# *Definability in Boolean bunched logic*

James Brotherston

Programming Principles, Logic and Verification Group
Dept. of Computer Science
University College London, UK
J.Brotherston@ucl.ac.uk

Logic Summer School, ANU, 11 December 2015

# *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,

# *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);

# *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 at least 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 at least 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 at least 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 at least 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 $\mathcal{C}$?

In the case of BBI, we are often interested in properties of the heap models used in separation logic.

# BBI, *proof-theoretically*

Recall:

Provability in BBI is given by extending a Hilbert system for propositional classical logic 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, *semantically (1)*

Recall:

A BBI-model is given by $\langle W, \circ, E \rangle$, where

- $W$ is a set (of "worlds"),
- $\circ$ is a binary function $W \times W \to \mathcal{P}(W)$; we extend $\circ$ to $\mathcal{P}(W) \times \mathcal{P}(W) \to \mathcal{P}(W)$ by

$$W_1 \circ W_2 \stackrel{\text{def}}{=} \bigcup_{w_1 \in W_1, w_2 \in W_2} w_1 \circ w_2$$

- $\circ$ is commutative and associative;
- the set of units $E \subseteq W$ satisfies $w \circ E = \{w\}$ for all $w \in W$.

A valuation for BBI-model $M = \langle W, \circ, E \rangle$ is a function $\rho$ from propositional variables to $\mathcal{P}(W)$.

# BBI, *semantically (2)*

Given $M$, $\rho$, and $w \in W$, we define the forcing relation $w \models_\rho A$ by induction on formula $A$:

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

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

# *Definable properties*

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

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

We'll consider properties that feature in various models of separation logic.

# *Definable properties*

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

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

We'll consider properties that feature in various models of separation logic.

To show a property is definable, just exhibit the defining formula!

# *Definable properties*

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

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

We'll consider properties that feature in various models of separation logic.

To show a property is definable, just exhibit the defining formula!

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

# *Properties of (some)* BBI-*models*

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

# *Properties of (some)* BBI-*models*

*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 $w_1 = w_2$;

## *Properties of (some)* BBI*-models*

*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 $w = w'$;

# *Properties of (some)* BBI-*models*

*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 $w \in E$;

# *Properties of (some)* BBI-*models*

*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 $w \in E$;

# *Properties of (some)* BBI*-models*

*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 $w \in w_1 \circ w_2$;

# *Properties of (some)* BBI-*models*

*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 $w_1 = w_2$;

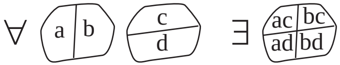
*Single unit:* $w, w' \in E$ implies $w = w'$;

*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 $d \in ad \circ bd$.



# *Two definable properties*

*Proposition*

*The following two properties are* BBI-*definable:*

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

$\mathrm{I} \wedge (A * B) \vdash A$

*Divisibility:* $\forall w \notin E . \exists w_1, w_2 \notin E$ *such that* $w \in w_1 \circ w_2$

$\neg \mathrm{I} \vdash \neg \mathrm{I} * \neg \mathrm{I}$

## *Disjoint unions of* BBI-*models*

*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)

# *Disjoint unions of* BBI-*models*

*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 $M_1 \uplus M_2$.*

# *Disjoint unions of* BBI-*models*

*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*

*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*

*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*

*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*

*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.

# *Bounded morphisms on* BBI-*models*

*Definition*

Let $M = \langle W, \circ, E \rangle$ and $M' = \langle W', \circ', E' \rangle$ be BBI-models.

## *Bounded morphisms on* BBI-*models*

*Definition*

Let $M = \langle W, \circ, E \rangle$ and $M' = \langle W', \circ', E' \rangle$ be BBI-models. A *bounded morphism* from $M$ to $M'$ is a function $f : W \to W'$ s.t.:

1. $w \in E$ iff $f(w) \in E'$;

# *Bounded morphisms on* BBI-*models*

*Definition*

Let $M = \langle W, \circ, E \rangle$ and $M' = \langle W', \circ', E' \rangle$ be BBI-models. A *bounded morphism* from $M$ to $M'$ is a function $f : W \to W'$ s.t.:

1. $w \in E$ iff $f(w) \in E'$;
2. $w \in w_1 \circ w_2$ implies $f(w) \in f(w_1) \circ' f(w_2)$;

# *Bounded morphisms on* BBI-*models*

*Definition*

Let $M = \langle W, \circ, E \rangle$ and $M' = \langle W', \circ', E' \rangle$ be BBI-models. A *bounded morphism* from $M$ to $M'$ is a function $f : W \to W'$ s.t.:

1. $w \in E$ iff $f(w) \in E'$;
2. $w \in w_1 \circ w_2$ implies $f(w) \in f(w_1) \circ' f(w_2)$;
3. $f(w) \in w'_1 \circ' w'_2$ implies $\exists w_1, w_2 \in W.\ w \in w_1 \circ w_2$ and $f(w_1) = w'_1$ and $f(w_2) = w'_2$;

# *Bounded morphisms on* BBI*-models*

*Definition*

Let $M = \langle W, \circ, E \rangle$ and $M' = \langle W', \circ', E' \rangle$ be BBI-models. A *bounded morphism* from $M$ to $M'$ is a function $f : W \to W'$ s.t.:

1. $w \in E$ iff $f(w) \in E'$;
2. $w \in w_1 \circ w_2$ implies $f(w) \in f(w_1) \circ' f(w_2)$;
3. $f(w) \in w'_1 \circ' w'_2$ implies $\exists w_1, w_2 \in W.\ w \in w_1 \circ w_2$ and $f(w_1) = w'_1$ and $f(w_2) = w'_2$;
4. $w'_2 \in f(w) \circ' w'_1$ implies $\exists w_1, w_2 \in W.\ w_2 \in w \circ w_1$ and $f(w_1) = w'_1$ and $f(w_2) = w'_2$.

## *Bounded morphisms on* BBI*-models*

*Definition*

Let $M = \langle W, \circ, E \rangle$ and $M' = \langle W', \circ', E' \rangle$ be BBI-models. A *bounded morphism* from $M$ to $M'$ is a function $f : W \to W'$ s.t.:

1. $w \in E$ iff $f(w) \in E'$;
2. $w \in w_1 \circ w_2$ implies $f(w) \in f(w_1) \circ' f(w_2)$;
3. $f(w) \in w'_1 \circ' w'_2$ implies $\exists w_1, w_2 \in W.\ w \in w_1 \circ w_2$ and $f(w_1) = w'_1$ and $f(w_2) = w'_2$;
4. $w'_2 \in f(w) \circ' w'_1$ implies $\exists w_1, w_2 \in W.\ w_2 \in w \circ w_1$ and $f(w_1) = w'_1$ and $f(w_2) = w'_2$.

*Proposition*

*Suppose there is a surjective bounded morphism from $M$ to $M'$. Then any formula valid in $M$ is also valid in $M'$.*

# *Undefinability via bounded morphisms*

*Lemma*

*Suppose there are* BBI*-models $M$ and $M'$ s.t. there is a surjective bounded morphism from $M$ to $M'$, and $M \in \mathcal{P}$ while $M' \notin \mathcal{P}$. Then $\mathcal{P}$ is not* BBI*-definable.*

# *Undefinability via bounded morphisms*

*Lemma*

*Suppose there are* BBI*-models* $M$ *and* $M'$ *s.t. there is a surjective bounded morphism from* $M$ *to* $M'$*, and* $M \in \mathcal{P}$ *while* $M' \notin \mathcal{P}$*. Then* $\mathcal{P}$ *is not* BBI*-definable.*

*Proof.* If $\mathcal{P}$ were definable via $A$ say, then $A$ would be true in $M$ but not in $M'$, contradicting previous Proposition.

# *Undefinability via bounded morphisms*

*Lemma*

*Suppose there are* BBI-*models $M$ and $M'$ s.t. there is a surjective bounded morphism from $M$ to $M'$, and $M \in \mathcal{P}$ while $M' \notin \mathcal{P}$. Then $\mathcal{P}$ is not* BBI-*definable.*

*Proof.* If $\mathcal{P}$ were definable via $A$ say, then $A$ would be true in $M$ but not in $M'$, contradicting previous Proposition.

*Theorem*

*None of the following properties is* BBI-*definable: (a) partial functionality; (b) cancellativity; (c) disjointness.*

# *Undefinability via bounded morphisms*

*Lemma*

*Suppose there are* BBI-*models* $M$ *and* $M'$ *s.t. there is a surjective bounded morphism from* $M$ *to* $M'$, *and* $M \in \mathcal{P}$ *while* $M' \notin \mathcal{P}$. *Then* $\mathcal{P}$ *is not* BBI-*definable.*

*Proof.* If $\mathcal{P}$ were definable via $A$ say, then $A$ would be true in $M$ but not in $M'$, contradicting previous Proposition.

*Theorem*

*None of the following properties is* BBI-*definable: (a) partial functionality; (b) cancellativity; (c) disjointness.*

*Proof.* In each case we build models $M$ and $M'$ such that there is a bounded morphism from $M$ to $M'$, but $M$ has the property while $M'$ doesn't.

# *Example:partial functionality*

Define BBI-models $M = \langle W, \circ, E \rangle$ and $M' = \langle W', \circ', E' \rangle$ by

$$W = \{e, v_1, v_2, x_1, x_2, y, z\} \qquad E = \{e\}$$
$$w \circ e = e \circ w = \{w\} \text{ for all } w \in W$$
$$x_1 \circ v_1 = v_1 \circ x_1 = \{y\} \qquad x_1 \circ v_2 = v_2 \circ x_1 = \{y\}$$
$$x_2 \circ v_1 = v_1 \circ x_2 = \{z\} \qquad x_2 \circ v_2 = v_2 \circ x_2 = \{z\}$$

# *Example:partial functionality*

Define BBI-models $M = \langle W, \circ, E \rangle$ and $M' = \langle W', \circ', E' \rangle$ by

$$
\begin{array}{ll}
W = \{e, v_1, v_2, x_1, x_2, y, z\} & E = \{e\} \\
w \circ e = e \circ w = \{w\} \text{ for all } w \in W & \\
x_1 \circ v_1 = v_1 \circ x_1 = \{y\} & x_1 \circ v_2 = v_2 \circ x_1 = \{y\} \\
x_2 \circ v_1 = v_1 \circ x_2 = \{z\} & x_2 \circ v_2 = v_2 \circ x_2 = \{z\}
\end{array}
$$

$$
\begin{array}{ll}
W' = \{e, v, x, y, z\} & E' = \{e\} \\
w \circ' e = e \circ' w = \{w\} \text{ for all } w \in W' & \\
x \circ' v = v \circ' x = \{y, z\} &
\end{array}
$$

# *Example:partial functionality*

Define BBI-models $M = \langle W, \circ, E \rangle$ and $M' = \langle W', \circ', E' \rangle$ by

$$W = \{e, v_1, v_2, x_1, x_2, y, z\} \qquad E = \{e\}$$
$$w \circ e = e \circ w = \{w\} \text{ for all } w \in W$$
$$x_1 \circ v_1 = v_1 \circ x_1 = \{y\} \qquad x_1 \circ v_2 = v_2 \circ x_1 = \{y\}$$
$$x_2 \circ v_1 = v_1 \circ x_2 = \{z\} \qquad x_2 \circ v_2 = v_2 \circ x_2 = \{z\}$$

$$W' = \{e, v, x, y, z\} \qquad E' = \{e\}$$
$$w \circ' e = e \circ' w = \{w\} \text{ for all } w \in W'$$
$$x \circ' v = v \circ' x = \{y, z\}$$

Easy to check $M, M'$ are both BBI-models, and $M$ is partial functional but $M'$ is not.

# *Example:partial functionality*

Define BBI-models $M = \langle W, \circ, E\rangle$ and $M' = \langle W', \circ', E'\rangle$ by

$$W = \{e, v_1, v_2, x_1, x_2, y, z\} \qquad E = \{e\}$$
$$w \circ e = e \circ w = \{w\} \text{ for all } w \in W$$
$$x_1 \circ v_1 = v_1 \circ x_1 = \{y\} \qquad x_1 \circ v_2 = v_2 \circ x_1 = \{y\}$$
$$x_2 \circ v_1 = v_1 \circ x_2 = \{z\} \qquad x_2 \circ v_2 = v_2 \circ x_2 = \{z\}$$

$$W' = \{e, v, x, y, z\} \qquad E' = \{e\}$$
$$w \circ' e = e \circ' w = \{w\} \text{ for all } w \in W'$$
$$x \circ' v = v \circ' x = \{y, z\}$$

Easy to check $M, M'$ are both BBI-models, and $M$ is partial functional but $M'$ is not. Our surjective morphism is:

$$f(v_1) = f(v_2) = v \quad f(x_1) = f(x_2) = x$$
$$f(w) = w \quad (w \in \{e, y, z\})$$

# HyBBI: *a hybrid extension of* BBI

- So, BBI cannot define some natural properties.

# HyBBI: *a hybrid extension of* BBI

- So, BBI cannot define some natural properties.
- Idea: conservatively increase the expressivity of BBI, using machinery of hybrid logic.

# HyBBI: *a hybrid extension of* BBI

- So, BBI cannot define some natural properties.
- Idea: conservatively increase the expressivity of BBI, using machinery of hybrid logic.
- HyBBI extends the language of BBI by: any nominal $\ell$ is a formula, and so is any formula of the form $@_\ell A$.

# HyBBI: *a hybrid extension of* BBI

- So, BBI cannot define some natural properties.
- Idea: conservatively increase the expressivity of BBI, using machinery of hybrid logic.
- HyBBI extends the language of BBI by: any nominal $\ell$ 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

- So, BBI cannot define some natural properties.
- Idea: conservatively increase the expressivity of BBI, using machinery of hybrid logic.
- HyBBI extends the language of BBI by: any nominal $\ell$ 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

- So, BBI cannot define some natural properties.
- Idea: conservatively increase the expressivity of BBI, using machinery of hybrid logic.
- HyBBI extends the language of BBI by: any nominal $\ell$ 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

- So, BBI cannot define some natural properties.
- Idea: conservatively increase the expressivity of BBI, using machinery of hybrid logic.
- HyBBI extends the language of BBI by: any nominal $\ell$ 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

*Theorem*

*The following properties are* HyBBI-*definable:*

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

# *Definable properties in* HyBBI

*Theorem*

*The following properties are* HyBBI*-definable:*

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

# *Definable properties in* HyBBI

*Theorem*

*The following properties are* HyBBI-*definable:*

| | |
|---|---|
| *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

*Theorem*

*The following properties are* HyBBI*-definable:*

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

# *Definable properties in* HyBBI

*Theorem*

*The following properties are* HyBBI-*definable:*

| | |
|---|---|
| *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:* | $\ell * \ell \vdash \mathrm{I} \wedge \ell$ |

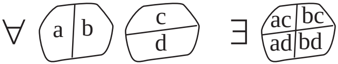
*Proof.*

Easy verifications! □

# *A word about cross-split*

We have brushed over the cross-split property:

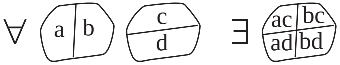
$(a \circ b) \cap (c \circ d) \neq \emptyset,$ *implies* $\exists ac, ad, bc, bd$ *with*
$a \in ac \circ ad,\ b \in bc \circ bd,\ c \in ac \circ bc,\ d \in ad \circ bd.$



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

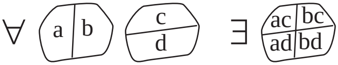



We conjecture this is not definable in BBI or in HyBBI.

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



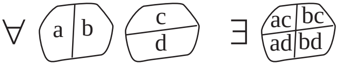

We conjecture this is not definable in BBI or in HyBBI. If we add the ↓ binder to HyBBI, defined by

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

# *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 ↓ 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

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

# *Statement of completeness*

We can write down a (quite complex) Hilbert-style proof system for HyBBI by adding rules for the hybrid operators. Soundness is easy, as usual.

# *Statement of completeness*

We can write down a (quite complex) Hilbert-style proof system for HyBBI by adding rules for the hybrid operators. Soundness is easy, as usual.

Following an approach based on a Lindenbaum construction using maximal consistent sets we obtain the following completeness result:

# Statement of completeness

We can write down a (quite complex) Hilbert-style proof system for HyBBI by adding rules for the hybrid operators. Soundness is easy, as usual.

Following an approach based on a Lindenbaum construction using maximal consistent sets we obtain the following completeness result:

*Theorem (Completeness)*

*Let Ax be a set of axioms not containing any propositional variables (nominals are OK).*

# *Statement of completeness*

We can write down a (quite complex) Hilbert-style proof system for HyBBI by adding rules for the hybrid operators. Soundness is easy, as usual.

Following an approach based on a Lindenbaum construction using maximal consistent sets we obtain the following completeness result:

*Theorem (Completeness)*

*Let $Ax$ be a set of axioms not containing any propositional variables (nominals are OK).*
*Suppose that $A$ is valid in the class of* BBI-*models satisfying $Ax$.*

# *Statement of completeness*

We can write down a (quite complex) Hilbert-style proof system for HyBBI by adding rules for the hybrid operators. Soundness is easy, as usual.

Following an approach based on a Lindenbaum construction using maximal consistent sets we obtain the following completeness result:

*Theorem (Completeness)*

*Let $Ax$ be a set of axioms not containing any propositional variables (nominals are OK).*
*Suppose that $A$ is valid in the class of* BBI*-models satisfying $Ax$.*

*Then $A$ is provable in the Hilbert system for* HyBBI*, extended with $Ax$.*

## *Conclusions and future work*

- BBI is insufficiently expressive to capture important classes of models.

# *Conclusions and future work*

- BBI is insufficiently expressive to capture important classes of models.
- We can gain this expressivity by deploying naming machinery from hybrid logic.

# *Conclusions and future work*

- BBI is insufficiently expressive to capture important classes of models.
- We can gain this expressivity by deploying naming machinery from hybrid logic.
- In $HyBBI$, we have parametric completeness for any set of axioms expressed as pure formulas.

# *Conclusions and future work*

- BBI is insufficiently expressive to capture important classes of models.
- We can gain this expressivity by deploying naming machinery from hybrid logic.
- In $HyBBI$, we have parametric completeness for any set of axioms expressed as pure formulas.
- In particular, this yields complete proof systems for previously undefinable classes of BBI-models.

# *Conclusions and future work*

- BBI is insufficiently expressive to capture important classes of models.
- We can gain this expressivity by deploying naming machinery from hybrid logic.
- In $HyBBI$, we have parametric completeness for any set of axioms expressed as pure formulas.
- In particular, this yields complete proof systems for previously undefinable classes of BBI-models.
- Future work on our hybrid logics could include

## *Conclusions and future work*

- BBI is insufficiently expressive to capture important classes of models.
- We can gain this expressivity by deploying naming machinery from hybrid logic.
- In $HyBBI$, we have parametric completeness for any set of axioms expressed as pure formulas.
- In particular, this yields complete proof systems for previously undefinable classes of BBI-models.
- Future work on our hybrid logics could include
  - identification of decidable fragments;

# *Conclusions and future work*

- BBI is insufficiently expressive to capture important classes of models.
- We can gain this expressivity by deploying naming machinery from hybrid logic.
- In $HyBBI$, we have parametric completeness for any set of axioms expressed as pure formulas.
- In particular, this yields complete proof systems for previously undefinable classes of BBI-models.
- 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 important classes of models.
- We can gain this expressivity by deploying naming machinery from hybrid logic.
- In $HyBBI$, we have parametric completeness for any set of axioms expressed as pure formulas.
- In particular, this yields complete proof systems for previously undefinable classes of BBI-models.
- Future work on our hybrid logics could include
  - identification of decidable fragments;
  - search for nice structural proof theories;
  - investigate possible applications to program analysis.

# *Further reading*


J. Brotherston and J. Villard.
Parametric completeness for separation theories.
In *Proc. POPL-41*. ACM, 2014.

P. Blackburn, M. de Rijke and Y. Venema.
Modal Logic.
Cambridge University Press, 2001.

Z. Hóu, R. Clouston, R. Goré and A. Tiu.
Proof search for propositional abstract separation logics via labelled sequents.
In *Proc. POPL-41*. ACM, 2014.

D. Larchey-Wendling and D. Galmiche.
Exploring the relation between intuitionistic BI and Boolean BI: an unexpected embedding.
In *Math. Struct. in Comp. Sci.*, vol. 19. Cambridge University Press, 2009.