Undecidability of propositional separation logic and its neighbours

James Brotherston[1] and Max Kanovich[2]

[1]Imperial College London

[2]Queen Mary University of London

LICS-25, University of Edinburgh, 12 July 2010

Separation logic (Reynolds, O'Hearn)

- Separation logic is a formalism for reasoning about memory.

Separation logic (Reynolds, O'Hearn)

- Separation logic is a formalism for reasoning about memory.
- Separation models are cancellative partial commutative monoids $\langle H, \circ, E \rangle$ ($E \subseteq H$ is a set of units).

Separation logic (Reynolds, O'Hearn)

- Separation logic is a formalism for reasoning about memory.
- Separation models are cancellative partial commutative monoids $\langle H, \circ, E\rangle$ ($E \subseteq H$ is a set of units).
- Propositional formulas combine standard Boolean connectives with "multiplicatives" $*$, $-\!\!*$ and I.

Separation logic (Reynolds, O'Hearn)

- Separation logic is a formalism for reasoning about memory.
- Separation models are cancellative partial commutative monoids $\langle H, \circ, E \rangle$ ($E \subseteq H$ is a set of units).
- Propositional formulas combine standard Boolean connectives with "multiplicatives" $*$, $-\!*$ and I.
- Separating conjunction $F * G$ defined by:

$$h \models_\rho F_1 * F_2 \quad \Leftrightarrow \quad h = h_1 \circ h_2 \text{ and } h_1 \models_\rho F_1 \text{ and } h_2 \models_\rho F_2$$

Separation logic (Reynolds, O'Hearn)

- Separation logic is a formalism for reasoning about memory.
- Separation models are cancellative partial commutative monoids $\langle H, \circ, E \rangle$ ($E \subseteq H$ is a set of units).
- Propositional formulas combine standard Boolean connectives with "multiplicatives" $*$, $-\!\!*$ and I.
- Separating conjunction $F * G$ defined by:

$$h \models_\rho F_1 * F_2 \;\;\Leftrightarrow\;\; h = h_1 \circ h_2 \text{ and } h_1 \models_\rho F_1 \text{ and } h_2 \models_\rho F_2$$

- Archetypal heap models are $\langle H, \circ, \{e\} \rangle$, where $H = L \rightharpoonup_{\mathrm{fin}} RV$ is a set of *heaps*, e is the empty heap, and $\circ$ is (partial) union of disjoint heaps.
  (Variations: stacks-and-heaps, heaps with permissions)

Validity: concrete models vs. classes of models

- F is valid in $\langle H, \circ, E \rangle$ if $h \models_\rho F$ for all $h \in H$ and for all valuations ρ of propositional variables.

Validity: concrete models vs. classes of models

- F is valid in $\langle H, \circ, E \rangle$ if $h \models_\rho F$ for all $h \in H$ and for all valuations ρ of propositional variables.
- Applications of separation logic are typically based on a fixed, heap-like model.

Validity: concrete models vs. classes of models

- F is valid in $\langle H, \circ, E \rangle$ if $h \models_\rho F$ for all $h \in H$ and for all valuations ρ of propositional variables.
- Applications of separation logic are typically based on a fixed, heap-like model.
- Validity in such a model is a subtler problem than validity in classes of models:

Validity: concrete models vs. classes of models

- F is valid in $\langle H, \circ, E \rangle$ if $h \models_\rho F$ for all $h \in H$ and for all valuations ρ of propositional variables.
- Applications of separation logic are typically based on a fixed, heap-like model.
- Validity in such a model is a subtler problem than validity in classes of models:
  - Normally, to show a property Q given that F is valid in a *class* of models $\mathcal{C}$, one chooses some model $M \in \mathcal{C}$ such that (F valid in M) $\rightarrow Q$;

Validity: concrete models vs. classes of models

- F is valid in $\langle H, \circ, E \rangle$ if $h \models_\rho F$ for all $h \in H$ and for all valuations ρ of propositional variables.
- Applications of separation logic are typically based on a fixed, heap-like model.
- Validity in such a model is a subtler problem than validity in classes of models:
  - Normally, to show a property Q given that F is valid in a *class* of models $\mathcal{C}$, one chooses some model $M \in \mathcal{C}$ such that $(F \text{ valid in } M) \rightarrow Q$;
  - but, when M is given *in advance*, we have no such freedom!

Axiomatisations of separation logic

- BI, which is intuitionistic logic plus the MILL axioms and rules for I, $*$ and $-\!\!*$;

Axiomatisations of separation logic

- BI, which is intuitionistic logic plus the MILL axioms and rules for I, $*$ and $-\!*$;
- BBI, which is BI plus $\neg\neg A \vdash A$;

Axiomatisations of separation logic

- BI, which is intuitionistic logic plus the MILL axioms and rules for I, $*$ and $-\!\!*$;
- BBI, which is BI plus $\neg\neg A \vdash A$;
- BBI+eW where eW is $\mathrm{I} \wedge (A * B) \vdash \mathrm{I} \wedge A$, which says "*you can't split the empty heap into two non-empty heaps*";

Axiomatisations of separation logic

- BI, which is intuitionistic logic plus the MILL axioms and rules for I, $*$ and $-\!\!*$;
- BBI, which is BI plus $\neg\neg A \vdash A$;
- BBI+eW where eW is $\mathrm{I} \wedge (A * B) \vdash \mathrm{I} \wedge A$, which says "*you can't split the empty heap into two non-empty heaps*";
- BBI+W where W is $A * B \vdash A$. This system collapses into classical logic!

Axiomatisations of separation logic

- BI, which is intuitionistic logic plus the MILL axioms and rules for I, $*$ and $-\!*$;
- BBI, which is BI plus $\neg\neg A \vdash A$;
- BBI+eW where eW is $\mathrm{I} \wedge (A * B) \vdash \mathrm{I} \wedge A$, which says "*you can't split the empty heap into two non-empty heaps*";
- BBI+W where W is $A * B \vdash A$. This system collapses into classical logic!

NB.

1. BI $\subset$ BBI $\subset$ BBI+eW $\subset$ BBI+W, and both BI, BBI+W are decidable;

Axiomatisations of separation logic

- BI, which is intuitionistic logic plus the MILL axioms and rules for I, $*$ and $-\!*$;
- BBI, which is BI plus $\neg\neg A \vdash A$;
- BBI+eW where eW is $\mathrm{I} \wedge (A * B) \vdash \mathrm{I} \wedge A$, which says "*you can't split the empty heap into two non-empty heaps*";
- BBI+W where W is $A * B \vdash A$. This system collapses into classical logic!

NB.

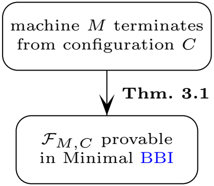
1. BI $\subset$ BBI $\subset$ BBI+eW $\subset$ BBI+W, and both BI, BBI+W are decidable;
2. BBI, BBI+eW are (obviously) incomplete wrt. validity in particular concrete models.

Undecidability

$\boxed{\text{machine } M \text{ terminates from configuration } C}$

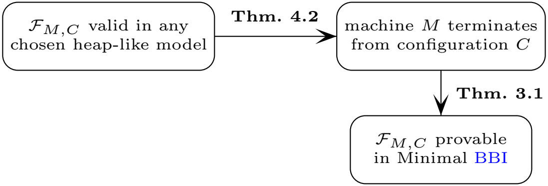
(M is a non-deterministic, 2-counter Minsky machine.)

Undecidability



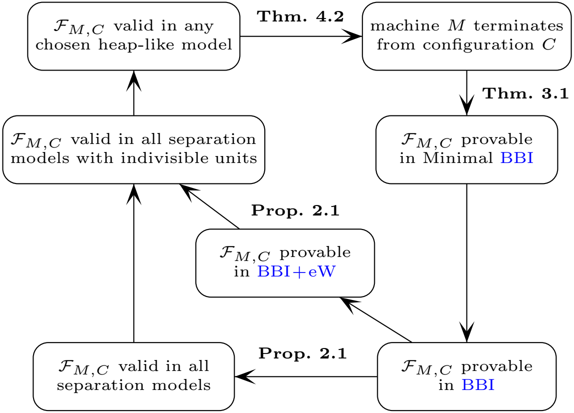
(M is a non-deterministic, 2-counter Minsky machine.)

Undecidability



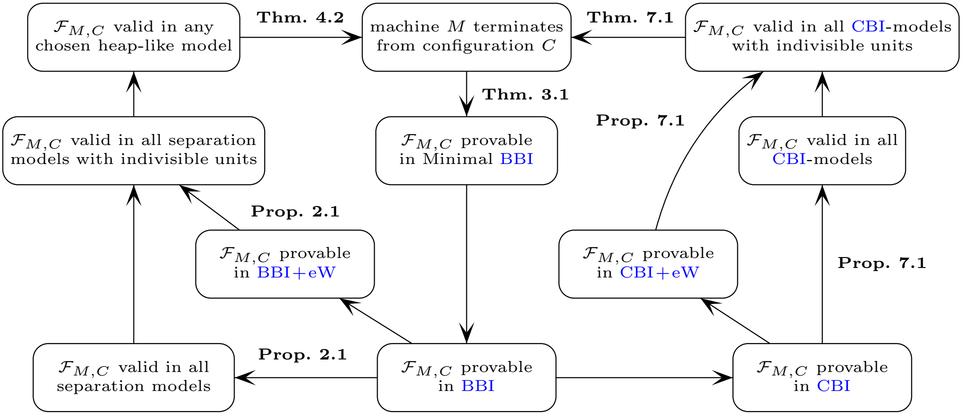
(M is a non-deterministic, 2-counter Minsky machine.)

Undecidability



(M is a non-deterministic, 2-counter Minsky machine.)

Undecidability



(M is a non-deterministic, 2-counter Minsky machine.)

Finite valuations

Undecidability is intimately related to infinite valuations of the propositional variables (as sets of model elements):

Theorem

There is a sequent $\mathcal{F}_{\mathcal{M},\mathcal{C}}$ such that, for any heap-like model M:

- *$\mathcal{F}_{\mathcal{M},\mathcal{C}}$ is not valid in M, but;*
- *$\mathcal{F}_{\mathcal{M},\mathcal{C}}$ is valid in M under every finite valuation!*

Finite valuations

Undecidability is intimately related to infinite valuations of the propositional variables (as sets of model elements):

Theorem
There is a sequent $\mathcal{F}_{\mathcal{M},\mathcal{C}}$ such that, for any heap-like model M:

- *$\mathcal{F}_{\mathcal{M},\mathcal{C}}$ is not valid in M, but;*
- *$\mathcal{F}_{\mathcal{M},\mathcal{C}}$ is valid in M under every finite valuation!*

So, to obtain decidable fragments of separation logic, one could:

1. give up infinite valuations (Calcagno et al., FSTTCS'01);

Finite valuations

Undecidability is intimately related to infinite valuations of the propositional variables (as sets of model elements):

Theorem
There is a sequent $\mathcal{F}_{\mathcal{M},\mathcal{C}}$ such that, for any heap-like model M:

- *$\mathcal{F}_{\mathcal{M},\mathcal{C}}$ is not valid in M, but;*
- *$\mathcal{F}_{\mathcal{M},\mathcal{C}}$ is valid in M under every finite valuation!*

So, to obtain decidable fragments of separation logic, one could:

1. give up infinite valuations (Calcagno et al., FSTTCS'01);
2. restrict the formula language (Berdine et al., FSTTCS'04).

Summary

For the purely propositional fragment of separation logic, we have the following new results:

Summary

For the purely propositional fragment of separation logic, we have the following new results:

- validity in any given heap-like model is undecidable;

Summary

For the purely propositional fragment of separation logic, we have the following new results:

- validity in any given heap-like model is undecidable;
- validity in such a model cannot be approximated by finite valuations for propositional variables (which imposes restrictions on decidable fragments);

Summary

For the purely propositional fragment of separation logic, we have the following new results:

- validity in any given heap-like model is undecidable;
- validity in such a model cannot be approximated by finite valuations for propositional variables (which imposes restrictions on decidable fragments);
- validity in various classes of models is undecidable;

Summary

For the purely propositional fragment of separation logic, we have the following new results:

- validity in any given heap-like model is undecidable;
- validity in such a model cannot be approximated by finite valuations for propositional variables (which imposes restrictions on decidable fragments);
- validity in various classes of models is undecidable;
- and provability in various axiomatisations (BBI, BBI+eW, CBI, CBI+eW,…) is undecidable too.

Separation logic vs. linear logic

Separation logic obeys two principles which are highly unorthodox from the perspective of linear logic:

1. The usual distributivity law

$$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$$

2. The exact equality

$$[\![A * B]\!] = [\![A]\!] \cdot [\![B]\!]$$

(In linear logic we typically have $[\![A * B]\!] \not\subseteq [\![A]\!] \cdot [\![B]\!]$.)

These two facts are entirely responsible for the undecidability of separation logic!