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(↓) with the usual ↓ 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 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.
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 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 $\ominus_\ell$ (parameterised by the nominal $\ell$), so that the hybrid formula $\ominus_\ell A$ is satisfied at any world in a model just when $A$ is satisfied at the world denoted by the nominal $\ell$.

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 binary operators $\forall$, $\exists$ and $\forall$ and $\exists$ have 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 ($\top, \bot, \neg, \land, \lor, \rightarrow$) of classical logic, and the so-called “multiplicative” connectives, consisting of the constant $I$ and binary operators $\ast$ and $\rightarrow$.

By convention, $\neg$ has the highest precedence, followed by $\ast$, $\land$ and $\lor$, with $\rightarrow$ and $\ast$ having lowest precedence.

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

$$W_1 \circ W_2 := \bigcup_{w_1 \in W_1, w_2 \in W_2} w_1 \circ w_2$$

A BBI-frame $(W, \circ, E)$ 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 $(W, \circ, E)$.

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

- $M, w \models_\rho P$ if $w \in \rho(P)$
- $M, w \models_\rho \perp$ always
- $M, w \models_\rho \neg A$ if $M, w \not\models_\rho A$
- $M, w \models_\rho A_1 \land A_2$ if $M, w \models_\rho A_1$ and $M, w \models_\rho A_2$
- $M, w \models_\rho A_1 \lor A_2$ if $M, w \models_\rho A_1$ or $M, w \models_\rho A_2$
- $M, w \models_\rho A_1 \rightarrow A_2$ if $M, w \models_\rho A_1$ implies $M, w \models_\rho A_2$
- $M, w \models_\rho \ast A_1 \ast A_2$ if $M, w \models_\rho A_1$ and $M, w \models_\rho A_2$
- $M, w \models_\rho A \rightarrow A_2$ if $M, w \models_\rho A_1$ and $M, w \models_\rho A_2$
- $A$ is said to be valid in $M$ if $M, w \models_\rho A$ for all valuations $\rho$ and for all $w \in W$. $A$ is valid if it is valid in all BBI-models.

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

$$A \ast B \vdash B \ast A \quad A \ast (B \ast C) \vdash (A \ast B) \ast C$$

$$A \vdash A \ast I \quad A \ast I \vdash A$$

$$A_1 \vdash B_1 \quad A_2 \vdash B_2 \quad A \ast B \vdash C \quad A \ast B \vdash C$$

$$A_1 \ast A_2 \vdash B_1 \ast B_2 \quad A \ast B \vdash C \quad A \ast B \vdash C$$
Galmiche and Larchey-Wendling showed [14] that $K_{\text{BBI}}$ 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 $K_{\text{BBI}}$-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 $M = (W, o, E)$ 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:** 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 $t \in tw, tv, u \in uv, uw, v \in vw$ and $w \in uv$.

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 “splitability” 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 $L$ of formulas, a property $P$ of BBI-models is said to be $L$-definable if there exists an $L$-formula $A$ such that for all BBI-models $M$,

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

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:

<table>
<thead>
<tr>
<th>Property</th>
<th>Formula</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indivisible units</td>
<td>$I \land (A \ast B) \vdash A$ (iu)</td>
</tr>
<tr>
<td>Divisibility</td>
<td>$-I \vdash -I \ast -I$ (div)</td>
</tr>
</tbody>
</table>

**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 $\rho$ be a valuation for $M$ and let $w \in W$. To show that (div) is valid, we suppose that $M, w \models \rho \models -I$, i.e., that $w \notin E$, and require to show that $M, w \models \rho \models -I \ast -I$. Divisibility gives us $w_1, w_2 \in W \setminus E$ such that $w \in w_1 \circ w_2$: thus, $M, w \models \rho \models -I \ast -I$.

(\(\Rightarrow\)) Assume that (div) is valid in $M$, and suppose that $w \notin E$. Then, $M, w \models \rho \models -I$, hence we have $M, w \models \rho \models -I \ast -I$ by validity of (div). This gives us $w_1, w_2$ such that $w \in w_1 \circ w_2$ where $M, w_1 \models \rho \models -I$ and $M, w_2 \models \rho \models -I$, i.e. $w_1, w_2 \notin E$ as required. \(\square\)

**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 $M = (W, o, E)$ and $M' = (W', o', E')$ be BBI-models. A bounded morphism from $M$ to $M'$ is a function $f : W \rightarrow W'$ 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. $f(w) = w_1' \circ w_2' \Leftrightarrow \exists w_1, w_2 \in W, w \in w_1 \circ w_2$ and $f(w_1) = w_1' \circ w_2'$ and $f(w_2) = w_2'$;
4. $w_1' \in f(w) \circ w_2' \Leftrightarrow \exists w_1, w_2 \in W, w \in w_1 \circ w_2$ and $f(w_1) = w_1' \circ w_2'$ and $f(w_2) = w_2'$.

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

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

**Proof.** We write $M = (W, o, E)$ and $M' = (W', o', E')$, and let $f : W \rightarrow W'$ 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 $\rho'$ for $M'$ and $w' \in W'$ such that $M', w' \not\models \rho' A$. We define a valuation $\rho$ for $M$ as follows:

$$\rho(P) \triangleq \{w' \in W \mid f(w) \in \rho'(P)\}$$

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 $M, w \models A$ 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 $\rho$, we have as required:

$$M, w \models A \iff w \in \rho(P) \iff f(w) \in \rho'(P) \iff M', f(w) \models \rho' A$$

**Case $A = I$.** Using condition 1 in Defn. 3.4, we have as required:

$$M, w \models I \iff w \in E \iff f(w) \notin E' \iff M', f(w) \not\models \rho' I$$

**Case $A = B \ast C$.** (\(\Rightarrow\)) Supposing that $M, w \models \rho B \ast C$, 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 $M', f(w) \models \rho' B \ast C$ as required.
Suppose 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 $A = B \rightarrow C$. (⇒) Suppose $M, w \models_{\rho} B \rightarrow C$. To show that $M', f(w) \models_{\rho'} B \rightarrow C$, 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 $M, w_2 \models_{\rho} C$, we obtain $M, w_2 \models_{\rho} C$, which yields the required $M', w_2 \models_{\rho'} C$ by induction hypothesis.

(⇐) Suppose $M', f(w) \models_{\rho'} B \rightarrow C$. To show that $M, w \models_{\rho} B \rightarrow C$, 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 $M', f(w) \models_{\rho'} B \rightarrow C$, 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 $P$ be a property of BBI-models, and let $M, M'$ be BBI-models such that $M \in P$, $M' \notin P$ and $M \rightarrow M'$. Then $P$ is not BBI-definable.

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

In fact, Lemma 3.6 applies to BBI-frames as well as BBI-models, and implies that if $M \rightarrow M'$ 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 $M \rightarrow M'$. We define BBI-models $M = (\langle W, O, E \rangle$ and $M' = (\langle W', O', E' \rangle$ as follows:

$$W \triangleq \{e, v_1, v_2, x_1, x_2, y_1, y_2\} \quad E \triangleq \{e\}$$

$$W' \triangleq \{e, v, x, y_1, y_2\} \quad E' \triangleq \{e\}$$

$$w \circ e = e = e \circ w \triangleq \{w\} \text{ for all } w \in W$$

$$x_1 \circ v_1 = v_2 \circ x_1 \triangleq \{y\} \quad x_1 \circ v_2 = v_2 \circ x_1 \triangleq \{y\}$$

$$x_2 \circ x_1 = v_2 \circ x_2 \triangleq \{y\}$$

with $w_1 \circ w_2 = w_1' \circ w_2' \triangleq \emptyset$ 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 $w_1 \circ (w' \circ w')$ 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 $M \rightarrow M'$, i.e., that there is a surjective bounded morphism from $M$ to $M'$. Define $f : W \rightarrow W'$ by:

$$f(w) \triangleq w \quad (w \in \{e, y, z\})$$

Clearly $f$ is surjective, so it just remains to check the four bounded morphism conditions for Defn. 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 $w_1 = x_1, w_2 = y$ are we 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 $K_{BBI}$ is incomplete for such models. What Theorem 3.7 shows in addition is that, if one were to add (perhaps infinitely many) axioms to $K_{BBI}$ 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 $K_{BBI}$’s commutativity axiom $A \ast B \vdash B \ast A$, 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, $M' \notin$ cancellative and $M \rightarrow M'$. We define BBI-models $M = (\langle W, O, E \rangle$ and $M' = (\langle W', O', E' \rangle$ as follows:

$$W \triangleq \{e, v_1, v_2, x, y_1, z_1\} \quad E \triangleq \{e\}$$

$$W' \triangleq \{e, v, x, y, z\} \quad E' \triangleq \{e\}$$

$$w \circ e = e = e \circ w \triangleq \{w\} \text{ for all } w \in W$$

$$x \circ v_1 = v_1 \circ x \triangleq \{z_1\} \quad x \circ v_2 = v_2 \circ x \triangleq \{z_2\}$$

$$y \circ v_1 = v_1 \circ y \triangleq \{z_2\} \quad y \circ v_2 = v_2 \circ y \triangleq \{z_1\}$$

with $w_1 \circ w_2 = w_1' \circ w_2' \triangleq \emptyset$ for all other $w_1$ and $w_2$.

First, it is straightforward to verify that $M$ and $M'$ are indeed BBI-models. 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 cancellative because, by construction, $\circ' \subseteq (\circ \cap (\circ \circ') \cap (\circ' \circ'))$ implies $w_1 = w_2 = v_1 = v_2 = v \neq y$. On the other hand, $M'$ is not cancellative, for $z \in (x \circ' x) \cap (v \circ' y)$ but $x \neq y$.

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

$$f(v_1) = f(v_2) \triangleq v \quad f(z_1) = f(z_2) \triangleq z$$

$$f(w) \triangleq w \quad (w \in \{e, x, y\})$$

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 $M \nrightarrow M'$. We define BBI-models $M = \langle W, \circ, E \rangle$ and $M' = \langle W', \circ', E' \rangle$ by:

$$
W \triangleq \{ e, x, y \} \quad E \triangleq \{ e \}
$$

$$
\circ \circ = e \circ w \triangleq \{ w \} \text{ for all } w \in W
$$

$$
x \circ y = y \circ x \triangleq \{ x, y \}
$$

$$
W' \triangleq \{ e, x \} \quad E' \triangleq \{ e \}
$$

$$
\circ' \circ = e \circ' w \triangleq \{ w \} \text{ for all } w \in W
$$

$$
x \circ' x \triangleq \{ x \}
$$

with $w_1 \circ w_2 = w_3 \circ' w_4 \triangleq \emptyset$ 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, $M'$ is disjoint by construction, whereas $M$ is not disjoint since $x \neq e$ and $x \circ' x \neq 0$. We define a surjective bounded morphism $f$ from $M$ to $M'$ by

$$
f(e) \overset{\text{def}}{=} e \quad f(x) \overset{\text{def}}{=} x \quad f(y) \overset{\text{def}}{=} x
$$

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 $K_{BBI}$. 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 disjunct 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:

$$
M_1 \uplus M_2 \triangleq \langle (W_1 \cup W_2), \circ_1 \cup \circ_2, E_1 \cup E_2 \rangle
$$

where $\circ_1 \cup \circ_2 : (W_1 \cup W_2) \times (W_1 \cup W_2) \rightarrow \mathcal{P}(W_1 \cup W_2)$ is defined as $\circ_1$ on $W_1 \times W_2$ 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 $\rho$ 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 $\rho_1$ for $M_1$ by

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

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 $M_1 \uplus M_2, w \models_{\rho_1} A$. 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 $M_1 \uplus M_2 \not\in \mathcal{P}$. 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 ultrablifer 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 $\ell$. 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 $j, k, \ell$ 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 $\ell$ 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 $\rho$ 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 $\rho$ 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:

$$
M, w \models_{\rho} @\ell A \iff M, \rho(\ell) \models_{\rho} A
$$

$$
M, w \models_{\rho} \ell \iff w = \rho(\ell)
$$
A is then said to be valid in $M$ if $M, w \models_\rho A$ for all hybrid valuations $\rho$ 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:

- **Functionality:** $@_2(\ell \ast k) \land @_2(\ell \ast k) \models @_2\ell' \ (\text{pfn})$
- **Cancellativity:** $\ell \ast j \land \ell \ast k \models @_2j \land @_2k \ (\text{cnc})$
- **Single unit:** $@_21 \land @_21 \land @_22 \ (\text{su})$
- **Indivisible units:** $1 \land (1 \ast 2) \models 1 \ (\text{iu}')$
- **Disjointness:** $\ell \ast \ell' \land 1 \land \ell \ (\text{dis})$

**Proof.** We treat each property individually.

- **Functionality:** $(\Rightarrow)$ Assume $M$ is partial functional, let $\rho$ be a valuation for $M$ and let $w \in W$. To show that (pfn) is valid in $M$, we assume that $M, w \models_\rho @_2(\ell \ast k) \land @_2(\ell \ast k)$, and must show that $M, w \models_\rho \ell'$. By assumption, we have $\rho(\ell) = \rho(\ell')$. Hence by partial functionality of $M$ we have $\rho(\ell) = \rho(\ell')$ as required.

- **Cancellativity:** $(\Rightarrow)$ Assume $M$ is cancellative, let $\rho$ be a valuation for $M$ and let $w \in W$. To show that (cnc) is valid in $M$, we suppose that $M, w \models_\rho \ell \ast j \land \ell \ast k$, i.e., that $\rho(\ell) = \rho(\ell')$. Then $\rho(j) = \rho(\ell) \land \rho(k)$. By cancellativity, we thus immediately get that $\rho(j') = \rho(k')$ as required.

- **Single unit:** $(\Rightarrow)$ Assume $M$ is cancellative, let $\rho$ be a valuation for $M$ and let $w \in W$. To show that (su) is valid in $M$, we suppose that $M, w \models_\rho @_21 \land @_21 \land @_22$, and require to show that $M, w \models_\rho 1$. By virtue of (cnc), we deduce that $M, w \models_\rho \ell \ast 1$, hence that $\rho(j) = \rho(k)$, and by construction that $w_1 = w_2$.

- **Indivisible units:** $(\Rightarrow)$ Assume $E = \{e\}$, let $\rho$ be a valuation for $M$ and let $w \in W$. We show (iu') is valid. Supposing that $M, w \models_\rho @_21 \land @_21 \land @_22$, we have that $\rho(\ell_1), \rho(\ell_2) \in E$. Thus $\rho(\ell_1) = \rho(\ell_2) = e$, which yields $M, w \models_\rho @_21 \land @_21 \land @_22$ as required.

$(\Rightarrow)$ Assume (su) is valid and let $e, e' \in E$. We need to show $e = e'$. Define a valuation $\rho$ for $M$ by $\rho(\ell_1) = e$ and $\rho(\ell_2) = e'$. Thus, to show $e = e'$, it suffices to show $M, w \models_\rho @_21 \land @_22$ (for any $w \in W$). Since (su) is valid, it suffices to show that $M, w \models_\rho @_21 \land @_22$. This follows from our construction of $\rho$.

- **Disjointness:** $(\Rightarrow)$ Assume the disjointness property, let $\rho$ be a valuation for $M$ and let $w \in W$. To show (dis) is valid in $M$, we assume that $M, w \models_\rho \ell \ast \ell'$ and require to show that $M, w \models_\rho 1 \land \ell$, i.e., that $w = \rho(\ell)$ and $w \in E$. That $M, w \models_\rho \ell \ast \ell'$ means that $w = \rho(\ell) \lor \rho(\ell')$. In particular, $\rho(\ell) \lor \rho(\ell') \not\equiv 0$ hence by disjointness, $\rho(\ell) \not\equiv E$. We thus get $w \in \rho(\ell) \lor \rho(\ell') = \{\rho(\ell)\}$ hence $w = \rho(\ell)$ and also $w \in E$ as required.

$(\Rightarrow)$ Assume (dis) is valid in $M$, and suppose that $w \not\equiv w'$. We require to show that $w = w'$. From (su) is valid in $M$, we have $M, w \not\models_\rho$, hence $M, w \models_\rho 1 \land \ell \not\models_\rho \ell$ as required.

- **Corollary 4.4.** Any separation property 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 $@_2$ 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 $-\land$, the De Morgan dual of $\land$ defined as $A -\land B \equiv \neg(A \land \neg B)$.

Unpacking the negations and $\land$ yields the following forcing relation for $-\land$:

$$M, w \models_\rho A_1 -\land A_2 \iff \exists w', w'' \in W. w', w'' \in w \lor w' \land M, w' \models_\rho A_1 \land M, w'' \models_\rho A_2$$

(Using $-\land$ rather than $\land$ 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 $K_{\text{HyBBI}}$ to be the proof system obtained by extending the proof system $K_{\text{BBI}}$ (see Definition 2.4) with the axioms and rules for nominals and $-\land$ given in Figure 1.

$K_{\text{HyBBI}}$ 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 $K_{\text{HyBBI}}$-provable formula is valid.

**Proof.** Let $M = (W, \circ, E)$ be a BBI-model. Then, assuming $A$ is $K_{\text{HyBBI}}$-provable, we must show that $A$ is valid in $M$. It suffices to show that all axioms of $K_{\text{HyBBI}}$ are valid and that validity
is preserved by every proof rule of $K_{HyBBI}$. 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 −→) here, as the others are similar.

**Case (Bridge∗).** Let $\rho$ be a valuation for $M$ and let $w \in W$. Suppose $M, w \models \rho \ell \land k \land k'$ and $M, \rho(k) \models A$ and $M, \rho(k') \models B$. The first of these means that $\rho(\ell) \models \rho(k) \circ \rho(k')$. Thus $M, \rho(\ell) \models \rho A \land B$, i.e. $M, w \models \rho \ell (A \land B)$ as required.

**Case (Paste −→).** Let $\rho$ be a valuation for $M$ and let $w \in W$. Suppose the premise of the rule is valid in $M$ and $M, w \models x_1 A \land x_2 B$, we have to show $M, w \models x_1 A \land x_2 B$. We use $M, \rho(\ell) \models x_1 A \land x_2 B$ which means that there exist $w', w'' \in W$ such that $w'' \models \rho(\ell) \circ \rho(\ell) \circ \rho(\ell)$ and $M, w' \models x_1 A$ and $M, w'' \models x_2 B$. Now define the valuation $\rho'' = \rho[k \mapsto w', k' \mapsto w'']$, where $k$ and $k'$ are the fresh nominals appearing in the premises of the rule. By construction, and using the fact that $\rho$ and $\rho'$ agree except possibly on the fresh nominals $k, k'$, we have $\rho''(k) = \rho(k)$ and $\rho''(k') = \rho(k')$. The first of these gives us $M, \rho''(\ell) \models x_1 A \land x_2 B$. Putting everything together, we obtain $M, w \models x_1 A \land x_2 B$.

Since the premise of the rule is valid by assumption, we obtain $M, w \models x_1 A \land x_2 B$. Again, since $\rho$ and $\rho'$ agree except on $k, k'$, which do not appear in $C$, we thus obtain $M, w \models x_1 A \land x_2 B$.

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

**Example 5.3.** The $HyBBI$-formula $\top \models (1 \land (\ell \rightarrow A)) \models x_1 A$ is provable in $HyBBI$.

(As above, the $\ell$ in the formula is a new, not occurring in $A$ or $x_1 A$.)

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

$$A \land x_1 B \models x_1 B$$

Let $j, k, k'$ be fresh nominals not occurring in A, B or $\ell$. We have $x_1 B, x_1 B \models x_1 B$ an instance of (Agree). By weakening for $\land$, we thus obtain $x_1 (k \land k') \land x_1 A \land x_1 B \land x_1 B$. Using the fact that $k, k'$ are fresh, we can apply the rule (Paste *) to derive $x_1 (A \land x_1 B) \models x_1 B$. Since the formula $j \land (A \land x_1 B) \models x_1 (A \land x_1 B)$ is an instance of (Self-intro), we obtain $j \land (A \land x_1 B) \models x_1 B$ by transitivity, and thus easily we have $j \land (A \land x_1 B) \models x_1 B$. Since $j$ is fresh, we obtain $A \land x_1 B \models x_1 B$ by applying (Name).

Next, we show that the following formula is provable:

$$I \land (\ell \rightarrow A) \models x_1 A$$

We have $\ell \land A \models x_1 A$ an instance of (Self-intro), whence by contraposition and use of (Self-dual) we obtain $\ell \land x_1 A \models \neg A$. Now, since $\ell \land x_1 A \models \neg A$ is provable as an instance of (1) above, we obtain $\ell \land (\ell \land x_1 A) \models \neg A$. By straightforward manipulation of plain BBI we can prove

$$(\ell \land x_1 A) \models \ell \land (\ell \land x_1 A)$$

Thus, by transitivity, we obtain $(1 \land (\ell \land x_1 A)) \models \ell \land x_1 A$. We can derive $\top \models (1 \land (\ell \land x_1 A)) \models \ell \land x_1 A$ using (2). As $\top \models x_1 A \models \ell \land x_1 A$ is an instance of (1), we have $\top \models 1 \land (\ell \land x_1 A) \models x_1 A$ by transitivity as required.

Interestingly, the converse of the formula in Example 5.3, that is $x_1 A \models x_1 A$, is not generally valid, but is valid in all single-unit models (and thus in such models $x_1 e$ 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 $x_1 e$ modality enables us to talk about worlds not accessible from the current world via the I, * and $\rightarrow$ modalities; but in single-unit models, there are no such worlds.

**6. Completeness for pure extensions of $K_{HyBBI}$**

In this section, we show a parametric completeness result: any extension of $K_{HyBBI}$ 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 $K_{HyBBI}$.

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 $\rightarrow$, 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 $\Gamma$ of formulas is said to be $K$-inconsistent if there are formulas $A_1, \ldots, A_n \in \Gamma$ such that $A_1 \land \ldots \land A_n \vdash \bot$ is provable in $K$. Otherwise $\Gamma$ is called $K$-consistent.

**Definition 6.2** (Maximal consistent set). Let $\mathcal{K}$ be any proof system. A set $\Gamma$ of formulas is maximal $K$-consistent (and we call $\Gamma$ a $K$-MCS) if $\Gamma$ is $K$-consistent and any $\Delta \supset \Gamma$ is $K$-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 $\text{K-HBDI}$ of $\text{K-HDI}$ with a finite set $\text{Ax}$ of axioms expressed as pure formulas.

We begin by recalling some basic facts about MCSs.

**Lemma 6.3.** For any MCS $\Gamma$ 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 $\bot \not\in \Gamma$;
3. either $A \in \Gamma$ or $\neg A \in \Gamma$;
4. $A \land B \in \Gamma$ iff $A, B \in \Gamma$;
5. $A \lor B \in \Gamma$ iff $A \in \Gamma$ or $B \in \Gamma$.

**Proof.** Standard in all cases. \(\square\)

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 $\Gamma$ is said to be named if there is at least one nominal $\ell \in \Gamma$; any such $\ell$ is called a name for $\Gamma$.

$\Gamma$ is said to be pasted if
- $\ell \in \Gamma$ implies $\ell \land \ell_2 \land \ell_1 \land \ell_2 B \in \Gamma$ for some $\ell_1, \ell_2$,
- $\ell \land \ell_1 \land \ell_2 B \in \Gamma$ implies $\ell \land \ell_1 \land \ell_2 B \in \Gamma$ for some $\ell_1, \ell_2$.

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

**Proof.** Let $k_0, k_1, k_2, \ldots$ be an enumeration of $N'$, and let $B_1, B_2, B_3, \ldots$ be an enumeration of all the formulas in the extended language given by $N' \cup N$. Given a consistent set $\Delta$ of formulas, we define a sequence $(\Delta_i)_{i \geq 0}$ of sets of formulas as follows:
- $\Delta_0 \equiv \Delta \cup \{k\}$;
- if $\Delta_i \cup \{B_i\}$ is inconsistent then $\Delta_{i+1} \equiv \Delta_i$;
- if $\Delta_i \cup \{B_i\}$ is consistent and the formula $B_i$ is not of the form $\ell \land \ell_1 \land \ell_2 B \in \Gamma$, then $\Delta_{i+1} \equiv \Delta_i$;
- if $\Delta_i \cup \{B_i\}$ is consistent and $B_i \equiv \ell \land \ell_1 \land \ell_2 B \in \Gamma$ then $\Delta_{i+1} \equiv \Delta_i \cup \{k \land \ell \land \ell_2 B \}$;
- if $\Delta_i \cup \{B_i\}$ is consistent and $B_i \equiv \ell \land \ell_1 \land \ell_2 B \in \Gamma$ then $\Delta_{i+1} \equiv \Delta_i \cup \{k \land \ell \land \ell_2 B \}$.

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

First, to see that $\Delta^+$ is consistent, it suffices to show that $\Delta_i$ 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 $A \land k \land \bot$ provable. Thus $k \land \bot$ is provable, whence the rule (Name) we have $\bot \land \bot$ provable and thus $\bot \land \bot$ provable, contradicting the consistency of $\Delta$. Now, assuming that $\Delta_i$ is consistent, we must show that $\Delta_{i+1}$ is consistent. This is immediate by induction hypothesis except in the case that $B_i = \ell \land \ell_1 \land \ell_2 B$. We show the case $B_i = \ell \land \ell_1 \land \ell_2 B$. In this case, assume for contradiction that there are $A_1, \ldots, A_n \in \Delta$, such that, writing $A = \bigwedge_{1 \leq i \leq n} A_i$, the following is provable:

$A \land \ell \land \ell_1 \land \ell_2 B \land \bot$\(\vdash\)

Thus we can also prove

$\ell \land \ell_1 \land \ell_2 B \land \bot$\(\vdash\)

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

$\ell \land \ell_1 \land \ell_2 B \land \bot$\(\vdash\)

Thus we obtain $A \land \ell \land \ell_1 \land \ell_2 B \land \bot$, contradicting the assumed consistency of $\Delta_i \cup \{B_i\}$. The case $B_i = \ell \land \ell_1 \land \ell_2 B$ is similar, using the rule (Paste $\ast$).

Next, we must show that $\Delta^+$ is maximal. Suppose that for some formula $A$, we have $\Delta^+ \not\supset \{A\}$ but $A \not\in \Delta^+$. Note that $A$ appears in our enumeration as $B_i$, so by construction it must be that $\Delta_i \cup \{A\}$ is inconsistent (otherwise $A \in \Delta_{i+1} \subseteq \Delta^+$). But then $\Delta^+ \not\supset \{A\}$ is inconsistent, contradiction.

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

Finally, we show $\Delta^+$ is pasted. First, suppose $\ell \land \ell_1 \land \ell_2 B \in \Delta^+$.

Then $\ell \land \ell_1 \land \ell_2 B \in \Delta^+$ as required. For similar reasons, whenever $\ell \land \ell_1 \land \ell_2 B \in \Delta^+$ we have $\ell \land \ell_1 \land \ell_2 B \in \Delta^+$.

In the following, we define a named set yielded by $\Gamma$ to be any set of formulas $\{A \mid \ell \land \ell_1 \land \ell_2 B \in \Delta\}$ for some nominal $\ell$.

**Lemma 6.6.** Let $\Gamma$ be an MCS, and let $\Delta_e \equiv \{A \mid \ell \land \ell_1 \land \ell_2 B \in \Delta\}$ be the named set yielded by $\Gamma$ for each nominal $\ell$. Then the following hold for all nominals $\ell, k$:
1. $\Delta_e$ is an MCS containing $\ell$;
2. if $\ell \in \Delta_e$ then $\Delta_k = \Delta_e$;
3. if $\ell \in \Delta_k$ then $\ell \land \ell_1 \land \ell_2 B \in \Delta$;
4. if $\ell$ is a name for $\Gamma$ then $\Gamma = \Delta_e$.

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

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

**Definition 6.8.** Let $\Gamma$ be a named, pasted MCS. Then the named model yielded by $\Gamma$ is defined as $M^\Gamma \equiv \langle W^\Gamma, \omega^\Gamma, E^\Gamma \rangle$, where:
1. $W^\Gamma$ is the set of all named sets yielded by $\Gamma$;
2. $\Delta_1 \land \Delta_2 \equiv \{A \mid A \in \Delta_1, A_2 \in \Delta_2\}$ implies $A_1 \land A_2 \in \Delta$;
3. $E^\Gamma \equiv \{A \mid A \in \Delta\}$.

The canonical valuation $\rho^\Gamma$ for $M^\Gamma$ is defined by

$\rho^\Gamma(P) \equiv \{A \mid A \in \Delta\}$ $P$ a proposition

$\rho^\Gamma(\ell) \equiv \{A \mid \ell \land \ell_1 \land \ell_2 B \in \Delta\}$ $\ell$ a nominal

We show that $M^\Gamma$ is indeed a BBI-model in Lemma 6.13 (but require for the intermediate results only that $M^\Gamma$ is a BBI-frame). We observe that $M^\Gamma$ is indeed named by $\rho^\Gamma$: for any $\Delta \in W^\Gamma$ we have $\Delta = \{A \mid \ell \land \ell_1 \land \ell_2 B \in \Delta\}$ for some $\ell$, whence $\rho^\Gamma(\ell) = \Delta$. 


Lemma 6.9 (Existence Lemma for ∆). For any ∆ ∈ W^1, if A_1 ∗ A_2 ∈ ∆ then there exist ∆_1, ∆_2 ∈ W^1 such that ∆ in ∆_1 ∩ ∆_2 and A_1 ∈ ∆_1, A_2 ∈ ∆_2.

Proof. Let A_1 + A_2 ∈ ∆. We have ∆ = {A | @_t A ∈ Γ} for some nominal t. Thus @_t(A_1 + A_2) ∈ Γ. As Γ is pasted, we have nominals t_1, t_2 such that @_t_1(t_2 + t_2) ∨ @_t_1 A_1 ∧ @_t_2 A_2 ∈ Γ. Thus A_1 ∈ ∆_1 and A_2 ∈ ∆_2, where Δ_1 = {A | @_t_1 A ∈ Γ} and Δ_2 = {A | @_t_2 A ∈ Γ} are named sets yielded by Γ.

It just remains to show that ∆ in Δ_1 ∩ Δ_2. Let B_1, B_2 in Δ_1, B_3 in Δ_2. By definition, @_t_1 B_1 ∈ Γ and @_t_2 B_2 ∈ Γ. As MCSs are closed under provability and conjunction, we have @_t(t_1 ∨ t_2) ∨ @_t_1 B_1 ∧ @_t_2 B_2 ∈ Γ. Thus, using the rule (Bridge *), we have @_t(B_1 + B_2) ∈ Γ. Thus B_1 + B_2 in Δ as required.

Lemma 6.10. ∆ in Δ_1 ∩ Δ_2 if and only if for all formulas A and B, A in Δ_2 and B in Δ implies A − − B in Δ as required.

Proof. We show each direction separately, making use of the fact that ∆_1, ∆_2 are MCSs by part 1 of Lemma 6.6.

(⇐) Assume the right-hand side of the implication and let A_1 ∈ ∆_1 and A_2 ∈ ∆_2. We must show A_1 + A_2 ∈ ∆. Suppose for contradiction that A_1 + A_2 /∈ Δ. Since ∆ is an MCS, (− (A_1 + A_2)) in ∆. By assumption, A_2 − − (− (A_1 + A_2)) in ∆_1, i.e. (− (A_2) − − (− (A_1 + A_2))) in ∆_1. As ∆_1 is an MCS, we have A_1 + (− (A_2) − − (− (A_1 + A_2))) in ∆_1. But A_1 ⊨ A_2 → (A_1 + A_2) is provable, hence so is A_1 + (− (A_2) − − (− (A_1 + A_2))) ⊨ Γ. This contradicts the consistency of Γ. Hence A_1 + A_2 /∈ ∆ as required.

(⇒) Let A, B ∈ Δ, B /∈ Δ, and suppose for contradiction that A − − B /∈ Δ. As Δ is an MCS, we have A − − B in Δ, so by the main assumption (A − − B) ∗ A ∈ Δ. As Δ is an MCS and (A − − B) ∗ A − − B is provable, ∗ A in Δ. This contradicts the consistency of Δ, so A−−B in Δ as required.

Lemma 6.11 (Existence Lemma for →). For any ∆ ∈ W^1, if A_1 − → A_2 in ∆ then there exist ∆', ∆'' ∈ W^1 such that ∆'' in ∆ ∩ ∆' and A_1 in ∆', A_2 in ∆''.

Proof. We have ∆ = {A | @_t A ∈ Γ} for some nominal t. Since A_1 − → A_2 in ∆ by assumption, @_t(A_1 − → A_2) in Γ. As Γ is pasted, we have @_t_1(t_2 + t_2) ∨ @_t_1 A_1 ∧ @_t_2 A_2 in Γ for some t_1, t_2. We obtain named sets Δ_1 = {A | @_t_1 A ∈ Γ} and Δ''_1 = {A | @_t_2 A ∈ Γ} yielded by Γ with A_1 in Δ_1 and A_2 in Δ''_1.

It remains to show that Δ'' in Δ ∩ Δ'. By Lemma 6.10, it suffices to show that A in Δ' and B in Δ'' implies A − − B in Δ. Supposing A in Δ', B in Δ'', we have @_t(A − − B) ∈ Γ and @_t B in Γ. Thus we obtain @_t(A − − B) ∨ @_t A ∧ @_t B ∈ Γ. Since Γ is an MCS, it is closed under the rule (Bridge *), and it follows that @_t(A − − B) ∈ Γ. Thus A−−B in Δ as required.

Lemma 6.12 (Truth Lemma). For any HyBBI-formula A and ∆ ∈ W^1, we have M^Γ, ∆ |=_{ρ^Γ} A if and only if A in ∆.

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^Γ, ∆ |=_{ρ^Γ} P ⇔ Δ in ρ^Γ(P) ⇔ P in Δ

Case A = t. Using the definition of ρ^Γ, we have

M^Γ, ∆ |=_{ρ^Γ} t ⇔ Δ = ρ^Γ(t) ⇔ Δ = {A | @_t A ∈ Γ}

Now, going from left to right, we have Δ = {A | @_t A ∈ Γ} and thus Δ in Δ by part 1 of Lemma 6.6. Conversely, assuming t in Δ, we have Δ = {A | @_t A ∈ Γ} for some k, and by part 2 of Lemma 6.6 we obtain Δ = {A | @_t A ∈ Γ} as required.

Case A = I. Using the definition of E^Γ, we easily have as required:

M^Γ, ∆ |=_{ρ^Γ} I ⇔ Δ in E^Γ ⇔ I in Δ

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

M^Γ, ∆ |=_{ρ^Γ} A_1 + A_2 ⇔ Δ in E^Γ and M^Γ, Δ_1 |=_{ρ^Γ} A_1 and M^Γ, Δ_2 |=_{ρ^Γ} A_2

Going from left to right, assume A_1 + A_2 in Δ given the above implication. We show the contrapositive. Assume A_1, A_2 /∈ Δ, i.e. Δ = Δ ∪ {A_1, A_2}. We must construct named sets Δ', Δ'' yielded by Γ, with Δ'' in Δ ∪ {A_1, A_2}, but A_2 /∈ Δ'', i.e. Δ_2 in Δ. This is provided by our Existence Lemma for → (Lemma 6.11).

Case A = @_t B. Using the induction hypothesis for B, we have:

M^Γ, Δ |=_{ρ^Γ} @_t B ⇔ M^Γ, ρ^Γ(t) |=_{ρ^Γ} B

Now, using part 3 of Lemma 6.6, we have that @_t B ∈ Γ if and only if @_t B in Δ. This completes the case, and the proof.

Lemma 6.13. Let M^Γ = (W^Γ, ρ^Γ, E^Γ) 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 Δ_1 ∩ Δ_2 ≤ Δ_2 ∩ Δ_1, Let Δ in Δ_1 ∩ Δ_2, and suppose A_1 in Δ_1, A_2 in Δ_2. To show Δ in Δ_2 ∩ Δ_1, we have to show A_1 + A_2 in Δ. As Δ in Δ_2 ∩ Δ_1, we have A_1 + A_2 in Δ. As MCSs are closed under modus ponens and A_1 + A_2 in Δ_2, it is provable, we have A_2 + A_1 in Δ.

Associativity. It suffices by commutativity to show that Δ_1 ∩ (Δ_2 ∩ Δ_3) ≤ (Δ_1 ∩ Δ_2) ∩ Δ_3. Assume that Δ in Δ_1 ∩ (Δ_2 ∩ Δ_3) and Δ in (Δ_1 ∩ Δ_2) ∩ Δ_3, which means that for some Δ', Δ'' in Δ_1, we have Δ in Δ' ∩ Δ''. Using part 1 of Lemma 6.6, we have t_1, t_2, t_3 such that t_i in Δ_i for each i ∈ {1, 2, 3}. Thus, Δ = Δ_1 ∩ Δ_2, we have t_1 + t_2 * t_3. Thus, as Δ in Δ_1 ∩ Δ_2, we have t_1 * (t_2 * t_3) ∈ Δ. By applying associativity, t_1 * (t_2 * t_3) = (t_1 * t_2) * t_3 is provable, so (t_1 + t_2) * t_3 ∈ Δ. By two applications of the Existence Lemma for * (Lemma 6.9) we obtain named sets Δ_1, Δ_2, Δ_3, Δ'' in W^Γ such that Δ_i in Σ_i, for each i ∈ {1, 2, 3}, and Δ in Δ ∩ Δ'' in W^Γ.
and $\Delta'' \in \Sigma_1 \circ^f \Sigma_2$. By part 2 of Lemma 6.6, $\Sigma_i = \Delta_i$ for each $i \in \{1, 2, 3\}$. Hence $\Delta \in (\Delta_1 \circ^f \Delta_2) \circ^f \Delta_3$ as required.

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

We still need to show that $\Delta \in E^f \circ^f \Delta$, i.e. that $\Delta \in E_{\Delta} \circ^f \Delta$ for some $\Delta \in E^f$. Using part 1 of Lemma 6.6, we have some $\ell \in \Delta$. Since $\vdash I \ast \ell$ is provable, we have $I \ast \ell \in \Delta$. Using the Existence Lemma for $\ast$ (Lemma 6.9) we obtain named sets $\Delta, \Delta^' \in W^f$ such that $\Delta \in E_{\Delta^'} \circ^f \Delta'$ and $I \in E_{\Delta^'} \circ^f \Delta'$. Thus $\Delta^' \in E^f$ 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 $\rho$ and let $A$ be a pure formula. Suppose that $M, w \models_\rho A[\theta]$ for all $w \in W$ and nominal substitutions $\theta$. Then $A$ is valid in $M$.

**Proof.** Let $\rho^'$ be a hybrid valuation and $w \in W$, we must show that $M, w \models_{\rho^'} A$. Since $M$ is named by $\rho$, we have that for any $\ell \in N$ there is a $k \in N$ such that $\rho(k) = \rho^'(\ell)$. Thus we can define the substitution $\theta$ of nominals for nominals by: $\theta(\ell) = \rho^'(\ell)$ is the first $k \in N$ 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 $\ell$, we must show that $\rho^'(\ell) = w$, and are done since by assumption $w = \rho^'(\ell) = \rho^'(\ell)$. 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 $\text{KB}_{\text{HyBBI}} + Ax$.

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

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

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

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

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

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

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

---

### 7. HyBBI with the $\down$ binder

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

#### 7.1 Formulas and expressivity

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

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

$$M, w \models_{\rho} \down A \iff M, w \models_{\rho[\ell := w]} A$$

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

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

$$(a \ast b) \land (c \ast d)$$

$$(\text{cs})$$

Using the fact that $a, ac$ and $d$ are distinct nominals, we have for any BBI-model $M = (W, \circ, E)$, valuation $\rho$ and $w \in W$,

$$M, w \models_{\rho} A \iff M, w \models_{\rho[\ell := w]} A$$

$$M, w \models_{\rho} A \iff M, w \models_{\rho[\ell := w]} A$$

$$M, w \models_{\rho} A \iff M, w \models_{\rho[\ell := w]} A$$

$$M, w \models_{\rho} A \iff M, w \models_{\rho[\ell := w]} A$$

By a similar chain of reasoning, we have

$$M, w \models_{\rho} A \iff M, w \models_{\rho[\ell := w]} A$$

$$M, w \models_{\rho} A \iff M, w \models_{\rho[\ell := w]} A$$

$$M, w \models_{\rho} A \iff M, w \models_{\rho[\ell := w]} A$$

$$M, w \models_{\rho} A \iff M, w \models_{\rho[\ell := w]} A$$

Putting everything together, we have

$$M, w \models_{\rho} A \iff M, w \models_{\rho[\ell := w]} A \iff M, w \models_{\rho[\ell := w]} A \iff M, w \models_{\rho[\ell := w]} A$$

With the above equivalence for $A$ in place, we can now show that (cs) defines the cross-split property of Definition 3.1.
(⇐) 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 ⊨ ρ (a → b) ∧ (c → d) then M, w ⊨ A. Supposing M, w ⊨ ρ (a → b) ∧ (c → d), we have w ∈ (ρ(a) ∧ ρ(b)) ∩ (ρ(c) ∧ ρ(d)). By the cross-split property, there then exist a, c, ad, bc, bd ∈ W such that ρ(a) ∈ ac ∩ ad, ρ(b) ∈ bc ∩ bd, ρ(c) ∈ ac ∩ bc and ρ(d) ∈ ad ∩ bd. Thus, by the equivalence above, M, w ⊨ A as required.

(⇒) Suppose the formula (cs) is valid in M. We require to show that M has the cross-split property. Suppose w ∈ (t ∨ u) ∩ (v ∨ w). Define a hybrid valuation ρ for M by

\[ ρ(a) = t \quad ρ(b) = u \quad ρ(c) = v \quad ρ(d) = w \]

where a, b, c, d are distinct nominals. We have that M, w \models_ρ (a → b) ∧ (c → d). Thus, as (cs) is valid in M, we have M, w \models_ρ A.

Using the equivalence above, there then exist tw, tw, uw, uw ∈ W such that t ∈ tw ∩ tw, u ∈ uw ∩ uw, v ∈ tw ∩ uw and w ∈ tw ∩ uw as required.

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

\[ M, w \models ρ \iff A \cup B \quad \Leftrightarrow \quad \exists w_1, w_2, w_3, w', w'' \in W. \]

\[ w' \in w_1 \circ w_2 \text{ and } w'' \in w_2 \circ w_3 \text{ and } w' \in w' \circ w_3 \text{ and } M, w'' \models ρ \iff A \cup B \quad \text{and} \quad M, w' \models ρ \iff A \cup B \]

We give below an equivalent formulation of A1 ⊥ A2 solely in terms of HyBBI(↓) connectives. We conjunct that this is not possible in BBI (for arbitrary A1 and A2).

**Proposition 7.4.** For any HyBBI(↓) formulas A1 and A2, the overlapping conjunction A1 ⊥ A2 is definable via the following HyBBI(↓) formula, where ℓ and ℓs do not occur in A1 or A2:

\[ \downarrow α \iff [\downarrow s] B \iff α \iff A \cup B \quad \Leftrightarrow \quad [\downarrow s] B \iff α \iff A \cup B \]

**Proof.** Let M = (W, ω, E) be a BBI-model, ρ a valuation for M, and w ∈ W.

\[ M, w \models ρ \downarrow α \iff \exists w_1, w_2, w_3, w', w'' \in W. \]

\[ w' \in w_1 \circ w_2 \text{ and } w'' \in w_2 \circ w_3 \text{ and } w' \in w' \circ w_3 \text{ and } M, w'' \models ρ \iff A \cup B \quad \text{and} \quad M, w' \models ρ \iff A \cup B \]

Notice now that

\[ M, w_1 \models ρ \iff \downarrow α \iff A_1 \quad \Leftrightarrow \quad \exists w', w_1, w_1' \in w_1 \circ w_1' \text{ and } M, w_1' \models ρ \iff \downarrow α \iff A_1 \quad \Leftrightarrow \quad \exists w', w_1' \in w_1 \circ w_1' \text{ and } M, w_1' \models ρ \iff A_1 \]

Consequently, after applying a similar line of reasoning to w3,

\[ M, w \models ρ \downarrow α \iff \exists w_1, w_2, w_3, w', w'' \in W. \]

\[ w' \in w_1 \circ w_2 \text{ and } w'' \in w_2 \circ w_3 \text{ and } w' \in w' \circ w_3 \text{ and } M, w'' \models ρ \iff A_1 \text{ and } M, w' \models ρ \iff A_2 \]

Since ℓ and ℓs are sufficiently fresh, this is equivalent to

M, w ⊨ ρ A1 ⊥ A2.

A three-place variant A1(ω : B)A2 of the overlapping conjunction was introduced in [9] to deal with forms of specified sharing. This variant tags the shared core of A1 and A2 with a formula B that it satisfies. Its satisfaction is defined as follows:

\[ M, w \models ρ A1(ω : B)A2 \iff \exists w_1, w_2, w_3, w', w'' \in W. \]

\[ w' \in w_1 \circ w_2 \text{ and } w'' \in w_2 \circ w_3 \text{ and } w' \in w' \circ w_3 \text{ and } M, w'' \models ρ \iff A_1 \text{ and } M, w' \models ρ \iff A_2 \]

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

\[ \downarrow α \iff \downarrow s \iff \Leftrightarrow B \iff α \iff \downarrow s \iff \Leftrightarrow B \]

**7.2 Proof theory, soundness and completeness**

**Definition 7.5.** We define [K]HyBBI(↓) to be the proof system obtained by adding the following axiom schema to [K]HyBBI:

\[ \text{ (Bind ↓) } \quad \downarrow α \iff \downarrow s \iff \Leftrightarrow B \iff α \iff \downarrow s \iff \Leftrightarrow B \]

**Lemma 7.6 (Nominal Substitution Lemma).** We have for any model M = (W, ω, E), hybrid valuation ρ, HyBBI(↓)-formula A and nominals j, ℓ,

\[ M, ρ(j) \models ρ A[j/ℓ] \iff M, ρ(j) \models ρ[ℓ := ρ(ℓ)] A \quad \text{where}[j/ℓ] \text{ is a (capture-avoiding) nominal substitution.} \]

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

Case A = k ∈ N. The required equivalence becomes:

\[ M, ρ(j) \models ρ k[j/ℓ] \iff M, ρ(j) \models ρ[ℓ := ρ(ℓ)] k \quad \text{i.e.} \]

\[ ρ(j) = ρ k[j/ℓ] \iff ρ(j) = ρ[ℓ := ρ(ℓ)](k) \quad \text{which follows from the identity above.} \]

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

\[ M, ρ(j) \models k/j B[j/ℓ] \iff M, ρ(j) \models[k/j := ρ(ℓ)] B[j/ℓ] \quad \text{by (ind. hyp.)} \]

\[ M, ρ(j) \models ρ[ℓ := ρ(ℓ)] B[j/ℓ] \text{ and } M \models ρ[ℓ := ρ(ℓ)] k/j B[j/ℓ] \]

This completes all cases.

**Proposition 7.7.** Any [K]HyBBI(↓)-provable formula is valid.

**Proof.** Given the soundness of [K]HyBBI (Proposition 5.2), we just need to show that the new axiom (Bind ↓) is valid in all BBI-models. Let M = (W, ω, E) be a BBI-model, let ρ be a valuation for M and let w ∈ W. We need to show that

M, w ⊨ ρ A, B \iff \text{M, ρ(j) ⊨ } j/k B[j/ℓ]

i.e.

M, ρ(j) ⊨ ρ k/j B \iff M, ρ(j) ⊨ ρ[ℓ := ρ(ℓ)] B[j/ℓ]

i.e.

M, ρ(j) ⊨ ρ[ℓ := ρ(ℓ)] B \iff M, ρ(j) ⊨ ρ B[j/ℓ]

which is guaranteed by Lemma 7.6.
We can obtain a parametric completeness result for $K_{\text{HyBBI}(\downarrow)}$ by repeating the Lindenbaum model construction for $K_{\text{HyBBI}}$ 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 $\text{HyBBI}(\downarrow)$-formula $A$ and $\Delta \in W^\uparrow$, we have $M^\uparrow, \Delta \models \rho \downarrow^\Delta A$ 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 $\Delta = \{ A \mid \emptyset \ell. A \in \Gamma \}$ for some nominal $j$, we proceed as follows:

\[
M^\uparrow, \Delta \models \rho \downarrow^\Delta \downarrow \ell. B \iff M^\uparrow, \Delta \models \rho \downarrow^{\ell(\ell^\Delta)} B
\]

\[
\iff M^\uparrow, \Delta \models \rho \downarrow^{\ell j B}\downarrow^\Delta j/\ell
\]

(by Lemma 7.6)

\[
\iff \emptyset j, B[j/\ell] \in \Delta
\]

(by ind. hyp.)

Now since $\Gamma$ is an MCS and thus closed under $(K_0)$ and the new axiom (Bind $\downarrow$), we have $\emptyset j, B[j/\ell] \in \Gamma$ if and only if $\emptyset, \downarrow \ell. B \in \Gamma$ if and only if $\ell. B \in \Delta$, which completes the case.

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

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

Corollary 7.10. Let $S$ be an any separation theory from Definition 3.1, and let $Ax$ be the set of pure $\text{HyBBI}(\downarrow)$-formulas defining the properties $S$, as given by Corollary 4.4 and Proposition 7.3. Then a $\text{HyBBI}(\downarrow)$-formula is provable in $K_{\text{HyBBI}(\downarrow)} + Ax$ if and only if it is valid in the class of BBI-models satisfying $S$.

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