An Epistemic Separation Logic with Action Models

Hans van Ditmarsch, Didier Galmiche, Marta Gawek

University of Lorraine, CNRS, LORIA

9th Indian Conference on Logic and Applications
March 2021

Outline

ESLAM

General context:

Extensions of Separation Logics (Bunched Implications Logics) with modalities in order to manage various dynamic aspects:

- Dynamic Modal BI (**DMBI**): to investigate how resource properties change over dynamic processes taking place, with an emphasis on concurrent processes.
- Epistemic Resource Logic (**ERL**): to have modalities parametrized with resources, with a differentiation between ambient resource and local resources and their compositions.
- Public Announcement Separation Logic (**PASL**): to model knowledge acquisition and information change over the course of truthful public communication.

ESLAM

Epistemic Separation Logic with Action Models (**ESLAM**)

- Public announcements replaced with Action models.
- Action models allow one to model factual change, and instances of a more nuanced, private communication.

A key point: relationships between **worlds/states** and **resources**.

- In PASL possible worlds are considered resources.
- In ESLAM a resource function r, maps every state (or several states) to a resource.

Language

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 $p \in P$:

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

$K_a\varphi$ means that *agent a knows that* φ.
The multiplicative connectives $*$ and $\mathrel{-\!\!*}$ refer to composition (separation) of resources and updates.
$[\mathcal{E}_e]\varphi$ means that after execution of action $\mathcal{E}_e$, φ is true.

Structures

Definition (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* $r \bullet r' \downarrow$*.*

Structures

Definition (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,* $r : S \to R$ *is a* resource function, *that maps each state to a resource (notation* 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* $\mathcal{M}_s$.

Structures

Definition (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,*
- $post : E \to P \not\to \mathcal{L}$ *is a postcondition function, that is partial, with a finite set of variables* $Q \subseteq P$ *as domain.*

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* $\mathcal{L}$*.*

Structures

Definition

$\mathcal{M}_s \models [\mathcal{E}_e]\varphi$ *iff* $\mathcal{M}_s \models pre(e)$ *implies* $(\mathcal{M} \otimes \mathcal{E})_{(s,e)} \models \varphi$

Definition

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 follows:*

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

Structures

Definition (Satisfaction relation 1/2)

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

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

$$
\begin{array}{lll}
\mathcal{M}_s \models \varphi \wedge \psi & \textit{iff} & \mathcal{M}_s \models \varphi \textit{ and } \mathcal{M}_s \models \psi \\
\mathcal{M}_s \models \varphi \to \psi & \textit{iff} & \mathcal{M}_s \not\models \varphi \textit{ or } \mathcal{M}_s \models \psi
\end{array}
$$

Structures

Definition (Satisfaction relation 2/2)

$$\begin{array}{lll} \mathcal{M}_s \models \varphi * \psi & \textit{iff} & \textit{there exist } t, u \in S \textit{ such that } r_s = r_t \bullet r_u, \\ & & \mathcal{M}_t \models \varphi \textit{ and } \mathcal{M}_u \models \psi \\ \mathcal{M}_s \models \varphi \mathrel{-\!\!*} \psi & \textit{iff} & \textit{for all } t \in S \textit{ such that } r_s \bullet r_t \downarrow \textit{ and } \mathcal{M}_t \models \varphi \\ & & \textit{there exists } u \in S \textit{ such that } r_u = r_s \bullet r_t \textit{ and } \mathcal{M}_u \models \psi \end{array}$$

$$\begin{array}{lll} \mathcal{M}_s \models K_a\varphi & \textit{iff} & \mathcal{M}_t \models \varphi \textit{ for all } t \in S \textit{ such that } s \sim_a t \\ \mathcal{M}_s \models [\mathcal{E}_e]\varphi & \textit{iff} & \mathcal{M}_s \models \textit{pre}(e) \textit{ implies } (\mathcal{M} \otimes \mathcal{E})_{(s,e)} \models \varphi \end{array}$$

Definition (Validity)

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 $\mathcal{M}$.

Eliminating Dynamic Modalities

We now define a set of ESLAM validities for action model modality elimination, by adding two novel reductions for $*$ and $-\!\!*$. to the reduction axioms for Action Model Logic with factual change.

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. $\langle \mathcal{E}_e \rangle K_a \psi \leftrightarrow (pre(e) \wedge \bigwedge_{e \sim_a f} K_a \langle \mathcal{E}_f \rangle \psi)$

Eliminating Dynamic Modalities

We now define a set of ESLAM validities for action model modality elimination, by adding two novel reductions for $*$ and $-\!\!*$. to the reduction axioms for Action Model Logic with factual change.

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. $\langle \mathcal{E}_e \rangle (\varphi -\!\!* \psi) \leftrightarrow (pre(e) \wedge \bigwedge_{f \in E} (\langle \mathcal{E}_f \rangle \varphi -\!\!* \bigvee_{g \in E} \langle \mathcal{E}_g \rangle \psi))$

Eliminating Dynamic Modalities

We now define a set of ESLAM validities for action model modality elimination, by adding two novel reductions for $*$ and $-\!\!*$. to the reduction axioms for Action Model Logic with factual change.

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. $\langle \mathcal{E}_e \rangle (\varphi -\!\!* \psi) \leftrightarrow (pre(e) \wedge \bigwedge_{f \in E} (\langle \mathcal{E}_f \rangle \varphi -\!\!* \bigvee_{g \in E} \langle \mathcal{E}_g \rangle \psi))$

The above validities are reduction rules using a complexity measure used to show the reduction for Public Announcement Logic.

The complexity of a formula $[\varphi]\psi$ is $c([\varphi]\psi) = (4 + c(\varphi)) \cdot c(\psi)$.
It is generalized for $[\mathcal{E}_e]\psi$ to $c([\mathcal{E}_e]\psi) = (4 + c(\mathcal{E})) \cdot c(\psi)$.

Library example revisited

We consider the modelling (library) example of PASL and illustrate what ESLAM allows us to express.

The example is the following one:

- two agents enter the library: $A = \{A_1, A_2\}$
- each of them can request either one book, two books, or zero book;
- the librarian can carry no more than two books at the time;
- the set of variables is $P = \{P_1, P_2, C\}$;

Library example revisited

The epistemic model $\mathcal{M} = (S, \sim, r, V)$ is defined as follows:

- $S = \{(i,j) \mid i,j \in \{0,1,2\}\}$
- $(i_1,j_1) \sim_{A_1} (i_2,j_2)$ iff $i_1 = i_2$ and $(i_1,j_1) \sim_{A_2} (i_2,j_2)$ iff $j_1 = j_2$
- $r_{(i,j)} = (i,j)$;
- $V(C) = \{(i,j) \mid i+j \leq 2\}$, $V(P_1) = \{(1,0)\}$, $V(P_2) = \{(0,1)\}$.

The partial resource monoid $\mathcal{R} = (S, \bullet, n)$ has as neutral element $n = (0,0)$, and a composition operator $\bullet$ defined as:

$$(i_1,j_1) \bullet (i_2,j_2) = \begin{cases} \uparrow & \text{if } i_1 + i_2 \geq 2 \text{ or } j_1 + j_2 \geq 2 \\ \text{otherwise,} & (i_1 + i_2, j_1 + j_2) \end{cases} \tag{1}$$

Library example revisited

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:
$E' = \{e, f\}$	$E = \{e, f\}$
$\approx'_{A_1} = \{(e,e),(f,f)\}$	$\approx_{A1} = \{(e,e),(f,f)\}$
$\approx'_{A_2} = \{(e,e),(f,f)\}$	$\approx_{A_2} = \{(e,f),(f,e),(e,e),(f,f)\}$
$pre'(e) = C$	$pre(e) = C$
$pre'(f) = \neg C$	$pre(f) = \neg C$
$post'(e) = post'(f)$ empty domain	$post(e) = post(f)$ empty domain

The difference between the two lies in the definition of $\approx_a$.

Library example revisited

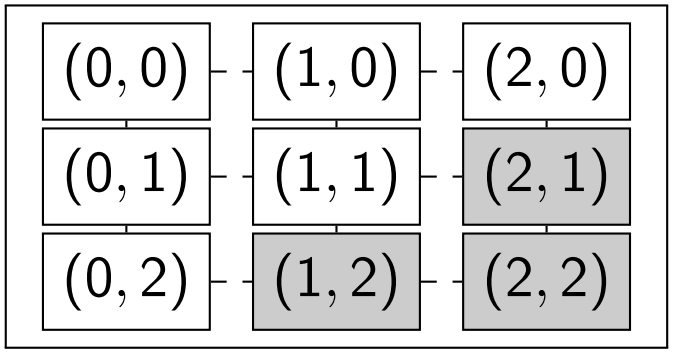

Figure: The initial model.

Dashed links represent the relation $\sim_{A_2}$.
Solid links represent the relation $\sim_{A_1}$.
Grey means "cannot be carried".

Library example revisited

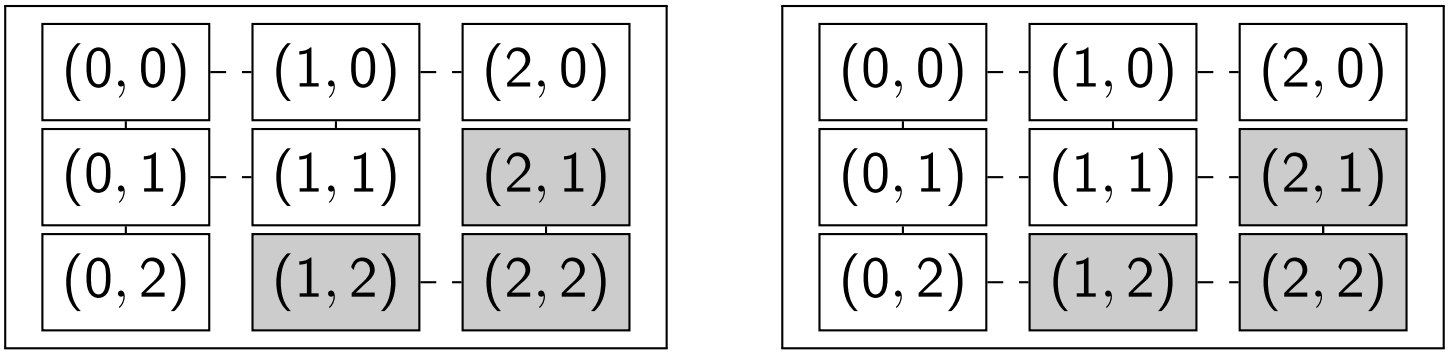

Figure: On the left (resp. right) the result of a public (resp. private) announcement $\mathcal{E}'_e$ (resp. $\mathcal{E}'_e$).

After the public announcement, both agents stopped considering the scenarios where the number of books requested exceeds the librarian's limit. After the private announcement this is the case only for A_2.

With ESLAM we can define instances of not only public announcement, but also private, more nuanced announcements as well as other forms of partial observation.

Conclusion and Perspectives

Epistemic Separation Logic with Action Models (ESLAM) which enables nuanced instances of private communication.

Future works will be developed in different directions:

- To define an additional action resource model monoid
  - allowing composition and separation of action points,
  - modelling sequential action point execution
- To investigate the optimal semantics for multiplicative connectives, taking into account the duality between these operations.