Parametric Completeness for Separation Theories

Jules Villard

University College London
Programming Principles, Logic and Verification Group

Joint work with James Brotherston (UCL)

Logics: Expressivity vs Complexity

Mathematical logics expressivity trade-off

- Weaker languages cannot capture interesting properties, but
- Richer languages have higher complexity, may lack sensible proof theories and may be unavoidably **incomplete** (cf. Gödel).

Logics: Expressivity vs Complexity

Mathematical logics expressivity trade-off

- Weaker languages cannot capture interesting properties, but
- Richer languages have higher complexity, may lack sensible proof theories and may be unavoidably **incomplete** (cf. Gödel).

A potential gap between two key concepts

- **provability** in some **formal system** for the logic; and

Logics: Expressivity vs Complexity

Mathematical logics expressivity trade-off

- Weaker languages cannot capture interesting properties, but
- Richer languages have higher complexity, may lack sensible proof theories and may be unavoidably **incomplete** (cf. Gödel).

A potential gap between two key concepts

- **provability** in some **formal system** for the logic; and
- **validity** in a (class of) **intended model**(s) of the logic.

Logics: Expressivity vs Complexity

Mathematical logics expressivity trade-off

- Weaker languages cannot capture interesting properties, but
- Richer languages have higher complexity, may lack sensible proof theories and may be unavoidably **incomplete** (cf. Gödel).

A potential gap between two key concepts

- **provability** in some **formal system** for the logic; and
- **validity** in a (class of) **intended model**(s) of the logic.

This talk

- Study this gap in the context of separation logic

Separation Theories

Separation Logic (SL)

- Compositional program logic for heap-manipulating programs (C, C++, Java, ...)

Separation Theories

Separation Logic (SL)

- Compositional program logic for heap-manipulating programs (C, C++, Java, . . .)
- Hoare triples $\{A\}$ *program* $\{B\}$

Separation Theories

Separation Logic (SL)

- Compositional program logic for heap-manipulating programs (C, C++, Java, . . .)
- Hoare triples $\{A\}$ *program* $\{B\}$
- Assertions A, B: **Boolean BI** (BBI)

Separation Theories

Separation Logic (SL)

- Compositional program logic for heap-manipulating programs (C, C++, Java, ...)
- Hoare triples $\{A\}$ *program* $\{B\}$
- Assertions A, B: **Boolean BI** (BBI)

Models of Separation Logic and BBI

- Models of BBI: partial commutative relational monoids

Separation Theories

Separation Logic (SL)

- Compositional program logic for heap-manipulating programs (C, C++, Java, ...)
- Hoare triples $\{A\}$ *program* $\{B\}$
- Assertions A, B: **Boolean BI** (BBI)

Models of Separation Logic and BBI

- Models of BBI: partial commutative relational monoids
- Concrete model: Heaps : Location $\rightharpoonup$ Values

Separation Theories

Separation Logic (SL)

- Compositional program logic for heap-manipulating programs (C, C++, Java, ...)
- Hoare triples $\{A\}$ *program* $\{B\}$
- Assertions A, B: **Boolean BI** (BBI)

Models of Separation Logic and BBI

- Models of BBI: partial commutative relational monoids
- Concrete model: Heaps : Location $\rightharpoonup$ Values
- In-between: **separation theories** satisfying some of
  functionality cancellativity single-unit ...

Definability of Classes of Models

Given a logical language $\mathcal{L}$, and an intended class $\mathcal{C}$ of models for that language,

1. Is $\mathcal{C}$ **finitely axiomatisable**, a.k.a. **definable** in $\mathcal{L}$?

Definability of Classes of Models

Given a logical language $\mathcal{L}$, and an intended class $\mathcal{C}$ of models for that language,

1. Is $\mathcal{C}$ **finitely axiomatisable**, a.k.a. **definable** in $\mathcal{L}$?
2. Is there a **complete proof system** for $\mathcal{L}$ w.r.t. validity in $\mathcal{C}$?

Definability of Classes of Models

Given a logical language $\mathcal{L}$, and an intended class $\mathcal{C}$ of models for that language,

1. Is $\mathcal{C}$ **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.)

Definability of Classes of Models

Given a logical language $\mathcal{L}$, and an intended class $\mathcal{C}$ of models for that language,

1. Is $\mathcal{C}$ **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.)

Pure separation logic

- $\mathcal{L}$ is **Boolean BI (BBI)**;

Definability of Classes of Models

Given a logical language $\mathcal{L}$, and an intended class $\mathcal{C}$ of models for that language,

1. Is $\mathcal{C}$ **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.)

Pure separation logic

- $\mathcal{L}$ is **Boolean BI (BBI)**;
- the intended models are given by **separation theories**

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 in 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 in this extension.
4. We show how to axiomatise validity in our hybrid system(s). Moreover, we do this such that completeness is **parametric** in the axioms defining separation theories.

Boolean BI

(Propositional) Boolean BI

BBI formula

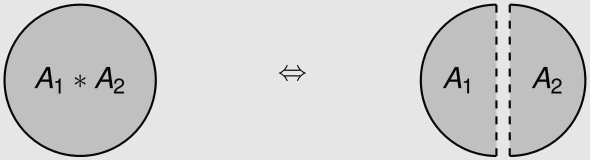
$$A ::= P \mid \top \mid \bot \mid \neg A \mid A_1 \wedge A_2 \mid A_1 \vee A_2 \mid A_1 \rightarrow A_2$$
$$\mid \mathrm{I} \mid A_1 * A_2 \mid A_1 \mathrel{-\!\!*} A_2$$

(Propositional) Boolean BI

BBI formula

$$A ::= P \mid \top \mid \bot \mid \neg A \mid A_1 \wedge A_2 \mid A_1 \vee A_2 \mid A_1 \rightarrow A_2$$
$$\mid \mathrm{I} \mid A_1 * A_2 \mid A_1 \mathrel{-\!\!*} A_2$$

Separating Conjunction $*$

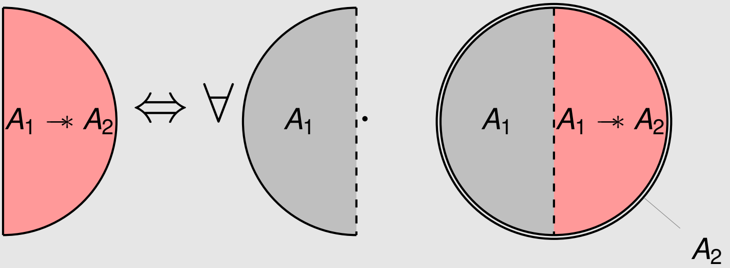


(Propositional) Boolean BI

BBI formula

$$A ::= P \mid \top \mid \bot \mid \neg A \mid A_1 \wedge A_2 \mid A_1 \vee A_2 \mid A_1 \rightarrow A_2$$
$$\mid \mathrm{I} \mid A_1 * A_2 \mid A_1 \mathrel{-\!\!*} A_2$$

Magic Wand $\mathrel{-\!\!*}$



Proof theory of BBI

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

BBI model $\langle W, \circ, E \rangle$

A **relational commutative monoid**, *i.e* a tuple $\langle W, \circ, E \rangle$ where

- $\circ : W \times W \to \mathcal{P}(W)$

$$\left(\text{lifted to } W_1 \circ W_2 \stackrel{\text{def}}{=} \bigcup_{w_1 \in W_1, w_2 \in W_2} w_1 \circ w_2\right)$$

- $\circ$ commutative and associative
- $E \subseteq W$ and $\forall w \in W.\, w \circ E = \{w\}$ (multi-units)

BBI-models

BBI model $\langle W, \circ, E \rangle$

A **relational commutative monoid**, *i.e* a tuple $\langle W, \circ, E \rangle$ where

- $\circ : W \times W \to \mathcal{P}(W)$

$$\left(\text{lifted to } W_1 \circ W_2 \stackrel{\text{def}}{=} \bigcup_{w_1 \in W_1, w_2 \in W_2} w_1 \circ w_2\right)$$

- $\circ$ commutative and associative
- $E \subseteq W$ and $\forall w \in W.\, w \circ E = \{w\}$ (multi-units)
  (that is, $\forall e \in E.\, w \circ e \subseteq \{w\}$ and $\exists e \in E.\, w \circ e = \{w\}$)

BBI-models

BBI model $\langle W, \circ, E \rangle$

A **relational commutative monoid**, *i.e* a tuple $\langle W, \circ, E \rangle$ where

- $\circ : W \times W \to \mathcal{P}(W)$

$$\left(\text{lifted to } W_1 \circ W_2 \stackrel{\text{def}}{=} \bigcup_{w_1 \in W_1, w_2 \in W_2} w_1 \circ w_2\right)$$

- $\circ$ commutative and associative
- $E \subseteq W$ and $\forall w \in W.\, w \circ E = \{w\}$ (multi-units)
  (that is, $\forall e \in E.\, w \circ e \subseteq \{w\}$ and $\exists e \in E.\, w \circ e = \{w\}$)

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

BBI-models

BBI model $\langle W, \circ, E \rangle$

A **relational commutative monoid**, *i.e* a tuple $\langle W, \circ, E \rangle$ where

- $\circ : W \times W \to \mathcal{P}(W)$

$$\left(\text{lifted to } W_1 \circ W_2 \stackrel{\text{def}}{=} \bigcup_{w_1 \in W_1, w_2 \in W_2} w_1 \circ w_2\right)$$

- $\circ$ commutative and associative
- $E \subseteq W$ and $\forall w \in W.\, w \circ E = \{w\}$ (multi-units)
  (that is, $\forall e \in E.\, w \circ e \subseteq \{w\}$ and $\exists e \in E.\, w \circ e = \{w\}$)

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

BBI model $\langle W, \circ, E\rangle$

A **relational commutative monoid**, *i.e* a tuple $\langle W, \circ, E\rangle$ where

- $\circ : W \times W \to \mathcal{P}(W)$

  $$\left(\text{lifted to } W_1 \circ W_2 \stackrel{\text{def}}{=} \bigcup_{w_1 \in W_1, w_2 \in W_2} w_1 \circ w_2\right)$$

- $\circ$ commutative and associative
- $E \subseteq W$ and $\forall w \in W.\, w \circ E = \{w\}$ (multi-units)
  (that is, $\forall e \in E.\, w \circ e \subseteq \{w\}$ and $\exists e \in E.\, w \circ e = \{w\}$)

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 the union of **domain-disjoint** heaps, and

BBI-models

BBI model $\langle W, \circ, E \rangle$

A **relational commutative monoid**, *i.e* a tuple $\langle W, \circ, E \rangle$ where

- $\circ : W \times W \to \mathcal{P}(W)$

$$\left(\text{lifted to } W_1 \circ W_2 \stackrel{\text{def}}{=} \bigcup_{w_1 \in W_1, w_2 \in W_2} w_1 \circ w_2\right)$$

- $\circ$ commutative and associative
- $E \subseteq W$ and $\forall w \in W.\, w \circ E = \{w\}$ (multi-units)
  (that is, $\forall e \in E.\, w \circ e \subseteq \{w\}$ and $\exists e \in E.\, w \circ e = \{w\}$)

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 the union of **domain-disjoint** heaps, and
- e is the empty heap that is undefined everywhere.

Semantics of BBI

Forcing relation $M, w \models_\rho A$ $\quad M = \langle W, \circ, E \rangle$

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

Semantics of BBI

Forcing relation $M, w \models_\rho A$ $\qquad M = \langle W, \circ, E \rangle$

$$M, w \models_\rho P \quad \Leftrightarrow \quad w \in \rho(P)$$
$$M, w \models_\rho A_1 \wedge A_2 \quad \Leftrightarrow \quad M, w \models_\rho A_1 \text{ and } M, w \models_\rho A_2$$

Semantics of BBI

Forcing relation $M, w \models_\rho A$ $\qquad M = \langle W, \circ, E \rangle$

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

Semantics of BBI

Forcing relation $M, w \models_\rho A$ $\qquad M = \langle W, \circ, E \rangle$

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

Semantics of BBI

Forcing relation $M, w \models_\rho A$ $\qquad M = \langle W, \circ, E \rangle$

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

Semantics of BBI

Forcing relation $M, w \models_\rho A$ $\qquad M = \langle W, \circ, E \rangle$

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

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

Semantics of BBI

Forcing relation $M, w \models_\rho A$ $\qquad M = \langle W, \circ, E \rangle$

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

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.*

(Un)definable properties in BBI

Separation theories

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

Separation theories

Applications of separation logic are typically based on models satisfying some **collection** of 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 models satisfying some **collection** of 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 models satisfying some **collection** of 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: $|E| = 1$;

Separation theories

Applications of separation logic are typically based on models satisfying some **collection** of 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: $|E| = 1$;

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

Separation theories

Applications of separation logic are typically based on models satisfying some **collection** of 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: $|E| = 1$;

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 models satisfying some **collection** of 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: $|E| = 1$;

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 models satisfying some **collection** of 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: $|E| = 1$;

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 $d \in ad \circ bd$.

Separation theories

Applications of separation logic are typically based on models satisfying some **collection** of 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 $w_1 = w_2$;

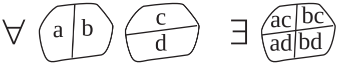
Single unit: $|E| = 1$;

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:



Separation Algebras throughout the Ages

Definition — Separation algebra (Calcagno et al. 07)

*A **separation algebra** is a* BBI*-model that is **partial functional**, **cancellative**, and with a **single unit**.*

Separation Algebras throughout the Ages

Definition — Separation algebra (Calcagno et al. 07)

*A **separation algebra** is a* BBI*-model that is **partial functional**, **cancellative**, and with a **single unit**.*

Definition — Separation algebra (Dockins et al. 09)

*A **separation algebra** is a* BBI*-model that is **partial functional** and **cancellative**.*

Separation Algebras throughout the Ages

Definition — Separation algebra (Calcagno et al. 07)

*A **separation algebra** is a* BBI*-model that is **partial functional**, **cancellative**, and with a **single unit**.*

Definition — Separation algebra (Dockins et al. 09)

*A **separation algebra** is a* BBI*-model that is **partial functional** and **cancellative**.*

Definition — Separation algebra (Dinsdale-Young et al. 13)

*A **separation algebra** is a* BBI*-model that is **partial functional**.*

Definable properties

A class $\mathcal{C}$ 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,

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

Definable properties

A class $\mathcal{C}$ 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,

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

Proposition

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

Definable properties

A class $\mathcal{C}$ 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,

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

Proposition

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

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

Definable properties

A class $\mathcal{C}$ 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,

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

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 class $\mathcal{C}$ 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,

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

Proposition

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

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

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*

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

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*

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

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*

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

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

Undefinability of single-unit property

Lemma

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

Proof.

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

Proof.

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

Proof.

If $\mathcal{C}$ 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. □

Hybrid 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 formula (extends BBI)

$$A ::= \ldots \mid \ell \mid @_\ell A$$

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 formula (extends BBI)

$$A ::= \ldots \mid \ell \mid @_\ell A$$

- 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 formula (extends BBI)

$$A ::= \ldots \mid \ell \mid @_\ell A$$

- Valuations interpret nominals as **individual worlds** in a BBI-model.

Forcing relation (extended)

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

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 formula (extends BBI)

$$A ::= \ldots \mid \ell \mid @_\ell A$$

- Valuations interpret nominals as **individual worlds** in a BBI-model.

Forcing relation (extended)

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

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 formula (extends BBI)

$$A ::= \ldots \mid \ell \mid @_\ell A$$

- Valuations interpret nominals as **individual worlds** in a BBI-model.

Forcing relation (extended)

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

- **Fact:** 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:*

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

Cancellativity: $\ell * j \wedge \ell * k \vdash @_j k$

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:*

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

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:	$@_{\ell_1}\mathrm{I} \wedge @_{\ell_2}\mathrm{I} \vdash @_{\ell_1}\ell_2$
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

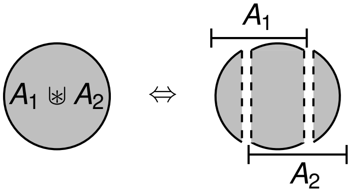
The following separation theory properties are HyBBI*-definable, using pure formulas:*

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.

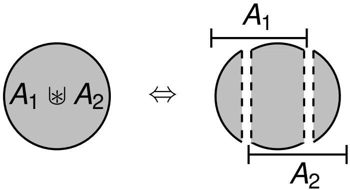
Easy verifications! □

Overlapping conjunction



$$M, w \models_\rho A_1 \circledast A_2 \Leftrightarrow \exists w_1, w_2, w_3, w', w'' \in W.$$
$$w' \in w_1 \circ w_2 \text{ and } w'' \in w_2 \circ w_3 \text{ and } w \in w' \circ w_3$$
$$\text{and } M, w' \models_\rho A_1 \text{ and } M, w'' \models_\rho A_2$$

Overlapping conjunction

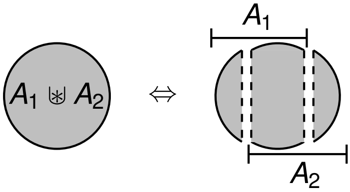


$$M, w \models_\rho A_1 \uplus A_2 \Leftrightarrow \exists w_1, w_2, w_3, w', w'' \in W. \; w' \in w_1 \circ w_2 \text{ and } w'' \in w_2 \circ w_3 \text{ and } w \in w' \circ w_3 \text{ and } M, w' \models_\rho A_1 \text{ and } M, w'' \models_\rho A_2$$

By naming the shared part, one can easily define the overlapping conjuction:

$$(\ell_s \mathrel{-\!\!*} A_1) * (\ell_s \mathrel{-\!\!*} A_2) * \ell_s$$

Overlapping conjunction



$$M, w \models_\rho A_1 \circledast A_2 \Leftrightarrow \exists w_1, w_2, w_3, w', w'' \in W.\ w' \in w_1 \circ w_2 \text{ and } w'' \in w_2 \circ w_3 \text{ and } w \in w' \circ w_3 \text{ and } M, w' \models_\rho A_1 \text{ and } M, w'' \models_\rho A_2$$

By naming the shared part, one can easily define the overlapping conjuction:

$$(\ell_s \mathrel{-\!*} A_1) * (\ell_s \mathrel{-\!*} A_2) * \ell_s$$

(but where does ℓ_s come from?..)

A word about cross-split

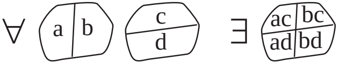
We have brushed over the **cross-split** property:

$(a \circ b) \cap (c \circ d) \neq \emptyset$, *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

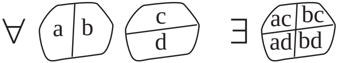
We have brushed over the **cross-split** property:

> $(a \circ b) \cap (c \circ d) \neq \emptyset$, *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:

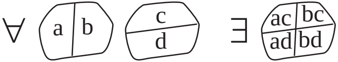
> $(a \circ b) \cap (c \circ d) \neq \emptyset$, *implies* $\exists ac, ad, bc, bd$ *with* $a \in ac \circ ad$, $b \in bc \circ bd$, $c \in ac \circ bc$, $d \in ad \circ bd$.
>
> 
>

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

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* $a \in ac \circ ad$, $b \in bc \circ bd$, $c \in ac \circ bc$, $d \in ad \circ bd$.



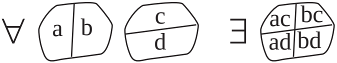
We conjecture this is not definable in BBI **or** in HyBBI. If we add the $\downarrow$ binder to HyBBI, defined by

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

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* $a \in ac \circ ad$, $b \in bc \circ bd$, $c \in ac \circ bc$, $d \in ad \circ bd$.



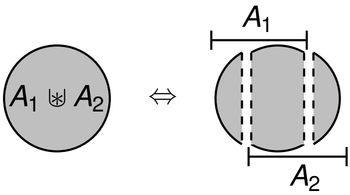
We conjecture this is not definable in BBI **or** in HyBBI. If we add the $\downarrow$ binder to HyBBI, defined by

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

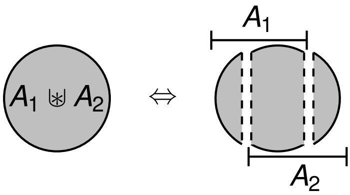
then cross-split is definable as the pure formula

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

Overlapping conjunction (bis)



Overlapping conjunction (bis)



Proposition

$A_1 \circledast A_2$ is definable via the following HyBBI(↓) *formula, where ℓ and ℓ_s do not occur in A_1 or A_2:*

$$\downarrow\ell.\, \top * \downarrow\ell_s.\, @_\ell(\ell_s \multimap\!\circledast\, A_1) * (\ell_s \multimap\!\circledast\, A_2) * \ell_s$$

(where $A \multimap\!\circledast\, B \stackrel{\text{def}}{=} \neg(A \multimap\!\!* \neg B)$)

Parametric completeness for HyBBI($\downarrow$)

Axiomatic proof systems for HyBBI($\downarrow$)

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

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:

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

Axiomatic proof systems for HyBBI(↓)

Our axiom system $\mathbf{K}_{\mathsf{HyBBI}(\downarrow)}$ 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($\downarrow$)

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($\downarrow$)

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 $\downarrow$.)	$\vdash\ @_j(\downarrow\ell.\, B \leftrightarrow B[j/\ell])$

$$\frac{@_\ell(k * k') \wedge @_k A \wedge @_{k'} B \vdash C}{@_\ell(A * B) \vdash C}$$

k, k' not in A, B, C or $\{\ell\}$
(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 $\downarrow$.)	$\vdash\ @_j(\downarrow\ell.\, B \leftrightarrow B[j/\ell])$

$$\frac{@_\ell(k * k') \wedge @_k A \wedge @_{k'} B \vdash C}{@_\ell(A * B) \vdash C}$$

k, k' not in A, B, C or $\{\ell\}$
(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 w iff $P \in w$.

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 w iff $P \in w$.
3. **Truth Lemma:** A is true at w iff $A \in w$ 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 w iff $P \in w$.
3. **Truth Lemma:** A is true at w iff $A \in w$ for any formula A.
4. Now, if A is unprovable, $\{\neg A\}$ is consistent so there is an MCS $w \supset \{\neg A\}$. Then A is false at w in the canonical model, hence invalid. $\square$

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 w iff $P \in w$.
3. **Truth Lemma:** A is true at w iff $A \in w$ for any formula A.
4. Now, if A is unprovable, $\{\neg A\}$ is consistent so there is an MCS $w \supset \{\neg A\}$. Then A is false at w in the canonical model, hence invalid. □

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

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* $\mathbf{K}_{\mathsf{HyBBI}(\downarrow)} + Ax$*.*

Corollary

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

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* $\mathbf{K}_{\mathsf{HyBBI}(\downarrow)} + Ax$*.*

Corollary

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

Conclusion

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!

Draft paper available from authors' webpages:

J. Brotherston and J. Villard.
Parametric completeness for separation theories.
To be presented at POPL'14.

Parametric Completeness for Separation Theories

Jules Villard

University College London
Programming Principles, Logic and Verification Group

Joint work with James Brotherston (UCL)