A separation logic with histories of epistemic actions as resources

Hans van Ditmarsch, Université de Toulouse, CNRS, IRIT, France
Didier Galmiche, Université de Lorraine, CNRS, LORIA, France
Marta Gawek, Université de Lorraine, CNRS, LORIA, France

Presentation for WoLLIC Halifax, July 11–14, 2023

Overview

We propose a separation logic AMHSL where resources are histories of epistemic actions so that resource composition (update) means concatenation of histories and resource decomposition means splitting of histories. In this logic we can reason about what was true in the past.

We show that the multiplicative connectives of separation logic can be eliminated from a logical language with also epistemic and action model modalities, given a maximum of permitted actions.

- proposals for epistemic separation logic
- language and semantics of AMHSL
- example : gossip
- eliminating multiplicative connectives $*$, $-\!\!*$, $*\!\!-$

Separation logic and epistemic logic

Dynamic epistemic logic formalizes multi-agent knowledge and change of knowledge. Public announcement logic models public information change. Action model logic models private information change. These extend the propositional (Boolean) language with knowledge modalities K_i and dynamic (update) modalities $[\varphi]$ for public announcements or $[\mathcal{E}_e]$ for action models $\mathcal{E}_e$.

[Plaza, Gerbrandy, Baltag, Moss, vBenthem, vD, vdHoek, ...]

Separation logic models separation and concatenation of resources. The logics of Bunched Implications (BI) and Boolean BI (BBI) extend the additive (Boolean) language with the multiplicative conjunction $*$, expressing separation of resources, and the multiplicative implication $-\!\!*$, expressing resource concatenation (also called update).

[O'Hearn, Pym, Galmiche, ...]

Combining separation logic and epistemic logic

Various proposals for epistemic separation logic

- *epistemic separation logic*: Worlds of Kripke models are resources. Resource composition and decomposition relate different worlds by way of their valuations. The Kripke model domain must define a resource monoid. Different worlds must have different valuations.
- *public announcement separation logic*: A generalization allowing public information update. The updated model must still define a resource monoid (the world that is the neutral element of the monoid cannot be eliminated).
- *action model separation logic*: A further generalization also allowing semi-public information update. Valuations are resources, because in updated models different worlds may have the same valuation.
- *separation logic with histories of epistemic actions as resources*: A very different epistemic separation logic ...

Resource composition and decomposition of histories

Given a set of actions (Anne announces she knows the access code, Bill opens the strongbox, Cath observes Bill typing the code, Bill runs away with the cash), consider sequences of actions. Actions need not be public and need not be informative actions.

- Actions are pointed action models (with factual change). We simply write $e, e', f, f', g, g', \ldots$ These are different points of one given action model $\mathcal{E}$. Histories are sequences of actions. This is iteration of updating the epistemic model with $\mathcal{E}$.
- Action composition: given histories ef (two actions) and ge (two actions), obtain $efge$ (four actions).
- Action decomposition: given history $efge$, obtain e and fge, or ef and ge, or ϵ and $efge$, ...

– Action composition is associative, but not commutative.
– Not all histories are executable:
You cannot run away with the cash before the strongbox is open.

Syntax and semantics AMHSL

Given a finite set of *agents* A and a countable set of *atoms* P.

Logical language $\mathcal{L}^{K*\mathcal{E}}(A,P)$, where e a pointed action model $\mathcal{E}_e$:

$$p \mid I \mid \bot \mid \neg\psi \mid (\psi \wedge \psi) \mid (\psi * \psi) \mid (\psi \mathrel{-\!\!*} \psi) \mid (\psi \mathrel{*\!\!-} \psi) \mid K_a\psi \mid [e]\psi$$

Satisfaction relation $\models$ given *epistemic history model* $\mathcal{ME}^{\omega}_{sh}$ ($\mathcal{ME}^{\mathbf{max}}_{sh}$):

$sh \models p$	iff	$s \models post(h)(p)$
$sh \models I$	iff	$h = \epsilon$
$sh \models \bot$	iff	false
$sh \models \neg\varphi$	iff	$sh \not\models \varphi$
$sh \models \varphi \wedge \psi$	iff	$sh \models \varphi$ and $sh \models \psi$
$sh \models \varphi * \psi$	iff	$\exists sh', sh'' : h = h'h'', sh' \models \varphi,$ and $sh'' \models \psi$
$sh \models \varphi \mathrel{-\!\!*} \psi$	iff	$\forall sh', shh' : sh' \models \varphi$ implies $shh' \models \psi$
$sh \models \varphi \mathrel{*\!\!-} \psi$	iff	$\forall sh', sh'h : sh' \models \varphi$ implies $sh'h \models \psi$
$sh \models K_a\varphi$	iff	$s'h' \models \varphi$ for all $s'h'$ such that $sh \sim_a s'h'$
$sh \models [e]\varphi$	iff	($\lvert h\rvert < max$ and) $sh \models pre(e)$ implies $she \models \varphi$

Examples: gossip protocol

Each agent holds a secret. Agents exchange all secrets they know in a call. The goal is for all agents to know all secrets (be *experts*).

— $ab.ac \models c_b \twoheadrightarrow Exp$: *assume three agents* a, b, c
Any subsequent call after which b knows the secret of c makes b, and thus all, experts: $ab.ac.\mathbf{bc} \models Exp$, and $ab.ac.\mathbf{ac.ac.ab} \models Exp$.

— $\models \varphi_{ab} \twoheadleftarrow K_a K_b(b_c \to a_c)$, with $\varphi_{ab} := a_b \wedge b_a \wedge \bigwedge_{c \neq a,b}(\neg c_b \wedge \neg c_a)$
A sequence where a and b first call each other, when prefixed to another sequence, makes c learning the secret of b also learn that of a: $cd.ab \models \varphi_{ab}$, so $\mathbf{cd.ab}.bc \models K_a K_b(b_c \to a_c)$.

— $\not\models \varphi_{ab} \twoheadrightarrow K_a K_b(b_c \to a_c)$:
But not postfixed: $cd.ab \models \varphi_{ab}$, but $bc.\mathbf{cd.ab} \not\models b_c \to a_c$ (so . . .)

– $\not\models a_c \wedge b_c \to a_c * b_c$:
Agent c may know the secrets of a and b but not after fewer calls.
$ab.ac \models a_c \wedge b_c$ but $ab.ac \not\models a_c * b_c$

Elimination of the multiplicative connectives and constant

Every formula with I, $*$, $-\!\!*$, or $*\!\!-$ is equivalent to a formula without. A formula in action model logic is equivalent to one in multi-agent S5, with only K_a modalities. (So AMHSL = S5.)

We consider the validities for the epistemic history models with empty histories, and given a maximum length of histories when evaluating formulas (the model $\mathcal{ME}_{sh}^{\mathbf{max}}$). Notation: $[h]\varphi$, for $h = e_1 \dots e_n$, means $[e_1] \dots [e_n]\varphi$; $\sqsubseteq$ means prefix; $\cdot\backslash\cdot$, postfix.

Reductions of I, $*$, $-\!\!*$, $*\!\!-$ (where $1 \leq |h| \leq \mathbf{max}$):

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

Proof of termination of the reduction

Complexity $c(p) = 1,\ c(\neg\varphi) = c(\varphi) + 1,\ \ldots,$ and:

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

Translation $t(p) = 1,\ t(\neg\varphi) = \neg t(\varphi),\ \ldots,$ and:

$$\begin{array}{lcl} t([h](\varphi * \psi)) & = & pre(h) \to t(\bigvee_{h' \sqsubseteq h}(\langle h' \rangle \varphi \wedge \langle h \backslash h' \rangle \psi)) \\ t([h](\varphi \mathrel{-\!\!*} \psi)) & = & pre(h) \to t(\bigwedge_{|h'| \leq \mathbf{max} - |h|}(\langle h' \rangle \varphi \to [hh'] \psi)) \end{array}$$

Inequalities the usual action model reductions, and:

$$\begin{array}{lcl} c([h](\varphi * \psi)) & > & c(pre(h) \to \bigvee_{h'.h''=h}(\langle h' \rangle \varphi \wedge \langle h'' \rangle \psi)) \\ c([h](\varphi \mathrel{-\!\!*} \psi)) & > & c(pre(h) \to \bigwedge_{|h'| \leq \mathbf{max} - |h|}(\langle h' \rangle \varphi \to [h.h'] \psi)) \end{array}$$

Termination atoms already terminal, other φ:

$c(\varphi) > c(t(\varphi))$ at each step, bounded by 0, so we're done.

Further research

- Reduction without a bound **max** on histories that can be interpreted, so for histories of arbitrary length. So, for $\varphi \twoheadrightarrow \psi$ to be true in h, for any of infinitely many h' satisfying φ, hh' should satisfy ψ. (Reductions with infinite conjunctions.)
- Decomposing histories into two subsequences instead of prefix and postfix. Now, $*$ is commutative and one $\twoheadrightarrow$ suffices. For $\varphi * \psi$ to be true in h, any subsequence h' and $h \backslash h'$ satisfying φ resp. ψ will suffice (in either order: $h \backslash h'$ is also a subsequ.).
- Axiomatization and reduction w.r.t. the class of arbitrary epistemic history models (instead of empty history models).
- More properties of $*$ and $\twoheadleftarrow$, such as $\neg I * \neg I * \neg I$ requiring at least three actions to have been executed. (I is true in ϵ.)

Thank you!