Completeness for Abstract Separation Logics

Dominique Larchey-Wendling & Didier Galmiche

TYPES team

LORIA – CNRS

Nancy, France

ANR-Dynres, Nancy, France

Separation Logic

- Introduced by Reynolds&O'Hearn 01 to model:
  - a resource logic
  - properties of the memory space (cells)
  - aggregation of cells into wider structures
- Combines:
  - classical logic connectives: $\wedge$, $\vee$, $\rightarrow$ $\ldots$
  - multiplicative conjunction: $*$
- Defined via Kripke semantics extended by:

$$m \Vdash A * B \quad \text{iff} \quad \exists a, b \text{ s.t. } a, b \triangleright m \wedge a \Vdash A \wedge b \Vdash B$$

Separation models, Separation Algebras

- Decomposition $a, b \triangleright m$ interpreted in various structures:
  - stacks in pointer logic (Reynolds&O'Hearn&Yang 01), $a \uplus b \subseteq m$
  - but also $a \uplus b = m$ (Calcagno&Yang&O'Hearn 01)
  - trees in spatial logics (Calcagno&Cardelli&Gordon 02) $a \mid b \equiv m$
- Additive $\rightarrow$ can be Boolean (pointwise) or intuitionistic
- Separation Algebra (SA) (Calcagno&O'Hearn&Yang 07) :
  - partial and cancellative commutative monoid
  - also, single units, indivisible units, disjointness

Boolean **BI** (**BBI**) and **PASL**

- BBI loosely defined by Pym as $\mathsf{BI} + \{\neg\neg A \rightarrow A\}$
  - Kripke semantics by ND-monoids, Hilbert system (LW&G 06)
  - Display Logic based cut-free proof-system (Brotherston 09)
  - Structure Sequent proof-search (Park&Seo&Park 13)
  - Labeled sequents (Hóu&Tiu&Goré 13)
- Propositionnal Abstract Separation Logic (PASL)
  - based on separation algebras, partial monoids + ...
  - labeled tableaux (Larchey&Galmiche 09, Larchey 13)
  - labeled sequents (Hóu&Clouston&Goré&Tiu 14)
- family of undecidable logics (LW&G 10, B&K 10)

Kripke semantics of **BBI**&**PASL** (i)

- Non-deterministic(/relational) monoid (ND) $(M, \circ, U)$
  - $\circ : M \times M \longrightarrow \mathcal{P}(M)$ and $U \subseteq M$
  - for $X, Y \in \mathcal{P}(M)$, $\boxed{X \circ Y = \{z \mid \exists x \in X, \exists y \in Y, z \in x \circ y\}}$
  - $x \circ U = \{x\}$ (neutrality), $x \circ y = y \circ x$ (commutativity)
  - $x \circ (y \circ z) = (x \circ y) \circ z$ (associativity)
  - $(\mathcal{P}(M), \circ, U)$ is a residuated commutative monoid
  - residuation on $\mathcal{P}(M)$: $X \multimap Y = \{z \mid z \circ X \subseteq Y\}$

Kripke semantics of **BBI&PASL** (ii)

- Boolean (pointwise) Kripke semantics extended by:

$$
\begin{array}{rcl}
m \Vdash A * B & \text{iff} & \exists a, b \text{ s.t. } m \in a \circ b \wedge a \Vdash A \wedge b \Vdash B \\
m \Vdash A \mathrel{-\!\!*} B & \text{iff} & \forall a, b \;\; (b \in a \circ m \wedge a \Vdash A) \Rightarrow b \Vdash B \\
m \Vdash \mathbb{I} & \text{iff} & m \in U
\end{array}
$$

- Validity in a ND-monoid $(M, \circ, U)$: $\forall \Vdash, \forall m,\ m \Vdash A$
- Validity in a sub-class $\mathcal{X} \subseteq \text{ND}$: $\forall M \in \mathcal{X}, M \Vdash A$
- Set of formula valid in $\mathcal{X}$: $\mathsf{BBI}_{\mathcal{X}}$
- $\mathcal{X} \subseteq \mathcal{Y}$ implies $\mathsf{BBI}_{\mathcal{Y}} \subseteq \mathsf{BBI}_{\mathcal{X}}$
- the full class ND: $\mathsf{BBI}_{\text{ND}} \subseteq \mathsf{BBI}_{\mathcal{X}}$

Classes of models for **BBI**

- Partial monoids (PD): $a \circ b \subseteq \{k\}$
- Total monoids (TD): $a \circ b = \{k\}$
- Single unit (SU): $\exists u \;\; U = \{u\}$
- Cancellative (CA): $\forall x, k, a, b \;\; x \in (k \circ a) \cap (k \circ b) \Rightarrow a = b$
- Indivisible units (IU): $\forall x, y \;\; x \circ y \cap U \neq \emptyset \Rightarrow x \in U$
- Disjointness (DI): $\forall x \;\; x \circ x \neq \emptyset \Rightarrow x \in U$

$$
\begin{tikzcd}
 & & \mathsf{BBI}_{\mathrm{PD+SU}} \arrow[dr, Rightarrow] & & & & \\
\mathsf{BBI}_{\mathrm{ND}} \arrow[r] & \mathsf{BBI}_{\mathrm{PD}} \arrow[ur, Rightarrow] \arrow[dr, Rightarrow] & & \mathsf{BBI}_{\mathrm{PD+CA+SU}} \arrow[r] & \mathsf{BBI}_{\mathrm{PD+CA+SU+IU}} \arrow[r, Rightarrow] & \mathsf{BBI}_{\mathrm{PD+CA+SU+IU+DI}} \arrow[r, Rightarrow] & \mathsf{BBI}_{\mathrm{HM}} \\
 & & \mathsf{BBI}_{\mathrm{PD+CA}} \arrow[ur, Rightarrow] & & & &
\end{tikzcd}
$$

Single unit models/multiple unit model

- Consider any ND-monoid $(M, \circ, U)$
- every element $x \in M$ has a unique unit $u_x \in U$ s.t. $x \circ u_x = \{x\}$
- if $x \in y \circ z$ then $u_x = u_y = u_z$
- the slice monoid:
  - $(M_u = \{x \in M \mid u_x = u\}, \circ \cap M_u \times M_u, \{u\})$ in class SU
  - $M = M_{u_1} \uplus \cdots \uplus M_{u_i} \uplus \cdots$
  - $M, x \nVdash F$ iff $M_{u_x}, x \nVdash F$ hence CM preserved by slicing
- $\mathsf{BBI}_{\mathrm{ND}} = \mathsf{BBI}_{\mathrm{SU}}$ and $\mathsf{BBI}_{\mathrm{PD}} = \mathsf{BBI}_{\mathrm{PD+SU}}$

Words and constraints based models for **BBI**

- Resources as Words of $L^\star$ = multisets of letters
- Constraints = (ordered) pairs of words: $m \multimap n$ with $m, n \in L^\star$
- Partial monoidal equivalence $\sim$ (PME)

$$\frac{}{\epsilon \multimap \epsilon}\langle\epsilon\rangle \qquad \frac{x \multimap y}{y \multimap x}\langle s\rangle \qquad \frac{ky \multimap ky \qquad x \multimap y}{kx \multimap ky}\langle c\rangle$$

$$\frac{xy \multimap xy}{x \multimap x}\langle d\rangle \qquad \frac{x \multimap y \qquad y \multimap z}{x \multimap z}\langle t\rangle$$

- PME = set of constraints closed under these rules
- given $\mathcal{C}$, the closure is $\overline{\mathcal{C}} = \sim_{\mathcal{C}}$; compactness prop.

Extra **PME** rules, quotients to PD + SU

Derived rules		Extra rules
$\dfrac{kx \multimap y}{x \multimap x}\ \langle p_l \rangle$	$\dfrac{x \multimap y \qquad yk \multimap m}{xk \multimap m}\ \langle e_l \rangle$	$\dfrac{kx \multimap ky}{x \multimap y}\ \langle ca \rangle$
$\dfrac{x \multimap ky}{y \multimap y}\ \langle p_r \rangle$	$\dfrac{x \multimap y \qquad m \multimap yk}{m \multimap xk}\ \langle e_r \rangle$	$\dfrac{\epsilon \multimap xy}{\epsilon \multimap x}\ \langle iu \rangle$

- Quotient to PD + SU:
  - $\sim$ is a partial equivalence relation: $L^\star/\!\sim\, = \{[x] \mid x \sim x\}$
  - composition of classes: $[z] \in [x] \bullet [y]$ iff $z \sim xy$
  - $(L^\star/\!\sim, \bullet, \{[\epsilon]\})$ of sub-class PD + SU; this map is onto
  - $L^\star/\!\sim$ of class CA (r. IU) iff $\sim$ closed under $\langle ca \rangle$ (r. $\langle iu \rangle$)

Labelled tableaux for **BBI** and basic constraints

- Statements $(\mathsf{T}A : m)$, assertions $(\text{ass} : \ m \mathrel{-\!\bullet\!-} n)$ and $\text{req} : m \sim n$

$$
\begin{array}{c|c|c}
\mathsf{T}\mathbb{I} : m & \mathsf{T}A * B : m & \mathsf{F}A \mathrel{-\!*} B : m \\
| & | & | \\
\text{ass} : \ \epsilon \mathrel{-\!\bullet\!-} m & \text{ass} : \ ab \mathrel{-\!\bullet\!-} m & \text{ass} : \ am \mathrel{-\!\bullet\!-} b \\
 & \mathsf{T}A : a & \mathsf{T}A : a \\
 & \mathsf{T}B : b & \mathsf{F}B : b
\end{array}
$$

- Basic extensions: $\sim + \{x \mathrel{-\!\bullet\!-} y\} = \overline{\sim \cup \{x \mathrel{-\!\bullet\!-} y\}}$

1. $\sim + \{\epsilon \mathrel{-\!\bullet\!-} m\}$ with $m \sim m$;
2. $\sim + \{\mathsf{ab} \mathrel{-\!\bullet\!-} m\}$ with $m \sim m$ and $\mathsf{a} \neq \mathsf{b} \in L \backslash \mathsf{A}_{\sim}$;
3. $\sim + \{\mathsf{a}m \mathrel{-\!\bullet\!-} \mathsf{b}\}$ with $m \sim m$ and $\mathsf{a} \neq \mathsf{b} \in L \backslash \mathsf{A}_{\sim}$.

PS generated constraints, Strong completeness

- Simple PME = infinite sequence of basic extensions from $\emptyset$
- Failed proof-search generates simple PME as counter-model
- $\mathsf{BBI}_{\mathrm{PD+SU}}$ is complete for the class of simple PMEs
- Study the properties of simple PMEs
- And obtain other refined completeness results

Extensions $\sim + \{\mathsf{ab} \multimap m\}$

- given $\sim$ PME over L.
- given $m, \alpha \in L^\star$ s.t. $m \sim m$, $mm \not\sim mm$, $\alpha \neq \epsilon$ and $A_\alpha \cap A_\sim = \emptyset$

$$\begin{aligned}\sim + \{\alpha \multimap m\} = \sim &\cup \big\{\delta x \multimap \delta y \mid x \sim y, mx \sim my, \delta \prec \alpha \text{ and } \delta \notin \{\epsilon, \alpha\}\big\} \\ &\cup \big\{\alpha x \multimap \alpha y \mid mx \sim my\big\} \\ &\cup \big\{\alpha x \multimap y \mid mx \sim y\big\} \\ &\cup \big\{x \multimap \alpha y \mid x \sim my\big\}\end{aligned}$$

- if $\sim$ is cancellative then $\sim + \{\alpha \multimap m\}$ is cancellative
- if α and $\sim$ have no square then $\sim + \{\alpha \multimap m\}$ has no square
- a more recent and general equation ($mm \sim mm$ allowed)

$$\sim + \{\alpha \multimap m\} = \{\delta\alpha^u x \multimap \delta\alpha^v y \mid m^u x \sim m^v y,\ m^{i+u} x \sim m^{i+v} y,\ \delta \prec \alpha^i \text{ for some } i\}$$

Extensions $\sim + \{\mathsf{a}m \multimap \mathsf{b}\}$

- $\sim$ is a PME over L
- $m, \alpha \in L^\star$ and $\mathsf{b} \in L$ s.t. $m \sim m$, $\alpha \neq \epsilon$, $\mathsf{A}_\sim \uplus \mathsf{A}_\alpha \uplus \{\mathsf{b}\}$

$$
\begin{aligned}
\sim + \{\alpha m \multimap \mathsf{b}\} = \sim &\cup \left\{\delta x \multimap \delta y \mid x \sim y, \epsilon \neq \delta \prec \alpha \text{ and } xk \sim m \text{ for some } k\right\} \\
&\cup \left\{\alpha x \multimap j\mathsf{b} \mid x \sim jm \text{ and } jkm \sim m \text{ for some } k\right\} \\
&\cup \left\{i\mathsf{b} \multimap \alpha y \mid y \sim im \text{ and } ikm \sim m \text{ for some } k\right\} \\
&\cup \left\{i\mathsf{b} \multimap j\mathsf{b} \mid ikm \sim m \text{ and } jkm \sim m \text{ for some } k\right\}
\end{aligned}
$$

- if $\sim$ is cancellative then $\sim + \{\alpha m \multimap \mathsf{b}\}$ is cancellative
- if α and $\sim$ have no square then $\sim + \{\alpha m \multimap \mathsf{b}\}$ has no square

Problem is with extensions $\sim + \{\epsilon \mathrel{-\!\!\bullet\!\!-} m\}$ (i)

$\boxed{\mathsf{kx} \sim_0 \mathsf{ab}}$ $\boxed{\mathsf{ac} \sim_0 \mathsf{ky}}$

$\boxed{\mathsf{k}}$ $\boxed{\mathsf{x}}$ $\boxed{\mathsf{y}}$ $\boxed{\mathsf{a}}$ $\boxed{\mathsf{b}}$ $\boxed{\mathsf{c}}$

$\boxed{\epsilon}$

- $\mathcal{C}_0 = \{\mathsf{kx} \mathrel{-\!\!\bullet\!\!-} \mathsf{ab}, \mathsf{ky} \mathrel{-\!\!\bullet\!\!-} \mathsf{ac}\}$
- $\sim_0 = \overline{\mathcal{C}_0}$
- $\sim_0$ is cancellative
- $\sim_0$ contains no squares

Problem is with extensions $\sim + \{\epsilon \mathrel{-\!\!\bullet\!\!-} m\}$ (ii)

$$\boxed{\mathsf{a} \sim_1 \mathsf{kx} \sim_1 \mathsf{ky}}$$

$$\boxed{\mathsf{k}} \qquad \boxed{\mathsf{x}} \qquad \boxed{\mathsf{y}}$$

$$\boxed{\epsilon}$$

- $\mathcal{C}_1 = \mathcal{C}_0 \cup \{\epsilon \mathrel{-\!\!\bullet\!\!-} \mathsf{b}, \epsilon \mathrel{-\!\!\bullet\!\!-} \mathsf{c}\}$
- $\sim_1 = \overline{\mathcal{C}_1} = \sim_0 + \{\epsilon \mathrel{-\!\!\bullet\!\!-} \mathsf{b}\} + \{\epsilon \mathrel{-\!\!\bullet\!\!-} \mathsf{c}\}$
- $\sim_1$ is not cancellative, $\mathsf{kx} \sim_1 \mathsf{ky}$ but $\mathsf{x} \not\sim_1 \mathsf{y}$
- $\sim_1$ contains no (non-invertible) squares
- i.e. $mm \not\sim_1 mm$ unless $\epsilon \sim_1 m\beta$ for some β

Problem is with extensions $\sim + \{\epsilon \multimap m\}$ (iii)

$$\boxed{\mathsf{a} \sim_2 \mathsf{k} \sim_2 \mathsf{ky} \sim_2 \cdots \sim_2 \mathsf{ky}^n \sim_2 \cdots}$$

$$\boxed{\epsilon} \quad \boxed{\mathsf{y}} \quad \boxed{\mathsf{y}^2} \quad \cdots \quad \boxed{\mathsf{y}^n} \quad \cdots$$

- $\mathcal{C}_2 = \mathcal{C}_1 \cup \{\epsilon \multimap \mathsf{x}\}$
- $\sim_2 = \overline{\mathcal{C}_2} = \sim_1 + \{\epsilon \multimap \mathsf{x}\}$
- $\sim_2$ is not cancellative, $\mathsf{y} \sim_2 \mathsf{yk}$ but $\epsilon \not\sim_2 \mathsf{k}$
- $\sim_2$ contains non-invertible squares, $\mathsf{yy} \sim_2 \mathsf{yy}$

Invertible elements

$$\frac{\epsilon \mathrel{-\!\!\bullet\!\!-} \alpha \qquad \epsilon \mathrel{-\!\!\bullet\!\!-} \beta}{\epsilon \mathrel{-\!\!\bullet\!\!-} \alpha\beta}\langle \epsilon_c \rangle \qquad \frac{x \mathrel{-\!\!\bullet\!\!-} y \qquad \epsilon \mathrel{-\!\!\bullet\!\!-} \alpha\beta}{\alpha x \mathrel{-\!\!\bullet\!\!-} \alpha y}\langle i_c \rangle \qquad \frac{x \mathrel{-\!\!\bullet\!\!-} \beta y \qquad \epsilon \mathrel{-\!\!\bullet\!\!-} \alpha\beta}{\alpha x \mathrel{-\!\!\bullet\!\!-} y}\langle i_\leftarrow \rangle$$

$$\frac{\epsilon \mathrel{-\!\!\bullet\!\!-} \alpha\beta \qquad \epsilon \mathrel{-\!\!\bullet\!\!-} \alpha\gamma}{\beta \mathrel{-\!\!\bullet\!\!-} \gamma}\langle i_\uparrow \rangle \qquad \frac{\alpha x \mathrel{-\!\!\bullet\!\!-} \alpha y \qquad \epsilon \mathrel{-\!\!\bullet\!\!-} \alpha\beta}{x \mathrel{-\!\!\bullet\!\!-} y}\langle i_s \rangle \qquad \frac{\alpha x \mathrel{-\!\!\bullet\!\!-} y \qquad \epsilon \mathrel{-\!\!\bullet\!\!-} \alpha\beta}{x \mathrel{-\!\!\bullet\!\!-} \beta y}\langle i_\rightarrow \rangle$$

- PME are closed under those rules
- invertible letters: $\mathsf{I}_\sim = \{\mathsf{i} \in L \mid \epsilon \sim \mathsf{i}m$ holds for some $m \in L^\star\}$
- invertible words: $\alpha \in \mathsf{I}_\sim^\star$ iff $\epsilon \sim \alpha\beta$ for some β
- for any $\alpha \in \mathsf{I}_\sim^\star$, $x \sim y$ iff $\alpha x \sim \alpha y$
- $\mathsf{I}_{\sim + \{x \mathrel{-\!\!\bullet\!\!-} y\}} = \mathsf{I}_\sim$ unless $\{x, y\} \cap \mathsf{I}_\sim^\star \neq \emptyset$
- group-PME: $\mathsf{A}_\sim = \mathsf{I}_\sim$, every defined letter is invertible

Primary PME

- for $\sim$ PME, $m, \alpha \in L^\star$ s.t. $m \sim m$, $\alpha \neq \epsilon$, $\mathsf{A}_\sim \cap \mathsf{A}_\alpha = \emptyset$
  - type-1 extension: $\sim + \{\alpha \rightarrowtail m\}$ with $m \notin \mathsf{I}^\star_\sim$
  - type-2 extension: $\sim + \{\alpha m \rightarrowtail \mathsf{b}\}$ with $\mathsf{b} \in L \backslash (\mathsf{A}_\sim \cup \mathsf{A}_\alpha)$
- primary extension: either a type-1 or a type-2 extension
- a primary PME is either
  - a group-PME
  - a primary extension of a primary PME
- group-PME are cancellative and have invertible squares
- primary extensions preserve both properties

Primary **PME** and Basic **PME**

- Primary PMEs are cancellative with invertible squares
- Basic PMEs can be transformed into primary PMEs
- Hence basic PMEs are cancellative
- Simple PMEs are cancellative (by compactness)
- $\mathsf{BBI}_{\mathrm{PD+SU}}$ is complete for CA: $\boxed{\mathsf{BBI}_{\mathrm{PD+SU+CA}} = \mathsf{BBI}_{\mathrm{PD+SU}}}$

Conclusion

- Labeled tableaux are sound and complete for PASL
- Cancellativity rule is redundant in labeled sequents for PASL
- other properties related to squares:
  - IU encoded by rule $\langle iu \rangle$
  - $mm \sim mm \Rightarrow \epsilon \mathrel{-\!\bullet\!-} m\beta \Rightarrow \epsilon \sim m$ (rule $\langle iu \rangle$)
  - $\mathsf{BBI}_{\mathrm{PD+SU+IU}}$ complete for disjointness DI