An Epistemic Separation Logic with Action Models

Hans van Ditmarsch, Didier Galmiche, and Marta Gawek

Université de Lorraine, CNRS, LORIA
Nancy, France

1 Introduction

The aim of the paper is to present Epistemic Separation Logic with Action Models (ESLAM), that can be seen as a generalization of Public Announcement Separation Logic (PASL [3]). The general context of this work is the study of extensions of Separation logics with modalities in order to manage various dynamic aspects and mainly here from Dynamic Epistemic Logic (with factual change) [1, 9, 8]. Let us remind that Separation Logics (SL) refer to a class of logics based on (intuitionistic) Logic of Bunched Implications (BI) or its classical counterpart Boolean BI (BBI) [6]. They combine both additive ($\wedge$, $\rightarrow$, $\vee$) and multiplicative ($*$, $-\!\!*$) connectives in the language, the latter expressing the concept of resource separation (or composition), and resource update [6]. Among extensions of Separation Logics with dynamics we mention Dynamic Modal BI (DMBI [2]) and Epistemic Resource Logic (ERL [4]). The first one is a BBI extension with the modalities $\Box$, $\Diamond$, and a dynamic modality $\langle a \rangle$, that allows us to investigate how resource properties change over dynamic processes taking place, with an emphasis on concurrent processes. The second one is a BBI extension with epistemic modalities, as well as a differentiation between ambient resource and local resources (assigned to each agent), and their compositions. A recent work on resource semantics to model updates and/or epistemic reasoning, lead to PASL, which extends BBI with a knowledge operator K_a, and a public announcement modality. The strenghts of this logic lie in its ability to model knowledge acquisition and information change over the course of truthful public communication [5].

In this paper we generalize the dynamic aspects of PASL, by defining Epistemic Separation Logic with Action Models (ESLAM), in which we replace public announcements with action models [1], motivated by their ability to model factual change, and instances of a more nuanced, private communication. A keypoint about integrating dynamic logics with BBI is that the available resources and the resource composition operator are based on the monoidal structure, which entails inclusion of a neutral element (neutral, or unit resource). As dynamic processes are carried out it is vital that – in any case – the structure of our updated model still contains the neutral element, so the monoidal structure is preserved. In PASL, possible worlds are considered resources and hence the issue was solved by a refinement semantics [7], that ensures that after an announcement of φ, all relations are severed between the states where φ is true, and the states where φ is false, but no state is ever removed from the model. In ESLAM, the relationship between states and resources is more implicit, as we define a resource function r, mapping every state (or several states) to a resource. Moreover, the updated epistemic resource model – obtained after action model execution – ensures that all state-to-resource mappings are preserved. We also require that an action model is covering, so a state assigned to a neutral resource is always part of the updated model domain.

In Section 2, we define ESLAM syntax, semantics, and associated structures. In Section 3, we propose a set of ESLAM reductions for elimination of the action model modality. In Section 4, a modelling example is presented, in which we can compare PASL and ESLAM with regard to their abilities to model public and private communications. In Section 5, we mention future works, as well as possible modifications of ESLAM to be investigated.

2 Epistemic Separation Logic with Action Models

The logic ESLAM is based on BBI, extended with a knowledge modality K_a and a dynamic modality $[\mathcal{E}_e]$ for action execution. Given a set of agents A and a set of propositional variables P, the language of ESLAM, $\mathcal{L}_{K*}$, is defined as follows, where $a \in A$ and $p \in P$:

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

Expression $K_a\varphi$ means that *agent a knows that* φ. There are two multiplicative connectives ($*$ and $\mathrel{-\!\!*}$) referring to the separation respectively composition of resources. Expression $[\mathcal{E}_e]\varphi$ stands for 'after execution of action $\mathcal{E}_e$, φ is true. Such actions $\mathcal{E}_e$ will be defined below.

Definition 1 (Resource monoid)**.** *A* partial resource monoid *(or* resource monoid*) is a structure* $\mathcal{R} = (R, \bullet, n)$ *where* R *is a set of* resources *containing a* neutral element $n \in R$, $\bullet : R \times R \to R$ *is a* resource composition operator *that is associative and commutative, that may be partial, and such for all* $r \in R$, $r \bullet n = n \bullet r = r$. *If* $r \bullet r'$ *is defined we write* $r \bullet r' \downarrow$ *and if* $r \bullet r'$ *is undefined we write* $r \bullet r' \uparrow$. *Whenever writing* $r \bullet r' = r''$ *we assume that* $r \bullet r' \downarrow$.

Definition 2 (Epistemic resource model)**.** *An* epistemic frame *(*frame*) is a structure* $(S, \sim)$ *such that* S *is a set of* states *and* $\sim : A \to \mathcal{P}(S \times S)$ *is a function that maps each agent* a *to an equivalence relation* $\sim(a)$ *denoted as* $\sim_a$. *Given a resource monoid* $\mathcal{R} = (R, \bullet, n)$, *an* epistemic resource model *is a structure* $\mathcal{M} = (S, \sim, r, V)$ *such that* $(S, \sim)$ *is an epistemic frame, surjection* $r : S \to R$ *is a* resource function*, that maps each state to a resource and where we write* r_s *for* $r(s)$, *and* $V : P \to \mathcal{P}(S)$ *is a* valuation function*, where* $V(p)$ *denotes the set of states where variable* p *is true. Given* $s \in S$, *the pair* $(\mathcal{M}, s)$ *is a* pointed epistemic resource model*, also denoted* $\mathcal{M}_s$.

Definition 3 (Action model)**.** *Given a logical language* $\mathcal{L}$, *an* action model $\mathcal{E}$ *is a structure* $\mathcal{E} = (E, \approx, pre, post)$, *such that* E *is a finite domain of* actions*,* $\approx_a$ *an equivalence relation on* E *for all* $a \in A$, $pre : E \to \mathcal{L}$ *is a precondition function, and* $post : E \to P \nrightarrow \mathcal{L}$ *is a postcondition function that is a partial function: its domain is 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* $\mathcal{E}_e$. *An action model* is covering *if* $\bigvee_{e \in E} pre(e)$ *is a validity of the logic of* $\mathcal{L}$.

Definition 4. *Given an epistemic resource model* $\mathcal{M} = (S, \sim, r, V)$ *and a covering action model* $\mathcal{E} = (E, \approx, pre, post)$, *the* updated epistemic resource model $\mathcal{M} \otimes \mathcal{E} = (S', \sim', r', V')$ *is defined as*

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

Definition 5 (Satisfaction relation)**.** *Let* $s \in S$. *The* satisfaction relation $\models$ *between pointed epistemic resource models* $\mathcal{M}_s$, *where* $\mathcal{M} = (S, \sim, r, V)$, *for resources* $\mathcal{R} = (R, \bullet, n)$, *and formulas in* $\mathcal{L}_{K*\otimes}(A, P)$, *is defined by structural induction as follows:*

$$\begin{array}{lll} \mathcal{M}_s \models p & \textit{iff} & s \in V(p) \\ \mathcal{M}_s \models \bot & \textit{iff} & \textit{false} \\ \mathcal{M}_s \models I & \textit{iff} & r_s = n \\ \mathcal{M}_s \models \neg\varphi & \textit{iff} & \mathcal{M}_s \not\models \varphi \\ \mathcal{M}_s \models \varphi \wedge \psi & \textit{iff} & \mathcal{M}_s \models \varphi \textit{ and } \mathcal{M}_s \models \psi \\ \mathcal{M}_s \models \varphi \to \psi & \textit{iff} & \mathcal{M}_s \not\models \varphi \textit{ or } \mathcal{M}_s \models \psi \end{array}$$

$\mathcal{M}_s \models \varphi * \psi$ *iff* *there are* $t, u \in S$ *such that* $r_s = r_t \bullet r_u, \mathcal{M}_t \models \varphi$ *and* $\mathcal{M}_u \models \psi$
$\mathcal{M}_s \models \varphi \mathrel{-\!\!*} \psi$ *iff* *for all* $t \in S$ *such that* $r_s \bullet r_t \downarrow$ *and* $\mathcal{M}_t \models \varphi$
there is $u \in S$ *such that* $r_u = r_s \bullet r_t$ *and* $\mathcal{M}_u \models \psi$
$\mathcal{M}_s \models K_a\varphi$ *iff* $\mathcal{M}_t \models \varphi$ *for all* $t \in S$ *such that* $s \sim_a t$
$\mathcal{M}_s \models [\mathcal{E}_e]\varphi$ *iff* $\mathcal{M}_s \models pre(e)$ *implies* $(\mathcal{M} \otimes \mathcal{E})_{(s,e)} \models \varphi$

A formula φ is valid on model $\mathcal{M}$ *(notation:* $\mathcal{M} \models \varphi$*) iff for all* $s \in S$, $\mathcal{M}_s \models \varphi$, *and* φ is valid *(notation:* $\models \varphi$*) iff* φ *is valid on all models* $\mathcal{M}$.

Note that $\mathcal{M} \otimes \mathcal{E}$ is again an epistemic resource model for the monoid $(\mathcal{R}, \bullet, n)$. For each resource r in $\mathcal{R}$ there is a state s in S such that $r_s = r$ (r was required to be a surjection). As the action model is covering, for each state s there is an action e such that $\mathcal{M}, s \models pre(e)$, so that $(s, e) \in S'$. As $r_{(s,e)} = r_s = r$, $\mathcal{M} \otimes \mathcal{E}$ is again a resource model for $(\mathcal{R}, \bullet, n)$.

The semantics for $*$ and $\mathrel{-\!\!*}$ are different from their standard semantics in BBI. This is because they are not formulated directly in terms of resource but only indirectly by way of states mapped to resources. As different states can be mapped to the same resource, this obliges us to choose where the semantics for $*$ and $\mathrel{-\!\!*}$ is defined in terms of all such states or some such states (there is an extra quantifier that can be universal or existential). We also consider other semantics, for example, for $\mathrel{-\!\!*}$:

$$\mathcal{M}_s \models \varphi \mathrel{-\!\!*} \psi \quad \textit{iff} \quad \textit{for all } t, u \in S \textit{ such that } r_u = r_s \bullet r_t, \mathcal{M}_t \models \varphi \textit{ implies } \mathcal{M}_u \models \psi$$

We are exploring such alternatives in view of their theoretical properties (does a reduction exist?) and their applicability (which typical BBI modelling challenges or benchmarks under partial observation are best described by which version of the semantics?).

3 Eliminating Dynamic Modalities

We now define a set of ESLAM validities for action model modality elimination. To the well-known reduction axioms for Action Model Logic with factual change [8] we add two novel reductions for $*$ and $\mathrel{-\!\!*}$. At this stage we have proved such reduction for $*$ and $\mathrel{-\!\!*}$ for the diamond version of the action model modality but not yet for the box version. Therefore the system is given with the diamond modality as the primitive.

1. $\langle \mathcal{E}_e \rangle p \leftrightarrow (pre(e) \wedge post(e)(p))$
2. $\langle \mathcal{E}_e \rangle (\psi \wedge \varphi) \leftrightarrow \langle \mathcal{E}_e \rangle \psi \wedge \langle \mathcal{E}_e \rangle \varphi$
3. $\langle \mathcal{E}_e \rangle \neg \psi \leftrightarrow (pre(e) \wedge \neg \langle \mathcal{E}_e \rangle \psi)$
4. $\langle \mathcal{E}_e \rangle K_a \psi \leftrightarrow (pre(e) \wedge \bigwedge_{e \sim_a f} K_a \langle \mathcal{E}_f \rangle \psi)$
5. $\langle \mathcal{E}_e \rangle (\varphi * \psi) \leftrightarrow (pre(e) \wedge \bigvee_{f,g \in E} (\langle \mathcal{E}_f \rangle \varphi * \langle \mathcal{E}_g \rangle \psi))$
6. $\langle \mathcal{E}_e \rangle (\varphi \mathrel{-\!\!*} \psi) \leftrightarrow (pre(e) \wedge \bigwedge_{f \in E} (\langle \mathcal{E}_f \rangle \varphi \mathrel{-\!\!*} \bigvee_{g \in E} \langle \mathcal{E}_g \rangle \psi))$

We have shown that the above validities are reduction rules using a complexity measure taken from [9], where it was used to show the reduction for public announcement logic. In [9], the complexity of a formula with public announcement is calculated as follows: $c([\varphi]\psi) = (4 + c(\varphi)) \cdot c(\psi)$. For our current purposes this is generalized to: $c([\mathcal{E}_e]\psi) = (4 + c(\mathcal{E})) \cdot c(\psi)$. The complexity of a pointed action $\mathcal{E}_e$ does not depend on the point, which is why we see $c(\mathcal{E})$ on the right-hand side and not $c(\mathcal{E}_e)$, as maybe expected. Then, $c(\mathcal{E}) = |E|^2 + \max\{c(pre(f)), c(post(f)(p)) \mid f \in \mathcal{E}, p \in P, p \in \mathcal{D}(post(f))\}$ (where E is the domain of $\mathcal{E}$).

4 Library example revisited

In this section we reconsider the modelling example of PASL [3] and illustrate what ESLAM allows us to express. The set of agents A is $\{A_1, A_2\}$ and the set of atoms (variables) P is $\{P_1, P_2, C\}$. The epistemic model $\mathcal{M} = (S, \sim, r, V)$ is now such that: $S = \{(i,j) \mid i,j \in \{0,1,2\}\}$; $(i_1,j_1) \sim_{A_1} (i_2,j_2)$ iff $i_1 = i_2$ and $(i_1,j_1) \sim_{A_2} (i_2,j_2)$ iff $j_1 = j_2$; $r_{(i,j)} = (i,j)$; and $V(C) = \{(i,j) \mid i+j \leq 2\}$, $V(P_1) = \{(1,0)\}$, $V(P_2) = \{(0,1)\}$. The atoms P_1 and P_2 express agents A_1 and A_2 (respectively) requesting one book each from a librarian, whereas C expresses that the librarian is capable of carrying the requested books. The partial resource monoid $\mathcal{R} = (S, \bullet, n)$, considered has as neutral element $n = (0,0)$, and a composition operator $\bullet$ defined as:

$$(i_1,j_1) \bullet (i_2,j_2) = \begin{cases} \uparrow & \text{if } i_1+i_2 \geq 2 \text{ or } j_1+j_2 \geq 2 \\ (i_1+i_2, j_1+j_2) & \text{otherwise} \end{cases}$$

We present two modelling examples for the library setting. The action model $\mathcal{E}'$ emulates public announcement (equivalent to one defined for PASL [3]) and the action model $\mathcal{E}$, defined with ESLAM which, compared to PASL, enables private communication. In both cases we model an action of the librarian telling either: both agents (by means of $\mathcal{E}'$), agent A_1 only (in $\mathcal{E}$) that they can carry the books.

Public announcement action model:	Private announcement action model:
$\mathcal{E}' = \{E', \approx'_a, pre', post'\}$, where:	$\mathcal{E} = \{E, \approx_a, pre, post\}$, where:
$E' = \{e, f\}$	$E = \{e, f\}$
$\approx'_{A_1} = \{(e,e),(f,f)\}$	$\approx_{A1} = \{(e,e),(f,f)\}$
$\approx'_{A_2} = \{(e,e),(f,f)\}$	$\approx_{A_2} = \{(e,f),(f,e),(e,e),(f,f)\}$
$pre'(e) = C$	$pre(e) = C$
$pre'(f) = \neg C$	$pre(f) = \neg C$
$post'(e)$ and $post'(f)$ have empty domain	$post(e)$ and $post(f)$ have empty domain

As presented above, the difference between the two lies in the definition of $\approx_a$. In $\mathcal{E}'$ all librarian's announcements are heard by both agents and their uncertainty is equally reduced as action model is executed. This is represented by the identity relation. In $\mathcal{E}$, the librarian addresses A_1 privately, that is why A_1 can tell $\mathcal{E}_e$ and $\mathcal{E}_f$ apart, but as A_2 is excluded from this communication, although A_2 can observe the communication taking place, A_2 cannot make that distinction.

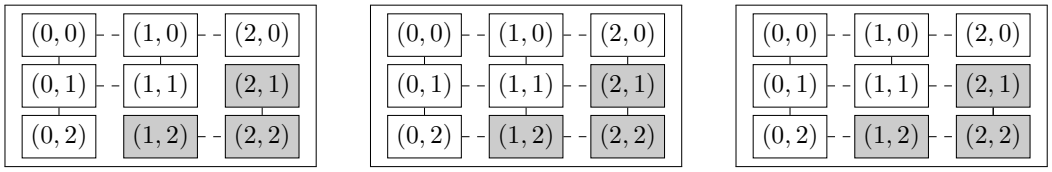

Figure 1: In the center, the initial model. On the left, the result a public announcement $\mathcal{E}'_e$. On the right, the result of a private announcement $\mathcal{E}'_e$. More explanations are found in the text.

Assume each agent wants one book, which corresponds to state $(1,1)$. Let us compare two model updates: the librarian telling both agents they can carry the books ($\mathcal{E}'_e$), and the librarian telling just A_1 that they can carry the books ($\mathcal{E}_e$). (In ESLAM, as in PASL, a public announcement is a two-event action model, because of the requirement that the action is covering.)

$(1,1) \models_{\mathcal{M}} \langle \mathcal{E}'_e \rangle (K_{A1}C \wedge K_{A2}C)$	$(1,1) \models_{\mathcal{M}} \langle \mathcal{E}_e \rangle (K_{A1}C \wedge \neg K_{A2}C)$
$\Leftrightarrow$	$\Leftrightarrow$
$(1,1) \models_{\mathcal{M}} C$	$(1,1) \models_{\mathcal{M}} C$
and	and
$((1,1),e) \models_{(\mathcal{M} \otimes \mathcal{E}')} K_{A1}C \wedge K_{A2}C$	$((1,1),e) \models_{(\mathcal{M} \otimes \mathcal{E})} K_{A1}C \wedge \neg K_{A2}C$

In the center of Figure 4 we see the initial model of knowledge. Dashed links - - - represent the relation $\sim_{A_2}$. Solid links — represent the relation $\sim_{A_1}$. We assume reflexivity and transitivity. Grey means "cannot be carried". On the left in the figure we see the update of the model with $\mathcal{E}'_e$. On the right in the figure we see the update of the model with $\mathcal{E}_e$. After the public announcement is made, both agents stopped considering the scenarios where the number of books requested exceeds the librarian's limit. This is illustrated by all links between gray and white areas in the graph disappearing. After the private announcement this is the case only for A_2. This example shows that with ESLAM, compared to PASL, we can define instances of not only public announcement, but also private, more nuanced announcements as well as other forms of partial observation.

5 Conclusions

We have presented Epistemic Separation Logic with Action Models, where the relationship between resources and Kripke semantics is based on the resource function, mapping each state to a resource. Future works will be developed in different directions: defining an additional action resource model monoid, allowing composition and separation of action points, as well as modelling sequential action point execution, achieved by means of action composition operator. Moreover we will investigate the optimal semantics for $*$ and $-\!\!*$, taking into account the duality between these operations.

References

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

[2] J.-R. Courtault and D. Galmiche. A Modal Separation Logic for Resource Dynamics . *Journal of Logic and Computation*, 28(4):733–778, 2018.

[3] J.-R. Courtault, H. van Ditmarsch, and D. Galmiche. A Public Announcement Separation Logic. *Mathematical Structures in Computer Science*, 29(6):828–871, 2019.

[4] D. Galmiche, P. Kimmel, and D. Pym. A Substructural Epistemic Resource Logic. In *Indian Conference on Logic and Its Applications*, pages 106–122. Springer, 2017.

[5] J.A. Plaza. Logics of public communications. In *Proc. of the 4th ISMIS*, pages 201–216. Oak Ridge National Laboratory, 1989.

[6] D. Pym. *The Semantics and Proof Theory of the Logic of Bunched Implications*, volume 26 of *Applied Logic Series*. Kluwer Academic Publishers, 2002.

[7] J. van Benthem and F. Liu. Dynamic logic of preference upgrade. *Journal of Applied Non-Classical Logics*, 17(2):157–182, 2007.

[8] H. van Ditmarsch and B. Kooi. Semantic results for ontic and epistemic change. In *Proc. of 7th LOFT*, Texts in Logic and Games 3, pages 87–117. Amsterdam University Press, 2008.

[9] H. van Ditmarsch, W. van der Hoek, and B. Kooi. *Dynamic Epistemic Logic*, volume 337 of *Synthese Library*. Springer, 2008.