}_{M\oslash N}| = |\mathsf{P}_M| + |\mathsf{P}_N|$,
- $|V_{M\oslash N}(p)| = \begin{cases} |V_M(p)| \times |W_N| & \text{if } p \in \mathsf{P}_M \\ |M_N| \times |V_N(p)| & \text{if } p \in \mathsf{P}_N \end{cases}$.

The first two equalities hold also with respect to the synchronous parallel composition between M and N. The other two are perhaps less familiar, and a bit more complicated. But clearly, the dimension of the composition $M \oslash N$ is much larger than the sum of the dimensions of the M and N when the vocabularies are disjoint. If the vocabularies of M and N are not disjoint or even coincide, the situation is more complicated. It is possible that the formulas are the same as above if the valuations of both models are uniform, providing each state with the same valuation. But it is also possible that some or even all the states be removed when eliminating the "inconsistent" states from the composition (such as when M and N have uniform valuations, but disagree on each atomic proposition), in which case the dimension of the composition can be much smaller. The techniques of this paper are most useful when the dimension of the composition is much

larger than the dimension of the parts, and where the formula translations do not increase the complexity of the formula too much.

As usual, we consider the complexity of a formula φ to be the number of occurrences of symbols in it, and call this its *dimension*.

Definition 6.1 (dimension) *Given a set* P *of atomic propositions and a function* $\alpha : \mathsf{P} \to \mathbb{N}$*, we define* $\dim[\alpha] : \mathcal{L}(\mathsf{P}) \to \mathbb{N}$ *as follows:*

- $\dim[\alpha](p) = \alpha(p)$,
- $\dim[\alpha](\neg\varphi) = \dim[\alpha](\langle i\rangle\varphi) = 1 + \dim[\alpha](\varphi)$,
- $\dim[\alpha](\varphi \vee \psi) = 1 + \dim[\alpha](\varphi) + \dim[\alpha](\psi)$
  (note that $\dim[\alpha](\bot) = \dim[\alpha](\bigvee_{i\in\emptyset}\phi_i) = 1$*.),*

When $\alpha : \mathsf{P} \to \{1\}$*, we write* dim *for* $\dim[\alpha]$.

For example, the dimension of the derived formula $p \wedge q$ is the dimension of its primitive form $\neg(\neg p \vee \neg q)$, and is thus 6.

We define $\alpha_{M\odot N} : \mathsf{P}_{M\odot N} \to \mathbb{N}$, such that

$$\alpha_{M\odot N} : \binom{\varphi}{\psi} \mapsto \dim(\varphi) + \dim(\psi) + 1.$$

We write $\rho()$ for $\dim[\alpha_{M\odot N}]$.

The formulas in the decomposition result are built in two stages, first using the function Z in Definition 3.3 and then generating the DNF of the resulting formula using the function $\mathbf{d}$ in Definition 3.7. For Z we use the Boolean formula $\diamond_{M\odot N}$ from (1).

Proposition 6.2 (Dimension of $\diamond$) *The dimensions of* $\sharp_{M\odot N}$ *and* $\diamond_{M\odot N}$ *from* (1) *are linear in the size of* $\mathsf{P}_M \cap \mathsf{P}_N$*. The dimension of the DNF of* $\diamond_{M\odot N}$ *is exponential in the size of* $\mathsf{P}_M \cap \mathsf{P}_N$*.*

Proof: It is easy to calculate that $\rho(\sharp_{M\odot N}) = 10 \times |\mathsf{P}_M \cap \mathsf{P}_N| - 1$. The presentation of $\sharp_{M\odot N}$ from (1) is also in DNF, cf. Definition 3.5. The dimension of $\diamond_{M\odot N}$ is only one more if we consider the presentation in (1) which is not in DNF. Nevertheless, when calculating the dimension of the formulas generated by $\mathbf{d}$ we need $\diamond_{M\odot N}$ in DNF. Now, $\diamond_{M\odot N}$ is the negation of a disjunction with $2 \times |\mathsf{P}_M \cap \mathsf{P}_N|$ disjuncts. Each disjunct in the DNF is a pair with complexity ranging from $4 \times |\mathsf{P}_M \cap \mathsf{P}_N|$ (where I in Definition 3.7 selects all and only the pairs whose upper coordinate is not negated)

to $6 \times |\mathsf{P}_M \cap \mathsf{P}_N|$ (where I selects all and only the pairs whose upper coordinate is negated). Thus the DNF form of $\diamond_{M \odot N}$ has dimension ranging from $2^{2 \times |\mathsf{P}_M \cap \mathsf{P}_N|}(4 \times |\mathsf{P}_M \cap \mathsf{P}_N| + 1) - 1$ to $2^{2 \times |\mathsf{P}_M \cap \mathsf{P}_N|}(6 \times |\mathsf{P}_M \cap \mathsf{P}_N| + 1) - 1$. □□

Since the dimension of $\diamond$ depends only on the (propositional vocabularies of the) models that are composed, we view it as a constant when calculating the dimension of the formula generated by Z with respect to the input formula.

Proposition 6.3 (Dimension of Z) *The dimension of the formula $Z(\varphi)$ from Definition 3.3 is linear in the size of the input formula φ.*

Proof: It is easy to calculate that

- $\rho(Z(p)) = 3$ for $p \in \mathsf{P}_M \cup \mathsf{P}_N$;
- $\rho(Z(\phi_1 \vee \phi_2)) = \rho(Z(\phi_1)) + \rho(Z(\phi_2))) + 1$;
- $\rho(Z(\neg\phi)) = \rho(Z(\phi)) + 1$;
- $\rho(Z(\langle i \rangle \phi)) = \rho(Z(\phi)) + 1 + \rho(\diamond)$.

The claim now follows immediately. □ □

To calculate the dimension of the formulas in disjunctive normal form, resulting from the function **d** in Definition 3.7, applied to formulas $Z(\varphi)$, we involve a notion of *disjunctive dimension*; this is the number of disjuncts in a DNF.

Definition 6.4 (Disjunctive dimension) *For a formula Φ in $\mathbf{D}(\mathsf{P}_{M \odot N})$, the* disjunctive dimension*, denoted $\delta(\Phi)$, is defined to be the number of occurrences in Φ of elements from $\mathsf{P}_{M \odot N}$.*

Note that the dimension of a formula in $\mathbf{D}(\mathsf{P}_{M \odot N})$ is at least as large as its disjunctive dimension.

Proposition 6.5 *Let $\Phi \in \mathcal{L}(\mathsf{P}_{M \odot N})$ be a formula with a nesting of $k+1$ ($k \geq 0$) negation symbols. Then*

$$\delta(\mathbf{d}(\Phi)) \geq \left.\begin{matrix} 2^{\cdot^{\cdot^{\cdot^{2}}}} \end{matrix}\right\} k \text{ occurrences of } 2.$$

Proof: (Sketch) From Definition 3.7, we observe that $\delta(\mathbf{d}(\neg\Phi)) = 2^{\delta(\mathbf{d}(\Phi))}$. The desired result follows from a simple induction on the number of negations that are nested. □ □

For calculating the disjunctive dimension of $\mathbf{d}$ applied to $Z(\varphi)$ in terms of the dimension of φ, observe that Z introduces, for every occurrence of a modal operator $\langle i\rangle$ in φ, a conjunction symbol, which is an abbreviation for an expression with negation symbols. Furthermore, for a nesting of $k > 0$ modal operators $\langle i\rangle$, Z introduces a nesting of $2k$ negation operators, and hence by Proposition 6.5, the disjunctive dimension of $\mathbf{d}(Z(\varphi))$ is at least a tower of $2k-1$ exponents. As the disjunctive dimension is a lower bound to the actual dimension, this means that the dimension of $\mathbf{d}(Z(\varphi))$ is at least a tower of $2k-1$ exponents.

To reduce these dimensions, one may investigate the use of *term graphs* (see [11] or [2, Sec. 4.4]) to identify repeated subformulas. One may also consider representing formulas as *binary decision diagrams* (see [6]). A direct method could be to process φ or $Z(\varphi)$, so as to remove double negations, or to identify patterns of negation and disjunction that allow us to apply the conjunctive item of Lemma 3.6. Furthermore, each step of the translation reduction methods in the style of [1] could be applied to eliminate redundant formulas by simple Boolean evaluations.

References

[1] H. R. Andersen. Partial model checking (extended abstract). In *10th IEEE Symposium on Logic in Computer Science (LICS'95)*, pages 398–407. IEEE Computer Society, 1995.

[2] F. Baader and T. Nipkow. *Term Rewriting and All That*. Cambridge University Press, 1998.

[3] J. C. M. Baeten, T. Basten, and M. A. Reniers. *Process Algebra: Equational Theories of Communicating Processes*. Cambridge Tracts in Theoretical Computer Science 50. Cambridge University Press, 2009.

[4] A. Baltag and L. S. Moss. Logics for epistemic programs. *Synthese*, 139(2):165–224, 2004.

[5] B. Bloom, W. Fokkink, and R. J. van Glabbeek. Precongruence formats for decorated trace semantics. *ACM Transactions on Computational Logic*, 5(1):26–78, 2004.

[6] R. E. Bryant. Graph-based algorithms for boolean function manipulation. *IEEE Trans. Computers*, 35(8):677–691, 1986.

[7] I. Castellani, M. Mukund, and P. Thiagarajan. Synthesizing distributed transition systems from global specifications. In C. Rangan, V. Raman, and R. Ramanujam, editors, *Foundations of Software Technology and Theoretical Computer Science*, volume 1738 of *Lecture Notes in Computer Science*, pages 219–231. Springer Berlin / Heidelberg, 1999.

[8] W. Fokkink, R. J. van Glabbeek, and P. de Wind. Compositionality of Hennessy-Milner logic by structural operational semantics. *Theoretical Computer Science*, 354(3):421–440, 2006.

[9] M. Hennessy and R. Milner. Algebraic laws for nondeterminism and concurrency. *Journal of ACM*, 32(1):137–161, 1985.

[10] C. A. R. Hoare. *Communicating Sequential Processes*. Prentice Hall, 1985.

[11] D. Kozen. Complexity of finitely presented algebras. In *Proceedings of the ninth annual ACM Symposium on Theory of Computing*, pages 164–177. ACM, 1977.

[12] D. Kozen. Results on the propositional mu-calculus. *Theoretical Computer Science*, 27:333–354, 1983.

[13] F. Laroussinie and K. G. Larsen. Compositional model checking of real time systems. In *6th International Conference on Concurrency Theory (CONCUR'95)*, volume 962 of *Lecture Notes in Computer Science*, pages 27–41. Springer, 1995.

[14] K. G. Larsen and L. Xinxin. Compositionality through an operational semantics of contexts. *Journal of Logic and Computation*, 1(6):761–795, 1991.

[15] A. Lomuscio and F. Raimondi. The complexity of model checking concurrent programs against CTLK specifications. In H. Nakashima, M. P. Wellman, G. Weiss, and P. Stone, editors, *5th International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS 2006)*, pages 548–550. ACM, 2006.

[16] G. F. McNulty. Fragments of first order logic, I: Universal Horn logic. *The Journal of Symbolic Logic*, 42(2):pp. 221–237, 1977.

[17] J.-J. C. Meyer and W. van der Hoek. *Epistemic Logic for Computer Science and Artificial Intelligence*. Cambridge Tracts in Theoretical Computer Science 41. Cambridge University Press, 1995.

[18] R. Milner. Calculi for synchrony and asynchrony. *Theorethical Computer Science*, 25:267–310, 1983.

[19] R. Milner. *Communication and Concurrency*. Prentice Hall, 1989.

[20] S. Mohalik and R. Ramanujam. A presentation of regular languages in the assumption - commitment framework. In *Proceedings of the 1998 International Conference on Application of Concurrency to System Design*, ACSD '98, pages 250–260, Washington, DC, USA, 1998. IEEE Computer Society.

[21] H. van Ditmarsch, W. van der Hoek, and B. Kooi. *Dynamic Epistemic Logic*. Springer, 2007.

[22] J. van Eijck, F. Sietsma, and Y. Wang. Composing models. *Journal of Applied Non-Classical Logics*, 21(3–4):397–425, 2011.

[23] G. Winskel. A complete system for SCCS with modal assertions. In S. N. Maheshwari, editor, *5th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'85)*, volume 206 of *Lecture Notes in Computer Science*, pages 392–410. Springer, 1985.

A Additional results and complete proofs

A.1 Synchronous vs asynchronous composition

As the primary composition that we have studied in the main body of the paper is a type of synchronous composition, we investigate some properties of synchronous composition.

Definition A.1 *Let* $K = (W_K, \to_K)$ *and* $J = (W_J, \to_J)$ *be two Kripke frames. Their* synchronous composition *is* $K\|_s J = (W, \to_s)$ *and their* asynchronous composition *is* $K\|_a J = (W, \to_a)$*, where*

- $W = W_K \times W_J$,
- $(w_1, v_1) \xrightarrow{i}_s (w_2, v_2)$ *if and only if* $w_1 \xrightarrow{i} w_2$ *and* $v_1 \xrightarrow{i} v_2$,
- $(w_1, v_1) \xrightarrow{i}_a (w_2, v_2)$ *if and only if both* $w_1 \xrightarrow{i} w_2$ *and* $v_1 = v_2$ *or both* $w_1 = w_2$ *and* $v_1 \xrightarrow{i} v_2$.

The following two results lend motivation for basing the composition $\oslash$ (originally from [22]) for epistemic models on the synchronous rather than the asynchronous composition.

Proposition A.2 *For relational structures (Kripke models, FSMs, etc.) the property of being equivalence relations (particularly the transitivity) is preserved under synchronous composition (under the standard definition from automata theory or process calculi).*

Proof: It is simple to check that all three properties of an equivalence relation, i.e., reflexivity, transitivity, and symmetry, are preserved. In other words, taking two S5 relational models (i.e., the relational models that represent equivalence relations) then their synchronous composition is also an S5 model. □ □

Proposition A.3 Asynchronous *composition does not preserve the transitivity property of epistemic models (S5^n) models, and hence epistemic models are* not *closed under asynchronous composition.*

Proof: Consider one model with states a and b, and transitions from each state to all states (i.e., $(a,b),(b,a),(a,a),(b,b) \in R$). Similarly consider a model with states x and y, and transitions from each state to all states. These two models are S5, but their asynchronous composition lacks transitivity: there are transitions from (a,x) to (a,y) and from (a,y) to (b,y), but there is no transition from (a,x) to (b,y). □ □

A.2 Belief models

The logic of belief, *doxastic logic*, often uses models that are *serial* (every relation R is such that for all elements x there is a y such that xRy), *transitive* (every relation R is such then if xRy and yRz, then xRz), and *Euclidean* (every relation R is such that if xRy and xRz, then yRz). We call this class of models KD45^n, after the axiom system KD45^n that characterizes them [17].

Proposition A.4 *The epistemic composition $\oslash$ (Definition 2.5) does not preserve the seriality property of KD45^n models, and hence the class of KD45^n models is not closed under $\oslash$.*

Proof : Consider one model with states a and b with aRb and bRb, and consider another model with states x and y with xRy and yRy. These relational structures are serial, transitive, and Euclidean, and hence KD45^n. Furthermore suppose both models have propositional vocabulary p, and the first model assigns p to both a and b, but the second model only assigns p to x. Then the composition will consist of just (a, x) and (b, x), and with no relational connections. Thus the model resulting from the composition is not serial. □ □

B Compositional reasoning for Dynamic Epistemic Logic

The results of this paper (Theorem 3.9 and Theorem 4.3) can indirectly be applied to dynamic epistemic logic (DEL) [21], and we show here how this can be done. Dynamic epistemic logic involves *action models*, which are tuples $(W, \rightarrow, \mathrm{pre})$, such that $(W, \rightarrow)$ is a Kripke frame (usually S5^n), and pre is a function mapping each point $a \in W$ to a formula of DEL. The language of DEL extends epistemic logic with formulas of the form $[A, a]\varphi$, where (A, a) is a pointed action model. As you can see, the language and the action model are defined by mutual recursion. The semantics of $[A, a]\varphi$ is defined by

- $(M, w) \models [A, a]\varphi$ if and only if whenever $(M, w) \models \mathrm{pre}(a)$, we also have $M[A], (w, a) \models \varphi$,

where $M[A]$ is the update product (a variation of synchronous composition) of M and A; and similar to $\oslash$, it also involves potentially removing states.

The theorem [22, Th.18] asserts that if A is a propositionally differentiated action model [22, Definition 7], then for any two S5^n Kripke models M and

N,

$$(M \oslash N)[A] \leftrightarrows (M[A] \oslash N[A]),$$

where $\leftrightarrows$ represents total bisimilarity over pointed epistemic models. So if we want to check if $(M \oslash N, (w, v)) \models [A, a]\varphi$, then we first check if $(M \oslash N, (w, v)) \models \mathrm{pre}(a)$. If not, then $(M \oslash N, (w, v)) \models [A, a]\varphi$ is true. If so, then the truth of $(M \oslash N, (w, v)) \models [A, a]\varphi$ is equivalent to the truth of $(M \oslash N)[A], ((w, v), a) \models \varphi$. By [22, Th.18] and the fact that bisimilar states satisfy the same dynamic epistemic logic formulas, this is equivalent to

$$(M[A] \oslash N[A]), ((w, a), (v, a)) \models \varphi.$$

If φ an epistemic logic formula, then we can apply the decomposition result Theorem 3.9 or quotenting result Theorem 4.3. If not, then the situation becomes more complicated. Decomposition or quotienting results have not yet been developed for dynamic epistemic logic formulas directly. But we can apply a truth preserving translation of φ into epistemic logic (see [21] for various types of truth preserving translations of DEL into epistemic logic), and then we can apply the results of this paper. Now we point out here that we could have applied a truth preserving translation to the original formula $[A, a]\varphi$. When it is advantageous to translate $[A, a]\varphi$ directly or to apply the method discussed in this section remains to be determined.