Parametric Completeness for Separation Theories

James Brotherston Jules Villard

Dept. of Computer Science, University College London, UK

Abstract

In this paper, we close the logical gap between provability in the logic BBI, which is the propositional basis for *separation logic*, and validity in an intended class of *separation models*, as employed in applications of separation logic such as program verification. An intended class of separation models is usually specified by a collection of axioms describing the specific model properties that are expected to hold, which we call a *separation theory*.

Our main contributions are as follows. First, we show that several typical properties of separation theories are not definable in BBI. Second, we show that these properties become definable in a suitable *hybrid extension* of BBI, obtained by adding a theory of *naming* to BBI in the same way that *hybrid logic* extends normal modal logic. The binder-free extension HyBBI captures most of the properties we consider, and the full extension HyBBI($\downarrow$) with the usual $\downarrow$ binder of hybrid logic covers all these properties. Third, we present an axiomatic proof system for our hybrid logic whose extension with any set of "pure" axioms is sound and complete with respect to the models satisfying those axioms. As a corollary of this general result, we obtain, in a parametric manner, a sound and complete axiomatic proof system for any separation theory from our considered class. To the best of our knowledge, this class includes all separation theories appearing in the published literature.

Categories and Subject Descriptors F.3.1 [*Logics and Meanings of Programs*]: Specifying and Verifying and Reasoning about Programs—Logics of programs; F.4.1 [*Mathematical Logic and Formal Languages*]: Mathematical Logic—Model theory, Proof theory, Modal logic

General Terms Theory, verification

Keywords Bunched logic, separation logic, hybrid logic

1. Introduction

Essentially, all models are wrong, but some are useful.

G. E. P. Box and N. R. Draper [3], 1987

In mathematical logic, there is a notable tension between *provability* in a deductive system — which typically captures *validity* in some general class of models of the underlying logic — and *validity in the intended model(s)* of practical or theoretical interest. For example, as famously demonstrated by Gödel [15], there are statements of Peano arithmetic (PA) that hold in its intended model, i.e. the natural numbers $\mathbb{N}$, but not in all of its possible models, and so these statements are not provable in PA. This *incompleteness* of logical proof systems with respect to a particular choice of intended model(s) is unavoidable for sufficiently expressive systems. In other cases, it might happen that a logical system is complete but insufficiently expressive to capture the interesting properties of the intended model; that is, some mathematical property of the model cannot be expressed by any formula of the logical language (in which case we say that the intended models are not *definable* or *axiomatisable* within the system). Thus, when formulating a logical system, there are at least two natural and essentially independent questions: first, whether the language of the system is expressive enough to axiomatise the intended models; and, second, whether the system is complete for validity in these intended models.

In this paper, we consider these questions in the context of *separation logic*, an established formalism for reasoning about heap-manipulating programs [24, 6, 26]. The purely propositional part of separation logic is usually considered to be given by Boolean BI (from now on BBI), which is a particular flavour of *bunched logic* obtained by freely combining the connectives of multiplicative intuitionistic linear logic with those of standard classical logic [18, 23]. Provability in BBI corresponds to validity in the general class of relational commutative monoids [14]. Applications of separation logic, on the other hand, typically deal with *specific* such models, or classes thereof, based on the composition of heaps (see [5] for a survey of the models used in practice). Unsurprisingly, these heap models exhibit various interesting mathematical properties that are not true of all relational commutative monoids, and thus are not captured by provability in BBI. For example, composition of disjoint heaps is a cancellative partial (binary) function, which is a special case of the ternary relation in a relational commutative monoid. Various collections of such properties have been advanced in the literature as abstractions over concrete heap models, suitable for program analysis, under the common name of *separation algebra* [8, 12, 11]. We list the model properties commonly found in the literature in Definition 3.1, and call a given collection of such properties a *separation theory*. Our aim is to obtain logical proof systems in which provability accurately captures (validity in) the class of models determined by a separation theory (and preferably by adding as little extra machinery as possible to BBI).

In this paper, we make three main contributions:

- First, we show in Section 3 that BBI is insufficiently expressive to axiomatise most separation theories. Specifically, we show that several commonly considered model properties are not definable by any BBI-formula (e.g., partial functionality and/or cancellativity of the composition operation). Undefinability of a property means that the logic is fundamentally incapable of distinguishing models with the property from those without it. In particular, we find that none of the three different classes of separation algebras found in the literature [8, 12, 11] are definable in BBI.

POPL '14, January 22–24, 2014, San Diego, CA, USA.

ACM 978-1-4503-2544-8/14/01.
http://dx.doi.org/10.1145/2535838.2535844

• Second, we introduce in Section 4 a simple *hybrid* extension HyBBI of BBI, which bears the same relation to BBI as normal hybrid logic does to normal modal logic (see [1, 2] for an overview). That is, HyBBI extends BBI with a theory of *naming*: we introduce a second sort of atoms, called *nominals*, which are interpreted as individual states in a model; and we also add a unary hybrid modality $@_\ell$ (parameterised by the nominal ℓ), so that the hybrid formula $@_\ell A$ is satisfied at any world in a model just when A is satisfied at the world denoted by the nominal ℓ.

Despite the simplicity of this extension, which is conservative over standard BBI, the hybrid logic HyBBI is expressive enough to define most of the separation theories we consider, including in particular all three concepts of separation algebras from the literature [8, 12, 11]. However, for more complex model properties such as the *cross-split* property of [12], still more expressivity is required: we show in Section 7 how to gain this expressivity by adding the $\downarrow$ binder of hybrid logic to HyBBI.

• Third, we provide a Hilbert-style axiomatic proof system for HyBBI that is *parametrically* sound and complete with respect to any given separation theory. That is, whenever the proof system is extended with the axioms defining a separation theory, the resulting extension is sound and complete with respect to the class of models determined by that theory. (E.g., by adding the axiom defining cancellativity, we obtain a sound and complete proof theory for cancellative models.) Such axiomatic proof systems provide a useful proof-theoretic characterisation of validity in separation theories which can be used as a baseline for, e.g., tableau or sequent-style proof systems.

We present the axiom system and its soundness result in Section 5, and give the completeness theorem in Section 6. Section 7 extends these results to HyBBI with the $\downarrow$ binder.

Related work. Most of our technical results are obtained by adaptations of techniques from modal and hybrid logic. This should come as no surprise, since bunched logics can quite straightforwardly be seen as modal logics; indeed, this view has been exploited previously in the literature on bunched logic, e.g. to obtain completeness results [7, 4]. However, as far as we know, this paper represents the first explicit introduction of hybrid logic into the setting of (abstract) separation logic. In particular, previous work on hybrid logics has seemingly been confined to modal logic with unary modalities connected by De Morgan duality, whereas in this setting we consider the case of binary modalities connected by residuation.

Interestingly, the key concept from hybrid logic, i.e. the explicit naming of elements in the underlying model, has been used implicitly several times in the literature on the proof theory of BBI. For example, the labelled tableau system for BBI [20], which was recently proven complete for partial functional BBI-models [19], relies on a system of semantic labels which pick out individual model states in much the same way as nominal atoms in hybrid logic. Even more recently, labelled nested [22] and non-nested [17] sequent calculi for BBI have appeared, employing semantic labels in a broadly similar way. While such works add names or labels to proof systems as auxiliary tools for simplifying proof search in standard BBI, here we consider these features to be first-class components of the logic. Indeed, we believe that it should be possible to adapt the labelled proof systems in the literature to yield cut-free proof theories for our hybrid extensions of BBI.

In a similar vein, the explicit naming of heaps arises naturally in several extensions of separation logic as an aid to practical program verification. Reynolds conjectured that referring explicitly to the current heap in specifications would allow one to verify programs that manipulate data structures with sharing, such as graphs [25]. Duck et al. recently vindicated this claim by providing automatic verification techniques for such programs, where specifications are written using a constraint language based on separation logic with explicit heaps [13]. In an independent line of research, David and Chin introduced *immutable specifications* [10], which extend separation logic to support the tagging of certain parts of the heap as *immutable*. This can be viewed as adding a heap label in the precondition of a command, corresponding to the immutable part, and asserting the same heap label in the postcondition. The hybrid logics introduced in this paper can be seen as providing a common formal foundation for adding explicit heap atoms and modalities to separation logic-based verification. Our main focus here is on the precise expressivity of these logics.

2. Syntax and semantics of BBI

In this section, we introduce formulas of BBI and their Kripke semantics, given by relational commutative monoids (cf. [14]).

Definition 2.1 (BBI-formula)**.** Let $\mathcal{V}$ be a countably infinite set of *propositional variables*. BBI-*formulas* are built from propositional variables $P \in \mathcal{V}$ using the usual connectives $(\top, \bot, \neg, \wedge, \vee, \rightarrow)$ of classical logic, and the so-called "multiplicative" connectives, consisting of the constant I and binary operators $*$ and $-\!\!*$.

By convention, $\neg$ has the highest precedence, followed by $*$, $\wedge$ and $\vee$, with $\rightarrow$ and $-\!\!*$ having lowest precedence.

Definition 2.2 (BBI frames and models)**.** A BBI-*frame* is a a tuple $\langle W, \circ, E\rangle$, where W is a set (of "worlds"), $\circ : W \times W \rightarrow \mathcal{P}(W)$ and $E \subseteq W$. We extend $\circ$ pointwise to $\mathcal{P}(W) \times \mathcal{P}(W) \rightarrow \mathcal{P}(W)$:

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

A BBI-frame $\langle W, \circ, E\rangle$ is a BBI-*model* if $\circ$ is commutative and associative, and $w \circ E = \{w\}$ for all $w \in W$ (that is, $w \circ e \subseteq \{w\}$ for all $e \in E$ and $w \circ e = \{w\}$ for some $e \in E$). We call E the set of *units* of the model $\langle W, \circ, E\rangle$.

Definition 2.3 (BBI-validity)**.** Let $M = \langle W, \circ, E\rangle$ be a BBI-frame. A *valuation* for M is a function ρ that assigns to each propositional variable $P \in \mathcal{V}$ a set $\rho(P) \subseteq W$. Given any valuation ρ for M, any $w \in W$ and any BBI-formula A, we define the forcing relation $M, w \models_\rho A$ by induction on A:

$$\begin{array}{rcl}
M, w \models_\rho P & \Leftrightarrow & w \in \rho(P) \\
M, w \models_\rho \top & & \text{always} \\
M, w \models_\rho \bot & & \text{never} \\
M, w \models_\rho \neg A & \Leftrightarrow & M, w \not\models_\rho A \\
M, w \models_\rho A_1 \wedge A_2 & \Leftrightarrow & M, w \models_\rho A_1 \text{ and } M, w \models_\rho A_2 \\
M, w \models_\rho A_1 \vee A_2 & \Leftrightarrow & M, w \models_\rho A_1 \text{ or } M, w \models_\rho A_2 \\
M, w \models_\rho A_1 \rightarrow A_2 & \Leftrightarrow & M, w \models_\rho A_1 \text{ implies } M, w \models_\rho A_2 \\
M, w \models_\rho \mathrm{I} & \Leftrightarrow & w \in E \\
M, w \models_\rho A_1 * A_2 & \Leftrightarrow & \exists w_1, w_2 \in W.\ w \in w_1 \circ w_2 \text{ and} \\
 & & M, w_1 \models_\rho A_1 \text{ and } M, w_2 \models_\rho A_2 \\
M, w \models_\rho A_1 -\!\!* A_2 & \Leftrightarrow & \forall w', w'' \in W. \text{ if } w'' \in w \circ w' \text{ and} \\
 & & M, w' \models_\rho A_1 \text{ then } M, w'' \models_\rho A_2
\end{array}$$

A is said to be *valid in* M if $M, w \models_\rho A$ for all valuations ρ and for all $w \in W$. A is *valid* if it is valid in all BBI-models.

Definition 2.4. We define $\mathbf{K}_{\mathrm{BBI}}$ to be the proof system obtained by extending a complete Hilbert system for classical logic with the following axioms and inference rules for $*$, $-\!\!*$ and I (where $A \vdash B$ is syntactic sugar for the formula $A \rightarrow B$):

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

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

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

Galmiche and Larchey-Wendling showed [14] that $\mathbf{K}_{\mathrm{BBI}}$ is sound and complete with respect to "single-unit" BBI-models, where the set of units is a singleton (cf. Definition 3.1). The corresponding result for our multi-unit setting is an easy corollary.

Theorem 2.5. *A* BBI*-formula is* $\mathbf{K}_{\mathrm{BBI}}$*-provable iff it is valid.*

3. Definable and undefinable properties in BBI

In this section, we review a number of interesting properties of BBI-models encountered in the literature on separation logic, and examine whether or not these properties can be axiomatised, or *defined*, by formulas of BBI. Specifically, we show that several such properties are *not* definable in BBI, by showing that they are not generally preserved by validity-preserving model constructions.

Definition 3.1 (Separation theories)**.** Letting $M = \langle W, \circ, E\rangle$ be a BBI-model, we introduce the following properties of interest:

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: $|E| = 1$, i.e. $w, w' \in E$ 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 $(t \circ u) \cap (v \circ w) \neq \emptyset$, there exist tv, tw, uv, uw such that $t \in tv \circ tw$, $u \in uv \circ uw$, $v \in tv \circ uv$ and $w \in tw \circ uw$.

Any given collection of model properties from the above list is called a *separation theory*.

All the above axioms are true of standard heap models with the exception of divisibility, which arises naturally in models with fractional permissions. The significance of the individual properties is explained in more detail in [12] (where disjointness and divisibility are referred to as "positivity" and "splittability" respectively). Various different separation theories have been considered in the literature on separation logic. For example, a BBI-model that is both partial functional and cancellative is called a *separation algebra* in [12], while in [8] the same term defines a BBI-model that is partial functional and cancellative with a single unit, and in the "views" framework of [11] the same term again refers to a BBI-model that is simply partial functional.

Definability in BBI. We now examine which of the characteristics of separation theories are *definable* within BBI. We abuse notation slightly by identifying a property of BBI-models with the class of BBI-models satisfying that property.

Definition 3.2 (Definability)**.** Given a language $\mathcal{L}$ of formulas, 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,

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

We remark that definability could equally well be defined on BBI-*frames*, not just BBI-models. Note that the property of being a BBI-model, among all frames, is itself BBI-definable: take as the defining formula the conjunction of the top four axioms in Definition 2.4 (which define associativity, commutativity and the unit law $E \circ w = \{w\}$). However, we shall be concerned mainly with the properties of BBI-*models* listed in Definition 3.1.

Proposition 3.3. *The indivisible units property and the divisibility property are both* BBI*-definable, as follows:*

$$\textit{Indivisible units:} \quad \mathrm{I} \wedge (A * B) \vdash A \qquad \text{(iu)}$$
$$\textit{Divisibility:} \quad \neg\mathrm{I} \vdash \neg\mathrm{I} * \neg\mathrm{I} \qquad \text{(div)}$$

Proof. The case of the indivisible units property is shown in [5]. For the case of divisibility, we proceed as follows:

($\Leftarrow$) Assume that M is divisible, let ρ be a valuation for M and let $w \in W$. To show that (div) is valid, we suppose that $M, w \models_\rho \neg\mathrm{I}$, i.e., that $w \notin E$, and require to show that $M, w \models_\rho \neg\mathrm{I} * \neg\mathrm{I}$. Divisibility gives us $w_1, w_2 \in W \setminus E$ such that $w \in w_1 \circ w_2$; thus, $M, w \models_\rho \neg\mathrm{I} * \neg\mathrm{I}$.

($\Rightarrow$) Assume that (div) is valid in M, and suppose that $w \in W \setminus E$. Then, $M, w \models_\rho \neg\mathrm{I}$, hence we have $M, w \models_\rho \neg\mathrm{I} * \neg\mathrm{I}$ by validity of (div). This gives us w_1, w_2 such that $w \in w_1 \circ w_2$ where $M, w_1 \models_\rho \neg\mathrm{I}$ and $M, w_2 \models_\rho \neg\mathrm{I}$, i.e. $w_1, w_2 \notin E$ as required. □

Undefinability in BBI. Here we show that four of the properties of Defn. 3.1 are not definable in BBI: partial functionality, cancellativity, disjointness and single unit. First, we introduce the *bounded morphic image* and *disjoint union* constructions for BBI-models and show that they preserve validity in a given model, which mirrors the situation arising from their analogues in modal logic [1]. Our undefinability results follow from the fact that the first three of the above properties are not preserved by bounded morphic images, while the last one is not preserved by disjoint unions.

Definition 3.4 (Bounded morphic image)**.** 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 $f : W \to W'$ satisfying the following:

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 $f(w_2) = w'_2$;

We say M' is a *bounded morphic image* of M, written $M \twoheadrightarrow M'$, if there is a surjective bounded morphism from M to M'.

Lemma 3.5. *Let M and M' be* BBI*-models with $M \twoheadrightarrow M'$. Then any* BBI*-formula valid in M is also valid in M'.*

Proof. We write $M = \langle W, \circ, E\rangle$ and $M' = \langle W', \circ', E'\rangle$, and let $f : W \to W'$ be a surjective bounded morphism from M to M'. Suppose for contradiction that A is valid in M, but not in M'. Thus there exists a valuation ρ' for M' and $w' \in W'$ such that $M', w' \not\models_{\rho'} A$. We define a valuation ρ for M as follows:

$$\rho(P) \stackrel{\text{def}}{=} \{w \in W \mid f(w) \in \rho'(P)\}$$

As f is surjective, there is a $w \in W$ such that $w' = f(w)$. To obtain the required contradiction, we claim that $M, w \not\models_\rho A$. To show this claim, we prove by structural induction on A that for all $w \in W$, we have $M, w \models_\rho A$ if and only if $M', f(w) \models_{\rho'} A$. We omit the cases for the classical connectives, as they are straightforward by induction hypothesis.

Case $A = P \in \mathcal{V}$. Using the definition of ρ, we have as required:

$$\begin{array}{rcl} M, w \models_\rho A & \Leftrightarrow & w \in \rho(P) \\ & \Leftrightarrow & f(w) \in \rho'(P) \\ & \Leftrightarrow & M', f(w) \models_{\rho'} P \end{array}$$

Case $A = \mathrm{I}$. Using condition 1 in Defn. 3.4, we have as required:

$$M, w \models_\rho \mathrm{I} \Leftrightarrow w \in E \Leftrightarrow f(w) \in E' \Leftrightarrow M', f(w) \models_{\rho'} \mathrm{I}$$

Case $A = B * C$. ($\Rightarrow$) Supposing that $M, w \models_\rho B * C$, we have $w \in w_1 \circ w_2$ with $M, w_1 \models_\rho B$ and $M, w_2 \models_\rho C$. Using condition 2 in Defn. 3.4, we have $f(w) \in f(w_1) \circ' f(w_2)$. Furthermore, by induction hypothesis, $M', f(w_1) \models_{\rho'} B$ and $M', f(w_2) \models_{\rho'} C$. Thus $M', f(w) \models_{\rho'} B * C$ as required.

($\Leftarrow$) Supposing that $M', f(w) \models_{\rho'} B * C$, we have $f(w) \in w'_1 \circ' w'_2$ with $M', w'_1 \models_{\rho'} B$ and $M', w'_2 \models_{\rho'} C$. By condition 3 in Defn. 3.4, there are $w_1, w_2 \in W$ with $w \in w_1 \circ w_2$ and $f(w_1) = w'_1$ and $f(w_2) = w'_2$. Thus, by the induction hypothesis, we have $M, w_1 \models_\rho B$ and $M, w_2 \models_\rho C$. Hence $M, w \models_\rho B * C$.

Case $A = B \mathrel{-\!*} C$. ($\Rightarrow$) Suppose $M, w \models_\rho B \mathrel{-\!*} C$. To show that $M', f(w) \models_{\rho'} B \mathrel{-\!*} C$, we assume that $w'_2 \in f(w) \circ' w'_1$ and $M', w'_1 \models_{\rho'} B$, and must show $M', w'_2 \models_{\rho'} C$. By condition 4 in Defn. 3.4, there are $w_1, w_2 \in W$ with $w_2 \in w \circ w_1$ and $f(w_1) = w'_1$ and $f(w_2) = w'_2$. Thus, by the induction hypothesis, $M, w_1 \models_\rho B$. Since $M, w \models_\rho B \mathrel{-\!*} C$, we obtain $M, w_2 \models_\rho C$, which yields the required $M', w'_2 \models_{\rho'} C$ by induction hypothesis.

($\Leftarrow$) Suppose $M', f(w) \models_{\rho'} B \mathrel{-\!*} C$. To show that $M, w \models_\rho B \mathrel{-\!*} C$, we assume that $w_2 \in w \circ w_1$ and $M, w_1 \models_\rho B$, and must show $M, w_2 \models_\rho C$. By condition 2 in Defn. 3.4, we have $f(w_2) \in f(w) \circ f(w_1)$, and by induction hypothesis we have $M', f(w_1) \models_{\rho'} B$. Since $M', f(w) \models_{\rho'} B \mathrel{-\!*} C$, we obtain $M', f(w_2) \models_{\rho'} C$, which then yields the required $M, w_2 \models_\rho C$ using the induction hypothesis. This completes all cases. □

Lemma 3.6. *Let $\mathcal{P}$ be a property of* BBI*-models, and let M, M' be* BBI*-models such that $M \in \mathcal{P}$, $M' \notin \mathcal{P}$ and $M \twoheadrightarrow M'$. Then $\mathcal{P}$ is not* BBI*-definable.*

Proof. Suppose for contradiction that the BBI-formula A is valid in exactly those BBI-models with property $\mathcal{P}$. Then A is valid in M. By Lemma 3.5, A must be valid in M', since $M \twoheadrightarrow M'$. Hence $M' \in \mathcal{P}$, contradicting the assumption that $M' \notin \mathcal{P}$. □

In fact, Lemma 3.6 applies to BBI-*frames* as well as BBI-models, and implies that if $M \twoheadrightarrow M'$ and M is a BBI-model, then so is M'. Otherwise the class of all BBI-models would not be BBI-definable among all BBI-frames, contradiction.

The following result shows that separation algebras as defined by the "views" framework [11] are not BBI-definable.

Theorem 3.7. *Partial functionality is not* BBI*-definable.*

Proof. By Lemma 3.6, it suffices to exhibit a pair of BBI-models M and M' such that M is partial functional, M' is not partial functional and $M \twoheadrightarrow M'$. We define BBI-models $M = \langle W, \circ, E\rangle$ and $M' = \langle W', \circ', E'\rangle$ as follows:

$$\begin{array}{ll} W \stackrel{\text{def}}{=} \{e, v_1, v_2, x_1, x_2, y, z\} & E \stackrel{\text{def}}{=} \{e\} \\ \multicolumn{2}{l}{w \circ e = e \circ w \stackrel{\text{def}}{=} \{w\} \text{ for all } w \in W} \\ x_1 \circ v_1 = v_1 \circ x_1 \stackrel{\text{def}}{=} \{y\} & x_1 \circ v_2 = v_2 \circ x_1 \stackrel{\text{def}}{=} \{y\} \\ x_2 \circ v_1 = v_1 \circ x_2 \stackrel{\text{def}}{=} \{z\} & x_2 \circ v_2 = v_2 \circ x_2 \stackrel{\text{def}}{=} \{z\} \end{array}$$

$$\begin{array}{ll} W' \stackrel{\text{def}}{=} \{e, v, x, y, z\} & E' \stackrel{\text{def}}{=} \{e\} \\ \multicolumn{2}{l}{w \circ' e = e \circ' w \stackrel{\text{def}}{=} \{w\} \text{ for all } w \in W'} \\ \multicolumn{2}{l}{x \circ' v = v \circ' x \stackrel{\text{def}}{=} \{y, z\}} \end{array}$$

with $w_1 \circ w_2 = w_1 \circ' w_2 \stackrel{\text{def}}{=} \emptyset$ for all other w_1 and w_2.

First, we verify that M and M' are indeed BBI-models. Commutativity and the unit law hold in both models by construction. Associativity of $\circ$ and $\circ'$ is straightforward to check since $w_1 \circ (w_2 \circ w_3)$ and $w_1 \circ' (w_2 \circ' w_3)$ are always empty unless one of w_1, w_2, w_3 is e.

Next, we note that M is partial functional since $|w_1 \circ w_2| \leq 1$ for all $w_1, w_2 \in W$ by construction, whereas M' is not partial functional since $z, y \in x \circ' v$ but $z \neq y$.

Finally, we claim that $M \twoheadrightarrow M'$, i.e., that there is a surjective bounded morphism from M to M'. Define $f : W \to W'$ by:

$$\begin{array}{ll} f(v_1) = f(v_2) \stackrel{\text{def}}{=} v & f(x_1) = f(x_2) \stackrel{\text{def}}{=} x \\ \multicolumn{2}{c}{f(w) \stackrel{\text{def}}{=} w \qquad (w \in \{e, y, z\})} \end{array}$$

Clearly f is surjective, so it just remains to check the four bounded morphism conditions in Definition 3.4:

1. Trivial, since $E = E' = \{e\}$ and $f(e) = e$.
2. We just check that every membership statement in the definition of $\circ$ maps under f to a corresponding membership statement in the definition of $\circ'$. E.g., since $y \in x_1 \circ v_2$, we need to check that $f(y) \in f(x_1) \circ' f(v_2)$, i.e., $y \in x \circ' v$, which is the case.
3. We need to check that every membership statement $f(w) \in w'_1 \circ w'_2$ in the definition of $\circ'$ can be "traced back" under f to a corresponding membership statement in the definition of $\circ$. E.g., since $f(z) \in x \circ' v$, we need w_1, w_2 such that $z \in w_1 \circ w_2$ and $f(w_1) = x, f(w_2) = v$. By taking, say, $w_1 = x_2$ and $w_2 = v_2$, we are done.
4. Similar to item 3 above, but for membership statements of the form $w'_2 \in f(w) \circ w'_1$. E.g., since $y \in f(v_2) \circ' x$, we need w_1, w_2 such that $w_2 \in v_2 \circ w_1$ and $f(w_1) = x$, $f(w_2) = y$. By taking $w_1 = x_1, w_2 = y$ we are done. □

We remark that there is no *a priori* connection between definability of a property on the one hand, and the existence of complete proof systems for models having the property on the other. In particular, Theorem 3.7 says nothing about the existence of proof theories for BBI that are complete for partial functional models. In fact, Larchey-Wendling and Galmiche showed in [21] that $\mathbf{K}_{\mathrm{BBI}}$ is incomplete for such models. What Theorem 3.7 shows in addition is that, if one were to add (perhaps infinitely many) axioms to $\mathbf{K}_{\mathrm{BBI}}$ so as to obtain a complete system for partial functional models, then provability in this system still would not exclude all models that are *not* partial functional. One can contrast this situation, e.g., with that of $\mathbf{K}_{\mathrm{BBI}}$'s commutativity axiom $A * B \vdash B * A$, which is easily seen to define commutativity and therefore to exclude all non-commutative models.

Theorem 3.8. *Cancellativity is not* BBI*-definable.*

Proof. By Lemma 3.6, it suffices to exhibit a pair of BBI-models M and M' such that M is cancellative, M' is not cancellative and $M \twoheadrightarrow M'$. We define BBI-models $M = \langle W, \circ, E\rangle$ and $M' = \langle W', \circ', E'\rangle$ as follows:

$$\begin{array}{ll} W \stackrel{\text{def}}{=} \{e, v_1, v_2, x, y, z_1, z_2\} & E \stackrel{\text{def}}{=} \{e\} \\ \multicolumn{2}{l}{w \circ e = e \circ w \stackrel{\text{def}}{=} \{w\} \text{ for all } w \in W} \\ x \circ v_1 = v_1 \circ x \stackrel{\text{def}}{=} \{z_1\} & x \circ v_2 = v_2 \circ x \stackrel{\text{def}}{=} \{z_2\} \\ y \circ v_1 = v_1 \circ y \stackrel{\text{def}}{=} \{z_2\} & y \circ v_2 = v_2 \circ y \stackrel{\text{def}}{=} \{z_1\} \end{array}$$

$$\begin{array}{ll} W' \stackrel{\text{def}}{=} \{e, x, v, y, z\} & E' \stackrel{\text{def}}{=} \{e\} \\ \multicolumn{2}{l}{w \circ' e = e \circ' w \stackrel{\text{def}}{=} \{w\} \text{ for all } w \in W'} \\ \multicolumn{2}{l}{v \circ' x = x \circ' v = v \circ' y = y \circ' v \stackrel{\text{def}}{=} \{z\}} \end{array}$$

with $w_1 \circ w_2 = w_1 \circ' w_2 \stackrel{\text{def}}{=} \emptyset$ for all other w_1 and w_2.

First, it is straightforward to verify that M and M' are indeed BBI-models, with associativity holding because $w_1 \circ (w_2 \circ w_3) \neq \emptyset$ implies one of w_1, w_2, w_3 is e (and similarly for $\circ'$).

Next, we note that M is cancellative because, by construction, $w' \in (w \circ w_1) \cap (w \circ w_2)$ implies $w_1 = w_2$. On the other hand, M' is not cancellative, for $z \in (v \circ' x) \cap (v \circ' y)$ but $x \neq y$.

Finally, we need a surjective bounded morphism from M to M'. We define a map $f : W \to W'$ by

$$\begin{array}{ll} f(v_1) = f(v_2) \stackrel{\text{def}}{=} v & f(z_1) = f(z_2) \stackrel{\text{def}}{=} z \\ \multicolumn{2}{c}{f(w) \stackrel{\text{def}}{=} w \qquad (w \in \{e, x, y\})} \end{array}$$

The verification that f is indeed a surjective bounded morphism is similar to that in the proof of Theorem 3.7. □

Notice that the proof of Theorem 3.8 in fact maps a model that is both partial functional and cancellative with a single unit to a non-cancellative model. Thus, it also establishes that neither the class of models that are partial functional *and* cancellative (the "separation algebras" of [12]) nor the subclass of such models having a single unit (the "separation algebras" of [8]) are BBI-definable.

Theorem 3.9. *Disjointness is not* BBI*-definable.*

Proof. By Lemma 3.6, it suffices to exhibit a pair of BBI-models M and M' such that M is disjoint, M' is not and $M \twoheadrightarrow M'$. We define BBI-models $M = \langle W, \circ, E\rangle$ and $M' = \langle W', \circ', E'\rangle$ by:

$$\begin{array}{l} W \stackrel{\text{def}}{=} \{e, x, y\} \qquad E \stackrel{\text{def}}{=} \{e\} \\ w \circ e = e \circ w \stackrel{\text{def}}{=} \{w\} \text{ for all } w \in W \\ x \circ y = y \circ x \stackrel{\text{def}}{=} \{x, y\} \end{array}$$

$$\begin{array}{l} W' \stackrel{\text{def}}{=} \{e, x\} \qquad E' \stackrel{\text{def}}{=} \{e\} \\ w \circ' e = e \circ' w \stackrel{\text{def}}{=} \{w\} \text{ for all } w \in W \\ x \circ' x \stackrel{\text{def}}{=} \{x\} \end{array}$$

with $w_1 \circ w_2 = w_1 \circ' w_2 \stackrel{\text{def}}{=} \emptyset$ for all other w_1 and w_2.

Similar to the previous Theorems 3.7 and 3.8, we can easily verify that M and M' are indeed BBI-models, with M disjoint by construction, whereas M' is not disjoint since $x \neq e$ and $x \circ' x \neq \emptyset$. We define a surjective bounded morphism f from M to M' by

$$f(e) \stackrel{\text{def}}{=} e \qquad f(x) \stackrel{\text{def}}{=} x \qquad f(y) \stackrel{\text{def}}{=} x$$

It just remains to check the bounded morphism conditions, which is similar to the verifications in Theorems 3.7 and 3.8. □

The fact that the single-unit property is not BBI-definable is a straightforward consequence of existing completeness results. We also present a direct proof for pedagogical interest.

Theorem 3.10. *The single-unit property is not* BBI*-definable.*

Proof. The result can be deduced from the completeness result for single-unit BBI-models in [14]. Suppose for contradiction that the single-unit property is definable by the formula A. Then, by completeness, A is provable in $\mathbf{K}_{\mathrm{BBI}}$. Hence, by soundness (Theorem 2.5), A is valid in *all* BBI-models, some of which fail to have the single-unit property. □

Theorem 3.10 can also be shown more directly: we show that the single-unit property is not preserved under the following *disjoint union* construction, which preserves validity.

Definition 3.11 (Disjoint union)**.** Let $M_1 = \langle W_1, \circ_1, E_1\rangle$, $M_2 = \langle W_2, \circ_2, E_2\rangle$ be BBI-models, where W_1 and W_2 are disjoint sets. Then $M_1 \uplus M_2$, the *disjoint union* of M_1 and M_2 is defined as

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

where $\circ_1 \cup \circ_2 : (W_1 \cup W_2) \times (W_1 \cup W_2) \to \mathcal{P}(W_1 \cup W_2)$ is defined as $\circ_i$ on $W_i \times W_i$ and undefined on $W_1 \times W_2$ and $W_2 \times W_1$.

Lemma 3.12. *Let M_1, M_2 be* BBI*-models. Then any* BBI*-formula valid in both M_1 and M_2 is also valid in $M_1 \uplus M_2$.*

Proof. We write $M_1 = \langle W_1, \circ_1, E_1\rangle$ and $M_2 = \langle W_2, \circ_2, E_2\rangle$. Suppose for contradiction that A is valid in M_1 and M_2, but not in $M_1 \uplus M_2$. Thus there exists a valuation ρ and $w \in W_1 \cup W_2$ such that $M_1 \uplus M_2, w \not\models_\rho A$. We show the case where $w \in W_1$; the case $w \in W_2$ is similar. We define a valuation ρ_1 for M_1 by

$$\rho_1(P) \stackrel{\text{def}}{=} \rho(P) \cap M_1$$

To obtain the required contradiction, we claim that $M_1, w \not\models_{\rho_1} A$ (contradicting the supposition that A is valid in M_1). To show this claim, we prove that for all $w \in W_1$, we have $M_1, w \models_{\rho_1} A$ if and only if $M_1 \uplus M_2, w \models_\rho A$. This is easily established by a straightforward structural induction on A, which we omit. □

Lemma 3.13. *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. Similar to the proof of Lemma 3.6. □

Note that it is straightforward to show that if M_1 and M_2 are BBI-models then so is $M_1 \uplus M_2$. (Alternatively, similarly to Lemma 3.6, Lemma 3.13 implies that otherwise BBI-models would be undefinable among all BBI-frames, contradiction.)

Alternative proof of Theorem 3.10. Let $M_1 = \langle \mathbb{N}, +, \{0\}\rangle$ and $M_2 = \langle \mathbb{N}', +', \{0'\}\rangle$ be disjoint, isomorphic copies of the monoid of natural numbers under addition. M_1 and M_2 are both single-unit BBI-models, but $M_1 \uplus M_2$ is not, as its set of units is $\{0, 0'\}$. Thus, by Lemma 3.13, the single-unit property is not BBI-definable. □

We have not yet considered the cross-split property from Definition 3.1. In Section 7, we show that this property is definable in a relatively strong hybrid extension of BBI including a binder (see Proposition 7.3). The complication of expressing the property even in that logic leads us to strongly suspect it is not definable in BBI.

Conjecture 3.14. *The cross-split property is not* BBI*-definable.*

Cross-split is seemingly preserved by bounded morphic images, disjoint unions and by *generated submodels* (cf. [1]). We believe it should be possible to show its undefinability in BBI by employing a model construction based on *ultrafilter extensions* (cf. [1]), but that is beyond the scope of the present paper.

4. HyBBI: a basic hybrid extension of BBI

In this section, we present an extension of BBI, called HyBBI, based upon a simple fragment of *hybrid logic* [1, 2]. This extension allows us to refer to individual elements of the underlying BBI-model (as opposed to sets of elements, as denoted by BBI-formulas) by introducing a second sort of propositional variables called *nominals*. We also introduce a new modality, $@_\ell$, enabling us to evaluate a formula at the world denoted by the nominal ℓ. The additional expressivity of HyBBI enables us to define the separation theory properties shown in the previous section to be undefinable in BBI.

Definition 4.1 (HyBBI-formula)**.** We assume a fixed, denumerably infinite set $\mathcal{N}$ of *nominals*, disjoint from the propositional variables. We write lower case letters j, k, ℓ etc. for nominals to distinguish them from propositional variables. A HyBBI-formula is defined as a BBI-formula (Defn. 2.1), except that (a) any nominal $\ell \in \mathcal{N}$ counts as an atomic HyBBI-formula, and (b) if A is a HyBBI-formula and ℓ a nominal then $@_\ell A$ is a HyBBI-formula.

A HyBBI-formula is said to be *pure* if it contains no propositional (or formula) variables.

Definition 4.2 (HyBBI-validity)**.** A *hybrid valuation* ρ for a BBI-model $M = \langle W, \circ, E\rangle$ extends a standard valuation (see Defn. 2.3) by additionally mapping every nominal $\ell \in \mathcal{N}$ to an element $\rho(\ell) \in W$. Given any hybrid valuation ρ for M, any $w \in W$ and a HyBBI-formula A, we define the forcing relation $M, w \models_\rho A$ by extending the definition of the forcing relation in Defn. 2.3 with the following clauses for nominals and the $@_\ell$ modality:

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

A is then said to be *valid in* M if $M, w \models_\rho A$ for all hybrid valuations ρ and all $w \in W$ (and simply *valid* if it is valid in all BBI-models).

We observe that HyBBI is a *conservative extension* of BBI; that is, every BBI-formula A is valid according to Definition 2.3 if and only if it is valid according to Definition 4.2 (because the forcing relations in the two definition coincide on BBI-formulas). Thus every property of BBI-models definable in BBI, in particular those described in Proposition 3.3, is also definable in HyBBI. However, HyBBI is strictly more expressive than BBI: several properties not definable in BBI become definable in HyBBI.

Theorem 4.3. *The following properties from Definition 3.1 are* HyBBI*-definable via pure formulas:*

$$\begin{array}{rrr} \textit{Functionality:} & @_\ell(j * k) \wedge @_{\ell'}(j * k) \vdash @_\ell \ell' & \text{(pfn)} \\ \textit{Cancellativity:} & \ell * j \wedge \ell * k \vdash @_j k & \text{(cnc)} \\ \textit{Single unit:} & @_{\ell_1}\mathrm{I} \wedge @_{\ell_2}\mathrm{I} \vdash @_{\ell_1}\ell_2 & \text{(su)} \\ \textit{Indivisible units:} & \mathrm{I} \wedge (\ell_1 * \ell_2) \vdash \ell_1 & \text{(iu')} \\ \textit{Disjointness:} & \ell * \ell \vdash \mathrm{I} \wedge \ell & \text{(dis)} \end{array}$$

Proof. We treat each property individually.
Functionality. ($\Leftarrow$) Assume M is partial functional, let ρ be a valuation for M and let $w \in W$. To show that (pfn) is valid in M, we assume that $M, w \models_\rho @_\ell(j * k) \wedge @_{\ell'}(j * k)$, and must show that $M, w \models_\rho @_\ell \ell'$, i.e., that $\rho(\ell) = \rho(\ell')$. By assumption, we have $\rho(\ell) \in \rho(j) \circ \rho(k)$ and $\rho(\ell') \in \rho(j) \circ \rho(k)$. Hence by partial functionality of M we have $\rho(\ell) = \rho(\ell')$ as required.

($\Rightarrow$) Assume that (pfn) is valid in M, and suppose $w', w \in w_1 \circ w_2$. We require to show that $w = w'$. Since (pfn) is valid in M, we have $M, w \models_\rho$ (pfn) for all $w \in W$ and for any hybrid valuation ρ. We define a hybrid valuation ρ for M as follows:

$$\rho(\ell) = w \qquad \rho(\ell') = w' \qquad \rho(j) = w_1 \qquad \rho(k) = w_2$$

Then, showing that $w = w'$ means showing that $M, \rho(\ell) \models_\rho \ell'$, i.e., that $M, w \models_\rho @_\ell \ell'$. As (pfn) is valid in M, it suffices to show that $M, w \models_\rho @_\ell(j * k) \wedge @_{\ell'}(j * k)$. Since $w, w' \in w_1 \circ w_2$ by assumption and $M, w_1 \models_\rho j$ and $M, w_2 \models_\rho k$ by construction, we obtain that $M, w \models_\rho j * k$ and that $M, w' \models_\rho j * k$, from which the result follows.

Cancellativity. ($\Leftarrow$) Assume M is cancellative, let ρ be a valuation for M and let $w \in W$. To show that (cnc) is valid in M, we suppose that $M, w \models_\rho (\ell * j) \wedge (\ell * k)$, and require to show that $M, w \models_\rho @_j k$, i.e., that $\rho(j) = \rho(k)$. That $M, w \models_\rho (\ell * j) \wedge (\ell * k)$ straightforwardly means that $w \in (\rho(\ell) \circ \rho(j)) \cap (\rho(\ell) \circ \rho(k))$. By cancellativity, we thus immediately get that $\rho(j) = \rho(k)$ as required.

($\Rightarrow$) Assume that (cnc) is valid in M, and suppose $w' \in (w \circ w_1) \cap (w \circ w_2)$. We require to show that $w_1 = w_2$. Since (cnc) is valid in M, we have $M, w \models_\rho$ (cnc) for all $w \in W$ and hybrid valuations ρ. We define a hybrid valuation ρ for M as follows:

$$\rho(\ell) = w \qquad \rho(j) = w_1 \qquad \rho(k) = w_2$$

Then by assumption $M, w' \models_\rho (\ell * j) \wedge (\ell * k)$. By validity of (cnc), we deduce that $M, w' \models_\rho @_j k$, hence that $\rho(j) = \rho(k)$, and by construction that $w_1 = w_2$.

Single unit. ($\Leftarrow$) Assume $E = \{e\}$, let ρ be a valuation for M and let $w \in W$. We show (su) is valid. Supposing that $M, w \models_\rho @_{\ell_1}\mathrm{I} \wedge @_{\ell_2}\mathrm{I}$, we have that $\rho(\ell_1), \rho(\ell_2) \in E$. Thus $\rho(\ell_1) = \rho(\ell_2) = e$, which yields $M, w \models_\rho @_{\ell_1}\ell_2$ as required.

($\Rightarrow$) Assume (su) is valid and let $e, e' \in E$. We need to show $e = e'$. Define a valuation ρ for M by $\rho(\ell_1) = e$ and $\rho(\ell_2) = e'$. Thus, to show $e = e'$, it suffices to show $M, w \models_\rho @_{\ell_1}\ell_2$ (for any $w \in W$). Since (su) is valid, it suffices to show that $M, w \models_\rho @_{\ell_1}\mathrm{I} \wedge @_{\ell_2}\mathrm{I}$. This follows from our construction of ρ.

Indivisible units. The equivalence holds by a straightforward modification of the argument for the formula (iu) (see [5]) in Prop. 3.3.

Disjointness. ($\Leftarrow$) Assume the disjointness property, let ρ be a valuation for M and let $w \in W$. To show (dis) is valid, we suppose that $M, w \models_\rho \ell * \ell$ and require to show that $M, w \models_\rho \mathrm{I} \wedge \ell$, i.e., that $w = \rho(\ell)$ and $w \in E$. That $M, w \models_\rho \ell * \ell$ means that $w \in \rho(\ell) \circ \rho(\ell)$. In particular, $\rho(\ell) \circ \rho(\ell) \neq \emptyset$ hence, by disjointness, $\rho(\ell) \in E$. We thus get $w \in \rho(\ell) \circ \rho(\ell) = \{\rho(\ell)\}$ hence $w = \rho(\ell)$ and also $w \in E$ as required.

($\Rightarrow$) Assume that (dis) is valid in M, and suppose that $w \circ w \neq \emptyset$. We require to show that $w \in E$. Let $w' \in w \circ w$ and ρ be such that $\rho(\ell) = w$. By construction, we have that $M, w' \models_\rho \ell * \ell$, hence by validity of (dis) we get $M, w' \models_\rho \mathrm{I} \wedge \ell$, i.e., $w' = \rho(\ell) = w$ and $w' \in E$, hence $w \in E$ as required. ☐

Corollary 4.4. *Any separation theory from Def. 3.1 not including the cross-split property is* HyBBI*-definable by pure formulas.*

Proof. Follows by taking as the defining formula the conjunction of the relevant formulas from Theorem 4.3 and Proposition 3.3. ☐

As is also the case for BBI (see Conjecture 3.14), we suspect (but do not know) that the cross-split property is not definable even in HyBBI. This is because a straightforward translation of the property into HyBBI would require some way of binding or existentially quantifying nominals, which is not provided by pure nominals or the $@_\ell$ modality. In Section 7 we add a binder to HyBBI, which enables us to express cross-split.

5. An axiomatic proof system for HyBBI

Here, we present a Hilbert-style axiomatic proof system for HyBBI, and show that it is sound with respect to validity in BBI-models; we examine questions of completeness in Section 6.

In the rest of the paper, it will often be convenient to reason in terms of $-\circledast$, the De Morgan dual of $-\!*$ defined as

$$A -\circledast B \stackrel{\text{def}}{=} \neg(A -\!* \neg B)\ .$$

Unpacking the negations and $-\!*$ yields the following forcing relation for $-\circledast$:

$$\begin{array}{lcl} M, w \models_\rho A_1 -\circledast A_2 & \Leftrightarrow & \exists w', w'' \in W.\ w'' \in w \circ w' \text{ and} \\ & & M, w' \models_\rho A_1 \text{ and } M, w'' \models_\rho A_2 \end{array}$$

(Using $-\circledast$ rather than $-\!*$ means that we deal exclusively with "diamond-type" modalities with an existential interpretation, which frequently makes life easier in our technical developments.)

Definition 5.1. We define $\mathbf{K}_{\mathrm{HyBBI}}$ to be the proof system obtained by extending the proof system $\mathbf{K}_{\mathrm{BBI}}$ (see Definition 2.4) with the axioms and rules for nominals and @ given in Figure 1.

$\mathbf{K}_{\mathrm{HyBBI}}$ is based on the proof system for basic hybrid logic in [1]. We have chosen the axioms and rules so as to make the subsequent completeness proof as simple as possible.

Proposition 5.2. *Any* $\mathbf{K}_{\mathrm{HyBBI}}$*-provable formula is valid.*

Proof. Let $M = \langle W, \circ, E\rangle$ be a BBI-model. Then, assuming A is $\mathbf{K}_{\mathrm{HyBBI}}$-provable, we must show that A is valid in M. It suffices to show that all axioms of $\mathbf{K}_{\mathrm{HyBBI}}$ are valid and that validity

($K_@$)	$@_\ell(A \to B) \vdash @_\ell A \to @_\ell B$	(Nom)	$@_\ell k \wedge @_k A \vdash @_\ell A$
(Self-dual)	$@_\ell A \vdash \neg @_\ell \neg A$ and $\neg @_\ell \neg A \vdash @_\ell A$	(Agree)	$@_k @_\ell A \vdash @_\ell A$ and $@_\ell A \vdash @_k @_\ell A$
(@-intro)	$\ell \wedge A \vdash @_\ell A$	(Bridge $*$)	$@_\ell(k * k') \wedge @_k A \wedge @_{k'} B \vdash @_\ell(A * B)$
(Refl)	$\vdash @_\ell \ell$	(Bridge $-\!\circledast$)	$@_\ell(k -\!\circledast\, k') \wedge @_k A \wedge @_{k'} B \vdash @_\ell(A -\!\circledast\, B)$
(Sym)	$@_\ell k \vdash @_k \ell$		

$$\frac{\vdash A}{\vdash A[\theta]}\ \text{(Subst)} \qquad \frac{\vdash A}{\vdash @_\ell A}\ \text{(Gen)} \qquad \frac{@_\ell(k * k') \wedge @_k A \wedge @_{k'} B \vdash C}{@_\ell(A * B) \vdash C}\ \begin{array}{l} k, k' \text{ not in } A, B, C \text{ or } \{\ell\} \\ \text{(Paste } *) \end{array}$$

$$\frac{\ell \vdash A}{\vdash A}\ \ell \text{ not in } A \text{ (Name)} \qquad \frac{@_\ell(k -\!\circledast\, k') \wedge @_k A \wedge @_{k'} B \vdash C}{@_\ell(A -\!\circledast\, B) \vdash C}\ \begin{array}{l} k, k' \text{ not in } A, B, C \text{ or } \{\ell\} \\ \text{(Paste } -\!\circledast) \end{array}$$

Figure 1. Rules and axioms for nominals in $\mathbf{K}_{\mathrm{HyBBI}}$. Note that θ in the the rule (Subst) is a substitution of nominals for nominals.

is preserved by every proof rule of $\mathbf{K}_{\mathrm{HyBBI}}$. This is a straightforward verification for all the rules and axioms except the two "bridge" axioms and the two "paste" rules. We just show the cases of (Bridge $*$) and (Paste $-\!\circledast$) here, as the others are similar.

Case (Bridge $*$). Let ρ be a valuation for M and let $w \in W$. Suppose $M, w \models_\rho @_\ell(k * k') \wedge @_k A \wedge @_{k'} B$. Then we have $M, \rho(\ell) \models_\rho k * k'$ and $M, \rho(k) \models_\rho A$ and $M, \rho(k') \models_\rho B$. The first of these means that $\rho(\ell) \in \rho(k) \circ \rho(k')$. Thus $M, \rho(\ell) \models_\rho A * B$, i.e. $M, w \models_\rho @_\ell(A * B)$ as required.

Case (Paste $-\!\circledast$). Let ρ be a valuation for M and let $w \in W$. Supposing the premise of the rule is valid in M and $M, w \models_\rho @_\ell(A -\!\circledast\, B)$, we have to show $M, w \models_\rho C$. We have $M, \rho(\ell) \models_\rho A -\!\circledast\, B$ which means that there exist $w', w'' \in W$ such that $w'' \in \rho(\ell) \circ w'$ and $M, w' \models_\rho A$ and $M, w'' \models_\rho B$. Now define the valuation $\rho' = \rho[k \mapsto w', k' \mapsto w'']$, where k and k' are the fresh nominals appearing in the premise of the rule. By construction, and using the fact that ρ and ρ' agree except possibly on the fresh nominals k, k', we have $\rho'(k') \in \rho'(\ell) \circ \rho'(k)$ and $M, \rho'(k) \models_{\rho'} A$ and $M, \rho'(k') \models_{\rho'} B$. The first of these gives us $M, \rho'(\ell) \models_{\rho'} k -\!\circledast\, k'$. Putting everything together, we obtain

$$M, w \models_{\rho'} @_\ell(k -\!\circledast\, k') \wedge @_k A \wedge @_{k'} B$$

Since the premise of the rule is valid by assumption, we obtain $M, w \models_{\rho'} C$. Again, since ρ and ρ' agree except on k, k', which do not appear in C, we thus obtain $M, w \models_\rho C$ as required. □

The following example illustrates how the hybrid axioms and rules are used in practice.

Example 5.3. The HyBBI-formula $\top * (\mathrm{I} \wedge (\ell -\!\circledast\, A)) \vdash @_\ell A$ is provable in HyBBI.

(Intuitively, the LHS of this formula says that from the current world w one may find a unit e such that $w \circ e$ is defined and $e \circ \rho(\ell)$ is defined and satisfies A. This implies that $\rho(\ell)$ itself satisfies A.)

Proof. First, we show that the following formula is provable:

$$A * @_\ell B \vdash @_\ell B \tag{1}$$

Let j, k, k' be fresh nominals not occurring in A, B or $\{\ell\}$. We have $@_{k'} @_\ell B \vdash @_\ell B$ an instance of (Agree). By weakening for $\wedge$, we thus obtain

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

Using the fact that k, k' are fresh, we can apply the rule (Paste $*$) to derive $@_j(A * @_\ell B) \vdash @_\ell B$. Since the formula

$$j \wedge (A * @_\ell B) \vdash @_j(A * @_\ell B)$$

is an instance of (@-intro), we obtain $j \wedge (A * @_\ell B) \vdash @_\ell B$ by transitivity, and thus easily we have $j \vdash (A * @_\ell B) \to @_\ell B$. Since j is fresh, we obtain $A * @_\ell B \vdash @_\ell B$ by applying (Name).

Next, we show that the following formula is provable:

$$\mathrm{I} \wedge (\ell -\!\circledast\, A) \vdash @_\ell A \tag{2}$$

We have $\ell \wedge A \vdash @_\ell A$ an instance of (@-intro), whence by contraposition and use of (Self-dual) we obtain $\ell \wedge @_\ell \neg A \vdash \neg A$. Now, since $\ell * @_\ell \neg A \vdash @_\ell \neg A$ is provable as an instance of (1) above, we obtain $\ell \wedge (\ell * @_\ell \neg A) \vdash \neg A$. By straightforward manipulations of plain BBI we can prove

$$(\mathrm{I} \wedge @_\ell \neg A) * \ell \vdash \ell \wedge (\ell * @_\ell \neg A)$$

Thus, by transitivity, we obtain $(\mathrm{I} \wedge @_\ell \neg A) * \ell \vdash \neg A$. This rearranges to $\mathrm{I} \wedge @_\ell \neg A \vdash \ell -\!* \neg A$ and then to $\mathrm{I} \wedge (\ell -\!\circledast\, A) \vdash \neg @_\ell \neg A$, which yields the required (2) by using (Self-dual).

Now we can supply the required derivation of the formula in the proposition. We can derive $\top * (\mathrm{I} \wedge (\ell -\!\circledast\, A)) \vdash \top * @_\ell A$ using (2). As $\top * @_\ell A \vdash @_\ell A$ is an instance of (1), we have $\top * (\mathrm{I} \wedge (\ell -\!\circledast\, A)) \vdash @_\ell A$ by transitivity as required. □

Interestingly, the converse of the formula in Example 5.3, that is $@_\ell A \vdash \top * (\mathrm{I} \wedge (\ell -\!\circledast\, A))$, is not generally valid, but is valid in all single-unit models (and thus in such models $@_\ell$ is definable already using plain nominals). This is because, in models with a single unit e, the composition $w \circ e$ must be defined for *all* $w \in W$, whereas this might fail in models with multiple units. The $@_\ell$ modality enables us to talk about worlds not accessible from the current world via the I, $*$ and $-\!*$ modalities; but in single-unit models, there are no such worlds.

6. Completeness for pure extensions of $\mathbf{K}_{\mathrm{HyBBI}}$

In this section, we show a parametric completeness result: any extension of $\mathbf{K}_{\mathrm{HyBBI}}$ with a set of pure axioms Ax is complete with respect to the class of BBI-models satisfying Ax. In particular, we can obtain complete proof systems for many separation theories simply by adding the axioms defining the theory to $\mathbf{K}_{\mathrm{HyBBI}}$.

We follow the basic structure of the corresponding completeness proof for normal hybrid logic in [1], which shows that any consistent set of formulas has a model based upon "named" maximal consistent sets. Compared to this proof, we encounter two additional difficulties. First, we have to work (at least implicitly) with the residuated binary connectives $*$ and $-\!*$, as opposed to a single diamond modality and its De Morgan dual. Second, we have to show that the model we construct is a BBI-model, as opposed to an unrestricted frame.

Definition 6.1 (Consistent set)**.** Let $\mathcal{K}$ be any proof system. A set Γ of formulas is said to be *$\mathcal{K}$-inconsistent* if there are formulas $A_1, \ldots, A_n \in \Gamma$ such that $A_1 \wedge \ldots \wedge A_n \vdash \bot$ is provable in $\mathcal{K}$. Otherwise Γ is called *$\mathcal{K}$-consistent*.

Definition 6.2 (Maximal consistent set)**.** Let $\mathcal{K}$ be any proof system. A set Γ of formulas is *maximal $\mathcal{K}$-consistent* (and we call Γ a $\mathcal{K}$-MCS) if Γ is $\mathcal{K}$-consistent and any $\Delta \supset \Gamma$ is $\mathcal{K}$-inconsistent.

In the rest of this section, whenever we talk about MCSs, consistency and provability, we *always* mean with reference to a fixed but arbitrary extension $\mathbf{K}_{\mathrm{HyBBI}} + \mathrm{Ax}$ of $\mathbf{K}_{\mathrm{HyBBI}}$ with a finite set Ax of axioms expressed as pure formulas.

We begin by recalling some basic facts about MCSs.

Lemma 6.3. *For any MCS Γ and formulas A, B, we have*

1. *if $A \vdash B$ is provable and $A \in \Gamma$ then $B \in \Gamma$;*
2. *$\top \in \Gamma$ and $\bot \notin \Gamma$;*
3. *either $A \in \Gamma$ or $\neg A \in \Gamma$;*
4. *$A \wedge B \in \Gamma$ iff $A, B \in \Gamma$;*
5. *$A \vee B \in \Gamma$ iff $A \in \Gamma$ or $B \in \Gamma$.*

Proof. Standard in all cases. □

In the following, we do not refer explicitly to uses of Lemma 6.3, as we use it so frequently.

Definition 6.4 (Named / pasted MCS)**.** An MCS Γ is said to be *named* if there is at least one nominal $\ell \in \Gamma$; any such ℓ is called a *name for* Γ.
Γ is said to be *pasted* if

- $@_\ell(A * B) \in \Gamma$ implies $@_\ell(\ell_1 * \ell_2) \wedge @_{\ell_1} A \wedge @_{\ell_2} B \in \Gamma$ for some ℓ_1, ℓ_2, and
- $@_\ell(A \multimap\!\!\circledast\, B) \in \Gamma$ implies $@_\ell(\ell_1 \multimap\!\!\circledast\, \ell_2) \wedge @_{\ell_1} A \wedge @_{\ell_2} B \in \Gamma$ for some ℓ_1, ℓ_2.

Lemma 6.5 (Extended Lindenbaum Lemma)**.** *Let $\mathcal{N}'$ be a countably infinite set of nominals disjoint from $\mathcal{N}$. If Δ is a consistent set of formulas then there is a named, pasted MCS Δ^+ (of formulas in the extended nominal language of $\mathcal{N} \cup \mathcal{N}'$) such that $\Delta \subseteq \Delta^+$.*

Proof. Let $k_0, k_1, k_2 \ldots$ be an enumeration of $\mathcal{N}'$, and let $B_1, B_2, B_3 \ldots$ be an enumeration of all formulas in the extended language given by $\mathcal{N} \cup \mathcal{N}'$. Given a consistent set Δ of formulas, we define a sequence $(\Delta_i)_{i \geq 0}$ of sets of formulas as follows:

- $\Delta_0 \stackrel{\text{def}}{=} \Delta \cup \{k\}$;
- if $\Delta_i \cup \{B_i\}$ is inconsistent then $\Delta_{i+1} \stackrel{\text{def}}{=} \Delta_i$;
- if $\Delta_i \cup \{B_i\}$ is consistent and the formula B_i is not of the form $@_\ell(A * B)$ or $@_\ell(A \multimap\!\!\circledast\, B)$, then $\Delta_{i+1} \stackrel{\text{def}}{=} \Delta_i \cup \{B_i\}$;
- if $\Delta_i \cup \{B_i\}$ is consistent and $B_i = @_\ell(A * B)$ then
$$\Delta_{i+1} \stackrel{\text{def}}{=} \Delta_i \cup \{B_i\} \cup \{@_\ell(k * k') \wedge @_k A \wedge @_{k'} B\}$$
- if $\Delta_i \cup \{B_i\}$ is consistent and $B_i = @_\ell(A \multimap\!\!\circledast\, B)$ then
$$\Delta_{i+1} \stackrel{\text{def}}{=} \Delta_i \cup \{B_i\} \cup \{@_\ell(k \multimap\!\!\circledast\, k') \wedge @_k A \wedge @_{k'} B\}$$

where k, k' in the first and last two clauses are fresh nominals from our enumeration of $\mathcal{N}'$. We claim that $\Delta^+ \stackrel{\text{def}}{=} \bigcup_{i \geq 0} \Delta_i$ is a named, pasted MCS.

First, to see that Δ^+ is consistent, it suffices to show that Δ_i is consistent for all i. We proceed by induction on i. In the case $i = 0$, we must show that $\Delta \cup \{k\}$ is consistent. If not, then there are formulas $A_1, \ldots, A_n \in \Delta$ such that, writing $A = \bigwedge_{1 \leq i \leq n} A_i$, we have $A \wedge k \vdash \bot$ provable. Thus $k \vdash \neg A$ is provable, whence by the rule (Name) we have $\vdash \neg A$ provable and thus $A \vdash \bot$ provable, contradicting the consistency of Δ. Now, assuming that Δ_i is consistent, we must show that Δ_{i+1} is consistent. This is immediate by induction hypothesis except in the case that $B_i = @_\ell(A * B)$ or $B_i = @_\ell(A \multimap\!\!\circledast\, B)$. We show the case $B_i = @_\ell(A * B)$. In this case, assume for contradiction that there are $A_1, \ldots, A_n \in \Delta_i$ such that, writing $A = \bigwedge_{1 \leq i \leq n} A_i$, the following is provable:

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

Thus we can also prove

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

Since k, k' are fresh nominals, we obtain by applying (Paste $*$):

$$@_\ell(A * B) \vdash \neg A \vee \neg @_\ell(A * B)$$

Thus we obtain $A \wedge @_\ell(A * B) \vdash \bot$, contradicting the assumed consistency of $\Delta_i \cup \{B_i\}$. The case $B_i = A \multimap\!\!\circledast\, B$ is similar, using the rule (Paste $\multimap\!\!\circledast$).

Next, we must show that Δ^+ is maximal. Suppose that for some formula A, we have $\Delta^+ \cup \{A\}$ consistent but $A \notin \Delta^+$. Note that A appears in our enumeration as B_i say, so by construction it must be that $\Delta_i \cup \{A\}$ is inconsistent (otherwise $A \in \Delta_{i+1} \subseteq \Delta^+$). But then $\Delta^+ \cup \{A\}$ is inconsistent, contradiction.

Next, to see that Δ^+ is named, observe that $k \in \Delta_0 \subseteq \Delta^+$, for some nominal k, by construction.

Finally, we show Δ^+ is pasted. First, suppose $@_\ell(A{*}B) \in \Delta^+$. Note that $@_\ell(A * B)$ appears as some B_i in our enumeration. Now every finite subset of an MCS is consistent, so $\Delta_i \cup \{B_i\}$ must be consistent. Thus, by construction, we have

$$@_\ell(k * k') \wedge @_k A \wedge @_{k'} B \in \Delta_{i+1} \subseteq \Delta^+$$

as required. For similar reasons, whenever $@_\ell(A \multimap\!\!\circledast\, B) \in \Delta^+$ we have $@_\ell(k \multimap\!\!\circledast\, k') \wedge @_k A \wedge @_{k'} B \in \Delta^+$. □

In the following, we define a *named set yielded by* Γ to be any set of formulas $\{A \mid @_\ell A \in \Gamma\}$ for some nominal ℓ.

Lemma 6.6. *Let Γ be an MCS, and let $\Delta_\ell \stackrel{\text{def}}{=} \{A \mid @_\ell A \in \Gamma\}$ be the named set yielded by Γ for each nominal ℓ. Then the following hold for all nominals ℓ, k:*

1. *Δ_ℓ is an MCS containing ℓ;*
2. *if $\ell \in \Delta_k$ then $\Delta_k = \Delta_\ell$;*
3. *$@_\ell A \in \Delta_k$ iff $@_\ell A \in \Gamma$;*
4. *if ℓ is a name for Γ then $\Gamma = \Delta_\ell$.*

Proof. The proof of the analogous result for normal hybrid logic, stated as Lemma 7.24 in [1], suffices for our setting. □

Definition 6.7. A BBI-model $\langle W, \circ, E\rangle$ is *named by* the hybrid valuation ρ if for all $w \in W$ there is an $\ell \in \mathcal{N}$ with $\rho(\ell) = w$.

Definition 6.8. Let Γ be a named, pasted MCS. Then the *named model yielded by* Γ is defined as $M^\Gamma \stackrel{\text{def}}{=} \langle W^\Gamma, \circ^\Gamma, E^\Gamma\rangle$, where:

1. W^Γ is the set of all named sets yielded by Γ;
2. $\Delta_1 \circ^\Gamma \Delta_2 \stackrel{\text{def}}{=} \{\Delta \mid A_1 \in \Delta_1, A_2 \in \Delta_2 \text{ implies } A_1 * A_2 \in \Delta\}$;
3. $E^\Gamma \stackrel{\text{def}}{=} \{\Delta \mid \mathrm{I} \in \Delta\}$.

The *canonical valuation* ρ^Γ for M^Γ is defined by

$$\begin{array}{rcll} \rho^\Gamma(P) & \stackrel{\text{def}}{=} & \{\Delta \mid P \in \Delta\} & P \text{ a proposition} \\ \rho^\Gamma(\ell) & \stackrel{\text{def}}{=} & \{A \mid @_\ell A \in \Gamma\} & \ell \text{ a nominal} \end{array}$$

We show that M^Γ is indeed a BBI-model in Lemma 6.13 (but require for the intermediate results only that M^Γ is a BBI-frame). We observe that M^Γ is indeed named by ρ^Γ: for any $\Delta \in W^\Gamma$ we have $\Delta = \{A \mid @_\ell A \in \Gamma\}$ for some ℓ, whence $\rho^\Gamma(\ell) = \Delta$.

Lemma 6.9 (Existence Lemma for $*$)**.** *For any $\Delta \in W^\Gamma$, if $A_1 * A_2 \in \Delta$ then there exist $\Delta_1, \Delta_2 \in W^\Gamma$ such that $\Delta \in \Delta_1 \circ^\Gamma \Delta_2$ and $A_1 \in \Delta_1$, $A_2 \in \Delta_2$.*

Proof. Let $A_1 * A_2 \in \Delta$. We have $\Delta = \{A \mid @_\ell A \in \Gamma\}$ for some nominal ℓ. Thus $@_\ell(A_1 * A_2) \in \Gamma$. As Γ is pasted, we have nominals ℓ_1, ℓ_2 such that $@_\ell(\ell_1 * \ell_2) \wedge @_{\ell_1} A_1 \wedge @_{\ell_2} A_2 \in \Gamma$. Thus $A_1 \in \Delta_1$ and $A_2 \in \Delta_2$, where $\Delta_1 = \{A \mid @_{\ell_1} A \in \Gamma\}$ and $\Delta_2 = \{A \mid @_{\ell_2} A \in \Gamma\}$ are named sets yielded by Γ.

It just remains to show that $\Delta \in \Delta_1 \circ^\Gamma \Delta_2$. Let $B_1 \in \Delta_1$, $B_2 \in \Delta_2$. By definition, $@_{\ell_1} B_1 \in \Gamma$ and $@_{\ell_2} B_2 \in \Gamma$. As MCSs are closed under provability and conjunction, we have $@_\ell(\ell_1 * \ell_2) \wedge @_{\ell_1} B_1 \wedge @_{\ell_2} B_2 \in \Gamma$. Thus, using the rule (Bridge $*$), we have $@_\ell(B_1 * B_2) \in \Gamma$. Thus $B_1 * B_2 \in \Delta$ as required. □

Lemma 6.10. *$\Delta \in \Delta_1 \circ^\Gamma \Delta_2$ if and only if for all formulas A and B, $A \in \Delta_2$ and $B \in \Delta$ implies $A \multimap\!\!\circledast\, B \in \Delta_1$.*

Proof. We show each direction separately, making use of the fact that $\Delta, \Delta_1, \Delta_2$ are MCSs by part 1 of Lemma 6.6.

($\Leftarrow$) Assume the right-hand side of the implication and let $A_1 \in \Delta_1$ and $A_2 \in \Delta_2$. We must show $A_1 * A_2 \in \Delta$. Suppose for contradiction that $A_1 * A_2 \notin \Delta$. Since Δ is an MCS, $\neg(A_1 * A_2) \in \Delta$. By assumption, $A_2 \multimap\!\!\circledast\, \neg(A_1 * A_2) \in \Delta_1$, i.e. $\neg(A_2 \mathrel{-\!\!*} \neg\neg(A_1 * A_2)) \in \Delta_1$. As Δ_1 is an MCS, we have $A_1 \wedge \neg(A_2 \mathrel{-\!\!*} (A_1 * A_2)) \in \Delta_1$. But $A_1 \vdash A_2 \mathrel{-\!\!*} (A_1 * A_2)$ is provable, hence so is $A_1 \wedge \neg(A_2 \mathrel{-\!\!*} (A_1 * A_2)) \vdash \bot$. This contradicts the consistency of Δ_1. Hence $A_1 * A_2 \in \Delta$ as required.

($\Rightarrow$) Let $A \in \Delta_2$, $B \in \Delta$ and suppose for contradiction that $A \multimap\!\!\circledast\, B \notin \Delta_1$. As Δ_1 is an MCS, we have $A \mathrel{-\!\!*} \neg B \in \Delta_1$, so by the main assumption $(A \mathrel{-\!\!*} \neg B) * A \in \Delta$. As Δ is an MCS and $(A \mathrel{-\!\!*} \neg B) * A \vdash \neg B$ is provable, $\neg B \in \Delta$. This contradicts the consistency of Δ, so $A \multimap\!\!\circledast\, B \in \Delta_1$ as required. □

Lemma 6.11 (Existence Lemma for $\mathrel{-\!\!*}$)**.** *For any $\Delta \in W^\Gamma$, if $A_1 \multimap\!\!\circledast\, A_2 \in \Delta$ then there exist $\Delta', \Delta'' \in W^\Gamma$ such that $\Delta'' \in \Delta \circ^\Gamma \Delta'$ and $A_1 \in \Delta'$, $A_2 \in \Delta''$.*

Proof. We have $\Delta = \{A \mid @_\ell A \in \Gamma\}$ for some nominal ℓ. Since $A_1 \multimap\!\!\circledast\, A_2 \in \Delta$ by assumption, $@_\ell(A_1 \multimap\!\!\circledast\, A_2) \in \Gamma$. As Γ is pasted, we have $@_\ell(\ell_1 \multimap\!\!\circledast\, \ell_2) \wedge @_{\ell_1} A_1 \wedge @_{\ell_2} A_2 \in \Gamma$ for some ℓ_1, ℓ_2. We obtain named sets $\Delta' = \{A \mid @_{\ell_1} A \in \Gamma\}$ and $\Delta'' = \{A \mid @_{\ell_2} A \in \Gamma\}$ yielded by Γ with $A_1 \in \Delta'$ and $A_2 \in \Delta''$.

It remains to show that $\Delta'' \in \Delta \circ^\Gamma \Delta'$. By Lemma 6.10, it suffices to show that $A \in \Delta'$ and $B \in \Delta''$ implies $A \multimap\!\!\circledast\, B \in \Delta$. Supposing $A \in \Delta', B \in \Delta''$, we have $@_{\ell_1} A \in \Gamma$ and $@_{\ell_2} B \in \Gamma$. Thus we obtain $@_\ell(\ell_1 \multimap\!\!\circledast\, \ell_2) \wedge @_{\ell_1} A \wedge @_{\ell_2} B \in \Gamma$. Since Γ is an MCS it is closed under the rule (Bridge $\multimap\!\!\circledast$), and it follows that $@_\ell(A \multimap\!\!\circledast\, B) \in \Gamma$. Thus $A \multimap\!\!\circledast\, B \in \Delta$ as required. □

Lemma 6.12 (Truth Lemma)**.** *For any HyBBI-formula A and $\Delta \in W^\Gamma$, we have $M^\Gamma, \Delta \models_{\rho^\Gamma} A$ if and only if $A \in \Delta$.*

Proof. By structural induction on A. We omit the cases for the classical connectives, as these are straightforward by induction hypothesis, using the properties of MCSs and the fact that any named set yielded by Γ is an MCS (see part 1 of Lemma 6.6).

Case $A = P$. Using the definition of ρ^Γ, we have as required:

$$M^\Gamma, \Delta \models_{\rho^\Gamma} P \;\Leftrightarrow\; \Delta \in \rho^\Gamma(P) \;\Leftrightarrow\; P \in \Delta$$

Case $A = \ell$. Using the definition of ρ^Γ, we have

$$M^\Gamma, \Delta \models_{\rho^\Gamma} \ell \;\Leftrightarrow\; \Delta = \rho^\Gamma(\ell) \;\Leftrightarrow\; \Delta = \{A \mid @_\ell A \in \Gamma\}$$

Now, going from left to right, we have $\Delta = \{A \mid @_\ell A \in \Gamma\}$ and thus $\ell \in \Delta$ by part 1 of Lemma 6.6. Conversely, assuming $\ell \in \Delta$, we have that $\Delta = \{A \mid @_k A \in \Gamma\}$ for some k, and by part 2 of Lemma 6.6 we obtain $\Delta = \{A \mid @_\ell A \in \Gamma\}$ as required.

Case $A = \mathrm{I}$. Using the definition of E^Γ, we easily have as required:

$$M^\Gamma, \Delta \models_{\rho^\Gamma} \mathrm{I} \;\Leftrightarrow\; \Delta \in E^c \;\Leftrightarrow\; \mathrm{I} \in \Delta$$

Case $A = A_1 * A_2$. Using the induction hypothesis, we have:

$$\begin{array}{ll} & M^\Gamma, \Delta \models_{\rho^\Gamma} A_1 * A_2 \\ \Leftrightarrow & \Delta \in \Delta_1 \circ^\Gamma \Delta_2 \text{ and } M^\Gamma, \Delta_1 \models_{\rho^\Gamma} A_1 \text{ and } M^\Gamma, \Delta_2 \models_{\rho^\Gamma} A_2 \\ \Leftrightarrow & \Delta \in \Delta_1 \circ^\Gamma \Delta_2 \text{ and } A_1 \in \Delta_1 \text{ and } A_2 \in \Delta_2 \end{array}$$

Going from left to right, we immediately get $A_1 * A_2 \in \Delta$ as required from the definition of $\circ^\Gamma$. Going from right to left, we have $A_1 * A_2 \in \Delta$ and must construct the required named sets Δ_1, Δ_2 yielded by Γ satisfying the statement above. This is precisely guaranteed by our Existence Lemma for $*$ (Lemma 6.9).

Case $A = A_1 \mathrel{-\!\!*} A_2$. Using the induction hypothesis for A_1 and A_2, we have:

$$\begin{array}{ll} & M^\Gamma, \Delta \models_{\rho^\Gamma} A_1 \mathrel{-\!\!*} A_2 \\ \Leftrightarrow & \forall \Delta', \Delta''.\ \Delta'' \in \Delta \circ^\Gamma \Delta' \text{ and } M^\Gamma, \Delta' \models_{\rho^\Gamma} A_1 \text{ implies} \\ & M^\Gamma, \Delta'' \models_{\rho^\Gamma} A_2 \\ \Leftrightarrow & \forall \Delta', \Delta''.\ \Delta'' \in \Delta \circ^\Gamma \Delta' \text{ and } A_1 \in \Delta' \text{ implies } A_2 \in \Delta'' \end{array}$$

Going from right to left, assume that $A_1 \mathrel{-\!\!*} A_2 \in \Delta$, $A_1 \in \Delta'$ and $\Delta'' \in \Delta \circ^\Gamma \Delta'$. By the definition of $\circ^\Gamma$, we have $(A_1 \mathrel{-\!\!*} A_2) * A_1 \in \Delta''$, whence we obtain $A_2 \in \Delta''$ as required by modus ponens.

Going from left to right, we must show that $A_1 \mathrel{-\!\!*} A_2 \in \Delta$ given the above implication. We show the contrapositive. Assume that $A_1 \mathrel{-\!\!*} A_2 \notin \Delta$, i.e. $\neg(A_1 \mathrel{-\!\!*} A_2) \in \Delta$. We must construct named sets Δ', Δ'' yielded by Γ, with $\Delta'' \in \Delta \circ^\Gamma \Delta'$ and $A_1 \in \Delta'$ but $A_2 \notin \Delta''$, i.e. $\neg A_2 \in \Delta$. This is provided by our Existence Lemma for $\mathrel{-\!\!*}$ (Lemma 6.11).

Case $A = @_\ell B$. Using the induction hypothesis for B, we have:

$$\begin{array}{lll} M^\Gamma, \Delta \models_{\rho^\Gamma} @_\ell B & \Leftrightarrow & M^\Gamma, \rho^\Gamma(\ell) \models_{\rho^\Gamma} B \\ & \Leftrightarrow & B \in \rho^\Gamma(\ell) \\ & \Leftrightarrow & B \in \{A \mid @_\ell A \in \Gamma\} \\ & \Leftrightarrow & @_\ell B \in \Gamma \end{array}$$

Now, using part 3 of Lemma 6.6, we have that $@_\ell B \in \Gamma$ if and only if $@_\ell B \in \Delta$. This completes the case, and the proof. □

Lemma 6.13. *Let $M^\Gamma = \langle W^\Gamma, \circ^\Gamma, E^\Gamma \rangle$ be the named model yielded by the named, pasted MCS Γ. Then M^Γ is a BBI-model.*

Proof. We must show that M^Γ satisfies the axioms in Defn. 2.2.

Commutativity. It suffices to show that $\Delta_1 \circ^\Gamma \Delta_2 \subseteq \Delta_2 \circ^\Gamma \Delta_1$. Let $\Delta \in \Delta_1 \circ^\Gamma \Delta_2$, and suppose $A_1 \in \Delta_1, A_2 \in \Delta_2$. To show $\Delta \in \Delta_2 \circ^\Gamma \Delta_1$, we have to show $A_2 * A_1 \in \Delta$. As $\Delta \in \Delta_1 \circ^\Gamma \Delta_2$, we have $A_1 * A_2 \in \Delta$. As MCSs are closed under modus ponens and $A_1 * A_2 \vdash A_2 * A_1$ is provable, we have $A_2 * A_1 \in \Delta$.

Associativity. It suffices by commutativity to show $\Delta_1 \circ^\Gamma (\Delta_2 \circ^\Gamma \Delta_3) \subseteq (\Delta_1 \circ^\Gamma \Delta_2) \circ^\Gamma \Delta_3$. Assume that $\Delta \in \Delta_1 \circ^\Gamma (\Delta_2 \circ^\Gamma \Delta_3)$, which means that for some $\Delta' \in \Delta_2 \circ^\Gamma \Delta_3$ we have $\Delta \in \Delta_1 \circ^\Gamma \Delta'$. Using part 1 of Lemma 6.6, we have ℓ_1, ℓ_2, ℓ_3 such that $\ell_i \in \Delta_i$ for each $i \in \{1, 2, 3\}$. As $\Delta' \in \Delta_2 \circ^\Gamma \Delta_3$, we have $\ell_2 * \ell_3 \in \Delta'$. Thus, as $\Delta \in \Delta_1 \circ^\Gamma \Delta'$, we have $\ell_1 * (\ell_2 * \ell_3) \in \Delta$. By applying associativity, $\ell_1 * (\ell_2 * \ell_3) \vdash (\ell_1 * \ell_2) * \ell_3$ is provable, so $(\ell_1 * \ell_2) * \ell_3 \in \Delta$. By two applications of the Existence Lemma for $*$ (Lemma 6.9) we obtain named sets $\Sigma_1, \Sigma_2, \Sigma_3, \Delta'' \in W^\Gamma$ such that $\ell_i \in \Sigma_i$ for each $i \in \{1, 2, 3\}$, and $\Delta \in \Delta'' \circ^\Gamma \Sigma_3$

and $\Delta'' \in \Sigma_1 \circ^\Gamma \Sigma_2$. By part 2 of Lemma 6.6, $\Sigma_i = \Delta_i$ for each $i \in \{1,2,3\}$. Hence $\Delta \in (\Delta_1 \circ^\Gamma \Delta_2) \circ^\Gamma \Delta_3$ as required.

Unit law. We must show that $E^\Gamma \circ^\Gamma \Delta = \{\Delta\}$ for any $\Delta \in W^\Gamma$. First we show that $E^\Gamma \circ^\Gamma \Delta \subseteq \{\Delta\}$. Suppose $\Delta' \in E^\Gamma \circ^\Gamma \Delta$, i.e. there is a $\Delta_E \in E^\Gamma$ such that $\Delta' \in \Delta_E \circ^\Gamma \Delta$. We need to show $\Delta' = \Delta$. First suppose $A \in \Delta$, and note that $\mathrm{I} \in \Delta_E$ by definition. By definition of $\circ^\Gamma$ we have $\mathrm{I} * A \in \Delta'$, and as $\mathrm{I} * A \vdash A$ is provable we must have $A \in \Delta'$. Thus $\Delta' \supseteq \Delta$. To see that $\Delta' = \Delta$ as required, we just observe that if $\Delta' \supset \Delta$ then, as Δ' is consistent, Δ is not maximal, contradiction.

We still need to show that $\Delta \in E^\Gamma \circ^\Gamma \Delta$, i.e. that $\Delta \in \Delta_E \circ^\Gamma \Delta$ for some $\Delta_E \in E^\Gamma$. Using part 1 of Lemma 6.6, we have some $\ell \in \Delta$. Since $\ell \vdash \mathrm{I} * \ell$ is provable, we have $\mathrm{I} * \ell \in \Delta$. Using the Existence Lemma for $*$ (Lemma 6.9) we obtain named sets $\Delta_E, \Delta' \in W^\Gamma$ such that $\Delta \in \Delta_E \circ^\Gamma \Delta'$ and $\mathrm{I} \in \Delta_E$ and $\ell \in \Delta'$. Thus $\Delta_E \in E^\Gamma$ and, by part 2 of Lemma 6.6, $\Delta' = \Delta$. This completes the proof. □

Lemma 6.14. *Let $M = \langle W, \circ, E\rangle$ be a* BBI*-model named by ρ and let A be a pure formula. Suppose that $M, w \models_\rho A[\theta]$ for all $w \in W$ and nominal substitutions θ. Then A is valid in M.*

Proof. Letting ρ' be a hybrid valuation and $w \in W$, we must show that $M, w \models_{\rho'} A$. Since M is named by ρ, we have that for any $\ell \in \mathcal{N}$ there is a $k \in \mathcal{N}$ such that $\rho(k) = \rho'(\ell)$. Thus we can define the substitution θ of nominals for nominals by: $\theta(\ell)$ is the first $k \in \mathcal{N}$ with $\rho(k) = \rho'(\ell)$. By hypothesis, we have that $M, w \models_\rho A[\theta]$ for all $w \in W$.

We now prove by structural induction on A that $M, w \models_{\rho'} A$. In the case that A is a nominal ℓ, we must show that $\rho'(\ell) = w$, and are done since by assumption $w = \rho(\ell[\theta]) = \rho'(\ell)$. Note that A cannot be a propositional variable since it is assumed pure. The other cases follow by induction hypothesis. □

Theorem 6.15 (Completeness)**.** *Let Ax be a set of pure* HyBBI*-formulas. Then if a* HyBBI*-formula is valid in the class of* BBI*-models satisfying Ax, then it is provable in $\mathbf{K}_{\mathrm{HyBBI}}$ + Ax.*

Proof. Let $\mathcal{C}$ be the class of BBI-models satisfying Ax. Suppose A is valid in all BBI-models $M \in \mathcal{C}$, but not provable in $\mathbf{K}_{\mathrm{HyBBI}}$ + Ax. Then $\{\neg A\}$ is consistent. Using the Extended Lindenbaum Lemma (6.5), we can construct a named, pasted MCS $\Gamma \supseteq \{\neg A\}$. Now let $M^\Gamma = \langle W^\Gamma, \circ^\Gamma, E^\Gamma\rangle$ be the named model yielded by Γ, and ρ^Γ the corresponding canonical valuation. By Lemma 6.13, M^Γ is a BBI-model.

Furthermore, for any pure formula $B \in$ Ax and any nominal substitution θ, we have that $\vdash B[\theta]$ is provable (using the rule (Subst)), which means that $B[\theta] \in \Delta$ for all $\Delta \in W^\Gamma$ since MCSs are closed under provability. By the Truth Lemma (6.12), we obtain

$$M^\Gamma, \Delta \models_{\rho^\Gamma} B[\theta] \quad \text{for all } B \in \text{Ax}, \Delta \in W^\Gamma, \text{and substitutions } \theta$$

Thus, by Lemma 6.14, all formulas in Ax are valid in M^Γ, i.e. $M^\Gamma \in \mathcal{C}$. Thus, by the main assumption, A is valid in M^Γ.

Since Γ is named by construction, we have $\Gamma \in W^\Gamma$ by part 4 of Lemma 6.6. Since $\neg A \in \Gamma$, we have $M^\Gamma, \Gamma \models_{\rho^\Gamma} \neg A$ by the Truth Lemma. That is, $M^\Gamma, \Gamma \not\models_{\rho^\Gamma} A$. Thus A is not valid in M^Γ, contradiction. We conclude A is provable in $\mathbf{K}_{\mathrm{HyBBI}}$ + Ax. □

Corollary 6.16. *Let $\mathcal{S}$ be any separation theory from Definition 3.1 not including the cross-split property, and let Ax be the set of pure* HyBBI *formulas defining $\mathcal{S}$, as given by Corollary 4.4.*

Then a HyBBI*-formula is provable in $\mathbf{K}_{\mathrm{HyBBI}}$ + Ax if and only if it is valid in the class of* BBI*-models satisfying $\mathcal{S}$.*

Proof. Follows from Prop. 5.2, Thm. 6.15 and Cor. 4.4. □

7. HyBBI with the ↓ binder

In this section, we study the extension of HyBBI with the $\downarrow$ binder from hybrid logic [2]. Specifically, we show that the elusive cross-split property from Definition 3.1 is definable in this extension, called HyBBI($\downarrow$), and we show how to extend our soundness and parametric completeness results for HyBBI in the previous sections to the setting of HyBBI($\downarrow$).

7.1 Formulas and expressivity

Definition 7.1 (HyBBI($\downarrow$)-formula)**.** A HyBBI($\downarrow$)-formula is defined as for HyBBI (Defn. 4.1), except that if A is a HyBBI($\downarrow$)-formula and ℓ a nominal then $\downarrow\ell.\, A$ is a HyBBI($\downarrow$)-formula.

Definition 7.2 (HyBBI($\downarrow$)-validity)**.** Given any hybrid valuation ρ for a BBI-model $M = \langle W, \circ, E\rangle$, and any $w \in W$, we extend the forcing relation for HyBBI in Defn. 4.2 by the following clause for the $\downarrow$ binder, which binds the given label to the current world:

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

where $\rho[\ell := w]$ is notation for the hybrid valuation defined as ρ except that $\rho[\ell := w](\ell) \stackrel{\text{def}}{=} w$. The definition of validity for HyBBI then extends immediately to HyBBI($\downarrow$).

Proposition 7.3. *The cross-split property (see Definition 3.1) is definable in* HyBBI($\downarrow$) *via the following pure formula:*

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

Proof. We use the following formula abbreviations:

$$\begin{array}{lcl} C & \stackrel{\text{def}}{=} & @_c(ac * bc) \wedge @_d(ad * bd)\\ B & \stackrel{\text{def}}{=} & @_b(\top * \downarrow bc.\, @_b(\top * \downarrow bd.\, @_b(bc * bd) \wedge C))\\ A & \stackrel{\text{def}}{=} & @_a(\top * \downarrow ac.\, @_a(\top * \downarrow ad.\, @_a(ac * ad) \wedge B))\end{array}$$

Using the fact that ac, ad and a are distinct nominals, we have for any BBI-model $M = \langle W, \circ, E\rangle$, valuation ρ and $w \in W$,

$$\begin{aligned}& M, w \models_\rho A\\ \Leftrightarrow\ & M, \rho(a) \models_\rho \top * \downarrow ac.\, @_a(\top * \downarrow ad.\, @_a(ac * ad) \wedge B)\\ \Leftrightarrow\ & \exists w', w_1.\, \rho(a) \in w' \circ w_1 \text{ and}\\ & \quad M, w_1 \models_\rho \downarrow ac.\, @_a(\top * \downarrow ad.\, @_a(ac * ad) \wedge B)\\ & \quad\Leftrightarrow M, w_1 \models_{\rho[ac:=w_1]} @_a(\top * \downarrow ad.\, @_a(ac * ad) \wedge B)\\ & \quad\Leftrightarrow M, \rho(a) \models_{\rho[ac:=w_1]} \top * \downarrow ad.\, @_a(ac * ad) \wedge B\\ & \quad\Leftrightarrow \exists w'', w_2.\, \rho(a) \in w'' \circ w_2 \text{ and}\\ & \qquad M, w_2 \models_{\rho[ac:=w_1]} \downarrow ad.\, @_a(ac * ad) \wedge B\\ & \qquad\Leftrightarrow M, w_2 \models_{\rho[ac:=w_1, ad:=w_2]} @_a(ac * ad) \wedge B\\ & \qquad\Leftrightarrow M, \rho(a) \models_{\rho[ac:=w_1, ad:=w_2]} (ac * ad) \wedge B\\ \Leftrightarrow\ & \exists w_1, w_2.\, \rho(a) \in w_1 \circ w_2 \text{ and } M, \rho(a) \models_{\rho[ac:=w_1, ad:=w_2]} B\end{aligned}$$

By a similar chain of reasoning, we have

$$\begin{aligned}& M, \rho(a) \models_{\rho[ac:=w_1, ad:=w_2]} B\\ \Leftrightarrow\ & \exists w_3, w_4.\, \rho(b) \in w_3 \circ w_4 \text{ and}\\ & \qquad M, \rho(b) \models_{\rho[ac:=w_1, ad;=w_2, bc:=w_3, bd:=w_4]} C\end{aligned}$$

Finally, we have

$$\begin{aligned}& M, \rho(b) \models_{\rho[ac:=w_1, ad;=w_2, bc:=w_3, bd:=w_4]} C\\ \Leftrightarrow\ & \rho(c) \in w_1 \circ w_3 \text{ and } \rho(d) \in w_2 \circ w_4\end{aligned}$$

Putting everything together, we have

$$\begin{aligned}& M, w \models_\rho A\\ \Leftrightarrow\ & \exists w_1, w_2, w_3, w_4.\, \rho(a) \in w_1 \circ w_2, \rho(b) \in w_3 \circ w_4,\\ & \qquad \rho(c) \in w_1 \circ w_3, \rho(d) \in w_2 \circ w_4\end{aligned}$$

With the above equivalence for A in place, we can now show that (cs) defines the cross-split property of Definition 3.1.

($\Leftarrow$) Suppose M has the cross-split property. We require to show that the formula (cs) is valid in M, i.e. that if $M, w \models_\rho (a * b) \wedge (c * d)$ then $M, w \models_\rho A$. Supposing $M, w \models_\rho (a * b) \wedge (c * d)$, we have $w \in (\rho(a) \circ \rho(b)) \cap (\rho(c) \circ \rho(d))$. By the cross-split property, there then exist $ac, ad, bc, bd \in W$ such that $\rho(a) \in ac \circ ad$, $\rho(b) \in bc \circ bd$, $\rho(c) \in ac \circ bc$ and $\rho(d) \in ad \circ bd$. Thus, by the equivalence above, $M, w \models_\rho A$ as required.

($\Rightarrow$) Suppose the formula (cs) is valid in M. We require to show that M has the cross-split property. Suppose $w \in (t \circ u) \cap (v \circ w)$. Define a hybrid valuation ρ for M by

$$\rho(a) = t \qquad \rho(b) = u \qquad \rho(c) = v \qquad \rho(d) = w$$

where a, b, c, d are distinct nominals. We have that $M, w \models_\rho (a * b) \wedge (c * d)$. Thus, as (cs) is valid in M, we have $M, w \models_\rho A$. Using the equivalence above, there then exist $tv, tw, uv, uw \in W$ such that $t \in tv \circ tw$, $u \in uv \circ uw$, $v \in tv \circ uv$ and $w \in tw \circ uw$ as required. $\square$

The $\downarrow$ binder of HyBBI($\downarrow$) also allows us to encode the definition of the *overlapping conjunction* $\uplus$ of separation logic, which has been used in specifying and verifying programs manipulating data structures with intrinsic sharing [25, 16, 13]. In these works, $\uplus$ is introduced as an new primitive connective, defined by extending the standard forcing relation for BBI (Definition 2.3) as follows:

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

We give below an equivalent formulation of $A_1 \uplus A_2$ solely in terms of HyBBI($\downarrow$) connectives. We conjecture that this is not possible in BBI (for arbitrary A_1 and A_2).

Proposition 7.4. *For any* HyBBI($\downarrow$) *formulas A_1 and A_2, the overlapping conjunction $A_1 \uplus A_2$ is definable via the following* HyBBI($\downarrow$) *formula, where ℓ and ℓ_s do not occur in A_1 or A_2:*

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

Proof. Let $M = \langle W, \circ, E\rangle$ be a BBI-model, ρ a valuation for M, and $w \in W$.

$$\begin{array}{l} M, w \models_\rho \downarrow\ell.\, \top * \downarrow\ell_s.\, @_\ell(\ell_s \multimap\!\!\circledast\, A_1) * (\ell_s \multimap\!\!\circledast\, A_2) * \ell_s \\ \Leftrightarrow M, w \models_{\rho[\ell:=w]} \top * \downarrow\ell_s.\, @_\ell(\ell_s \multimap\!\!\circledast\, A_1) * (\ell_s \multimap\!\!\circledast\, A_2) * \ell_s \\ \Leftrightarrow w \in w_s' \circ w_s \text{ and} \\ \qquad M, w_s \models_{\rho[\ell:=w]} \downarrow\ell_s.\, @_\ell(\ell_s \multimap\!\!\circledast\, A_1) * (\ell_s \multimap\!\!\circledast\, A_2) * \ell_s \\ \quad \Leftrightarrow M, w \models_{\rho[\ell:=w,\ell_s:=w_s]} (\ell_s \multimap\!\!\circledast\, A_1) * (\ell_s \multimap\!\!\circledast\, A_2) * \ell_s \\ \Leftrightarrow \exists w_1, w_2, w_3, w'.\, w' \in w_1 \circ w_2 \text{ and } w \in w' \circ w_3 \\ \quad \text{and } M, w_1 \models_{\rho'} \ell_s \multimap\!\!\circledast\, A_1 \text{ and } M, w_3 \models_{\rho'} \ell_s \multimap\!\!\circledast\, A_2 \\ \quad \text{and } M, w_2 \models_{\rho'} \ell_s \qquad \text{(letting } \rho' = \rho[\ell := w, \ell_s := w_s]) \end{array}$$

Notice now that

$$\begin{array}{l} M, w_1 \models_{\rho'} \ell_s \multimap\!\!\circledast\, A_1 \\ \Leftrightarrow \exists w', w_1'.\, w' \in w_1 \circ w_1' \text{ and } M, w_1' \models_{\rho'} \ell_s \text{ and } M, w' \models_{\rho'} A_1 \\ \Leftrightarrow \exists w'.\, w' \in w_1 \circ w_s \text{ and } M, w' \models_{\rho'} A_1 \end{array}$$

Consequently, after applying a similar line of reasoning to w_3,

$$\begin{array}{l} M, w \models_\rho \downarrow\ell.\, \top * \downarrow\ell_s.\, @_\ell(\ell_s \multimap\!\!\circledast\, A_1) * (\ell_s \multimap\!\!\circledast\, A_2) * \ell_s \\ \Leftrightarrow \exists w_1, w_2, w_3, w', w'' \in W.\, w' \in w_1 \circ w_2 \text{ and } w'' \in w_2 \circ w_3 \\ \quad \text{and } w \in w' \circ w_3 \text{ and } M, w' \models_{\rho'} A_1 \text{ and } M, w'' \models_{\rho'} A_2 \\ \Leftrightarrow M, w \models_{\rho'} A_1 \uplus A_2 \end{array}$$

Since ℓ and ℓ_s are sufficiently fresh, this is equivalent to $M, w \models_\rho A_1 \uplus A_2$. $\square$

A three-place variant $A_1\langle\uplus : B\rangle A_2$ of the overlapping conjunction was introduced in [9] to deal with some forms of specified sharing. This variant tags the shared core of A_1 and A_2 with a formula B that it satisfies. Its satisfaction is defined as follows:

$$\begin{array}{l} M, w \models_\rho A_1\langle\uplus : B\rangle A_2 \\ \Leftrightarrow \exists w_1, w_2, w_3, w', w'' \in W. \\ \quad w' \in w_1 \circ w_2 \text{ and } w'' \in w_2 \circ w_3 \text{ and } w \in w' \circ w_3 \\ \quad \text{and } M, w' \models_\rho A_1 \text{ and } M, w'' \models_\rho A_2 \text{ and } M, w_2 \models_\rho B \end{array}$$

It is easy to modify the defining HyBBI($\downarrow$)-formula of Proposition 7.4 so as to accommodate this variant:

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

7.2 Proof theory, soundness and completeness

Definition 7.5. We define $\mathbf{K}_{\mathrm{HyBBI}(\downarrow)}$ to be the proof system obtained by adding the following axiom schema to $\mathbf{K}_{\mathrm{HyBBI}}$:

$$\text{(Bind}\downarrow) \qquad \vdash @_j(\downarrow\ell.\, B \leftrightarrow B[j/\ell])$$

Lemma 7.6 (Nominal Substitution Lemma)**.** *We have for any model $M = \langle W, \circ, E\rangle$, hybrid valuation ρ,* HyBBI($\downarrow$)*-formula A and nominals j, ℓ,*

$$M, \rho(j) \models_\rho A[j/\ell] \quad \Leftrightarrow \quad M, \rho(j) \models_{\rho[\ell:=\rho(j)]} A$$

where $[j/\ell]$ is a (capture-avoiding) nominal substitution.

Proof. By structural induction on A. The cases not involving nominals are straightforward. We examine the nominal cases, making use of the identity $\rho[\ell := \rho(j)](k) = \rho(k[j/\ell])$:

Case $A = k \in \mathcal{N}$. The required equivalence becomes:

$$\begin{array}{ll} & M, \rho(j) \models_\rho k[j/\ell] \Leftrightarrow M, \rho(j) \models_{\rho[\ell:=\rho(j)]} k \\ \text{i.e.} & \rho(j) = \rho(k[j/\ell]) \Leftrightarrow \rho(j) = \rho[\ell := \rho(j)](k) \end{array}$$

which follows from the identity above.

Case $A = @_k B$. We have $(@_k B)[j/\ell] = @_{k[j/\ell]} B[j/\ell]$ (noting that @ is not a binder, so the nominal substitution applies to the argument k), and proceed as follows:

$$\begin{array}{ll} M, \rho(j) \models_\rho @_{k[j/\ell]} B[j/\ell] & \\ \Leftrightarrow M, \rho(k[j/\ell]) \models_\rho B[j/\ell] & \\ \Leftrightarrow M, \rho[\ell := \rho(j)](k) \models_\rho B[j/\ell] & \text{(by above identity)} \\ \Leftrightarrow M, \rho[\ell := \rho(j)](k) \models_{\rho[\ell:=\rho(j)]} B & \text{(by ind. hyp.)} \\ \Leftrightarrow M, \rho(j) \models_{\rho[\ell:=\rho(j)]} @_k B & \end{array}$$

Case $A = \downarrow k.\, B$. Without loss of generality, we can assume that $k \neq \ell$. In this case, we have $(\downarrow k.\, B)[j/\ell] = \downarrow k.\, B[j/\ell]$, and can proceed as follows:

$$\begin{array}{ll} M, \rho(j) \models_\rho \downarrow k.\, B[j/\ell] & \\ \Leftrightarrow M, \rho(j) \models_{\rho[k:=\rho(j)]} B[j/\ell] & \\ \Leftrightarrow M, \rho(j) \models_{\rho[k:=\rho(j)][\ell:=\rho(j)]} B & \text{(by ind. hyp.)} \\ \Leftrightarrow M, \rho(j) \models_{\rho[\ell:=\rho(j)][k:=\rho(j)]} B & \\ \Leftrightarrow M, \rho(j) \models_{\rho[\ell:=\rho(j)]} \downarrow k.\, B & \end{array}$$

This completes all cases. $\square$

Proposition 7.7. *Any $\mathbf{K}_{\mathrm{HyBBI}(\downarrow)}$-provable formula is valid.*

Proof. Given the soundness of $\mathbf{K}_{\mathrm{HyBBI}}$ (Proposition 5.2), we just need to show that the new axiom (Bind$\downarrow$) is valid in all BBI-models. Let $M = \langle W, \circ, E\rangle$ be a BBI-model, let ρ be a valuation for M and let $w \in W$. We need to show that

$$\begin{array}{ll} & M, w \models_\rho @_j((\downarrow\ell.\, B) \leftrightarrow B[j/\ell]) \\ \text{i.e.} & M, \rho(j) \models_\rho \downarrow\ell.\, B \Leftrightarrow M, \rho(j) \models_\rho B[j/\ell] \\ \text{i.e.} & M, \rho(j) \models_{\rho[\ell:=\rho(j)]} B \Leftrightarrow M, \rho(j) \models_\rho B[j/\ell] \end{array}$$

which is guaranteed by Lemma 7.6. $\square$

We can obtain a parametric completeness result for $\mathbf{K}_{\mathrm{HyBBI}(\downarrow)}$ by repeating the Lindenbaum model construction for $\mathbf{K}_{\mathrm{HyBBI}}$ in Section 6. The only difference is that the crucial Truth Lemma needs to be extended to account for the $\downarrow$ binder case (cf. [2]).

Lemma 7.8 (Extended Truth Lemma). *For any* $\mathrm{HyBBI}(\downarrow)$*-formula* A *and* $\Delta \in W^\Gamma$*, we have* $M^\Gamma, \Delta \models_{\rho^\Gamma} A$ *if and only if* $A \in \Delta$.

Proof. By induction on the size of A, with all cases except $A = {\downarrow}\ell.\, B$ covered by Lemma 6.12. In this case, using the fact that $\Delta = \{A \mid @_j A \in \Gamma\}$ for some nominal j, we proceed as follows:

$$\begin{aligned} M^\Gamma, \Delta \models_{\rho^\Gamma} {\downarrow}\ell.\, B &\Leftrightarrow M^\Gamma, \Delta \models_{\rho^\Gamma[\ell:=\Delta]} B \\ &\Leftrightarrow M^\Gamma, \Delta \models_{\rho^\Gamma[\ell:=\rho^\Gamma(j)]} B \\ &\Leftrightarrow M^\Gamma, \Delta \models_{\rho^\Gamma} B[j/\ell] && \text{(by Lemma 7.6)} \\ &\Leftrightarrow B[j/\ell] \in \Delta && \text{(by ind. hyp.)} \\ &\Leftrightarrow @_j B[j/\ell] \in \Gamma \end{aligned}$$

Now since Γ is an MCS and thus closed under $(K_@)$ and the new axiom (Bind $\downarrow$), we have $@_j B[j/\ell] \in \Gamma$ if and only if $@_j {\downarrow}\ell.\, B \in \Gamma$ if and only if ${\downarrow}\ell.\, B \in \Delta$, which completes the case. ☐

Theorem 7.9 (Completeness). *Let Ax be any set of pure* $\mathrm{HyBBI}(\downarrow)$*-formulas. Then if a* $\mathrm{HyBBI}(\downarrow)$*-formula is valid in the class of* BBI*-models satisfying Ax, then it is provable in* $\mathbf{K}_{\mathrm{HyBBI}(\downarrow)} + Ax$.

Proof. Exactly as Theorem 6.15, using the Extended Truth Lemma (Lemma 7.8) for $\mathrm{HyBBI}(\downarrow)$ in place of Lemma 6.12. ☐

Corollary 7.10. *Let* $\mathcal{S}$ *be any separation theory from Definition 3.1, and let Ax be the set of pure* $\mathrm{HyBBI}(\downarrow)$ *formulas defining the properties* $\mathcal{S}$*, as given by Corollary 4.4 and Proposition 7.3.*

Then a $\mathrm{HyBBI}(\downarrow)$*-formula is provable in* $\mathbf{K}_{\mathrm{HyBBI}(\downarrow)} + Ax$ *if and only if it is valid in the class of* BBI*-models satisfying* $\mathcal{S}$.

Proof. Follows from Props. 7.7, 7.3, Thm. 7.9 and Cor. 4.4. ☐

8. Conclusions and future work

In this paper, we show that many separation theories that arise naturally in applications of separation logic, and in particular the various notions of separation algebras introduced in the literature so far, are not definable in the standard propositional basis for separation logic, namely BBI. To overcome these limitations in expressivity, we introduce new hybrid versions of BBI, obtained by marrying BBI with the machinery of hybrid logic, in which the separation theories are definable. In addition, we show how to obtain axiomatic proof systems for these hybrid logics that are sound and complete for any separation theory obtained by combining properties from a list of those we found in the separation logic literature.

In future work, we plan to explore possible applications of our hybrid logics to program analysis, e.g. by adding support for nominals to separation logic. More broadly, we hope that our introduction of more expressive intermediaries between BBI and full first-order logic will help facilitate the expression and verification of more complex program properties, particularly those involving overlapping data structures.

Acknowledgments

Many thanks to Hongseok Yang for pointing out to us the need for Lemma 6.10, and to Adam Barwell for crucial typing assistance.

Brotherston was supported by an EPSRC Career Acceleration Fellowship and Villard by the EPSRC grant EP/H008373/2.

References

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

[2] P. Blackburn and B. ten Cate. Pure extensions, proof rules, and hybrid axiomatics. *Studia Logica*, 84(2), 2006.

[3] G. E. P. Box and N. R. Draper. *Empirical model-building and response surfaces*. Wiley series in probability and mathematical statistics. John Wiley & Sons, Inc., 1987.

[4] J. Brotherston and C. Calcagno. Classical BI: Its semantics and proof theory. *Logical Methods in Computer Science*, 6(3), 2010.

[5] J. Brotherston and M. Kanovich. Undecidability of propositional separation logic and its neighbours. To appear in *Journal of the ACM*.

[6] C. Calcagno, D. Distefano, P. O'Hearn, and H. Yang. Compositional shape analysis by means of bi-abduction. *Journal of the ACM*, 58(6), 2011.

[7] C. Calcagno, P. Gardner, and U. Zarfaty. Context logic as modal logic: Completeness and parametric inexpressivity. In *POPL-34*. ACM, 2007.

[8] C. Calcagno, P. O'Hearn, and H. Yang. Local action and abstract separation logic. In *LICS-22*. IEEE Computer Society, 2007.

[9] R. Cherini and J. O. Blanco. Local reasoning for abstraction and sharing. In *SAC-24*. ACM, 2009.

[10] C. David and W.-N. Chin. Immutable specifications for more concise and precise verification. In *OOPSLA-11*. ACM, 2011.

[11] T. Dinsdale-Young, L. Birkedal, P. Gardner, M. J. Parkinson, and H. Yang. Views: compositional reasoning for concurrent programs. In *POPL-40*. ACM, 2013.

[12] R. Dockins, A. Hobor, and A. W. Appel. A fresh look at separation algebras and share accounting. In *APLAS-7*. Springer, 2009.

[13] G. J. Duck, J. Jaffar, and N. C. H. Koh. Constraint-based program reasoning with heaps and separation. 2013. To appear in *CP-19*.

[14] D. Galmiche and D. Larchey-Wendling. Expressivity properties of Boolean BI through relational models. In *FSTTCS-26*. Springer, 2006.

[15] K. Gödel. On formally undecidable propositions of Principia Mathematica and related systems. 1962. English translation by B. Meltzer.

[16] A. Hobor and J. Villard. The ramifications of sharing in data structures. In *POPL-40*. ACM, 2013.

[17] Z. Hou, A. Tiu, and R. Goré. A labelled sequent calculus for Boolean BI: Proof theory and proof search. To appear in *TABLEAUX-22*, 2013.

[18] S. Ishtiaq and P. W. O'Hearn. BI as an assertion language for mutable data structures. In *POPL-28*. ACM, 2001.

[19] D. Larchey-Wendling. The formal strong completeness of Boolean BI. Submitted, 2012.

[20] D. Larchey-Wendling and D. Galmiche. Exploring the relation between intuitionistic BI and Boolean BI: An unexpected embedding. *Mathematical Structures in Computer Science*, 19(3), 2009.

[21] D. Larchey-Wendling and D. Galmiche. The undecidability of Boolean BI through phase semantics. In *LICS-25*. IEEE Computer Society, 2010.

[22] J. Park, J. Seo, and S. Park. A theorem prover for Boolean BI. In *POPL-40*. ACM, 2013.

[23] D. Pym. *The Semantics and Proof Theory of the Logic of Bunched Implications*. Applied Logic Series. Kluwer, 2002.

[24] J. C. Reynolds. Separation logic: A logic for shared mutable data structures. In *LICS-17*. IEEE Computer Society, 2002.

[25] J. C. Reynolds. A short course on separation logic. `http://www.cs.cmu.edu/afs/cs.cmu.edu/project/fox-19/member/jcr/wwwaac2003/aac.html`, 2003.

[26] H. Yang, O. Lee, J. Berdine, C. Calcagno, B. Cook, D. Distefano, and P. O'Hearn. Scalable shape analysis for systems code. In *CAV-20*. Springer, 2008.