Parametric completeness for separation theories (via hybrid logic)

James Brotherston

University College London

New York University, 11 December 2014

Joint work with Jules Villard

Part I

Introduction, motivation and background

Introduction

- In mathematical logic, there is usually a trade-off between expressivity and complexity of a logical language:

Introduction

- In mathematical logic, there is usually a trade-off between expressivity and complexity of a logical language:
  - weaker languages cannot capture interesting properties, but

Introduction

- In mathematical logic, there is usually a trade-off between expressivity and complexity of a logical language:
    - weaker languages cannot capture interesting properties, but
    - richer languages have higher complexity, may lack sensible proof theories and may be unavoidably incomplete (cf. Gödel).

Introduction

- In mathematical logic, there is usually a trade-off between expressivity and complexity of a logical language:
  - weaker languages cannot capture interesting properties, but
  - richer languages have higher complexity, may lack sensible proof theories and may be unavoidably incomplete (cf. Gödel).
- Incompleteness manifests as a gap between two key concepts:

Introduction

- In mathematical logic, there is usually a trade-off between expressivity and complexity of a logical language:
  - weaker languages cannot capture interesting properties, but
  - richer languages have higher complexity, may lack sensible proof theories and may be unavoidably incomplete (cf. Gödel).
- Incompleteness manifests as a gap between two key concepts:
  - provability in some formal system for the logic (which corresponds to validity in some class of models); and

Introduction

- In mathematical logic, there is usually a trade-off between expressivity and complexity of a logical language:
  - weaker languages cannot capture interesting properties, but
  - richer languages have higher complexity, may lack sensible proof theories and may be unavoidably incomplete (cf. Gödel).
- Incompleteness manifests as a gap between two key concepts:
  - provability in some formal system for the logic (which corresponds to validity in some class of models); and
  - validity in a (class of) intended model(s) of the logic.

Introduction (contd.)

- Thus, given a logical language $\mathcal{L}$, and an intended class $\mathcal{C}$ of models for that language, there are two natural questions:

Introduction (contd.)

- Thus, given a logical language $\mathcal{L}$, and an intended class $\mathcal{C}$ of models for that language, there are two natural questions:
  1. Is the class $\mathcal{C}$ finitely axiomatisable, a.k.a. definable in $\mathcal{L}$?

Introduction (contd.)

- Thus, given a logical language $\mathcal{L}$, and an intended class $\mathcal{C}$ of models for that language, there are two natural questions:
  1. Is the class $\mathcal{C}$ finitely axiomatisable, a.k.a. definable in $\mathcal{L}$?
  2. Is there a complete proof system for $\mathcal{L}$ w.r.t. validity in $\mathcal{C}$?

Introduction (contd.)

- Thus, given a logical language $\mathcal{L}$, and an intended class $\mathcal{C}$ of models for that language, there are two natural questions:
  1. Is the class $\mathcal{C}$ finitely axiomatisable, a.k.a. definable in $\mathcal{L}$?
  2. Is there a complete proof system for $\mathcal{L}$ w.r.t. validity in $\mathcal{C}$?

  (Note that these questions are not connected, in general.)

Introduction (contd.)

- Thus, given a logical language $\mathcal{L}$, and an intended class $\mathcal{C}$ of models for that language, there are two natural questions:
  1. Is the class $\mathcal{C}$ finitely axiomatisable, a.k.a. definable in $\mathcal{L}$?
  2. Is there a complete proof system for $\mathcal{L}$ w.r.t. validity in $\mathcal{C}$?

  (Note that these questions are not connected, in general.)
- Here, we examine these questions in the context of pure separation logic, where

Introduction (contd.)

- Thus, given a logical language $\mathcal{L}$, and an intended class $\mathcal{C}$ of models for that language, there are two natural questions:
  1. Is the class $\mathcal{C}$ finitely axiomatisable, a.k.a. definable in $\mathcal{L}$?
  2. Is there a complete proof system for $\mathcal{L}$ w.r.t. validity in $\mathcal{C}$?

  (Note that these questions are not connected, in general.)
- Here, we examine these questions in the context of pure separation logic, where
  - the language is given by the logic Boolean BI (BBI);

Introduction (contd.)

- Thus, given a logical language $\mathcal{L}$, and an intended class $\mathcal{C}$ of models for that language, there are two natural questions:
  1. Is the class $\mathcal{C}$ finitely axiomatisable, a.k.a. definable in $\mathcal{L}$?
  2. Is there a complete proof system for $\mathcal{L}$ w.r.t. validity in $\mathcal{C}$?

  (Note that these questions are not connected, in general.)

- Here, we examine these questions in the context of pure separation logic, where
  - the language is given by the logic Boolean BI (BBI);
  - the intended models are given by separation theories, which specify a collection of useful model properties.

Outline

The rest of the talk goes as follows:

1. First, we recall the standard presentation of BBI.

Outline

The rest of the talk goes as follows:

1. First, we recall the standard presentation of BBI.
2. We introduce separation theories, which describe practically interesting classes of models, and show that many such theories are not definable in BBI.

Outline

The rest of the talk goes as follows:

1. First, we recall the standard presentation of BBI.
2. We introduce separation theories, which describe practically interesting classes of models, and show that many such theories are not definable in BBI.
3. We then propose an extension of BBI based on hybrid logic, which adds a theory of naming to BBI, and show that these properties become definable to this extension.

Outline

The rest of the talk goes as follows:

1. First, we recall the standard presentation of BBI.
2. We introduce separation theories, which describe practically interesting classes of models, and show that many such theories are not definable in BBI.
3. We then propose an extension of BBI based on hybrid logic, which adds a theory of naming to BBI, and show that these properties become definable to this extension.
4. We give proof systems for our hybrid logic that is parametrically complete w.r.t. the axioms defining separation theories.

Part II

Boolean BI

BBI: *language and provability*

- BBI extends standard classical logic with "multiplicative" connectives $*$, $-\!*$ and I.

BBI: *language and provability*

- BBI extends standard classical logic with "multiplicative" connectives $*$, $-\!*$ and I.
- Provability for the multiplicatives is given by

BBI: *language and provability*

- BBI extends standard classical logic with "multiplicative" connectives $*$, $\mathrel{-\!\!*}$ and I.
- Provability for the multiplicatives is given by

$$A * B \vdash B * A \qquad A * (B * C) \vdash (A * B) * C$$

$$A \vdash A * \mathrm{I} \qquad A * \mathrm{I} \vdash A$$

$$\frac{A_1 \vdash B_1 \quad A_2 \vdash B_2}{A_1 * A_2 \vdash B_1 * B_2} \qquad \frac{A * B \vdash C}{A \vdash B \mathrel{-\!\!*} C} \qquad \frac{A \vdash B \mathrel{-\!\!*} C}{A * B \vdash C}$$

BBI-*models*

A BBI-model is a relational commutative monoid, i.e. a tuple $\langle W, \circ, E \rangle$, where

BBI-*models*

A BBI-model is a relational commutative monoid, i.e. a tuple $\langle W, \circ, E \rangle$, where

- $\circ : W \times W \to \mathcal{P}(W)$ is associative and commutative (we extend $\circ$ pointwise to sets), and

BBI-*models*

A BBI-model is a relational commutative monoid, i.e. a tuple $\langle W, \circ, E \rangle$, where

- $\circ : W \times W \to \mathcal{P}(W)$ is associative and commutative (we extend $\circ$ pointwise to sets), and
- $E \subseteq W$ satisfies $w \circ E = \{w\}$ for all $w \in W$ (we call E the set of units of $\circ$).

BBI-*models*

A BBI-model is a relational commutative monoid, i.e. a tuple $\langle W, \circ, E \rangle$, where

- $\circ : W \times W \to \mathcal{P}(W)$ is associative and commutative (we extend $\circ$ pointwise to sets), and
- $E \subseteq W$ satisfies $w \circ E = \{w\}$ for all $w \in W$ (we call E the set of units of $\circ$).

Typical example: heap models $\langle H, \circ, \{e\} \rangle$, where

BBI-*models*

A BBI-model is a relational commutative monoid, i.e. a tuple $\langle W, \circ, E \rangle$, where

- $\circ : W \times W \to \mathcal{P}(W)$ is associative and commutative (we extend $\circ$ pointwise to sets), and
- $E \subseteq W$ satisfies $w \circ E = \{w\}$ for all $w \in W$ (we call E the set of units of $\circ$).

Typical example: heap models $\langle H, \circ, \{e\} \rangle$, where

- H is the set of heaps, i.e. finite partial maps from locations to values,

BBI-*models*

A BBI-model is a relational commutative monoid, i.e. a tuple $\langle W, \circ, E \rangle$, where

- $\circ : W \times W \to \mathcal{P}(W)$ is associative and commutative (we extend $\circ$ pointwise to sets), and
- $E \subseteq W$ satisfies $w \circ E = \{w\}$ for all $w \in W$ (we call E the set of units of $\circ$).

Typical example: heap models $\langle H, \circ, \{e\} \rangle$, where

- H is the set of heaps, i.e. finite partial maps from locations to values,
- $\circ$ is union of domain-disjoint heaps, and

BBI-*models*

A BBI-model is a relational commutative monoid, i.e. a tuple $\langle W, \circ, E \rangle$, where

- $\circ : W \times W \to \mathcal{P}(W)$ is associative and commutative (we extend $\circ$ pointwise to sets), and
- $E \subseteq W$ satisfies $w \circ E = \{w\}$ for all $w \in W$ (we call E the set of units of $\circ$).

Typical example: heap models $\langle H, \circ, \{e\} \rangle$, where

- H is the set of heaps, i.e. finite partial maps from locations to values,
- $\circ$ is union of domain-disjoint heaps, and
- e is the empty heap that is undefined everywhere.

Semantics of BBI

Semantics of formula A wrt. BBI-model $M = \langle W, \circ, E \rangle$, valuation ρ, and $w \in W$ given by relation $M, w \models_\rho A$:

Semantics of BBI

Semantics of formula A wrt. BBI-model $M = \langle W, \circ, E \rangle$, valuation ρ, and $w \in W$ given by relation $M, w \models_\rho A$:

$$M, w \models_\rho P \quad \Leftrightarrow \quad w \in \rho(P)$$

Semantics of BBI

Semantics of formula A wrt. BBI-model $M = \langle W, \circ, E \rangle$, valuation ρ, and $w \in W$ given by relation $M, w \models_\rho A$:

$$\begin{array}{rcl} M, w \models_\rho P & \Leftrightarrow & w \in \rho(P) \\ M, w \models_\rho A_1 \wedge A_2 & \Leftrightarrow & M, w \models_\rho A_1 \text{ and } M, w \models_\rho A_2 \end{array}$$

Semantics of BBI

Semantics of formula A wrt. BBI-model $M = \langle W, \circ, E \rangle$, valuation ρ, and $w \in W$ given by relation $M, w \models_\rho A$:

$$\begin{array}{rcl} M, w \models_\rho P & \Leftrightarrow & w \in \rho(P) \\ M, w \models_\rho A_1 \wedge A_2 & \Leftrightarrow & M, w \models_\rho A_1 \text{ and } M, w \models_\rho A_2 \\ \vdots & & \\ M, w \models_\rho \mathrm{I} & \Leftrightarrow & w \in E \end{array}$$

Semantics of BBI

Semantics of formula A wrt. BBI-model $M = \langle W, \circ, E\rangle$, valuation ρ, and $w \in W$ given by relation $M, w \models_\rho A$:

$$
\begin{array}{rcl}
M, w \models_\rho P & \Leftrightarrow & w \in \rho(P) \\
M, w \models_\rho A_1 \wedge A_2 & \Leftrightarrow & M, w \models_\rho A_1 \text{ and } M, w \models_\rho A_2 \\
\vdots & & \\
M, w \models_\rho \mathrm{I} & \Leftrightarrow & w \in E \\
M, w \models_\rho A_1 * A_2 & \Leftrightarrow & w \in w_1 \circ w_2 \text{ and } M, w_1 \models_\rho A_1 \text{ and } M, w_2 \models_\rho A_2
\end{array}
$$

Semantics of BBI

Semantics of formula A wrt. BBI-model $M = \langle W, \circ, E \rangle$, valuation ρ, and $w \in W$ given by relation $M, w \models_\rho A$:

$$
\begin{array}{rcl}
M, w \models_\rho P & \Leftrightarrow & w \in \rho(P) \\
M, w \models_\rho A_1 \wedge A_2 & \Leftrightarrow & M, w \models_\rho A_1 \text{ and } M, w \models_\rho A_2 \\
\vdots & & \\
M, w \models_\rho \mathrm{I} & \Leftrightarrow & w \in E \\
M, w \models_\rho A_1 * A_2 & \Leftrightarrow & w \in w_1 \circ w_2 \text{ and } M, w_1 \models_\rho A_1 \text{ and } M, w_2 \models_\rho A_2 \\
M, w \models_\rho A_1 \mathrel{-\!\!*} A_2 & \Leftrightarrow & \forall w', w'' \in W. \text{ if } w'' \in w \circ w' \text{ and } M, w' \models_\rho A_1 \\
 & & \text{then } M, w'' \models_\rho A_2
\end{array}
$$

Semantics of BBI

Semantics of formula A wrt. BBI-model $M = \langle W, \circ, E \rangle$, valuation ρ, and $w \in W$ given by relation $M, w \models_\rho A$:

$$
\begin{array}{rcl}
M, w \models_\rho P & \Leftrightarrow & w \in \rho(P) \\
M, w \models_\rho A_1 \wedge A_2 & \Leftrightarrow & M, w \models_\rho A_1 \text{ and } M, w \models_\rho A_2 \\
& \vdots & \\
M, w \models_\rho \mathrm{I} & \Leftrightarrow & w \in E \\
M, w \models_\rho A_1 * A_2 & \Leftrightarrow & w \in w_1 \circ w_2 \text{ and } M, w_1 \models_\rho A_1 \text{ and } M, w_2 \models_\rho A_2 \\
M, w \models_\rho A_1 \mathrel{-\!\!*} A_2 & \Leftrightarrow & \forall w', w'' \in W.\ \text{if } w'' \in w \circ w' \text{ and } M, w' \models_\rho A_1 \\
& & \text{then } M, w'' \models_\rho A_2
\end{array}
$$

A is valid in M iff $M, w \models_\rho A$ for all ρ and $w \in W$.

Semantics of BBI

Semantics of formula A wrt. BBI-model $M = \langle W, \circ, E \rangle$, valuation ρ, and $w \in W$ given by relation $M, w \models_\rho A$:

$$
\begin{array}{rcl}
M, w \models_\rho P & \Leftrightarrow & w \in \rho(P) \\
M, w \models_\rho A_1 \wedge A_2 & \Leftrightarrow & M, w \models_\rho A_1 \text{ and } M, w \models_\rho A_2 \\
\vdots & & \\
M, w \models_\rho \mathrm{I} & \Leftrightarrow & w \in E \\
M, w \models_\rho A_1 * A_2 & \Leftrightarrow & w \in w_1 \circ w_2 \text{ and } M, w_1 \models_\rho A_1 \text{ and } M, w_2 \models_\rho A_2 \\
M, w \models_\rho A_1 \mathrel{-\!\!*} A_2 & \Leftrightarrow & \forall w', w'' \in W.\text{ if } w'' \in w \circ w' \text{ and } M, w' \models_\rho A_1 \\
& & \text{then } M, w'' \models_\rho A_2
\end{array}
$$

A is valid in M iff $M, w \models_\rho A$ for all ρ and $w \in W$.

Theorem (Galmiche and Larchey-Wendling 2006)

Provability in BBI *coincides with validity in* BBI*-models.*

Part III

(Un)definable properties in BBI

Separation theories

Applications of separation logic are typically based on BBI-models satisfying some collection of algebraic properties which we call a separation theory.

Separation theories

Applications of separation logic are typically based on BBI-models satisfying some collection of algebraic properties which we call a separation theory. We consider the following:

Partial functionality: $w, w' \in w_1 \circ w_2$ implies $w = w'$;

Separation theories

Applications of separation logic are typically based on BBI-models satisfying some collection of algebraic properties which we call a separation theory. We consider the following:

Partial functionality: $w, w' \in w_1 \circ w_2$ implies $w = w'$;

Cancellativity: $(w \circ w_1) \cap (w \circ w_2) \neq \emptyset$ implies $w_1 = w_2$;

Separation theories

Applications of separation logic are typically based on BBI-models satisfying some collection of algebraic properties which we call a separation theory. We consider the following:

Partial functionality: $w, w' \in w_1 \circ w_2$ implies $w = w'$;

Cancellativity: $(w \circ w_1) \cap (w \circ w_2) \neq \emptyset$ implies $w_1 = w_2$;

Single unit: $w, w' \in E$ implies $w = w'$;

Separation theories

Applications of separation logic are typically based on BBI-models satisfying some collection of algebraic properties which we call a separation theory. We consider the following:

Partial functionality: $w, w' \in w_1 \circ w_2$ implies $w = w'$;

Cancellativity: $(w \circ w_1) \cap (w \circ w_2) \neq \emptyset$ implies $w_1 = w_2$;

Single unit: $w, w' \in E$ implies $w = w'$;

Indivisible units: $(w \circ w') \cap E \neq \emptyset$ implies $w \in E$;

Separation theories

Applications of separation logic are typically based on BBI-models satisfying some collection of algebraic properties which we call a separation theory. We consider the following:

Partial functionality: $w, w' \in w_1 \circ w_2$ implies $w = w'$;

Cancellativity: $(w \circ w_1) \cap (w \circ w_2) \neq \emptyset$ implies $w_1 = w_2$;

Single unit: $w, w' \in E$ implies $w = w'$;

Indivisible units: $(w \circ w') \cap E \neq \emptyset$ implies $w \in E$;

Disjointness: $w \circ w \neq \emptyset$ implies $w \in E$;

Separation theories

Applications of separation logic are typically based on BBI-models satisfying some collection of algebraic properties which we call a separation theory. We consider the following:

Partial functionality: $w, w' \in w_1 \circ w_2$ implies $w = w'$;

Cancellativity: $(w \circ w_1) \cap (w \circ w_2) \neq \emptyset$ implies $w_1 = w_2$;

Single unit: $w, w' \in E$ implies $w = w'$;

Indivisible units: $(w \circ w') \cap E \neq \emptyset$ implies $w \in E$;

Disjointness: $w \circ w \neq \emptyset$ implies $w \in E$;

Divisibility: for every $w \notin E$ there are $w_1, w_2 \notin E$ such that $w \in w_1 \circ w_2$;

Separation theories

Applications of separation logic are typically based on BBI-models satisfying some collection of algebraic properties which we call a separation theory. We consider the following:

Partial functionality: $w, w' \in w_1 \circ w_2$ implies $w = w'$;

Cancellativity: $(w \circ w_1) \cap (w \circ w_2) \neq \emptyset$ implies $w_1 = w_2$;

Single unit: $w, w' \in E$ implies $w = w'$;

Indivisible units: $(w \circ w') \cap E \neq \emptyset$ implies $w \in E$;

Disjointness: $w \circ w \neq \emptyset$ implies $w \in E$;

Divisibility: for every $w \notin E$ there are $w_1, w_2 \notin E$ such that $w \in w_1 \circ w_2$;

Cross-split property: whenever $(a \circ b) \cap (c \circ d) \neq \emptyset$, there exist ac, ad, bc, bd such that $a \in ac \circ ad$, $b \in bc \circ bd$, $c \in ac \circ bc$ and $d \in ad \circ bd$.

Definable properties

A property $\mathcal{P}$ of BBI-models is said to be $\mathcal{L}$-definable if there exists an $\mathcal{L}$-formula A such that for all BBI-models M,

$$A \text{ is valid in } M \iff M \in \mathcal{P}.$$

Definable properties

A property $\mathcal{P}$ of BBI-models is said to be $\mathcal{L}$-definable if there exists an $\mathcal{L}$-formula A such that for all BBI-models M,

$$A \text{ is valid in } M \iff M \in \mathcal{P}.$$

Proposition

The following separation theory properties are BBI-*definable:*

Definable properties

A property $\mathcal{P}$ of BBI-models is said to be $\mathcal{L}$-definable if there exists an $\mathcal{L}$-formula A such that for all BBI-models M,

$$A \text{ is valid in } M \iff M \in \mathcal{P}.$$

Proposition

The following separation theory properties are BBI-*definable:*

$$\textit{Indivisible units:} \quad \mathrm{I} \wedge (A * B) \vdash A$$

Definable properties

A property $\mathcal{P}$ of BBI-models is said to be $\mathcal{L}$-definable if there exists an $\mathcal{L}$-formula A such that for all BBI-models M,

$$A \text{ is valid in } M \iff M \in \mathcal{P}.$$

Proposition

The following separation theory properties are BBI-*definable:*

$$\begin{array}{ll} \textit{Indivisible units:} & \mathrm{I} \wedge (A * B) \vdash A \\ \textit{Divisibility:} & \neg\mathrm{I} \vdash \neg\mathrm{I} * \neg\mathrm{I} \end{array}$$

Definable properties

A property $\mathcal{P}$ of BBI-models is said to be $\mathcal{L}$-definable if there exists an $\mathcal{L}$-formula A such that for all BBI-models M,

$$A \text{ is valid in } M \iff M \in \mathcal{P}.$$

Proposition

The following separation theory properties are BBI*-definable:*

$$\begin{array}{lr} \textit{Indivisible units:} & \mathrm{I} \wedge (A * B) \vdash A \\ \textit{Divisibility:} & \neg\mathrm{I} \vdash \neg\mathrm{I} * \neg\mathrm{I} \end{array}$$

Proof.

Just directly verify the needed biimplication. □

Undefinability via disjoint union

To show a property is not BBI-definable, we show it is not preserved by some validity-preserving model construction.

Undefinability via disjoint union

To show a property is not BBI-definable, we show it is not preserved by some validity-preserving model construction.

Definition

If $M_1 = \langle W_1, \circ_1, E_1 \rangle$ and $M_2 = \langle W_2, \circ_2, E_2 \rangle$ are BBI-models and W_1, W_2 are disjoint then their disjoint union is given by

Undefinability via disjoint union

To show a property is not BBI-definable, we show it is not preserved by some validity-preserving model construction.

Definition

If $M_1 = \langle W_1, \circ_1, E_1 \rangle$ and $M_2 = \langle W_2, \circ_2, E_2 \rangle$ are BBI-models and W_1, W_2 are disjoint then their disjoint union is given by

$$M_1 \uplus M_2 \stackrel{\text{def}}{=} \langle W_1 \cup W_2, \circ_1 \cup \circ_2, E_1 \cup E_2 \rangle$$

(where $\circ_1 \cup \circ_2$ is lifted to $W_1 \cup W_2$ in the obvious way)

Undefinability via disjoint union

To show a property is not BBI-definable, we show it is not preserved by some validity-preserving model construction.

Definition

If $M_1 = \langle W_1, \circ_1, E_1 \rangle$ and $M_2 = \langle W_2, \circ_2, E_2 \rangle$ are BBI-models and W_1, W_2 are disjoint then their disjoint union is given by

$$M_1 \uplus M_2 \stackrel{\text{def}}{=} \langle W_1 \cup W_2, \circ_1 \cup \circ_2, E_1 \cup E_2 \rangle$$

(where $\circ_1 \cup \circ_2$ is lifted to $W_1 \cup W_2$ in the obvious way)

Proposition

If A is valid in M_1 and in M_2, and $M_1 \uplus M_2$ is defined, then it is also valid in $M_1 \uplus M_2$.

Undefinability via disjoint union

To show a property is not BBI-definable, we show it is not preserved by some validity-preserving model construction.

Definition

If $M_1 = \langle W_1, \circ_1, E_1 \rangle$ and $M_2 = \langle W_2, \circ_2, E_2 \rangle$ are BBI-models and W_1, W_2 are disjoint then their disjoint union is given by

$$M_1 \uplus M_2 \stackrel{\text{def}}{=} \langle W_1 \cup W_2, \circ_1 \cup \circ_2, E_1 \cup E_2 \rangle$$

(where $\circ_1 \cup \circ_2$ is lifted to $W_1 \cup W_2$ in the obvious way)

Proposition

If A is valid in M_1 and in M_2, and $M_1 \uplus M_2$ is defined, then it is also valid in $M_1 \uplus M_2$.

Proof.

Structural induction on A. □

Undefinability of single-unit property

Lemma

Let $\mathcal{P}$ *be a property of* BBI-*models, and suppose that there exist* BBI-*models* M_1 *and* M_2 *such that* $M_1, M_2 \in \mathcal{P}$ *but* $M_1 \uplus M_2 \notin \mathcal{P}$. *Then* $\mathcal{P}$ *is not* BBI-*definable.*

Undefinability of single-unit property

Lemma

Let $\mathcal{P}$ be a property of BBI-*models, and suppose that there exist* BBI-*models M_1 and M_2 such that $M_1, M_2 \in \mathcal{P}$ but $M_1 \uplus M_2 \notin \mathcal{P}$. Then $\mathcal{P}$ is not* BBI-*definable.*

Proof.

If $\mathcal{P}$ were definable via A say, then A would be true in M_1 and M_2 but not in $M_1 \uplus M_2$, contradicting previous Proposition. □

Undefinability of single-unit property

Lemma

Let $\mathcal{P}$ be a property of BBI-*models, and suppose that there exist* BBI-*models M_1 and M_2 such that $M_1, M_2 \in \mathcal{P}$ but $M_1 \uplus M_2 \notin \mathcal{P}$. Then $\mathcal{P}$ is not* BBI-*definable.*

Proof.

If $\mathcal{P}$ were definable via A say, then A would be true in M_1 and M_2 but not in $M_1 \uplus M_2$, contradicting previous Proposition. □

Theorem

The single unit property is not BBI-*definable.*

Undefinability of single-unit property

Lemma

Let $\mathcal{P}$ be a property of BBI-*models, and suppose that there exist* BBI-*models M_1 and M_2 such that $M_1, M_2 \in \mathcal{P}$ but $M_1 \uplus M_2 \notin \mathcal{P}$. Then $\mathcal{P}$ is not* BBI-*definable.*

Proof.

If $\mathcal{P}$ were definable via A say, then A would be true in M_1 and M_2 but not in $M_1 \uplus M_2$, contradicting previous Proposition. □

Theorem

The single unit property is not BBI-*definable.*

Proof.

The disjoint union of any two single-unit BBI-models (e.g. two copies of $\mathbb{N}$ under addition) is not a single-unit model, so we are done by the above Lemma. □

Undefinability via bounded morphisms

We adapt the notion of bounded morphism from modal logic to BBI-models, and can show it is also validity-preserving.

Undefinability via bounded morphisms

We adapt the notion of bounded morphism from modal logic to BBI-models, and can show it is also validity-preserving.

Theorem

None of the following separation theory properties (or any combination thereof) is BBI*-definable:*

Undefinability via bounded morphisms

We adapt the notion of bounded morphism from modal logic to BBI-models, and can show it is also validity-preserving.

Theorem

None of the following separation theory properties (or any combination thereof) is BBI-*definable:*

- *functionality;*

Undefinability via bounded morphisms

We adapt the notion of bounded morphism from modal logic to BBI-models, and can show it is also validity-preserving.

Theorem

None of the following separation theory properties (or any combination thereof) is BBI-*definable:*

- *functionality;*
- *cancellativity;*

Undefinability via bounded morphisms

We adapt the notion of bounded morphism from modal logic to BBI-models, and can show it is also validity-preserving.

Theorem

None of the following separation theory properties (or any combination thereof) is BBI-*definable:*

- *functionality;*
- *cancellativity;*
- *disjointness.*

Undefinability via bounded morphisms

We adapt the notion of bounded morphism from modal logic to BBI-models, and can show it is also validity-preserving.

Theorem

None of the following separation theory properties (or any combination thereof) is BBI-*definable:*

- *functionality;*
- *cancellativity;*
- *disjointness.*

Proof.

E.g., for functionality, we build models M and M' such that there is a bounded morphism from M to M', but M is functional while M' is not. See paper for details. □

Part IV

Hybrid extensions of BBI

HyBBI*: a hybrid extension of* BBI

- We saw that BBI is not expressive enough to accurately capture many separation theories.

HyBBI*: a hybrid extension of* BBI

- We saw that BBI is not expressive enough to accurately capture many separation theories.
- Idea: conservatively increase the expressivity of BBI, using machinery of hybrid logic.

HyBBI: *a hybrid extension of* BBI

- We saw that BBI is not expressive enough to accurately capture many separation theories.
- Idea: conservatively increase the expressivity of BBI, using machinery of hybrid logic.
- HyBBI extends the language of BBI by: any nominal ℓ is a formula, and so is any formula of the form $@_\ell A$.

HyBBI: *a hybrid extension of* BBI

- We saw that BBI is not expressive enough to accurately capture many separation theories.
- Idea: conservatively increase the expressivity of BBI, using machinery of hybrid logic.
- HyBBI extends the language of BBI by: any nominal ℓ is a formula, and so is any formula of the form $@_\ell A$.
- Valuations interpret nominals as individual worlds in a BBI-model.

HyBBI: *a hybrid extension of* BBI

- We saw that BBI is not expressive enough to accurately capture many separation theories.
- Idea: conservatively increase the expressivity of BBI, using machinery of hybrid logic.
- HyBBI extends the language of BBI by: any nominal ℓ is a formula, and so is any formula of the form $@_\ell A$.
- Valuations interpret nominals as individual worlds in a BBI-model.
- We extend the forcing relation by:

$$M, w \models_\rho \ell \quad \Leftrightarrow \quad w = \rho(\ell)$$

HyBBI: *a hybrid extension of* BBI

- We saw that BBI is not expressive enough to accurately capture many separation theories.
- Idea: conservatively increase the expressivity of BBI, using machinery of hybrid logic.
- HyBBI extends the language of BBI by: any nominal ℓ is a formula, and so is any formula of the form $@_\ell A$.
- Valuations interpret nominals as individual worlds in a BBI-model.
- We extend the forcing relation by:

$$\begin{array}{rcl} M, w \models_\rho \ell & \Leftrightarrow & w = \rho(\ell) \\ M, w \models_\rho @_\ell A & \Leftrightarrow & M, \rho(\ell) \models_\rho A \end{array}$$

HyBBI: *a hybrid extension of* BBI

- We saw that BBI is not expressive enough to accurately capture many separation theories.
- Idea: conservatively increase the expressivity of BBI, using machinery of hybrid logic.
- HyBBI extends the language of BBI by: any nominal ℓ is a formula, and so is any formula of the form $@_\ell A$.
- Valuations interpret nominals as individual worlds in a BBI-model.
- We extend the forcing relation by:

$$\begin{array}{rcl} M, w \models_\rho \ell & \Leftrightarrow & w = \rho(\ell) \\ M, w \models_\rho @_\ell A & \Leftrightarrow & M, \rho(\ell) \models_\rho A \end{array}$$

Easy to see that HyBBI is a conservative extension of BBI.

Definable properties in HyBBI

A formula is pure if it contains no propositional variables. Pure formulas have particularly nice properties wrt. completeness.

Definable properties in HyBBI

A formula is pure if it contains no propositional variables. Pure formulas have particularly nice properties wrt. completeness.

Theorem

The following separation theory properties are HyBBI-*definable, using pure formulas:*

Definable properties in HyBBI

A formula is pure if it contains no propositional variables. Pure formulas have particularly nice properties wrt. completeness.

Theorem

The following separation theory properties are HyBBI*-definable, using pure formulas:*

$$\textit{Functionality:} \quad @_\ell(j * k) \wedge @_{\ell'}(j * k) \vdash @_\ell \ell'$$

Definable properties in HyBBI

A formula is pure if it contains no propositional variables. Pure formulas have particularly nice properties wrt. completeness.

Theorem

The following separation theory properties are HyBBI-*definable, using pure formulas:*

$$\begin{array}{ll} \textit{Functionality:} & @_\ell(j * k) \land @_{\ell'}(j * k) \vdash @_\ell \ell' \\ \textit{Cancellativity:} & \ell * j \land \ell * k \vdash @_j k \end{array}$$

Definable properties in HyBBI

A formula is pure if it contains no propositional variables. Pure formulas have particularly nice properties wrt. completeness.

Theorem

The following separation theory properties are HyBBI-*definable, using pure formulas:*

Functionality:	$@_\ell(j * k) \wedge @_{\ell'}(j * k) \vdash @_\ell \ell'$
Cancellativity:	$\ell * j \wedge \ell * k \vdash @_j k$
Single unit:	$@_{\ell_1}\mathrm{I} \wedge @_{\ell_2}\mathrm{I} \vdash @_{\ell_1}\ell_2$

Definable properties in HyBBI

A formula is pure if it contains no propositional variables. Pure formulas have particularly nice properties wrt. completeness.

Theorem

The following separation theory properties are HyBBI-*definable, using pure formulas:*

Functionality:	$@_\ell(j * k) \wedge @_{\ell'}(j * k) \vdash @_\ell \ell'$
Cancellativity:	$\ell * j \wedge \ell * k \vdash @_j k$
Single unit:	$@_{\ell_1}\mathrm{I} \wedge @_{\ell_2}\mathrm{I} \vdash @_{\ell_1}\ell_2$
Disjointness:	$\ell * \ell \vdash \mathrm{I} \wedge \ell$

Definable properties in HyBBI

A formula is pure if it contains no propositional variables. Pure formulas have particularly nice properties wrt. completeness.

Theorem

The following separation theory properties are HyBBI-*definable, using pure formulas:*

Functionality:	$@_\ell(j * k) \wedge @_{\ell'}(j * k) \vdash @_\ell \ell'$
Cancellativity:	$\ell * j \wedge \ell * k \vdash @_j k$
Single unit:	$@_{\ell_1}\mathrm{I} \wedge @_{\ell_2}\mathrm{I} \vdash @_{\ell_1}\ell_2$
Disjointness:	$\ell * \ell \vdash \mathrm{I} \wedge \ell$

Proof.

Easy verifications! □

A word about cross-split

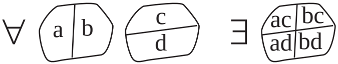
We have brushed over the cross-split property:

$(a \circ b) \cap (c \circ d) \neq \emptyset$, *implies* $\exists ac, ad, bc, bd$ *with*
$a \in ac \circ ad$, $b \in bc \circ bd$, $c \in ac \circ bc$, $d \in ad \circ bd$.

A word about cross-split

We have brushed over the cross-split property:

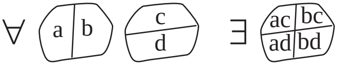
$(a \circ b) \cap (c \circ d) \neq \emptyset$, *implies* $\exists ac, ad, bc, bd$ *with*
$a \in ac \circ ad$, $b \in bc \circ bd$, $c \in ac \circ bc$, $d \in ad \circ bd$.



A word about cross-split

We have brushed over the cross-split property:

$(a \circ b) \cap (c \circ d) \neq \emptyset,\ \textit{implies}\ \exists ac, ad, bc, bd\ \textit{with}$
$a \in ac \circ ad,\ b \in bc \circ bd,\ c \in ac \circ bc,\ d \in ad \circ bd.$

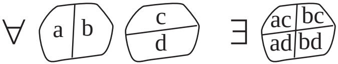


We conjecture this is not definable in BBI or in HyBBI.

A word about cross-split

We have brushed over the cross-split property:

$(a \circ b) \cap (c \circ d) \neq \emptyset,$ *implies* $\exists ac, ad, bc, bd$ *with*
$a \in ac \circ ad,\ b \in bc \circ bd,\ c \in ac \circ bc,\ d \in ad \circ bd.$



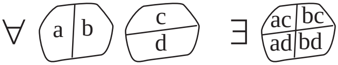
We conjecture this is not definable in BBI or in HyBBI. If we add the ↓ binder to HyBBI, defined by

$$M, w \models_\rho \downarrow\ell.\, A \quad \Leftrightarrow \quad M, w \models_{\rho[\ell := w]} A$$

A word about cross-split

We have brushed over the cross-split property:

$(a \circ b) \cap (c \circ d) \neq \emptyset$, *implies* $\exists ac, ad, bc, bd$ *with*
$a \in ac \circ ad$, $b \in bc \circ bd$, $c \in ac \circ bc$, $d \in ad \circ bd$.



We conjecture this is not definable in BBI or in HyBBI. If we add the $\downarrow$ binder to HyBBI, defined by

$$M, w \models_{\rho} \downarrow\ell.\, A \quad \Leftrightarrow \quad M, w \models_{\rho[\ell := w]} A$$

then cross-split is definable as the pure formula

$$\begin{aligned}(a * b) \wedge (c * d) \vdash\ & @_a(\top * \downarrow ac.\, @_a(\top * \downarrow ad.\, @_a(ac * ad) \\ & \wedge @_b(\top * \downarrow bc.\, @_b(\top * \downarrow bd.\, @_b(bc * bd) \\ & \wedge @_c(ac * bc) \wedge @_d(ad * bd)))))\end{aligned}$$

Part V

Parametric completeness for HyBBI(↓)

Axiomatic proof systems for HyBBI($\downarrow$)

Our axiom system $\mathbf{K}_{\mathrm{HyBBI}(\downarrow)}$ is chosen to make the completeness proof as clean as possible.

Axiomatic proof systems for HyBBI(↓)

Our axiom system $\mathbf{K}_{\mathrm{HyBBI}(\downarrow)}$ is chosen to make the completeness proof as clean as possible.
Some example axioms and rules:

$$(K_{@}) \qquad @_\ell(A \to B) \vdash @_\ell A \to @_\ell B$$

Axiomatic proof systems for HyBBI(↓)

Our axiom system $\mathbf{K}_{\text{HyBBI}(\downarrow)}$ is chosen to make the completeness proof as clean as possible.
Some example axioms and rules:

$(K_@)$	$@_\ell(A \to B) \vdash @_\ell A \to @_\ell B$
(@-intro)	$\ell \wedge A \vdash @_\ell A$

Axiomatic proof systems for HyBBI(↓)

Our axiom system $\mathbf{K}_{\mathrm{HyBBI}(\downarrow)}$ is chosen to make the completeness proof as clean as possible.
Some example axioms and rules:

$(K_{@})$	$@_\ell(A \to B) \vdash @_\ell A \to @_\ell B$
(@-intro)	$\ell \wedge A \vdash @_\ell A$
(Bridge $*$)	$@_\ell(k * k') \wedge @_k A \wedge @_{k'} B \vdash @_\ell(A * B)$

Axiomatic proof systems for HyBBI(↓)

Our axiom system $\mathbf{K}_{\text{HyBBI}(\downarrow)}$ is chosen to make the completeness proof as clean as possible.
Some example axioms and rules:

$(K_{@})$	$@_\ell(A \to B) \vdash @_\ell A \to @_\ell B$
(@-intro)	$\ell \wedge A \vdash @_\ell A$
(Bridge $*$)	$@_\ell(k * k') \wedge @_k A \wedge @_{k'} B \vdash @_\ell(A * B)$
(Bind $\downarrow$)	$\vdash\ @_j(\downarrow\ell.\, B \leftrightarrow B[j/\ell])$

Axiomatic proof systems for HyBBI(↓)

Our axiom system $\mathbf{K}_{\mathrm{HyBBI}(\downarrow)}$ is chosen to make the completeness proof as clean as possible.
Some example axioms and rules:

$(K_@)$	$@_\ell(A \to B) \vdash @_\ell A \to @_\ell B$
(@-intro)	$\ell \wedge A \vdash @_\ell A$
(Bridge $*$)	$@_\ell(k * k') \wedge @_k A \wedge @_{k'} B \vdash @_\ell(A * B)$
(Bind $\downarrow$)	$\vdash\ @_j(\downarrow\ell.\, B \leftrightarrow B[j/\ell])$

$$\frac{@_\ell(k * k') \wedge @_k A \wedge @_{k'} B \vdash C}{@_\ell(A * B) \vdash C} \quad k, k' \text{ not in } A,\ B,\ C \text{ or } \{\ell\} \quad \text{(Paste } *)$$

Axiomatic proof systems for HyBBI(↓)

Our axiom system $\mathbf{K}_{\mathrm{HyBBI}(\downarrow)}$ is chosen to make the completeness proof as clean as possible.
Some example axioms and rules:

$(K_@)$	$@_\ell(A \to B) \vdash @_\ell A \to @_\ell B$
(@-intro)	$\ell \wedge A \vdash @_\ell A$
(Bridge $*$)	$@_\ell(k * k') \wedge @_k A \wedge @_{k'} B \vdash @_\ell(A * B)$
(Bind $\downarrow$)	$\vdash\ @_j(\downarrow\ell.\, B \leftrightarrow B[j/\ell])$

$$\frac{@_\ell(k * k') \wedge @_k A \wedge @_{k'} B \vdash C}{@_\ell(A * B) \vdash C} \quad k, k' \text{ not in } A,\ B,\ C \text{ or } \{\ell\} \quad \text{(Paste } *)$$

Proposition (Soundness)

Any $\mathbf{K}_{\mathrm{HyBBI}(\downarrow)}$*-provable sequent is valid in all* BBI*-models.*

Completeness

Standard modal logic approach to completeness via maximal consistent sets (MCSs):

Completeness

Standard modal logic approach to completeness via maximal consistent sets (MCSs):

1. Show that any consistent set of formulas can be extended to an MCS (known as the Lindenbaum construction);

Completeness

Standard modal logic approach to completeness via maximal consistent sets (MCSs):

1. Show that any consistent set of formulas can be extended to an MCS (known as the Lindenbaum construction);
2. Define a canonical model whose worlds are MCSs, and a valuation s.t. proposition P is true at Γ iff $P \in \Gamma$.

Completeness

Standard modal logic approach to completeness via maximal consistent sets (MCSs):

1. Show that any consistent set of formulas can be extended to an MCS (known as the Lindenbaum construction);
2. Define a canonical model whose worlds are MCSs, and a valuation s.t. proposition P is true at Γ iff $P \in \Gamma$.
3. Truth Lemma: A is true at Γ iff $A \in \Gamma$ for any formula A.

Completeness

Standard modal logic approach to completeness via maximal consistent sets (MCSs):

1. Show that any consistent set of formulas can be extended to an MCS (known as the Lindenbaum construction);
2. Define a canonical model whose worlds are MCSs, and a valuation s.t. proposition P is true at Γ iff $P \in \Gamma$.
3. Truth Lemma: A is true at Γ iff $A \in \Gamma$ for any formula A.
4. Now, if A is unprovable, $\{\neg A\}$ is consistent so there is an MCS $\Gamma \supset \{\neg A\}$. Then A is false at Γ in the canonical model, hence invalid. □

Completeness

Standard modal logic approach to completeness via maximal consistent sets (MCSs):

1. Show that any consistent set of formulas can be extended to an MCS (known as the Lindenbaum construction);
2. Define a canonical model whose worlds are MCSs, and a valuation s.t. proposition P is true at Γ iff $P \in \Gamma$.
3. Truth Lemma: A is true at Γ iff $A \in \Gamma$ for any formula A.
4. Now, if A is unprovable, $\{\neg A\}$ is consistent so there is an MCS $\Gamma \supset \{\neg A\}$. Then A is false at Γ in the canonical model, hence invalid. $\square$

(In our case, we also have to show that the canonical model is really a BBI-model.)

Parametric completeness

- Call a BBI-model $M = \langle W, \circ, E \rangle$ named by ρ iff for all $w \in W$ there is a nominal ℓ with $\rho(\ell) = w$.

Parametric completeness

- Call a BBI-model $M = \langle W, \circ, E \rangle$ named by ρ iff for all $w \in W$ there is a nominal ℓ with $\rho(\ell) = w$.

Lemma

Let M be named by ρ and let A be a pure formula. If $M, w \models_\rho A[\theta]$ for any nominal substitution θ and $w \in W$, then A is valid in M.

Parametric completeness

- Call a BBI-model $M = \langle W, \circ, E \rangle$ named by ρ iff for all $w \in W$ there is a nominal ℓ with $\rho(\ell) = w$.

Lemma
Let M be named by ρ and let A be a pure formula. If $M, w \models_\rho A[\theta]$ for any nominal substitution θ and $w \in W$, then A is valid in M.

- So, for an extension of $\mathbf{K}_{\mathrm{HyBBI}(\downarrow)} + \mathrm{Ax}$ with pure axioms Ax, we build a canonical model M named by our valuation.

Parametric completeness

- Call a BBI-model $M = \langle W, \circ, E \rangle$ named by ρ iff for all $w \in W$ there is a nominal ℓ with $\rho(\ell) = w$.

Lemma

Let M be named by ρ and let A be a pure formula. If $M, w \models_\rho A[\theta]$ for any nominal substitution θ and $w \in W$, then A is valid in M.

- So, for an extension of $\mathbf{K}_{\mathrm{HyBBI}(\downarrow)} + \mathrm{Ax}$ with pure axioms Ax, we build a canonical model M named by our valuation.
- By the above Lemma + MCS properties, the Ax are valid in M.

Parametric completeness

- Call a BBI-model $M = \langle W, \circ, E \rangle$ named by ρ iff for all $w \in W$ there is a nominal ℓ with $\rho(\ell) = w$.

Lemma

Let M be named by ρ and let A be a pure formula. If $M, w \models_\rho A[\theta]$ for any nominal substitution θ and $w \in W$, then A is valid in M.

- So, for an extension of $\mathbf{K}_{\mathrm{HyBBI}(\downarrow)} + \mathrm{Ax}$ with pure axioms Ax, we build a canonical model M named by our valuation.
- By the above Lemma + MCS properties, the Ax are valid in M.
- That is, $\mathbf{K}_{\mathrm{HyBBI}(\downarrow)} + \mathrm{Ax}$ is complete for the models s.t. Ax!

Statement of completeness

Following the above approach (non-trivial; details in paper) we obtain the following, for any set of pure axioms Ax:

Statement of completeness

Following the above approach (non-trivial; details in paper) we obtain the following, for any set of pure axioms Ax:

Theorem (Parametric completeness)

If A is valid in the class of BBI*-models satisfying Ax, then it is provable in $\mathbf{K}_{\mathrm{HyBBI}(\downarrow)} + Ax$.*

Statement of completeness

Following the above approach (non-trivial; details in paper) we obtain the following, for any set of pure axioms Ax:

Theorem (Parametric completeness)

If A is valid in the class of BBI-*models satisfying Ax, then it is provable in* $\mathbf{K}_{\mathrm{HyBBI}(\downarrow)} + Ax$.

Corollary

By a suitable choice of axioms, we have a sound and complete axiomatic proof system for any given separation theory from our collection.

Conclusions and future work

- BBI is insufficiently expressive to capture the classes of models of typical practical interest.

Conclusions and future work

- BBI is insufficiently expressive to capture the classes of models of typical practical interest.
- One way to gain this expressivity is to incorporate naming machinery from hybrid logic.

Conclusions and future work

- BBI is insufficiently expressive to capture the classes of models of typical practical interest.
- One way to gain this expressivity is to incorporate naming machinery from hybrid logic.
- We have parametric completeness for any set of axioms expressed as pure formulas.

Conclusions and future work

- BBI is insufficiently expressive to capture the classes of models of typical practical interest.
- One way to gain this expressivity is to incorporate naming machinery from hybrid logic.
- We have parametric completeness for any set of axioms expressed as pure formulas.
- In particular, this yields complete proof systems for any separation theory from those we consider.

Conclusions and future work

- BBI is insufficiently expressive to capture the classes of models of typical practical interest.
- One way to gain this expressivity is to incorporate naming machinery from hybrid logic.
- We have parametric completeness for any set of axioms expressed as pure formulas.
- In particular, this yields complete proof systems for any separation theory from those we consider.
- Future work on our hybrid logics could include

Conclusions and future work

- BBI is insufficiently expressive to capture the classes of models of typical practical interest.
- One way to gain this expressivity is to incorporate naming machinery from hybrid logic.
- We have parametric completeness for any set of axioms expressed as pure formulas.
- In particular, this yields complete proof systems for any separation theory from those we consider.
- Future work on our hybrid logics could include
  - identification of decidable fragments;

Conclusions and future work

- BBI is insufficiently expressive to capture the classes of models of typical practical interest.
- One way to gain this expressivity is to incorporate naming machinery from hybrid logic.
- We have parametric completeness for any set of axioms expressed as pure formulas.
- In particular, this yields complete proof systems for any separation theory from those we consider.
- Future work on our hybrid logics could include
  - identification of decidable fragments;
  - search for nice structural proof theories;

Conclusions and future work

- BBI is insufficiently expressive to capture the classes of models of typical practical interest.
- One way to gain this expressivity is to incorporate naming machinery from hybrid logic.
- We have parametric completeness for any set of axioms expressed as pure formulas.
- In particular, this yields complete proof systems for any separation theory from those we consider.
- Future work on our hybrid logics could include
  - identification of decidable fragments;
  - search for nice structural proof theories;
  - investigate possible applications to program analysis.

Thanks for listening!

Prelim version of paper available from authors' webpages:

J. Brotherston and J. Villard.
Parametric completeness for separation theories.
To appear at *POPL'14*.