The Logic of Separation Logic: Models and Proofs[1]

Frank de Boer (LIACS & CWI)
Hans Dieter Hiep (LIACS) Stijn de Gouw (OU)

[1] Automated Reasoning with Analytic Tableaux and Related Methods (TABLEAUX 2023)

Finite heaps

Finite model theory =
non-compactness =
no finitary sound and complete logic

Finite heaps

Finite model theory =
non-compactness =
no finitary sound and complete logic

But, oh sorry ...

For me, the finiteness of the heap is one of the fundamental decisions about separation logic. Of course, it is very natural to try to see what happens if some assumption is weakened or removed. Sometimes one finds something very interesting, sometimes less so.

Semantics Separation Logic

We have the following main cases ($M = (D, I)$ denotes a first-order model).

- $M, h, s \models (t \hookrightarrow t')$ if and only if $\langle I_s(t), I_s(t') \rangle \in h$.
- $M, h, s \models (p * q)$ if and only if $M, h_1, s \models p$ and $M, h_2, s \models q$, for some heaps $h_1, h_2 \subseteq D \times D$ such that $h = h_1 \cup h_2$ and $h_1 \perp h_2$.
- $M, h, s \models (p \mathrel{-\!\!*} q)$ if and only if $M, h', s \models p$ implies $M, h \cup h', s \models q$, for all heaps $h' \subseteq D \times D$ such that $h \perp h'$.

Semantics Separation Logic

We have the following main cases ($M = (D, I)$ denotes a first-order model).

- $M, h, s \models (t \hookrightarrow t')$ if and only if $\langle I_s(t), I_s(t') \rangle \in h$.
- $M, h, s \models (p * q)$ if and only if $M, h_1, s \models p$ and $M, h_2, s \models q$, for some heaps $h_1, h_2 \subseteq D \times D$ such that $h = h_1 \cup h_2$ and $h_1 \perp h_2$.
- $M, h, s \models (p \mathrel{-\!\!*} q)$ if and only if $M, h', s \models p$ implies $M, h \cup h', s \models q$, for all heaps $h' \subseteq D \times D$ such that $h \perp h'$.

*... you also make use of the affine version of the points-to predicate ($p \mapsto v$ * true). ... You need to be a lot more precise about what it does. At any rate, this is sometimes called "a poor man's garbage collector" as $p \mapsto v$ * $q \mapsto w$ * true $\vdash p \mapsto v$ * true and by using it you have moved into an affine logic where it's possible to forget resources.*

Semantics Separation Logic

We have the following main cases ($M = (D, I)$ denotes a first-order model).

- $M, h, s \models (t \hookrightarrow t')$ if and only if $\langle I_s(t), I_s(t') \rangle \in h$.
- $M, h, s \models (p * q)$ if and only if $M, h_1, s \models p$ and $M, h_2, s \models q$, for some heaps $h_1, h_2 \subseteq D \times D$ such that $h = h_1 \cup h_2$ and $h_1 \perp h_2$.
- $M, h, s \models (p \mathrel{-\!\!*} q)$ if and only if $M, h', s \models p$ implies $M, h \cup h', s \models q$, for all heaps $h' \subseteq D \times D$ such that $h \perp h'$.

*... you also make use of the affine version of the points-to predicate ($p \mapsto v$ * true). ... You need to be a lot more precise about what it does. At any rate, this is sometimes called "a poor man's garbage collector" as $p \mapsto v$ * $q \mapsto w$ * true $\vdash p \mapsto v$ * true and by using it you have moved into an affine logic where it's possible to forget resources.*

Non-compactness

$\exists x_1, \ldots, x_n((x_1 \hookrightarrow -) * \ldots * (x_n \hookrightarrow -))$

General Model theory: Finiteness and Countability

- expressibility finiteness of first-order models
- existence of both countably infinite and uncountable first-order models

The Transcendental Magic Wand (or the Baron von Münchhausen effect)

Let $\Box p$ abbreviate

$$\mathbf{true} * (\mathbf{emp} \wedge (\mathbf{true} \mathrel{-\!\!*} p))$$

We have
$M, h, s \models \Box p$ if and only if
$M, h', s \models p$, for *every* $h' \subseteq D \times D$.

The Transcendental Magic Wand (or the Baron von Münchhausen effect)

Let $\Box p$ abbreviate

$$\mathbf{true} * (\mathbf{emp} \wedge (\mathbf{true} \mathrel{-\!\!*} p))$$

We have
$M, h, s \models \Box p$ if and only if
$M, h', s \models p$, for *every* $h' \subseteq D \times D$.

The box modality effectively universally quantifies over all $R' \subseteq D \times D$. So it is a bit strange that we want to write $M, R, s \models \Box\ p$. The R to the left of $\models$ is clearly superfluous (I'd even say misleading), since $\Box p$ doesn't care about a specific interpretation of R at all.

The Transcendental Magic Wand (or the Baron von Münchhausen effect)

Let $\Box p$ abbreviate

$$\mathbf{true} * (\mathbf{emp} \wedge (\mathbf{true} \mathrel{-\!\!*} p))$$

We have
$M, h, s \models \Box p$ if and only if
$M, h', s \models p$, for *every* $h' \subseteq D \times D$.

The box modality effectively universally quantifies over all $R' \subseteq D \times D$. So it is a bit strange that we want to write $M, R, s \models \Box\ p$. The R to the left of $\models$ is clearly superfluous (I'd even say misleading), since $\Box p$ doesn't care about a specific interpretation of R at all.

So why introduce the box modality at all and then use it in a way that refers to a superfluous interpretation of R? Why not just say $M, \emptyset, s \models (true \mathrel{-\!\!*} p)$?

Finiteness

Total, injective heap

- $\forall x \exists y (x \hookrightarrow y)$
- $\forall x, y, z ((x \hookrightarrow z \wedge y \hookrightarrow z) \rightarrow x = y)$

Every total, injective heap is a surjection

$M, h, s \models \Box(inj \rightarrow \forall x \exists y (y \hookrightarrow x))$

Well-foundedness

Let $\blacksquare p$ abbreviate

$$\neg(\mathbf{true} * \neg p)$$

We have
$M, h, s \models \blacksquare p$ if and only if
$M, h', s \models p$, for *every* sub-heap h' of h.

Every non-empty sub-heap has a minimal element

$\blacksquare(\mathbf{emp} \vee \exists x((x \hookrightarrow -) \wedge \forall y((y \hookrightarrow -) \rightarrow (y \not\mapsto x))))$

Consequently, SL without $-\!\!*$ is already non-compact ($x_{n+1} \hookrightarrow x_n$, $n \in \mathbb{N}$)

Countable first-order models

Heap enumeration

- total and injective
- unique minimal element: $\exists! x \forall y (y \not\hookrightarrow x)$
- well-founded

Countability

$$\Diamond \mathrm{enum}$$

Uncountable models

$$\neg(\Diamond \mathit{enum} \vee \mathit{fin})$$

Separation Logic vs Second-Order Logic

Binding operator $\downarrow R(p)$

$M, \mathcal{R}, s \models \downarrow R(p)$ if and only if $M, \mathcal{R}, s[R := \mathcal{R}] \models p$

Translation second-order dyadic logic

$T(\exists R(\phi)) = \Diamond(\downarrow R(T(\phi)))$

Weak SL = weak second-order logic

Stéphane Demri and Morgan Deters. Expressive completeness of separation logic with two variables and no separating conjunction. ACM Trans. Comput. Log., 17(2):12, 2016.

Some Open Problems

- finiteness heaps
- general expressiveness SL

Some Open Problems

- finiteness heaps
- general expressiveness SL

But, oh sorry (again) ...

> *the author(s) present several problems claimed to be open (I'm not claiming I have solutions to these). Are these to be considered as contributions? I would strongly vote against this.*

Some Open Problems

- finiteness heaps
- general expressiveness SL

But, oh sorry (again) ...

the author(s) present several problems claimed to be open (I'm not claiming I have solutions to these). Are these to be considered as contributions? I would strongly vote against this.

The examples used in the non-compactness arguments are fairly standard and straightforward.

Some Open Problems

- finiteness heaps
- general expressiveness SL

But, oh sorry (again) ...

the author(s) present several problems claimed to be open (I'm not claiming I have solutions to these). Are these to be considered as contributions? I would strongly vote against this.

The examples used in the non-compactness arguments are fairly standard and straightforward.

Further, the authors have strongly rebutted that compactness of consequence relation holds for FOL. Let us consider the same kind counterexample they have provided for their variant of SL in the paper.

Proof Theory: The Binding Operator $p@q$

$M, \mathcal{R}, s \models p@q(x, y)$ if and only if $M, \mathcal{R}', s \models p$
where
$\mathcal{R}' = \{(d, d') \mid M, \mathcal{R}, s[x, y := d, d'] \models q\}$

Axioms

- $p = p@(x \hookrightarrow y)$
- $(e \hookrightarrow e')@r = r(e, e')$
- $(p \circ q)@r = p@r \circ q@r$
- $(\neg p)@r = \neg(p@r)$
- $(\forall x p)@r = \forall x(p@r)$
- $p@(q@r) = (p@q)@r$

Sequent calculus

Separating conjunction

$$\mathbf{L}_* \quad \frac{\Gamma, r = R_1 \uplus R_2, p@R_1, q@R_2 \Rightarrow \Delta}{\Gamma, (p * q)@r \Rightarrow \Delta}$$

$$\mathbf{R}_* \quad \frac{\Gamma \Rightarrow \Delta, r = r_1 \uplus r_2 \quad \Gamma \Rightarrow \Delta, p@r_1 \quad \Gamma \Rightarrow \Delta, q@r_2}{\Gamma \Rightarrow \Delta, (p * q)@r}$$

Separating implication

$$\mathbf{L}_{-\!\!*} \quad \frac{\Gamma \Rightarrow \Delta, r \perp r' \quad \Gamma \Rightarrow \Delta, p@r' \quad \Gamma, q@(r \vee r') \Rightarrow \Delta}{\Gamma, (p -\!\!* q)@r \Rightarrow \Delta}$$

$$\mathbf{R}_{-\!\!*} \quad \frac{\Gamma, R \perp r, p@R \Rightarrow \Delta, q@(r \vee R)}{\Gamma \Rightarrow \Delta, (p -\!\!* q)@r}$$

Soundness and Completeness

General models

$M = (D, I, J)$, where $J \subseteq \mathcal{P}(D \times D)$

Comprehensive models

$\{(d, d') \mid M, \mathcal{R}, s[x, y := d, d'] \models p(x, y)\} \in J$
for every $\mathcal{R} \in J$ and $p(x, y)$

$$\Gamma \models p \Leftrightarrow \Gamma \vdash p$$

Arithmetic comprehension axiom

$$\Diamond(\forall x, y((x \hookrightarrow y) \leftrightarrow \phi(x, y)))$$

where $\phi(x, y)$ is a pure first-order formula

Related Work

- Leon Henkin. Completeness in the theory of types. The Journal of Symbolic Logic 15, 15(2), 1950.
- Zhe Hou and Alwen Tiu. Completeness for a first-order abstract separation logic. In Atsushi Igarashi, editor, Programming Languages and Systems - 14th Asian Symposium, APLAS 2016, Hanoi, Vietnam, November 21-23, 2016, Proceedings, volume 10017 of Lecture Notes in Computer Science, pages 444–463, 2016.
- Ralf Jung, Robbert Krebbers, Jacques-Henri Jourdan, Aleš Bizjak, Lars Birkedal, and Derek Dreyer. Iris from the ground up: A modular foun- dation for higher-order concurrent separation logic. Journal of Functional Programming, 28, 2018.
- David J. Pym. The semantics and proof theory of the logic of bunched implications. In Applied Logic Series, 2002.
- Sl-comp: competition of solvers for separation logic. In International Conference on Tools and Al- gorithms for the Construction and Analysis of Systems, pages 116–132.

Related Work (cont'd)

- Peter Sewell. Bad Reasons to Reject Good Papers, and vice versa by , Dec 7, 2021. https://blog.sigplan.org/2021/12/07/bad-reasons-to-reject-good-papers-and-vice-versa/.

Conclusion: The Killer Application

$$\{(u \hookrightarrow -) \wedge (z = 0 \triangleleft u = v \triangleright v \hookrightarrow z)\}$$
$$[u] := 0$$
$$\{v \hookrightarrow z\}$$

versus

$$\{(u \mapsto -) * (u \mapsto 0 \mathrel{-\!\!*} v \hookrightarrow z)\}$$
$$[u] := 0$$
$$\{v \hookrightarrow z\}$$

Odysseus: The Sirens of Abstraction