Dynamic Epistemic Separation Logic

Marta Gawek
(joint work with Hans van Ditmarsch and Didier Galmiche)

University of Lorraine, CNRS, LORIA

Open University of the Netherlands, Heerlen
November 2nd 2021

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 [Courtault, Galmiche 2018].
- Epistemic Resource Logic (**ERL**): to have modalities parametrized with resources, with a differentiation between ambient resource and local resources and their compositions (Galmiche, Kimmel-Pym 2019).
- Public Announcement Separation Logic (**PASL**): to model knowledge acquisition and information change over the course of truthful public communication (Courtault, van Ditmarsch, Galmiche 2019).

General context

Dynamic Epistemic Separation Logic (**DESL**)

- 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 DESL a resource function r maps every state (or several states) to a resource.

DESL – language and structures

The logic DESL 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 DESL, $\mathcal{L}_{K*}$, 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 resource composition (separation) and resource update.
$[\mathcal{E}_e]\varphi$ means that after execution of action $\mathcal{E}_e$, φ is true.

DESL – language and 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* $r \bullet r' \downarrow$.

DESL – language and 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 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* $\mathcal{M}_s$.

DESL – language and 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,*
- $post : E \to P \to \mathcal{L}$ *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* $\mathcal{L}$*.*

DESL – language and 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:*

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

DESL – language and structures

Remarks on the semantics:
The standard BI semantics for $*$ and $-\!\!*$ is as follows:

$$r \models \varphi * \psi \quad \text{iff} \quad \text{there are } r', r'' \in R, r = r' \bullet r'' \,\&\, r' \models \varphi \;\&\; r'' \models \psi$$

$$r \models \varphi -\!\!* \psi \quad \text{iff} \quad \text{for all } r' \in R, r \bullet r' \downarrow \;\&\; r' \models \varphi \Rightarrow r \bullet r' \models \psi$$

In the standard approach a resource and a state (possible world) are the same object.

DESL – language and 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:*

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

DESL – language and structures

Definition (Satisfaction relation 2/2)

$$\mathcal{M}_s \models \varphi * \psi \quad \textit{iff} \quad \exists r', r'' : r_s = r' \bullet r'' \;\&\; (\exists t : r_t = r' \;\&\; \mathcal{M}_t \models \varphi) \;\&\; (\exists u : r_u = r'' \;\&\; \mathcal{M}_u \models \psi)$$

$$\mathcal{M}_s \models \varphi \mathrel{-\!\!*} \psi \quad \textit{iff} \quad \forall r' : r_s \bullet r' \downarrow \;\&\; (\exists t : r_t = r' \;\&\; \mathcal{M}_t \models \varphi) \Rightarrow (\exists u : r_u = r_s \bullet r' \;\&\; \mathcal{M}_u \models \psi)$$

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 Action Models

We now define a set of DESL 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 Action Models

We now define a set of DESL 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 Action Models

We now define a set of DESL 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

Let us consider the modelling (library) example of PASL:

- two agents (Alice and Bob) enter the library: $A = \{A, B\}$
- 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;

Library example revisited

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

- $S = \{(i,j) \mid i,j \in \{0,1,2\}\}$
- $(i_1,j_1) \sim_A (i_2,j_2)$ iff $i_1 = i_2$;
- $(i_1,j_1) \sim_B (i_2,j_2)$ iff $j_1 = j_2$
- $r_{(i,j)} = (i,j)$;
- $V(C) = \{(i,j) \mid i+j \leq 2\}$, $V(P_A) = \{(1,0)\}$, $V(P_B) = \{(0,1)\}$.

Library example revisited

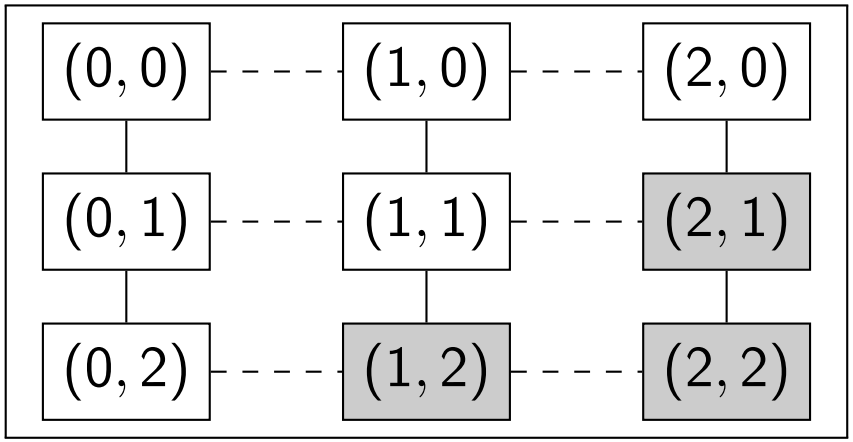

Figure: The initial model.

Dashed links represent the relation $\sim_B$.
Solid links represent the relation $\sim_A$.
Grey means "cannot be carried".

Library example revisited

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

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

We read $\uparrow$ as: *the composition is undefined*.

Example: $(1, 1) \bullet (0, 1) = (1 + 0, 1 + 1) = (1, 2)$.

Library example revisited

Public vs Private Announcement:

We model an action of the librarian telling either: both agents (by means of $\mathcal{E}'$), Alice only (in $\mathcal{E}$) that they can carry the books.

Public announcement action model:

$\mathcal{E}' = \{E', \approx'_a, pre', post'\}$, where:
$E' = \{e, f\}$
$\approx'_A = \{(e,e),(f,f)\}$
$\approx'_B = \{(e,e),(f,f)\}$
$pre'(e) = C$
$pre'(f) = \neg C$
$post'(e) = post'(f)$ empty domain

Private announcement action model:

$\mathcal{E} = \{E, \approx_a, pre, post\}$, where:
$E = \{e, f\}$
$\approx_A = \{(e,e),(f,f)\}$
$\approx_B = \{(e,f),(f,e),(e,e),(f,f)\}$
$pre(e) = C$
$pre(f) = \neg C$
$post(e) = post(f)$ empty domain

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

Library example revisited

Public vs Private Announcement:

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 that they can carry the books ($\mathcal{E}_e$). (In DESL, as in PASL, a public announcement is a two-event action model, because of the requirement that the action is covering.)

$$\mathcal{M}_{(1,1)} \models \langle \mathcal{E}'_e \rangle (K_A C \wedge K_B C)$$
$$\Leftrightarrow$$
$$\mathcal{M}_{(1,1)} \models C$$
and
$$(\mathcal{M} \otimes \mathcal{E})_{((1,1),e)} \models K_A C \wedge K_B C$$

$$\mathcal{M}_{(1,1)} \models \langle \mathcal{E}_e \rangle (K_A C \wedge \neg K_B C)$$
$$\Leftrightarrow$$
$$\mathcal{M}_{(1,1)} \models_{\mathcal{M}} C$$
and
$$(\mathcal{M} \otimes \mathcal{E})_{((1,1),e)} \models K_A C \wedge \neg K_B C$$

Library example revisited

Public vs Private Announcement:

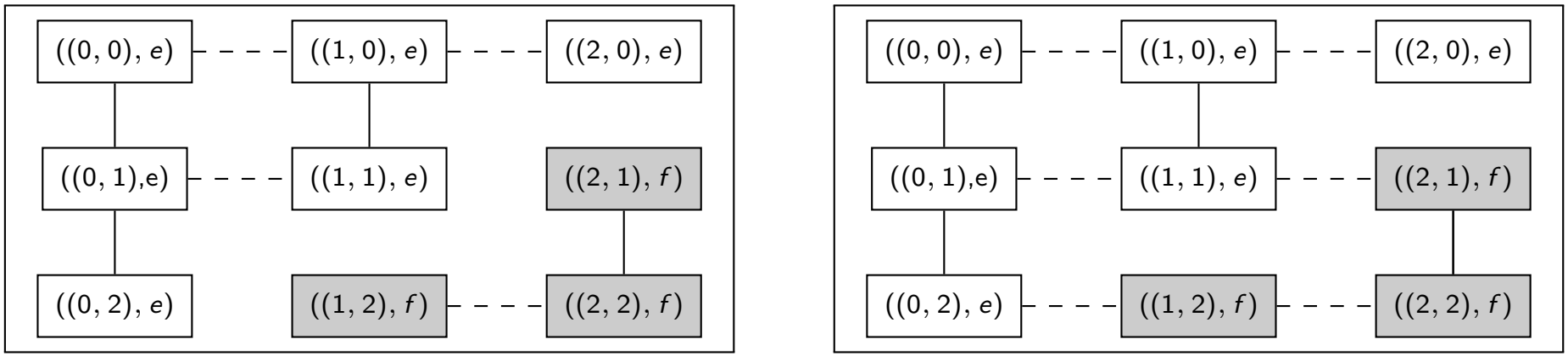

Figure: On the left (resp. right) the result of a public (resp. private) announcement $\mathcal{E}'_e$ (resp. $\mathcal{E}'_e$).

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 Alice.

Conclusion and Perspectives

Dynamic Epistemic Separation Logic (DESL) which enables nuanced instances of private communication.

Future works will be developed in different directions:

- Modelling sequential action point execution through composition and separation of action points
- To investigate the optimal semantics for multiplicative connectives.

Thank you!