A separation logic with histories of epistemic actions as resources

Hans van Ditmarsch[1], Didier Galmiche[2], and Marta Gawek[2]

[1] Université de Toulouse, CNRS, IRIT, France
[2] Université de Lorraine, CNRS, LORIA, France

Abstract. We propose a separation logic where resources are histories (sequences) of epistemic actions so that resource update means concatenation of histories and resource decomposition means splitting of histories. This separation logic, called AMHSL, allows us to reason about the past: does what is true now depend on what was true in the past, before certain actions were executed? We show that the multiplicative connectives can be eliminated from a logical language with also epistemic and action model modalities, if the horizon of epistemic actions is bounded.

1 Introduction

In an action that is an informative update, what the agents know about facts and about each other may change (I learn that it rains in Spain), and these facts themselves may also change (it stopped raining). We present a logic wherein the amount of change, as measured by sequences of actions that are informative updates, is considered as a resource. In an epistemic context such updates often depend on each other (after it stopped raining, I cannot learn that it rains in Spain), so it is relevant when, as resources, they can be separated and combined with the multiplicative connectives of the Bunched Implications logic (BI) [15]. Let us survey the relevant areas dynamic epistemic logic and bunched separation logic, and describe prior proposals to combine both.

Knowledge and change of knowledge, and in particular for multiple agents, are the abode of epistemic logic [19], a modal logic interpreted on relational models consisting of possible worlds. The analysis of multiple agents publicly informing each other of their ignorance and knowledge culminated in Public Announcement Logic [14], and a further generalization non-public information change such as private or secret announcements resulted in Action Model Logic [3], further extended with factual change in [17]. Another source of our ideas is the logic of Bunched Implications (BI) and its variants, like Boolean BI (BBI) [15], that mainly focus on resource sharing and separation. These logics combine additive ($\wedge$, $\rightarrow$, $\vee$) and multiplicative ($*$, $-\!*$) connectives. The multiplicative conjunction $*$ expresses separation of resources and the multiplicative implication $-\!*$ expresses resource update [15]. Here the term "separation logics" denotes the class of logics based on BI or BBI and their modal extensions, even if so-called Separation Logic is such a logic with resources being memory areas [10].

How can we combine knowledge and resources? It is a two-way traffic. One can go in the direction of modelling uncertainty about resources [8,7]. But one can also go in the direction of modelling information as a resource. We very clearly go in that, novel, direction. We notice that this is a dangerous road: incoming information is highly dependent on context and may have side effects, so it is difficult to separate/decompose, which goes against the grain of separation logics. But it is therefore a challenge we propose to meet. Both directions, inasfar as discussed here, have in common that we add modalities to separation logics (either epistemic or dynamic) [8]. Epistemic extensions of separation logic include Public Announcement Separation Logic [7], and the further generalization called Action Model Separation Logic [18]. In these logics the states or worlds of an epistemic model represent resources, resource decomposition and update relate different states in the domain of the model, and the members of the domain of a Kripke model should therefore represent a resource monoid. In [18] the valuation of a state is a resource, instead of the state, so that different states with the same valuation can represent the same resource.

In this work we consider *histories of epistemic actions* as resources. It is both according to the philosophy of separation, as in many epistemic contexts one can run of out resources, such as exceeding the permitted number of calls in a gossip protocol or the number of manipulations in epistemic planning [5]; but also somewhat against the philosophy of separation, as the knowledge consequences of epistemic actions highly depend on their order and may also lack certain monotonicity of knowledge consequences. However, in the special case where factual change is absent, ignorance can only be lost, whereas positive knowledge (the universal fragment) continues to grow.

We propose a new separation logic with sequences of actions (informative updates) as resources, called Action Model History Separation Logic (AMHSL). Instead of states we consider sequences of actions (histories) to be resources, and consequently we define resource composition as the concatenation of histories. This requires another interpretation of the multiplicative connectives. As the order of actions is non-trivial, the multiplicative conjunction interpreting resource composition is non-commutative, and there are two ways of resource update: appending a history to the end of a given history, or before its beginning. We therefore need two multiplicative implications in the logical language. After defining this logical semantics of separation and composition of actions histories we illustrate the interest of AMHSL with an example about gossip protocols. Finally we show that, given a maximum length of action histories, any AMHSL formula with multiplicative connectives is equivalent to a formula without them: a so-called reduction. As the latter is a formula in action model logic, we have thus also axiomatized AMSHL.

2 Semantics with informative actions as resources

We first present the syntax of the logical language and the semantical structures.

Let a finite set of *agents* A and a (disjoint) countable set of *atoms* (or *propositional variables*) P be given.

Definition 1 (Language). *The logical language* $\mathcal{L}^{K*\otimes}(A,P)$ *is defined by a BNF, where* $p \in P$*,* $a \in A$*, and* $\mathcal{E}_e$ *is a pointed action model, defined below.*

$$\psi ::= \quad p \mid I \mid \bot \mid \neg\psi \mid (\psi \wedge \psi) \mid (\psi * \psi) \mid (\psi \mathrel{-\!\!*} \psi) \mid (\psi \mathrel{*\!\!-} \psi) \mid K_a\psi \mid [\mathcal{E}_e]\psi$$

The parameters A and P are often omitted from $\mathcal{L}^{K*\otimes}(A,P)$. We also consider the sublanguage $\mathcal{L}^{K\otimes}$ without the constructs containing $*$, $\mathrel{-\!\!*}$ and $\mathrel{*\!\!-}$ and without the constant I (the language of action model logic), the sublanguage $\mathcal{L}^{K*}$ without the construct $[\mathcal{E}_e]\psi$ (the language of epistemic separation logic), and the sublanguage $\mathcal{L}^{K}$ without either (the language of epistemic logic). It is implicit in the definition that the pre- and postcondition formulas of $\mathcal{E}$ are in $\mathcal{L}^{K\otimes}$ (Def. 4). For the sublanguage of $\mathcal{L}^{K*\otimes}$ only allowing the unique action model $\mathcal{E}$ we write $\mathcal{L}^{K*\mathcal{E}}$ and similarly for other fragments. Other propositional connectives are defined by notational abbreviation and also the dual modality $\langle\mathcal{E}_c\rangle\varphi := \neg[\mathcal{E}_e]\neg\varphi$.

Definition 2 (Resource monoid). *A* partial resource monoid *(or* resource monoid*) is a structure* $\mathcal{R} = (R, \circ, n)$ *where* R *is a set of* resources *(denoted* $r, r', r_1, r_2, \dots$*) containing a* neutral element n*, and where* $\circ : R \times R \to R$ *is a* resource composition operator *that is associative, that may be partial and such for all* $r \in R$*,* $r \circ n = n \circ r = r$*. If* $r \circ r'$ *is defined we write* $r \circ r'{\downarrow}$ *and if* $r \circ r'$ *is undefined we write* $r \circ r'{\uparrow}$*. When writing* $r \circ r' = r''$ *we assume that* $r \circ r'{\downarrow}$*.*

Definition 3 (Epistemic model). *An* epistemic model *is a structure* $\mathcal{M} = (S, \sim, V)$ *such that* S *is a non-empty* domain *of* states *(or* worlds*),* $\sim : A \to \mathcal{P}(S \times S)$ *is a function that maps each agent* a *to an equivalence relation* $\sim_a$*, and* $V : P \to \mathcal{P}(S)$ *is a* valuation function*, where* $V(p)$ *denotes where variable* p *is true. Given* $s \in S$*, the pair* $(\mathcal{M}, s)$ *is a* pointed epistemic model*, denoted* $\mathcal{M}_s$*.*

Definition 4 (Action model). *An* action model *is a structure* $\mathcal{E} = (E, \approx, pre, post)$*, where* E *is a non-empty finite domain of* actions *(denoted* $e, f, g, \dots$*),* $\approx_a$ *an equivalence relation on* E *for all* $a \in A$*,* $pre : E \to \mathcal{L}^{K\otimes}$ *is a* precondition *function, and* $post : E \to P \to \mathcal{L}^{K\otimes}$ *is a* postcondition *function such that every* $post(e)$ *is only finitely different from the identity: we can see its domain as a finite set of variables* $Q \subseteq P$*. Given* $e \in E$*, a* pointed action model *(or* epistemic action*) is a pair* $(\mathcal{E}, e)$*, denoted* $\mathcal{E}_e$*.*

2.1 Knowledge and informative actions

We distinguish the semantics of knowledge and action model execution on epistemic models, from the more involved semantics of the full language on epistemic history models. The distinction is made to keep the exposition transparant, because we wish to focus on information change as separation and composition, and because it allows us to use a simpler, abbreviated, notation for the latter.

For the satisfaction relation of the former we write $\models_0$ and for that of the latter we write $\models$. The $\models_0$ update semantics is standard fare (although less so with the variation involving factual change) and can be found in, for example [17,13]. Definitions. 5 and 6 are assumed to be given by simultaneous recursion.

Definition 5 (Satisfaction relation for the restricted language). *The* satisfaction relation $\models_0$ *between pointed epistemic models* $\mathcal{M}_s$ *and formulas in* $\mathcal{L}^{K\otimes}(A,P)$*, where* $\mathcal{M} = (S, \sim, V)$ *and* $s \in S$*, is defined by induction on formula structure.*

$$\begin{array}{lll}
\mathcal{M}_s \models_0 p & \textit{iff} & s \in V(p) \\
\mathcal{M}_s \models_0 \bot & \textit{iff} & \textit{false} \\
\mathcal{M}_s \models_0 \neg\varphi & \textit{iff} & \mathcal{M}_s \not\models_0 \varphi \\
\mathcal{M}_s \models_0 \varphi \wedge \psi & \textit{iff} & \mathcal{M}_s \models_0 \varphi \textit{ and } \mathcal{M}_s \models_0 \psi \\
\mathcal{M}_s \models_0 K_a\varphi & \textit{iff} & \mathcal{M}_{s'} \models_0 \varphi \textit{ for all } s' \in S \textit{ such that } s \sim_a s' \\
\mathcal{M}_s \models_0 [\mathcal{E}_e]\varphi & \textit{iff} & \mathcal{M}_s \models_0 \textit{pre}(e) \textit{ implies } (\mathcal{M} \otimes \mathcal{E})_{(s,e)} \models_0 \varphi
\end{array}$$

Definition 6 (Action model execution). *Given are epistemic model* $\mathcal{M} = (S, \sim, V)$ *and action model* $\mathcal{E} = (E, \approx, \textit{pre}, \textit{post})$*. The updated epistemic model* $\mathcal{M} \otimes \mathcal{E} = (S', \sim', V')$ *is such that — where* $s, t \in S$*,* $a \in A$*,* $e, f \in E$*,* $p \in P$*:*

$$\begin{array}{lll}
S' & = & \{(s,e) \mid \mathcal{M}_s \models_0 \textit{pre}(e)\} \\
(s,e) \sim_a (t,f) & \textit{iff} & s \sim_a t \textit{ and } e \approx_a f \\
(s,e) \in V'(p) & \textit{iff} & \mathcal{M}_s \models_0 \textit{post}(e)(p)
\end{array}$$

2.2 Semantics for separation and composition of action histories

We now present the $\models$ semantics, that is defined on the full language. The semantics interprets formulas with respect to states in an initial model and sequences of informative actions (or events). This is known as a history-based semantics, where the sequence of actions is the history of past actions [16]. The corresponding semantic objects are often known as 'history-based models' and called here *history models*. Updates of models with action models construct such history models. However, as constructing history models requires evaluating formulas and as formulas are interpreted in history models, the semantics are given by simultaneous induction involving both.

Definition 7 (Epistemic history model). *Given are epistemic model* $\mathcal{M} = (S, \sim, V)$ *and action model* $\mathcal{E} = (E, \approx, \textit{pre}, \textit{post})$*. First, we define* $\mathcal{M} \otimes \mathcal{E}^n$ *by induction on* $n \in \mathbb{N}$ *as:* $\mathcal{M} \otimes \mathcal{E}^0 := \mathcal{M}$*, and* $\mathcal{M} \otimes \mathcal{E}^{n+1} := (\mathcal{M} \otimes \mathcal{E}^n) \otimes \mathcal{E}$*. The* epistemic history model $\mathcal{M}\mathcal{E}^\omega$ *is now defined as* $\oplus_{n\in\mathbb{N}}(\mathcal{M} \otimes \mathcal{E}^n)$*, where* $\oplus$ *is the direct sum. We also distinguish the* bounded *epistemic history model* $\mathcal{M}\mathcal{E}^{\mathbf{max}}$ *defined as* $\oplus_{n\leq\mathbf{max}}(\mathcal{M} \otimes \mathcal{E}^n)$*, where we assume that* $\mathbf{max} \geq 1$.

Histories of actions. The elements of the domain of $\mathcal{M}\mathcal{E}^\omega$ have the shape $(s, e_1, \ldots, e_n)$ where $e_1, \ldots, e_n \in E$ for $n \in \mathbb{N}$, and where for $n = 0$ the domain element is s. The tuple of actions $(e_1, \ldots, e_n)$ is called a *history*, denoted h, where ϵ is the empty history. Given $(s, e_1, \dots, e_n)$, we also say that the history $(e_1, \dots, e_n)$ can be *executed* in the state s. For $(s, e_1, \dots, e_n)$ we write $se_1 \dots e_n$ or sh, where $h = e_1 \dots e_n$. In other words, we consider a history h to be a member of E^*. Given history h, $|h|$ denotes its length, and for concatenation of histories h, h' we write hh'. We let $\sqsubseteq$ be the prefix relation on histories, ($\epsilon \sqsubseteq h$, and if $h \sqsubseteq h'$, then $h \sqsubseteq h'e$), and if $h' \sqsubseteq h$, then $h \backslash h'$ is the 'postfix' following h', that is, $h = h'(h \backslash h')$. Indistinguishability of histories is defined as: $\epsilon \sim_a \epsilon$, and if $h \sim_a h'$ for histories h, h' and also $e \sim_a e'$, then $he \sim_a h'e'$. Finally, given $sh, s'h' \in \mathcal{D}(\mathcal{M}\mathcal{E}^\omega)$, $sh \sim_a s'h'$ means that $s \sim_a s'$ and $h \sim_a h'$. Note that indistinguishable histories are of the same length (in this synchronous semantics).

Alternative history models. Another way to define history-based models seems more common in the literature [16,20]. We then enrich the model $\mathcal{M}\mathcal{E}^\omega$ with relations $\to_e$ for all $e \in E$ defined as: $sh \to_e she$ for all $sh, she \in \mathcal{D}(\mathcal{M}\mathcal{E}^\omega)$. Note that this assumes $\mathcal{M}\mathcal{E}^\omega_{sh} \models pre(e)$. In other words, the model transforming updates induced by action models $\mathcal{E}$ are internalized as transitions between the (state,history) pairs of the domain of the epistemic history model. This modelling facilitates the comparison with temporal epistemic logics.

Histories as resources. Inspired by the action monoids of [6], we now take histories as resources, such that the set of histories of actions is a resource monoid with concatenation of histories as resource composition and the empty history ϵ as neutral element. For $h \circ h'$ we write hh', as above. Evidently this 'resource composition' (concatenation) is associative, and also $\epsilon \circ h = h \circ \epsilon = h$. As histories can always be concatenated, resource composition is always defined. However, for some applications there is a maximum length **max** of histories, such that $hh'\!\uparrow$ then means that $|hh'| > \mathbf{max}$. Seeing histories as resources, it seems to make sense that you run out of actions if you execute too many. As the order of actions, and histories, matters, the multiplicative conjunction $(*)$ is not commutative, and to maintain duality we need two different multiplicative implications: one for what is true after appending an arbitrary history to a given history $(-\!\!*)$, and another one for what is true after appending a given history to an arbitrary history $(*\!\!-)$.

We now define the semantics. Instead of interpreting a formula in a state of an epistemic model, we interpret it in a (state,history) pair of an epistemic history model.

Below, 'there is sh' means 'there is h such that $sh \in \mathcal{D}(\mathcal{M}\mathcal{E}^\omega)$', in other words, there is a history h such that h can be executed in state s; and similarly for 'for all sh'. Note that both imply that $h\!\downarrow$, that is, $|h| \leq \mathbf{max}$. For example, "for all sh, shh'" in the clause for $-\!\!*$ means "for all $h' \in E^*$ such that $|hh'| \leq \mathbf{max}$ and $shh' \in \mathcal{D}(\mathcal{M})$". We recall that $h = h'h''$ means that $h'h''\!\downarrow$ and $h = h'h''$.

Definition 8 (Satisfaction relation). *The* satisfaction relation $\models$ *between a pointed epistemic history model* $\mathcal{M}\mathcal{E}^\omega_{sh}$ *and formulas in* $\mathcal{L}^{K*\mathcal{E}}(A, P)$*, where* $\mathcal{M} = (S, \sim, V)$*,* $\mathcal{E} = (E, \approx, pre, post)$*,* $s \in S$*, and* $h \in E^*$*, is defined by induction on formula structure. Model* $\mathcal{M}\mathcal{E}^\omega$ *is left implicit in the notation, and* $\mathcal{E}$ *is left* *implicit in* $[\mathcal{E}_e]\varphi$.

$$\begin{array}{lll}
sh \models p & \textit{iff} & s \models \mathit{post}(h)(p) \\
sh \models I & \textit{iff} & h = \epsilon \\
sh \models \bot & \textit{iff} & \textit{false} \\
sh \models \neg\varphi & \textit{iff} & sh \not\models \varphi \\
sh \models \varphi \wedge \psi & \textit{iff} & sh \models \varphi \textit{ and } sh \models \psi \\
sh \models \varphi * \psi & \textit{iff} & \textit{there are } sh', sh'' \textit{ with } h = h'h'' \textit{ such that } sh' \models \varphi \textit{ and } sh'' \models \psi \\
sh \models \varphi \mathrel{-\!\!*} \psi & \textit{iff} & \textit{for all } sh', shh' : sh' \models \varphi \textit{ implies } shh' \models \psi \\
sh \models \varphi \mathrel{*\!\!-} \psi & \textit{iff} & \textit{for all } sh', sh'h : sh' \models \varphi \textit{ implies } sh'h \models \psi \\
sh \models K_a\varphi & \textit{iff} & s'h' \models \varphi \textit{ for all } s'h' \textit{ such that } sh \sim_a s'h' \\
sh \models [e]\varphi & \textit{iff} & sh \models \mathit{pre}(e) \textit{ implies } she \models \varphi
\end{array}$$

On $\mathcal{ME}^{\mathbf{max}}$ *all clauses are the same except the last one, that then becomes:*

$$sh \models [e]\varphi \textit{ iff } |h| < \mathbf{max} \textit{ and } sh \models \mathit{pre}(e) \textit{ imply } she \models \varphi$$

For $s\epsilon \models \varphi$ *we write* $s \models \varphi$. *The simplified notation is justified because all formulas are interpreted in the one and only model* $\mathcal{ME}^\omega$, *unlike in the* $\models_0$ *semantics. We emphasize that the language of interpretation is* $\mathcal{L}^{K*\mathcal{E}}$ *(with action modalities only for* $\mathcal{E}$*) and not* $\mathcal{L}^{K*\otimes}$ *(for arbitrary action model modalities).*

There are two notions of validity. A formula φ *is* valid, *notation* $\models \varphi$, *iff for all* $\mathcal{M} = (S, \sim, V)$ *and* $s \in S$, $s \models \varphi$. *A formula* φ *is* $*$-valid, *or* always-valid, *notation* $\models^* \varphi$,[3] *iff for all* $\mathcal{M} = (S, \sim, V)$ *and* $\mathcal{E} = (E, \approx, \mathit{pre}, \mathit{post})$ *and for all* $sh \in \mathcal{D}(\mathcal{ME}^\omega)$, $sh \models \varphi$. *Validity is similarly defined on* $\mathcal{ME}^{\mathbf{max}}$.

In fact we defined two semantics, one without a bound on action histories and one with the bound **max**, but we write $\models$ for both satisfaction relations (and $\models^*$). The validities in Section 4 are restricted to the semantics with bound **max**.

Lemma 1.

1. *For all* $\varphi \in \mathcal{L}^{K*\mathcal{E}}$*:* $\models \varphi$ *iff* $\models^* I \to \varphi$.
2. *For all* $\varphi \in \mathcal{L}^{K*\mathcal{E}}$*:* $\models^* \varphi$ *implies* $\models \varphi$.
3. *For all* $\varphi \in \mathcal{L}^{K\mathcal{E}}$*:* $\models_0 \varphi$ *iff* $\models \varphi$.

Proof.

1. Observe that I is only true for the empty history.
2. If a formula is true for arbitrary histories, then also for the empty history.
3. Let $\mathcal{M} = (S, \sim, V)$, and $s \in S$ be given. Then $\mathcal{M}_s \models_0 \varphi$, iff $s \models \varphi$, where the latter is in model $\mathcal{ME}^\omega$. The proof by induction on φ is obvious except for the case $[e]\varphi$ that directly follows from the semantics.

[3] The $*$ of multiplicative conjunction $\varphi * \psi$ is as the $*$ in $*$-valid, but the latter is motivated by the Kleene-$*$ of arbitrary iteration.

Histories in the language. A fair number of properties of our history semantics are more elegantly presented if we allow histories in the language. For example it is convenient to think of the precondition or the postcondition of a history, not only of an action. We recursively define by notational abbreviation: (i) $[\epsilon]\varphi := \varphi$ and $[he]\varphi := [h][e]\varphi$; (ii) $\mathit{pre}(\epsilon) := \top$ and $\mathit{pre}(he) := \langle h\rangle \mathit{pre}(e)$; (iii) $\mathit{post}(\epsilon)(p) := p$ and $\mathit{post}(he)(p) := \langle h\rangle \mathit{post}(e)(p)$.

Given modalities for histories, the usual reduction axioms for action model logic can generalized in an obvious way. That is, all except the reduction axiom $[e][f]\varphi \leftrightarrow [e \circ f]\varphi$, where $\circ$ is action model composition, as $\mathcal{E} \circ \mathcal{E}$ is typically another action model than $\mathcal{E}$, that is not in the language $\mathcal{L}^{K\mathcal{E}}$ for the unique action model $\mathcal{E}$. As we reduce history modalities instead of action modalities we do not need that axiom.

Proposition 1. *All valid in the* $\models_0$ *semantics are*

$$\begin{array}{ll|ll}
[e]p & \leftrightarrow \mathit{pre}(e) \rightarrow \mathit{post}(e)(p) & [h]p & \leftrightarrow \mathit{pre}(h) \rightarrow \mathit{post}(h)(p) \\
[e]\neg\varphi & \leftrightarrow \mathit{pre}(e) \rightarrow \neg[e]\varphi & [h]\neg\varphi & \leftrightarrow \mathit{pre}(h) \rightarrow \neg[h]\varphi \\
[e](\varphi \wedge \psi) & \leftrightarrow [e]\varphi \wedge [e]\psi & [h](\varphi \wedge \psi) & \leftrightarrow [h]\varphi \wedge [h]\psi \\
[e]K_a\varphi & \leftrightarrow \mathit{pre}(e) \rightarrow \bigwedge_{e \sim_a f} K_a[f]\varphi & [h]K_a\varphi & \leftrightarrow \mathit{pre}(h) \rightarrow \bigwedge_{h \sim_a h'} K_a[h']\varphi
\end{array}$$

Proof. All the left are standard [21]. All the right follow from the left. The proof is by induction on the length of history h. The inductive clauses are all elementary (omitted, however for inductive case $[he]K_a\varphi$ observe that $he \sim_a h'e'$ if $h \sim_a h'$ and $e \sim_a e'$), and only the basic clause $h = \epsilon$ may need some attention.

- $[\epsilon]p = p$ which is equivalent to $\mathit{pre}(\epsilon) \rightarrow \mathit{post}(\epsilon)(p) = \top \rightarrow p$.
- $[\epsilon]\neg\varphi = \neg\varphi$, which is equivalent to $\mathit{pre}(\epsilon) \rightarrow \neg[\epsilon]\varphi = \top \rightarrow \neg\varphi$.
- $[\epsilon](\varphi \wedge \psi) = \varphi \wedge \psi$, which is equivalent to $[\epsilon]\varphi \wedge [\epsilon]\psi = \varphi \wedge \psi$.
- $[\epsilon]K_a\varphi = K_a\varphi$, which is equivalent to $\mathit{pre}(\epsilon) \rightarrow \bigwedge_{\epsilon \sim_a h'} K_a[h']\varphi = \top \rightarrow K_a[\epsilon]\varphi = \top \rightarrow K_a\varphi$, which is equivalent to $K_a\varphi$.

A corollary of Lemma 1 and Prop. 1 is that these history reduction axioms are also valid for the $\models$ semantics, where the formulas φ, ψ ocurring in them are from $\mathcal{L}^{K\mathcal{E}}$, and it is also straightforward to observe that they remain $\models$ valid if $\varphi, \psi \in \mathcal{L}^{K*\mathcal{E}}$. This is what we need in Section 4.[4]

3 Gossip protocols with AMHSL

In gossip protocols we investigate dissemination of information through a network by way of peer-to-peer calls. Each agent holds a ‘secret’, that is, some piece of information private to that agent only. The goal of the information exchanges is that all agents know all secrets. In a call the callers exchange all the secrets they know. In an epistemic gossip protocol [22] only calls are permitted that

[4] They are all even $*$-valid in the $\models$ semantics, on models $\mathcal{ME}^{\omega}$, but not on models $\mathcal{ME}^{\mathbf{max}}$ as that would need relativization of each axiom to $\neg[h]\bot \rightarrow$. However we will not use (nor claim) that.

satisfy a certain logical condition. In the protocol LNS [1] you may only call another agent if you do not know that agent's secret. In the protocol CMO [22] you may only call another agent if you have not been involved in a call with that agent. Note that a LNS-permitted call is also CMO-permitted.

In our setting, a permitted call sequence is a resource, and a call is represented as an action model [1]. We provide (novel) action models for synchronous CMO- and LNS-calls.

Given a set A of n agents, and $a, b \in A$, propositional variables a_b represent that the secret of agent a is known by agent b, a *call* is a pair (a, b) denoted ab, a *call sequence* σ is a finite sequence $ab.cd.\dots$ of calls, and variables ab^+ represent that call ab took place. A *secret distribution* is an n-tuple of subsets of A. We execute gossip protocols in the model $\mathcal{I}$ with the *initial secret distribution* wherein all agents only know their own secret (a_b is only true when $a = b$, and all ab^+ are false). An agent who knows all secrets is an expert. We let *Exp* represent that all agents know all secrets, that is, $\bigwedge_{a,b \in A} a_b$. In protocol LNS the condition for making a call ab is $\neg b_a$ and in CMO the condition is $\neg ab^+ \wedge \neg ba^+$.

The action model representing a synchronous call in CMO is defined as $\mathcal{G} = (E, \approx, \mathit{pre}, \mathit{post})$ where $E = \{ab \mid a, b \in A, a \neq b\}$, $ab \approx_c de$ iff ($c \neq a, b, c, d$, or $c = a = d$ and $b = e$, or $c = b = e$ and $a = d$), $\mathit{pre}(ab) = \neg ab^+ \wedge \neg ba^+$, and $\mathit{post}(ab)(c_a) = \mathit{post}(ab)(c_b) = c_a \vee c_b$ (a secret c is known by a after the call ab if before the call it was known by a or by b, and similarly for b), $\mathit{post}(ab)(ab^+) = \top$, and otherwise facts do not change value (i.e., $\mathit{post}(ab)(p) = p$). The action model for a synchronous LNS call is the same except that $\mathit{pre}(ab) = \neg b_a$.

Given n agents, we now investigate $\mathcal{IG}^{\mathbf{max}}$ for synchronous CMO so that $\mathbf{max} = \binom{n}{2}$. Given three agents, a call sequence after which all agents are experts is $ab.ac.bc$. We now represent some scenarios involving K, $\ast$, $-\!\!\ast$, and $\ast\!\!-$.

– $ab.ac \models c_b \ast\!\!- \mathit{Exp}$:
Given three agents a, b, c and call sequence $ab.ac$, after which a and c but not b are experts (in the second call ac, a informs c of a, b and c informs a of c, so that both are now experts), any subsequent call resulting in b knowing the secret of c makes all agents experts. For example, $bc \models c_b$ and indeed $ab.ac.\boldsymbol{bc} \models \mathit{Exp}$. But also $ac.ac.ab \models c_b$ and $ab.ac.\boldsymbol{ac.ac.ab} \models \mathit{Exp}$.

– $\models \varphi_{ab} \ast\!\!- K_a K_b (b_c \to a_c)$: (where $\varphi_{ab} := a_b \wedge b_a \wedge \bigwedge_{c \neq a} \neg c_b \wedge \bigwedge_{c \neq b} \neg c_a$)
Formula φ_{ab} holds after any call sequence σ wherein the only call(s) involving a and b was (were) to each other. Any extension $\sigma\tau$ of a σ satisfying φ_{ab} will pass along the secrets of a and b jointly. Therefore, $\models ab^+ \ast\!\!- (b_c \to a_c)$ and also $\models \varphi_{ab} \ast\!\!- K_a K_b (b_c \to a_c)$. On the other hand, $\not\models \varphi_{ab} -\!\!\ast K_a K_b (b_c \to a_c)$: when appending σ to a τ containing a call between b and another agent c, $b_c \to a_c$ is false, and a subsequent call ab also fails to guarantee that it holds. For example, $cd.ab \models \varphi_{ab}$, and therefore $\boldsymbol{cd.ab}.bc \models b_c \to a_c$, whereas $bc.\boldsymbol{cd.ab} \not\models b_c \to a_c$. So this example showed that there are φ and ψ for which $\models \varphi \ast\!\!- \psi$ but $\not\models \varphi -\!\!\ast \psi$.

– $\not\models a_c \wedge b_c \to a_c \ast b_c$:
Agent c may know the secrets of a and b now but not necessarily after fewer calls, although agent c may still know the secret of a or the secret of b. For example, $ab.ac \models a_c \wedge b_c$ but $ab.ac \not\models a_c \ast b_c$.

4 Reduction from $\mathcal{L}^{K*\mathcal{E}}$ to $\mathcal{L}^{K\mathcal{E}}$ given a bound max

In this section we show that every formula in $\mathcal{L}^{K*\mathcal{E}}$ (we recall that $\mathcal{L}^{K*\mathcal{E}}$ is the language $\mathcal{L}^{K*\otimes}$ where only action model $\mathcal{E}$ is allowed) is equivalent to a formula in $\mathcal{L}^{K\mathcal{E}}$, without $*$, $\mathrel{-\!\!*}$, and $\mathrel{-\!\!*}$ modalities, and without I. We show this by the time-honoured technique of a reduction system: a number of validities that are equivalences [11]. As every formula in $\mathcal{L}^{K\mathcal{E}}$ is equivalent to a formula in $\mathcal{L}^{K}$ [3,17], we then have shown that AMHSL is as expressive as the base multi-agent epistemic logic S5.

Our result is restricted in two ways. First, it is with respect to truth in the empty history models. Without that restriction already the language $\mathcal{L}^{K*}$ is more expressive than the language $\mathcal{L}^{K}$, as it is easy to see: a model wherein a knows that p and p is announced, is different from a model wherein a is uncertain about p and p is announced. However, after the announcement they satisfy the same epistemic formulas. However, to restrict validities to those for models with empty histories is usual in history-based semantics. The first restriction therefore keeps our result still relevant. Second, we can only show this if there is a bound $\mathbf{max} \in \mathbb{N}$ on the number of actions that can be executed. Without that we do not have a reduction, and we conjecture that one may not exist, given the well-known theoretical issues with arbitrary iteration of updates (undecidable logics, etc.) [12], and given that the semantics of $\mathrel{-\!\!*}$ and $\mathrel{*\!\!-}$ involve arbitrarily large histories of actions. The second restriction makes our result less relevant.

A dual question is whether every formula in $\mathcal{L}^{K*\mathcal{E}}$ is equivalent to a formula in $\mathcal{L}^{K*}$: can we also get rid of the action model modalities and stick with the epistemic separation language only? We are uncertain about the answer to this question. However, the language $\mathcal{L}^{K*}$ wherein we can only indirectly refer to actions by way of $*$ and $\mathrel{-\!\!*}$, already permits some $*$-validities of interest. It is succinctly discussed in Section 5.

4.1 Validities for empty histories and a bound max

We assume bound **max** throughout Section 4, and also that $\mathcal{E} = (E, \approx, \mathit{pre}, \mathit{post})$. The crucial validities in the reduction are as follows. They will be successively shown in subsequent lemmas and propositions. Recall that $\models$ is validity with respect to empty history models. The obvious proof of Lemma 2 is omitted.

$$\begin{array}{lll}
\models I & \leftrightarrow \top & \\
\models [h]\varphi & \leftrightarrow \top & \text{where } |h| > \mathbf{max} \\
\models [h](\varphi * \psi) & \leftrightarrow \mathit{pre}(h) \to \bigvee_{h' \sqsubseteq h}(\langle h' \rangle \varphi \wedge \langle h \backslash h' \rangle \psi) & \text{where } |h| \leq \mathbf{max} \\
\models [h](\varphi \mathrel{-\!\!*} \psi) & \leftrightarrow \mathit{pre}(h) \to \bigwedge_{|h'| \leq \mathbf{max} - |h|}(\langle h' \rangle \varphi \to [hh']\psi) & \text{where } |h| \leq \mathbf{max} \\
\models [h](\varphi \mathrel{*\!\!-} \psi) & \leftrightarrow \mathit{pre}(h) \to \bigwedge_{|h'| \leq \mathbf{max} - |h|}(\langle h' \rangle \varphi \to [h'h]\psi) & \text{where } |h| \leq \mathbf{max}
\end{array}$$

Lemma 2. $\models I \leftrightarrow \top$

Lemma 3. $\models [h]\varphi \leftrightarrow \top$, *where* $|h| > \mathbf{max}$.

Proof. We show that $\models [h]\varphi$, which is equivalent to $\models [h]\varphi \leftrightarrow \top$. Given $\mathcal{ME}^{\mathbf{max}}$ with $s \in \mathcal{D}(\mathcal{ME}^{\mathbf{max}})$. Let $h' \sqsubset h$ be the prefix of h with $|h'| = \mathbf{max}$, and assume $s \models \mathit{pre}(h')$. We need to show that $sh' \models [h\backslash h']\varphi$. Let $h\backslash h' = eh''$. According to the semantics of dynamic modalities, $sh' \models [e][h'']\varphi$ is equivalent to ($|h'| < \mathbf{max}$ and $sh' \models \mathit{pre}(e)$ imply $sh'e \models [h'']\varphi$). As $|h'| < \mathbf{max}$ is false, the whole implication is true.

Proposition 2. *$\models [h](\varphi * \psi) \leftrightarrow (\mathit{pre}(h) \rightarrow \bigvee_{h' \sqsubseteq h}(\langle h'\rangle\varphi \wedge \langle h\backslash h'\rangle\psi))$, where $|h| \leq \mathbf{max}$.*

Proof. Given $\mathcal{ME}^{\mathbf{max}}$ and $s \in \mathcal{D}(\mathcal{ME}^{\mathbf{max}})$, assume $s \models [h](\varphi * \psi)$. In order to prove that $s \models \mathit{pre}(h) \rightarrow \bigvee_{h' \sqsubseteq h}(\langle h'\rangle\varphi \wedge \langle h\backslash h'\rangle\psi)$, let us further assume that $s \models \mathit{pre}(h)$. From that and the initial assumption we obtain that $sh \models \varphi * \psi$. Then, there are h', h'' such that $h = h'h''$, $sh' \models \varphi$, and $sh'' \models \psi$ (note that $h'' = h\backslash h'$). From that we obtain $s \models \langle h'\rangle\varphi$ respectively $s \models \langle h''\rangle\psi$, and therefore $sh' \models \langle h'\rangle\varphi \wedge \langle h''\rangle\psi$, and therefore (using that $h'' = h\backslash h'$) $s \models \bigvee_{h' \sqsubseteq h}(\langle h'\rangle\varphi \wedge \langle h\backslash h'\rangle\psi)$, as required. For the other direction, now assume $s \models \mathit{pre}(h) \rightarrow \bigvee_{h' \sqsubseteq h}(\langle h'\rangle\varphi \wedge \langle h\backslash h'\rangle\psi)$, and towards showing that $s \models [h](\varphi * \psi)$, let us again further assume that $s \models \mathit{pre}(h)$. Thus $s \models \bigvee_{h' \sqsubseteq h}(\langle h'\rangle\varphi \wedge \langle h\backslash h'\rangle\psi)$. Let h' be such that $s \models \langle h'\rangle\varphi \wedge \langle h\backslash h'\rangle\psi$. Then, as before, $sh' \models \varphi$ and $s(h\backslash h') \models \psi$ so that $sh \models \varphi * \psi$.

Proposition 3. *$\models [h](\varphi \mathrel{-\!\!*} \psi) \leftrightarrow (\mathit{pre}(h) \rightarrow \bigwedge_{|h'| \leq \mathbf{max} - |h|}(\langle h'\rangle\varphi \rightarrow [hh']\psi))$, where $|h| \leq \mathbf{max}$.*

Proof. Given $\mathcal{ME}^{\mathbf{max}}$ and $s \in \mathcal{D}(\mathcal{ME}^{\mathbf{max}})$, assume $s \models [h](\varphi \mathrel{-\!\!*} \psi)$. Towards showing that $s \models \mathit{pre}(h) \rightarrow \bigwedge_{|h'| \leq \mathbf{max} - |h|}(\langle h'\rangle\varphi \rightarrow [hh']\psi)$, further assume $s \models \mathit{pre}(h)$, let h' be such that $|h'| \leq \mathbf{max} - |h|$ and let $s \models \langle h'\rangle\varphi$. It then remains to show that $s \models [hh']\psi$. In order to obtain that we make one final assumption namely $s \models \mathit{pre}(hh')$, so that $shh' \in \mathcal{D}(\mathcal{ME}^{\mathbf{max}})$. It then remains to show that $shh' \models \psi$. From $s \models \langle h'\rangle\varphi$ we obtain that $s \models \mathit{pre}(h')$ and $sh' \models \varphi$. From $s \models [h](\varphi \mathrel{-\!\!*} \psi)$ and $s \models \mathit{pre}(h)$ we deduce $sh \models \varphi \mathrel{-\!\!*} \psi$. From that, $sh' \models \varphi$, and $shh' \in \mathcal{D}(\mathcal{ME}^{\mathbf{max}})$ we then get $shh' \models \psi$, as required.

For the other direction, we now assume $s \models (\mathit{pre}(h) \rightarrow \bigwedge_{|h'| \leq \max - |h|}(\langle h'\rangle\varphi \rightarrow [hh']\psi))$, and towards showing that $s \models [h](\varphi \mathrel{-\!\!*} \psi)$ we further assume that $s \models \mathit{pre}(h)$, so that it remains to show that $sh \models \varphi \mathrel{-\!\!*} \psi$. Let now h' be such that $|h'| \leq \mathbf{max} - |h|$, $s \models \mathit{pre}(h')$, $s \models \mathit{pre}(hh')$, and $sh' \models \varphi$. We need to show that $shh' \models \psi$. From $sh' \models \varphi$ we get $s \models \langle h'\rangle\varphi$. Now using the initial assumption, $s \models \mathit{pre}(h)$, $s \models \langle h'\rangle\varphi$, and $s \models \mathit{pre}(hh')$, we obtain that $shh' \models \psi$, as required.

Proposition 4. *$\models [h](\varphi \mathrel{*\!\!-} \psi) \leftrightarrow (\mathit{pre}(h) \rightarrow \bigwedge_{|h'| \leq \mathbf{max} - |h|}(\langle h'\rangle\varphi \rightarrow [h'h]\psi))$, where $|h| \leq \mathbf{max}$.*

Proof. The proof is obtained from the proof of Prop. 3 by replacing hh' by $h'h$ everywhere in that proof. The order of h and h' does not play a role in the proof.

From Props. 2 and 3 it follows in particular, as the empty history can only be decomposed into empty and empty, and as $pre(\epsilon) = \top$, that:

Corollary 1.

$$\begin{aligned}
&\models \varphi * \psi \;\;\leftrightarrow \varphi \wedge \psi \\
&\models \varphi \mathrel{-\!\!*} \psi \leftrightarrow \textstyle\bigwedge_{|h| \leq \mathbf{max}} (\langle h \rangle \varphi \to [h]\psi) \\
&\models \varphi \mathrel{*\!\!-} \psi \leftrightarrow \textstyle\bigwedge_{|h| \leq \mathbf{max}} (\langle h \rangle \varphi \to [h]\psi)
\end{aligned}$$

4.2 Termination of reduction from $\mathcal{L}^{K*\mathcal{E}}$ to $\mathcal{L}^{K\mathcal{E}}$

We now show termination of the reduction. We define a translation t from $\mathcal{L}^{K*\mathcal{E}}$ to $\mathcal{L}^{K\mathcal{E}}$, and a complexity/weight measure c from $\mathcal{L}^{K*\mathcal{E}}$ to $\mathbb{N}$ and we then show that the translation is correct (is truth –value– preserving) and terminates.

For the translation it is of tantamount importance that we use an outside-in reduction strategy. This is because the reductions are $\models$ validities, they are **not** $\models^*$ validities: they are validities with respect to models with empty histories. In other words, the translation t to be defined is only correct when all modalities $[h]$ occurring in formulas are interpreted in models with empty histories only. For example, given $[h](K_a p \to [h']q)$, we can only rewrite $[h]$ and we cannot (at this stage) rewrite $[h']$. This can only happen at a later stage in the rewriting procedure after the formula has been massaged into a shape wherein $[h']$ (or some modality derived from it in the process of rewriting) can be interpreted in an empty history model. It is for this reason that the translation below does not contain a clause for $[h][h']\varphi$: in such a case we are compelled to reduce $[hh']\varphi$, or more precisely (as the formulas are identical by notational abbreviation), to find a clause in the translation function for the main logical connective of φ.

If an inside-out reduction had been possible, a proof by natural induction on the number of $*$, $\mathrel{-\!\!*}$, and $\mathrel{*\!\!-}$ occurrences would have been possible (in a slightly refined lexicographic way comparing triples of natural numbers). As the reduction is outside-in, applying an equivalence such as $[h](\varphi * \psi) \leftrightarrow (pre(h) \to \bigvee_{h' \sqsubseteq h} (\langle h' \rangle \varphi \wedge \langle h \backslash h' \rangle \psi)$ does not necessarily reduce the number of separation connectives on the righthand side of the equation. Any further $*$ occurring in φ on the left, will now occur as many times on the right as there as prefixes h' of h. Therefore we have to resort to the standard method of defining a weight/complexity measure on formulas.

Definition 9 (Complexity).

$$\begin{aligned}
c(p) = c(\bot) = c(I) &= 1 \\
c(\neg\varphi) &= 1 + c(\varphi) \\
c(\varphi \wedge \psi) &= 1 + \max\{c(\varphi), c(\psi)\} \\
c(\varphi * \psi) &= \mathbf{max} + 1 + \max\{c(\varphi), c(\psi)\} \\
c(\varphi \mathrel{-\!\!*} \psi) = c(\varphi \mathrel{*\!\!-} \varphi) &= 3 + \Sigma_{i=0}^{\mathbf{max}} |E|^i + c(\mathcal{E})^{\mathbf{max}} \cdot \max\{c(\varphi), c(\psi)\} \\
c(K_a\varphi) &= 1 + c(\varphi) \\
c([e]\varphi) &= c(\mathcal{E}) \cdot c(\varphi) \\
c(\mathcal{E}) &= 3 + |E| + \max\{pre(e), post(e)(p) \mid e \in E, p \in P\}
\end{aligned}$$

From $c([e]\varphi) = c(\mathcal{E}) \cdot c(\varphi)$ we obtain that $c([h]\varphi) = c(\mathcal{E})^{|h|} \cdot c(\varphi)$ for arbitrary histories h. We may abuse the language and write $c(h)$ for $c(\mathcal{E})^{|h|}$. In $c(\varphi \mathrel{-\!\!*} \psi)$ and $c(\varphi \mathrel{-\!\!*} \psi)$, the conjunction $\bigwedge_{h \leq \max}$ is over all histories of length at most **max**, where each action e in that history can be one of $|E|$. The total number of histories therefore involves a geometric series $\Sigma_{i=0}^{\mathbf{max}} |E|^i$.

Definition 10 (Translation). *Where* $1 \leq |h| \leq \mathbf{max}$ *except in clause* $t([h]\varphi)$.

$$\begin{array}{lll}
t(p) & = p & \\
t(\bot) & = \bot & \\
t(I) & = \top & \\
t(\neg\varphi) & = \neg t(\varphi) & \\
t(\varphi \wedge \psi) & = t(\varphi) \wedge t(\psi) & \\
t(K_a\varphi) & = K_a t(\varphi) & \\
t(\varphi * \psi) & = t(\varphi \wedge \psi) & \\
t(\varphi \mathrel{-\!\!*} \psi) & = t(\bigwedge_{|h| \leq \mathbf{max}} (\langle h \rangle \varphi \rightarrow [h]\psi)) & \\
t(\varphi \mathrel{*\!\!-} \psi) & = t(\bigwedge_{|h| \leq \mathbf{max}} (\langle h \rangle \varphi \rightarrow [h]\psi)) & \\
t([h]\varphi) & = \top & \textit{where } |h| > \mathbf{max} \\
t([h]p) & = \mathit{pre}(h) \rightarrow \mathit{post}(h)(p) & \\
t([h]\bot) & = \neg \mathit{pre}(h) & \\
t([h]I) & = \neg \mathit{pre}(h) & \\
t([h]\neg\varphi) & = \mathit{pre}(h) \rightarrow t(\neg[h]\varphi) & \\
t([h](\varphi \wedge \psi)) & = t([h]\varphi \wedge [h]\psi) & \\
t([h]K_a\varphi) & = \mathit{pre}(h) \rightarrow t(\bigwedge_{h \sim_a h'} K_a[h']\varphi) & \\
t([h](\varphi * \psi)) & = \mathit{pre}(h) \rightarrow t(\bigvee_{h' \sqsubseteq h} (\langle h' \rangle \varphi \wedge \langle h \backslash h' \rangle \psi)) & \\
t([h](\varphi \mathrel{-\!\!*} \psi)) & = \mathit{pre}(h) \rightarrow t(\bigwedge_{|h'| \leq \mathbf{max} - |h|} (\langle h' \rangle \varphi \rightarrow [hh']\psi)) & \\
t([h](\varphi \mathrel{*\!\!-} \psi)) & = \mathit{pre}(h) \rightarrow t(\bigwedge_{|h'| \leq \mathbf{max} - |h|} (\langle h' \rangle \varphi \rightarrow [h'h]\psi)) &
\end{array}$$

As action model pre- and postconditions are in $\mathcal{L}^{K\mathcal{E}}$ (contain no I, $*$, $\mathrel{-\!\!*}$, and $\mathrel{*\!\!-}$), we need not to translate (i.e., eliminate those operators from) those parts.

Lemma 4. *All the following hold:*

1. $c(\mathcal{E}) \geq 5$
2. $c(\varphi \vee \psi) \leq 3 + \max\{c(\varphi), c(\psi)\}$
3. $c(\varphi \rightarrow \psi) \leq 3 + \max\{c(\varphi), c(\psi)\}$
4. $c(\mathit{pre}(h)) \leq c(h)$

Proof. We prove the successive items.

1. $c(\mathcal{E}) = 3 + |E| + \mathbf{max}\{\mathit{pre}(e), \mathit{post}(e)(p) \mid e \in E, p \in P\} \geq 3 + 1 + 1 = 5$.
2. $c(\varphi \vee \psi) = c(\neg(\neg\varphi \wedge \neg\psi)) = 1 + c(\neg\varphi \wedge \neg\psi)) \leq 3 + \max\{c(\varphi), c(\psi)\}$
3. $c(\varphi \rightarrow \psi) = c(\neg(\varphi \wedge \neg\psi) = 1 + c(\varphi \wedge \neg\psi) = 2 + \max\{c(\varphi), c(\psi) + 1\} \leq 3 + \max\{c(\varphi), c(\psi)\}$
4. This follows from: $c(h) = c(\mathcal{E})^{|h|}$, $c(\mathit{pre}(e)) \leq \max\{c(\mathit{pre}(e)), c(\mathit{post}(e)(p)) \mid e \in E, p \in P\}$, and (as $|h| > 1$ so that $h = h'e'$) $\mathit{pre}(h) = \langle h' \rangle \mathit{pre}(e')$.

Lemma 5. *The following inequalities hold for arbitrary formulas, where $1 \leq |h| \leq \mathbf{max}$ except in the clause for $c([h]\varphi)$.*

$$\begin{array}{lll}
c(\varphi * \psi) & > c(\varphi \wedge \psi) & \\
c(\varphi \mathrel{-\!\!*} \psi) & > c(\bigwedge_{|h| \leq \mathbf{max}}(\langle h \rangle \varphi \rightarrow [h]\psi)) & \\
c(\varphi \mathrel{*\!\!-} \psi) & > c(\bigwedge_{|h| \leq \mathbf{max}}(\langle h \rangle \varphi \rightarrow [h]\psi)) & \\
c([h]\varphi) & > c(\top) & \textit{where } |h| > \mathbf{max} \\
c([h]p) & > c(\mathit{pre}(h) \rightarrow \mathit{post}(h)(p)) & \\
c([h]\bot) & > c(\neg \mathit{pre}(h)) & \\
c([h]I) & > c(\neg \mathit{pre}(h)) & \\
c([h]\neg\varphi) & > c(\mathit{pre}(h) \rightarrow \neg[h]\varphi) & \\
c([h](\varphi \wedge \psi)) & > c([h]\varphi \wedge [h]\psi) & \\
c([h]K_a\varphi) & > c(\mathit{pre}(h) \rightarrow \bigwedge_{h' \sim_a h} K_a[h']\varphi) & \\
c([h](\varphi * \psi)) & > c(\mathit{pre}(h) \rightarrow \bigvee_{h'.h''=h}(\langle h' \rangle \varphi \wedge \langle h'' \rangle \psi)) & \\
c([h](\varphi \mathrel{-\!\!*} \psi)) & > c(\mathit{pre}(h) \rightarrow \bigwedge_{|h'| \leq \mathbf{max}-|h|}(\langle h' \rangle \varphi \rightarrow [h.h']\psi)) & \\
c([h](\varphi \mathrel{*\!\!-} \psi)) & > c(\mathit{pre}(h) \rightarrow \bigwedge_{|h'| \leq \mathbf{max}-|h|}(\langle h' \rangle \varphi \rightarrow [h'.h]\psi)) &
\end{array}$$

Proof. We prove the separate items one by one.

$$\begin{array}{rll}
c(\varphi * \psi) & = \mathbf{max} + 1 + \max\{c(\varphi), c(\psi)\} & \\
& > 1 + \max\{c(\varphi), c(\psi)\} & \text{this bound is sharp} \\
& = c(\varphi \wedge \psi) &
\end{array}$$

$$\begin{array}{rll}
c(\varphi \mathrel{-\!\!*} \psi) & = 3 + \Sigma_{i=0}^{\mathbf{max}}|E|^i + c(\mathcal{E})^{\mathbf{max}} \cdot \max\{c(\varphi), c(\psi)\} & \\
& > \Sigma_{i=0}^{\mathbf{max}}|E|^i - 1 + 3 + c(\mathcal{E})^{\mathbf{max}} \cdot \max\{c(\varphi), c(\psi)\} & (@) \\
& \geq c(\bigwedge_{|h| \leq \mathbf{max}}(\langle h \rangle \varphi \rightarrow [h]\psi)) &
\end{array}$$

(@): The number of h with $|h| \leq \mathbf{max}$ is bounded by $\Sigma_{i=0}^{\mathbf{max}}|E|^i$, so one less for the number of $\wedge$-symbols. Then, $c(\mathcal{E})^{\mathbf{max}}$ is the weight of the largest such h.

The case $c(\varphi \mathrel{*\!\!-} \psi)$ is treated just as the case $c(\varphi \mathrel{-\!\!*} \psi)$.

$$c([h]\varphi) = c(h) \cdot c(\varphi) \geq 5c(\varphi) \geq 5 > 2 = c(\neg\bot) = c(\top) \qquad \text{when } |h| \geq \mathbf{max}$$

Note that $c(h) = c(\mathcal{E})^{|h|} \geq c(\mathcal{E}) \geq 5$. We do not use $|h| \geq \mathbf{max}$ but only $|h| \geq 1$.

$$\begin{array}{rl}
c([h]p) & = c(\mathcal{E})^{|h|} \cdot c(p) \\
& = c(\mathcal{E})^{|h|} \cdot 1 \\
& = c(\mathcal{E})^{|h|} \\
& \geq c(\mathcal{E}) \\
& = 3 + |E| + \max\{c(\mathit{pre}(e)), c(\mathit{post}(e)(p)) \mid e \in E, p \in P\} \\
& > 3 + \max\{c(\mathit{pre}(e)), c(\mathit{post}(e)(p)) \mid e \in E, p \in P\} \\
& \geq c(\mathit{pre}(e) \rightarrow \mathit{post}(e)(p))
\end{array}$$

$$\begin{array}{rl}
c([h]\bot) & = c(\mathcal{E})^{|h|} \cdot c(\bot) \\
& = c(\mathcal{E})^{|h|} \\
& \geq c(\mathcal{E}) \\
& = 3 + |E| + \max\{c(\mathit{pre}(e)), c(\mathit{post}(e)(p)) \mid e \in E, p \in P\} \\
& > 1 + c(\mathit{pre}(h)) \\
& = c(\neg \mathit{pre}(h))
\end{array}$$

$$c([h]I) > c(\neg \mathit{pre}(h))$$

The case $c([h]I)$ is treated as the case $c([h]\bot)$, as $c(I) = c(\bot) = 1$.

$$\begin{aligned}
c([h]\neg\varphi) &= c(\mathcal{E})^{|h|} \cdot c(\neg\varphi) \\
&= c(\mathcal{E})^{|h|} \cdot (1 + c(\varphi)) \\
&= c(\mathcal{E})^{|h|} + c(\mathcal{E})^{|h|} \cdot c(\varphi) && c(\mathcal{E}) \geq 5, |h| \geq 1 \\
&\geq 5 + c(\mathcal{E})^{|h|} \cdot c(\varphi) && \text{note that this bound is sharp} \\
&> 4 + c(\mathcal{E})^{|h|} \cdot c(\varphi) && \text{use that } c(\mathit{pre}(h)) \leq c(h) \\
&= 3 + \max\{c(\mathit{pre}(h)), 1 + c(\mathcal{E})^{|h|} \cdot c(\varphi)\} \\
&= 3 + \max\{c(\mathit{pre}(h)), 1 + c([h]\varphi)\} \\
&= 3 + \max\{c(\mathit{pre}(h)), c(\neg[h]\varphi)\} \\
&\geq c(\mathit{pre}(h) \to \neg[h]\varphi)
\end{aligned}$$

$$\begin{aligned}
c([h](\varphi \wedge \psi)) &= c(\mathcal{E})^{|h|} \cdot c(\varphi \wedge \psi) \\
&= c(\mathcal{E})^{|h|} \cdot (1 + \max\{c(\varphi), c(\psi)\}) \\
&= c(\mathcal{E})^{|h|} + c(\mathcal{E})^{|h|} \cdot \max\{c(\varphi), c(\psi)\} \\
&> 1 + c(\mathcal{E})^{|h|} \cdot \max\{c(\varphi), c(\psi)\} \\
&= 1 + \max\{c(\mathcal{E})^{|h|} \cdot c(\varphi), c(\mathcal{E})^{|h|} \cdot c(\psi)\} \\
&= 1 + \max\{c([h]\varphi), c([h]\psi)\} \\
&= c([h]\varphi \wedge [h]\psi)
\end{aligned}$$

$$\begin{aligned}
c([h]K_a\varphi) &= c(\mathcal{E})^{|h|} \cdot c(K_a\varphi) \\
&= c(\mathcal{E})^{|h|} \cdot (1 + c(\varphi)) \\
&= c(\mathcal{E})^{|h|} + c(\mathcal{E})^{|h|} \cdot c(\varphi) \\
&\geq c(\mathcal{E})^{|h|} + c(\mathcal{E})^{|h|} \cdot c(\varphi) \\
&\geq 3 + |E|^{|h|} + \max\{c(\mathit{pre}(e)), c(\mathit{post}(e)(p)) \mid \ldots\} + c(\mathcal{E})^{|h|} \cdot c(\varphi) \\
&\geq 4 + |E|^{|h|} + c(\mathcal{E})^{|h|} \cdot c(\varphi) && \text{this bound is sharp when } h = 1 \\
&> 3 + |E|^{|h|} + c(\mathcal{E})^{|h|} \cdot c(\varphi) \\
&= 3 + |E|^{|h|} - 1 + c(K_a[h]\varphi) && (*) \\
&\geq 3 + c(\textstyle\bigwedge_{h' \sim_a h} K_a[h']\varphi) && \text{as } c(\mathit{pre}(h)) \leq c(h) \\
&\geq 3 + \max\{c(\mathit{pre}(h)), c(\textstyle\bigwedge_{h' \sim_a h} K_a[h']\varphi)\} \\
&\geq c(\mathit{pre}(h) \to \textstyle\bigwedge_{h' \sim_a h} K_a[h']\varphi)
\end{aligned}$$

$(*)$: There are at most $|E|$ indistinguishable f from a given e, therefore there are at most $|E|^{|h|}$ indistinguishable h' from a given h. Minus 1 when counting the number of $\wedge$-symbols in a conjunction of that length.

$$\begin{aligned}
c([h](\varphi * \psi)) &= c(\mathcal{E})^{|h|} \cdot c(\varphi * \psi) \\
&= c(\mathcal{E})^{|h|} \cdot (\mathbf{max} + 1 + \max\{c(\varphi), c(\psi)\}) \\
&= \mathbf{max} \cdot c(\mathcal{E})^{|h|} + c(\mathcal{E})^{|h|} + c(\mathcal{E})^{|h|} \cdot \max\{c(\varphi), c(\psi)\} \\
&\geq 5 + 3\mathbf{max} + c(\mathcal{E})^{|h|} \cdot \max\{c(\varphi), c(\psi)\} && \mathbf{max} \geq |h| \\
&> 3 + 3|h| + 1 + c(\mathcal{E})^{|h|} \cdot \max\{c(\varphi), c(\psi)\} && (**) \\
&\geq 3 + c(\textstyle\bigvee_{h' \sqsubseteq h}(\langle h'\rangle\varphi \wedge \langle h \backslash h'\rangle\psi)) \\
&= 3 + \max\{c(\mathit{pre}(e)), c(\textstyle\bigvee_{h' \sqsubseteq h}(\langle h'\rangle\varphi \wedge \langle h \backslash h'\rangle\psi))\} \\
&\geq c(\mathit{pre}(h) \to \textstyle\bigvee_{h' \sqsubseteq h}(\langle h'\rangle\varphi \wedge \langle h \backslash h'\rangle\psi))
\end{aligned}$$

($**$): Each of $|h|$ disjunctions adds 3, plus 1 for the conjunction.

$$\begin{aligned}
c([h](\varphi \mathrel{-\!\!*} \psi)) &= c(\mathcal{E})^{|h|} \cdot c(\varphi \mathrel{-\!\!*} \psi) \\
&= c(\mathcal{E})^{|h|} \cdot (3 + \varSigma_{i=0}^{\mathbf{max}} |E|^i + c(\mathcal{E})^{\mathbf{max}} \cdot \max\{c(\varphi), c(\psi)\}) \\
&> 2 \cdot (3 + \varSigma_{i=0}^{\mathbf{max}} |E|^i + c(\mathcal{E})^{\mathbf{max}} \cdot \max\{c(\varphi), c(\psi)\}) \\
&> 3 + 3 + \varSigma_{i=0}^{\mathbf{max}-1} |E|^i - 1 + c(\mathcal{E})^{\mathbf{max}} \cdot \max\{c(\varphi), c(\psi)\} \\
&\geq 3 + c(\textstyle\bigwedge_{|h'| \leq \mathbf{max}-|h|} (\langle h' \rangle \varphi \to [hh']\psi)) \\
&= 3 + \max\{c(pre(h), c(\textstyle\bigwedge_{|h'| \leq \mathbf{max}-|h|} (\langle h' \rangle \varphi \to [hh']\psi))\} \\
&\geq c(pre(h) \to \textstyle\bigwedge_{|h'| \leq \mathbf{max}-|h|} (\langle h' \rangle \varphi \to [hh']\psi))
\end{aligned}$$

The case $c([h](\varphi \mathrel{-\!\!*} \psi))$ is serious overkill, as in $c(\varphi \mathrel{-\!\!*} \psi)$ weight $c(h)$ is already factored in. But in case $c(\varphi \mathrel{-\!\!*} \varphi)$ this was indispensable. We also use that the h' we quantify over must have length at most $\mathbf{max} - 1$ (as $|h| \geq 1$), one less therefore than in the case $c(\varphi \mathrel{-\!\!*} \psi)$.

The case of $[h](\varphi \mathrel{*\!\!-} \psi)$ is similar to the case $[h](\varphi \mathrel{*\!\!-} \psi)$.

Theorem 1. *Every formula in* $\mathcal{L}^{K*\mathcal{E}}$ *is equivalent to a formula in* $\mathcal{L}^{K\mathcal{E}}$

Proof. We recall that the reduction is outside-in. Consider a formula $\varphi \in \mathcal{L}^{K*\mathcal{E}}$, and apply a clause of translation t (Def. 10) on φ. Consider $c(\varphi)$. If φ is one of p, $\bot$, or $\top$, termination is trivial (such as $t(p) = p$). If the main logical connective of φ commutes with t (such as in $t(\psi \wedge \chi) = t(\psi) \wedge t(\chi)$), then it is obvious that the complexities of subformulas of φ are strictly lower than the complexities of φ (such as $c(\psi) < c(\psi \wedge \chi)$ above, since the complexity of a conjunction is that of its conjuncts **plus one**). If the main logical connective of φ does not commute with t, we have one of the cases spelled out in Lemma 5 and use that for all those cases $c(\varphi) > c(t(\varphi))$. Therefore, in every step of translation t that we apply, the weight c is strictly less. As $c(\varphi)$ is a natural number, this is bounded by 0. Therefore the reduction terminates.

Corollary 2. *Every formula in* $\mathcal{L}^{K*\mathcal{E}}$ *is equivalent to a formula in* $\mathcal{L}^{K}$.

As a consequence, the logic AMHSL (for empty history models, and given bound **max**) is therefore completely axiomatized by the reduction axioms of Section 4.1 and the axiomatization of action model logic with factual change [17] (where we recall Prop. 1) that extends S5.

5 Remarks and Perspectives

Considering the history-based logical semantics with the bound **max** of the epistemic history model, it appears that model checking is decidable. Satisfiability may be a different matter as the $\mathrel{-\!\!*}$ and $\mathrel{*\!\!-}$ connectives quantify over histories of arbitrary finite length, even if we know that quantifying over action models results in a decidable logic [9]. If histories are unbounded, we are uncertain if $*$, $\mathrel{*\!\!-}$ and $\mathrel{-\!\!*}$ can be eliminated by reduction from the language $\mathcal{L}^{K*\mathcal{E}}$. It is also highly uncertain if action model modalities can be eliminated by reduction from the language $\mathcal{L}^{K*\mathcal{E}}$, so that we get a $\mathcal{L}^{K*}$ formula.

The logical semantics for the language $\mathcal{L}^{K*}$ is interesting in its own right. Dynamic epistemic logics allowing reasoning about the past are very rare [2,4]. In $\mathcal{L}^{K*}$ we can refer to the past in novel and unexpected ways. For example, $sh \models \psi * \top$ formalizes that ψ was true in the past (there must be h', h'' with $h'h'' = h$ such that $sh' \models \psi$ and $sh'' \models \top$, where the latter is trivially true). A formula like $\neg I * \neg I * \neg I$ is only true after at least three actions have been executed (etcetera). Would such a logic be axiomatizable? We can see that $(K_a\varphi * K_a\psi) \rightarrow K_a(\varphi * \psi)$ is valid. However, $K_a(\varphi * \psi) \rightarrow (K_a\varphi * K_a\psi)$ is invalid.

Finally, instead of decomposing action histories into prefixes and postfixes, such that resource update required distinct $-\!\!*$ (append postfix) and $*\!\!-$ (append prefix) connectives, and where $\varphi * \psi$ may not be equivalent to $\psi * \varphi$, we could also contemplate decomposing an action history into a subsequence and its complement (such as when decomposing $a.b.c.d$ into $a.c$ and $b.d$). Now, one $-\!\!*$ connective suffices that can be interpreting as 'enriching' a given history with bits and pieces of action sequences where it pleases us, and $*$ has become commutative. This comes closer to the philosophy of separation.

Acknowledgements We very much wish to thank the reviewers for their comments. A reviewer pointed out an error in the proof of the case $c([h](\varphi * \psi))$ of Lemma 5, that needed repair by strengthening the weight of case $c(\varphi * \psi)$ in Def. 9. Another reviewer mentioned that AMHSL allows to reason about the length of histories. We added an example.

References

1. M. Attamah, H. van Ditmarsch, D. Grossi, and W. van der Hoek. Knowledge and gossip. In *Proc. of 21st ECAI*, pages 21–26. IOS Press, 2014.
2. P. Balbiani, H. van Ditmarsch, and A. Herzig. Before announcement. In L.D. Beklemishev, S. Demri, and A. Maté, editors, *Advances in Modal Logic 11*, pages 58–77. College Publications, 2016.
3. A. Baltag, L.S. Moss, and S. Solecki. The logic of public announcements, common knowledge, and private suspicions. In *Proc. of 7th TARK*, pages 43–56, 1998.
4. A. Baltag, A. Özgün, and A.L. Vargas Sandoval. Arbitrary public announcement logic with memory. *Journal of Philosophical Logic*, 2022. doi:https://doi.org/10.1007/s10992-022-09664-6.
5. V. Belle, T. Bolander, A. Herzig, and B. Nebel. Epistemic planning: Perspectives on the special issue. *Artificial Intelligence*, 2022. doi:10.1016/j.artint.2022.103842.
6. J.-R. Courtault and D. Galmiche. A modal separation logic for resource dynamics. *Journal of Logic and Computation*, 28(4):733–778, 2018.
7. J.-R. Courtault, H. van Ditmarsch, and D. Galmiche. A public announcement separation logic. *Math. Struct. Comput. Sci.*, 29(6):828–871, 2019.
8. D. Galmiche, P. Kimmel, and D. Pym. A substructural epistemic resource logic: theory and modelling applications. *J. Log. Comput.*, 29(8):1251–1287, 2019.
9. J. Hales. Arbitrary action model logic and action model synthesis. In *Proc. of 28th LICS*, pages 253–262. IEEE, 2013.
10. S. Ishtiaq and P. O'Hearn. BI as an assertion language for mutable data structures. In *Proc. of 28th POPL*, pages 14–26, 2001.

11. B. Kooi. Expressivity and completeness for public update logics via reduction axioms. *Journal of Applied Non-Classical Logics*, 17(2):231–254, 2007.
12. J.S. Miller and L.S. Moss. The undecidability of iterated modal relativization. *Studia Logica*, 79(3):373–407, 2005.
13. L.S. Moss. Dynamic epistemic logic. In H. van Ditmarsch, J.Y. Halpern, W. van der Hoek, and B. Kooi, editors, *Handbook of epistemic logic*, pages 261–312. College Publications, 2015.
14. J.A. Plaza. Logics of public communications. In *Proc. of the 4th ISMIS*, pages 201–216. Oak Ridge National Laboratory, 1989.
15. D. Pym. *The Semantics and Proof Theory of the Logic of Bunched Implications*, volume 26 of *Applied Logic Series*. Springer, 2002.
16. J. van Benthem, J.D. Gerbrandy, T. Hoshi, and E. Pacuit. Merging frameworks for interaction. *Journal of Philosophical Logic*, 38:491–526, 2009.
17. J. van Benthem, J. van Eijck, and B. Kooi. Logics of communication and change. *Information and Computation*, 204(11):1620–1662, 2006.
18. H. van Ditmarsch, D. Galmiche, and M. Gawek. An epistemic separation logic with action models. *Journal of Logic Language and Information*, 32(1):89–116, 2023. doi:10.1007/s10849-022-09372-z.
19. H. van Ditmarsch, J.Y. Halpern, W. van der Hoek, and B. Kooi. An introduction to logics of knowledge and belief. In H. van Ditmarsch, J.Y. Halpern, W. van der Hoek, and B. Kooi, editors, *Handbook of epistemic logic*, pages 1–51, 2015.
20. H. van Ditmarsch, J. Ruan, and W. van der Hoek. Connecting dynamic epistemic and temporal epistemic logics. *Logic journal of the IGPL*, 21(3):380–403, 2013.
21. H. van Ditmarsch, W. van der Hoek, and B. Kooi. *Dynamic Epistemic Logic*, volume 337 of *Synthese Library*. Springer, 2008.
22. H. van Ditmarsch, J. van Eijck, P. Pardo, R. Ramezanian, and F. Schwarzentruber. Epistemic protocols for dynamic gossip. *J. Applied Logic*, 20:1–31, 2017.