Relational semantics and finite models of separation logics

Didier Galmiche, Dominique Larchey, Daniel Mery

LORIA – UHP Nancy 1 – CNRS

Nancy, France

CMF'2007 – Nancy, France

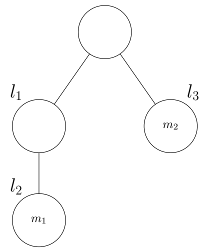
Separation Logic

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

$$m \Vdash A * B \quad \text{iff} \quad \exists a, b \text{ s.t. } a \uplus b \subseteq m \text{ and } a \Vdash A \text{ and } b \Vdash B$$

Separation models

- Decomposition $a, b \triangleright m$ interpreted in various structures:
  - stacks in pointer logic (Reynolds, O'Hearn), $a \uplus b \subseteq m$
  - trees in spatial logics (Cardelli, Gardner et al.) $a \mid b \equiv m$
  - resource trees in BI-Loc (Biri, Galmiche)



- Additives $\wedge$, $\vee$, $\rightarrow$ can be classical or intuitionistic
- Aggregation property:

$$a, b \triangleright \mathrm{e} \quad \text{implies} \quad a = b = \mathrm{e}$$

Separation Logic vs BI Logic

- Decomposition interpreted by $a \circ b \leqslant m$:
  - resource monoids (partial, ordered, no aggregation)
  - intuitionistic additives and a linear adjoint $-\!\!*$ to $*$
- BI has proof systems:
  - cut-free bunched sequent calculus (Pym)
  - resource tableaux (Galmiche, Mery, Pym)
  - inverse method (Donnelly, Gibson et al.)

What is Boolean BI logic ?

- No unequivocal logical definition:
  - no cut-free proof system (BI $+ \neg\neg A \rightarrow A$)
  - no nice semantics for this system (relational)
- No unequivocal semantic definition:
  - various Kripke models
  - often no associated proof-systems
  - besides model checking
  - notable exception of Pointer Logic PL
  - finite model property? decidability?

What about Boolean **BI** logic ?

- Long term goals: CL $\oplus$ MILL
  - classical additives ($\wedge$, $\vee$, $\rightarrow$)
  - orthogonally to intuitionistic multiplicatives ($*$, $-\!\!*$)
  - cut-free sequent calculus and tableaux systems
  - abstract model (partial monoids), no aggregation ?
  - a corresponding Kripke semantics:

$$a \circ b \sim m$$

Some of our results (i)

- Intuitionistic: BI
  - soundness/completeness wrt partially ordered partial monoids
  - tableaux calculi with label constraints
  - decidability and finite model property
- Classical: Pointer Logic (PL)
  - soundness/completeness wrt partial monoid of heaps
  - decidability and finite model property through tableaux calculus

Some of our results (ii)

- Classical: BBI
  - soundness/completeness wrt ND (non deterministic) monoids
  - S4 faithfully embedded into BBI
  - IL faithfully embedded into BBI
  - at least P-SPACE
- Open problems for BBI:
  - decidability, finite model property
  - (deterministic) monoidal completeness

Kripke semantics for Separation logics (i)

$m \Vdash \bot$ iff never $\qquad m \Vdash A \vee B$ iff $m \Vdash A$ or $m \Vdash B$

$m \Vdash \top$ iff always $\qquad m \Vdash A \wedge B$ iff $m \Vdash A$ and $m \Vdash B$

$m \Vdash A * B$ iff $\exists a, b$ s.t. $a, b \triangleright m$ and $a \Vdash A$ and $b \Vdash B$

$m \Vdash A \mathrel{-\!\!*} B$ iff $\forall a, b\ (m, a \triangleright b$ and $a \Vdash A)$ implies $b \Vdash B$

- Intuitionistic (Reynolds or BI):
  - $m \Vdash \mathsf{I}$ iff $\mathsf{e} \leqslant m$
  - $m \Vdash A \to B$ iff $\forall m' \geqslant m,\ m' \nVdash A$ or $m' \Vdash B$
- Classical (PL or BBI):
  - $m \Vdash \mathsf{I}$ iff $m = \mathsf{e}$
  - $m \Vdash A \to B$ iff $m \nVdash A$ or $m \Vdash B$

Kripke semantics for Separation logics (ii)

- Intuitionistic (Reynolds or BI):
  - $\forall m' \geqslant m,\ m' \nVdash A$ or $m' \Vdash B$
  - a (pre-)order $\leqslant$ between resources
  - compatible with composition: $\quad \mathrm{e}, a \rhd b \quad$ iff $\quad a \leqslant b$
- Classical (PL or BBI):
  - (pre-)order needs to be flat because of $\neg\neg A \sim A$
  - several models for composition/decomposition $a, b \rhd m$
  - partial monoids: $\quad a, b \rhd m \quad$ iff $\quad a \circ b \sim m$

Partially ordered partial monoids for BI

- A structure $(\mathcal{M}, \circ, \mathrm{e}, \leqslant)$ where $\circ : \mathcal{M} \times \mathcal{M} \rightharpoonup \mathcal{M}$

  1. $\forall a \in \mathcal{M}, \mathrm{e} \circ a \sim a$ (identity)
  2. $\forall a, b \in \mathcal{M}, a \circ b \sim b \circ a$ (commutativity)
  3. $\forall a, b, c \in \mathcal{M}, a \circ (b \circ c) \sim (a \circ b) \circ c$ (associativity)
  4. $\forall x, a, b \in \mathcal{M}, a \leqslant b$ implies $x \circ a \leqslant x \circ b$ (monotonicity)

- Relations vs composition: $\boxed{a, b \triangleright m \text{ is } a \circ b \leqslant m}$
- Partiality (incompatibility) when $a \circ b$ is not defined
- But partiality should be compatible with the axioms

Partial Monoids of Heaps for **PL**

- Heap: finite partial function $Location \rightharpoonup_{fin} Value \times Value$
- Composition $\circ = \uplus$, disjoint union of partial functions
- A structure $(\mathcal{M}, \circ, \mathrm{e})$ where $\circ : \mathcal{M} \times \mathcal{M} \rightharpoonup \mathcal{M}$

  1. $\forall a \in \mathcal{M}, \mathrm{e} \circ a = a$ (identity)
  2. $\forall a, b \in \mathcal{M}, a \circ b = b \circ a$ (commutativity)
  3. $\forall a, b, c \in \mathcal{M}, a \circ (b \circ c) = (a \circ b) \circ c$ (associativity)
  4. $\forall a, b \in \mathcal{M}, a \circ b = \mathrm{e}$ implies $a = b = \mathrm{e}$ (aggregation)

- Relation vs composition: $\boxed{a, b \triangleright m \text{ is } a \circ b = m}$
- Partiality: $a \circ b$ defined iff a and b have disjoint domains

Non deterministic monoids for BBI

- Powerset extension of $\circ$: $X \circ Y = \bigcup\{x \circ y \mid x \in X, y \in Y\}$
- A structure $(\mathcal{M}, \circ, \mathrm{e})$ where $\circ : \mathcal{M} \times \mathcal{M} \longrightarrow \mathcal{P}(\mathcal{M})$

  1. $\forall a \in \mathcal{M}, \mathrm{e} \circ a = \{a\}$ (identity)
  2. $\forall a, b \in \mathcal{M}, a \circ b = b \circ a$ (commutativity)
  3. $\forall a, b, c \in \mathcal{M}, a \circ (b \circ c) = (a \circ b) \circ c$ (associativity)

- Relations vs composition: $\boxed{a, b \triangleright m \text{ is } m \in a \circ b}$
- Non determinism: $a \circ b = \{m_1, m_2\}$ then $a, b \triangleright m_1$ and $a, b \triangleright m_2$
- Partiality (incompatibility) when $a \circ b = \emptyset$

A Hilbert calculus for BI/BBI

- Axioms for additives: $\ldots A \rightarrow (B \rightarrow A), \boxed{\neg\neg A \rightarrow A} \ldots$

- Linear axioms

  1. $A \rightarrow (\mathsf{I} * A)$
  2. $(\mathsf{I} * A) \rightarrow A$
  3. $(A * B) \rightarrow (B * A)$
  4. $(A * (B * C)) \rightarrow ((A * B) * C)$

- Logical rules

$$\frac{\vdash A \qquad \vdash A \rightarrow B}{\vdash B}\,[\mathrm{MP}] \qquad \frac{\vdash A \rightarrow C \qquad \vdash B \rightarrow D}{\vdash (A * B) \rightarrow (C * D)}\,[*]$$

$$\frac{\vdash A \rightarrow (B \mathrel{-\!\!*} C)}{\vdash (A * B) \rightarrow C}\,[\mathrel{-\!\!*}_1] \qquad \frac{\vdash (A * B) \rightarrow C}{\vdash A \rightarrow (B \mathrel{-\!\!*} C)}\,[\mathrel{-\!\!*}_2]$$

Soundness and completeness for **BI/BBI**

- Soundness is simple:
  - the axioms are valid
  - the four rules are sound
- For completeness:
  - Lindenbaum algebra: formulae up to equivalence
  - prime filters define a partially ordered or ND monoid
  - $F_p \bullet G_p = \uparrow\{a * b \mid a \in A \text{ and } b \in B\}$ not prime
  - relation (BBI): $H_p \in F_p \circ G_p$ iff $F_p \bullet G_p \subseteq H_p$
  - for BI, $\uparrow \mathsf{I}$ is a prime filter (cut elimination) thus the unit
  - for BBI, units (s.t. $\mathsf{I} \in I_p$) are not unique

Finite model property (i)

- Tableaux systems with label constraints
- Countermodel construction (open branch)
- For IL:
  - $a \circ a = a$ (contraction)
  - same symbol need not occur twice in a label
- For PL:
  - $a \circ a = \perp$ (disjointness)
  - same symbol must not occur twice in a label

$\Longrightarrow$ finite number of labels in an open branch

$\Longrightarrow$ completeness for finite monoids of labels

Finite model property (ii)

- For BI:
  - $a \circ a \neq a$ in general
  - but we can add $a^n = a$ for some n (redundancy)

$\Longrightarrow$ finite number of labels under redundancy

$\Longrightarrow$ completeness for finite partially ordered monoids of labels

- For BBI:
  - $a \circ b \sim \mathrm{e}$ then a and b are invertible
  - $a^2, a^3, \ldots, a^n, \ldots$ should be defined

$\Longrightarrow$ not a finite number of labels, quotient ?

$\Longrightarrow$ finite model property ?

Embedding of **S4** into **BBI**

- A modality: $\Box A \equiv \top \mathrel{-\!\!*} A$
- S4 axioms are valid:

$$\Box A \to A \qquad \Box A \to \Box\Box A \qquad \Box(A \to B) \to (\Box A \to \Box B)$$

- S4 rule is sound: $\vdash A$ then $\vdash \Box A$
- Embedding (for $\otimes \in \{\wedge, \vee, \to\}$, $X \in \mathsf{Var} \cup \{\bot, \top\}$):

$$\begin{aligned} (\neg A)^{\Box} &= \neg A^{\Box} & X^{\Box} &= X \\ (\Box A)^{\Box} &= \top \mathrel{-\!\!*} A^{\Box} & (A \otimes B)^{\Box} &= A^{\Box} \otimes B^{\Box} \end{aligned}$$

- Soundness: if $A \in$ S4 then $A^{\Box} \in$ BBI

Faithful embedding

- (Infinite) trees complete for S4
  - trees: $(\mathcal{T}, \leqslant, r)$
  - $\exists k(a \leqslant k$ and $b \leqslant k)$ then $(a \leqslant b$ or $b \leqslant a)$
  - $a, b \triangleright m$ iff $m = \max\{a, b\}$
  - $(\mathcal{T}, \triangleright, r)$ D (partial) monoid
  - Kripke semantics preserved
- If $(\mathcal{T}, \leqslant, r)$ counter-model of $A \in$ S4

  Then $(\mathcal{T}, \triangleright, r)$ counter-model of $A^{\Box} \in$ BBI
- Corollary: IL faithfully embedded in BBI

Conclusion and perspectives

- Monoidal models for BI and PL
  - soundness/completeness wrt label monoids
  - finite model property for BI and PL
  - tableaux calculi for BI and PL
- Towards a (deterministic) monoidal semantics for BBI
  - soundness/completeness wrt ND monoids for BBI
  - embedding of S4 and at least P-SPACE hardness
  - FMP: problem to avoid redundancy and non determinism
  - decidability still open