Sub-classical Boolean Bunched Logics and the Meaning of Par

James Brotherston[1] and Jules Villard[2]

1 **Department of Computer Science, University College London, UK**
2 **Department of Computing, Imperial College London, UK**

Abstract

We investigate intermediate logics between the bunched logics Boolean BI and Classical BI, obtained by combining classical propositional logic with various flavours of Hyland and De Paiva's full intuitionistic linear logic. Thus, in addition to the usual multiplicative conjunction (with its adjoint implication and unit), our logics also feature a multiplicative *disjunction* (with its adjoint co-implication and unit). The multiplicatives behave "sub-classically", in that disjunction and conjunction are related by a *weak distribution* principle, rather than by De Morgan equivalence.

We formulate a Kripke semantics, covering all our sub-classical bunched logics, in which the multiplicatives are naturally read in terms of resource operations. Our main theoretical result is that validity according to this semantics coincides with provability in a corresponding Hilbert-style proof system.

Our logical investigation sheds considerable new light on how one can understand the multiplicative disjunction, better known as linear logic's "par", in terms of resource operations. In particular, and in contrast to the earlier Classical BI, the models of our logics include the heap-like memory models of separation logic, in which disjunction can be interpreted as a property of intersection operations over heaps.

1998 ACM Subject Classification F.3.1 Logics and Meanings of Programs, F.4.1 Mathematical Logic and Formal Languages

Keywords and phrases Bunched logic, linear logic, modal logic, Kripke semantics, model theory

Digital Object Identifier 10.4230/LIPIcs.CSL.2015.325

1 Introduction

Bunched logics, which are free combinations of a standard propositional logic with some variety of multiplicative linear logic [3, 19], have applications in computer science as a means of expressing and manipulating properties of *resource* [18, 20]. Most notably, *separation logic* [21], which has been successfully employed in large-scale program verification [7, 22, 14] is based upon the bunched logic *Boolean BI* (BBI) obtained by combining ordinary classical logic with *multiplicative intuitionistic linear logic* (MILL) [13].

BBI has a simple Kripke semantics under which a formula of BBI is read as a set of elements ("resources") in an underlying *model*, essentially a generalised commutative monoid. The classical connectives have their usual meanings, and the MILL connectives (called *multiplicative*) are given "resource composition" readings: A multiplicative conjunction of formulas $A * B$ denotes those elements which divide, via the monoid operation, into two elements satisfying A and B respectively; the unit $\top^*$ of $*$ denotes the set of units of the monoid; and an implication (or "magic wand") $A \mathrel{-\!\!*} B$ denotes those elements that, when extended with an element satisfying A, always yield an element satisfying B.

24th EACSL Annual Conference on Computer Science Logic (CSL 2015).
Editor: Stephan Kreutzer; pp. 325–342
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

In this paper, we set out to answer the following question: What is the right way of adding a multiplicative *disjunction* – a.k.a. linear logic's notoriously tricky "par" – to BBI? A first answer to this question came previously in the study of *Classical BI* (CBI) [4], given by extending classical logic with *classical* multiplicative linear logic, i.e., MLL rather than MILL. Similar to MLL, the multiplicative disjunction $\mathbin{\rotatebox[origin=c]{180}{$\&$}}$ in CBI is the De Morgan dual of $*$ with respect to the multiplicative negation $\sim$: we have $(A \mathbin{\rotatebox[origin=c]{180}{$\&$}} B \equiv \sim(\sim A * \sim B))$. However, this is not very semantically informative. Furthermore, the heap-like models of BBI employed in separation logic (see e.g. [10]) turn out not to be models of CBI. This naturally raises the question of whether there might be bunched logics between BBI and CBI permitting the interpretation of multiplicative disjunction in such models.

Here, we shed new light on multiplicative disjunction by investigating "sub-classical" versions of bunched logic, under the common name BiBBI, obtained by combining classical logic with Hyland and De Paiva's *full intuitionistic linear logic* (FILL) [16]. In FILL, the conjunction $*$ and disjunction $\mathbin{\rotatebox[origin=c]{180}{$\&$}}$ are related not by De Morgan equivalence, but rather by *weak distribution*, i.e.

$$A * (B \mathbin{\rotatebox[origin=c]{180}{$\&$}} C) \vdash (A * B) \mathbin{\rotatebox[origin=c]{180}{$\&$}} C,$$

which follows from De Morgan equivalence, but is not equivalent to it. The disjunction $\mathbin{\rotatebox[origin=c]{180}{$\&$}}$ can also be endowed with a unit $\bot^*$ and an adjoint *co-implication*, $\setminus^*$ ("magic slash").

We define provability in BiBBI simply by combining suitable Hilbert systems for classical logic and for FILL; the resulting Hilbert system can equivalently be reformulated as a *display calculus* proof system with the cut-elimination property, cf. [1, 3]. Our main technical contribution in this paper is a suitable Kripke frame semantics for BiBBI in which validity of BiBBI-formulas exactly coincides with provability. We obtain completeness of provability for validity in our semantics by embedding BiBBI into a suitable modal logic and deploying Sahlqvist's well-known completeness theorem (see e.g. [2]).

We consider a number of variants of BiBBI, based on whether or not various natural logical principles of FILL are included. For each such principle, we can write down an equivalent first-order condition on the Kripke models of BiBBI, with the frame condition corresponding to the above weak distribution law being particularly interesting. This fact enables us to present soundness and completeness results that are modular with respect to any choice of BiBBI-variant from our considered class.

We also undertake an investigation into the models of BiBBI, and present some general constructions for building them. From the program logic perspective, perhaps the most interesting aspect of BiBBI is that the standard heap-like models of separation logic can be extended into BiBBI-models obeying the weak distribution law, by interpreting disjunction using a notion of *intersection* between heaps (and there are at least two natural such intersection operations). We show that the typical unit law for $\mathbin{\rotatebox[origin=c]{180}{$\&$}}$, given by $A \mathbin{\rotatebox[origin=c]{180}{$\&$}} \bot^* \equiv A$, must fail in such models. However, we also show how to build more complicated models in which both weak distribution and the unit law do hold.

The remainder of this paper is structured as follows. In Section 2 we recall the model-theoretic and proof-theoretic characterisations of BBI and CBI. We then introduce our sub-classical bunched logic BiBBI, via both a Kripke frame semantics and a Hilbert-style axiomatic proof system, in Section 3. In Section 4 we investigate the models of BiBBI in more detail, and present some general model constructions and conservativity results. Section 5 presents the details of our completeness proof, and Section 7 concludes.

Due to space limitations, the proofs of the results in this paper have been abbreviated. Most of the full proofs can be found in an associated technical report [5].

2 Boolean and Classical BI

In this section, we recall the basic characterisations of *provability* and *validity* (based on Kripke semantics) in the bunched logics BBI [17, 11] and CBI [4]. We assume a countably infinite set $\mathcal{V}$ of propositional variables, and write $\mathcal{P}(X)$ for the powerset of a set X.

2.1 Boolean BI

▶ **Definition 2.1.** *BBI-formulas* are built from propositional variables $P \in \mathcal{V}$ using the standard connectives $\top, \bot, \neg, \wedge, \vee, \rightarrow$ of propositional classical logic, and the so-called "multiplicative" connectives: the constant $\top^*$ and binary operators $*$ and $\mathrel{-\!\!*}$. By convention, $\neg$ has the highest precedence, followed by $*$, $\wedge$ and $\vee$, with $\rightarrow$ and $\mathrel{-\!\!*}$ having lowest precedence.

▶ **Definition 2.2.** *Provability* in BBI is given by extending a complete Hilbert system for classical logic with the following axioms and inference rules for $*$, $\mathrel{-\!\!*}$ and $\top^*$. The "sequent" notation $A \vdash B$ is syntactic sugar for the formula $A \rightarrow B$.

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

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

▶ **Definition 2.3.** 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 $\mathcal{P}(W) \times \mathcal{P}(W) \rightarrow \mathcal{P}(W)$ by $W_1 \circ W_2 = \bigcup_{w_1 \in W_1, w_2 \in W_2} w_1 \circ w_2$.

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 $w \in W$. (By definition, the latter means that $\bigcup_{e \in E} w \circ e = \{w\}$ for all $w \in W$.) We call E the set of *units* of the model $\langle W, \circ, E\rangle$.

If in a BBI-model $M = \langle W, \circ, E\rangle$ we have $|w_1 \circ w_2| \leq 1$ for all $w_1, w_2 \in W$, then we say that M is *partial functional* and understand $\circ$ as a partial function of type $W \times W \rightharpoonup W$.

▶ **Example 2.4.** The standard *heap model* $\langle \text{Heaps}, \circ, \{e\}\rangle$ of separation logic [21] is defined as follows. First, $\text{Heaps} = \text{Loc} \rightharpoonup_{\text{fin}} \text{Val}$ is the set of partial functions mapping finitely many *locations* in Loc to *values* in Val (typically Loc, Val are both infinite sets, with $\text{Loc} \subset \text{Val}$). We write $\mathsf{dom}(h)$ for the set of locations on which h is defined. We define $h_1 \circ h_2$ to be the union of heaps h_1 and h_2 if $\mathsf{dom}(h_1)$ and $\mathsf{dom}(h_2)$ are disjoint (and undefined otherwise), and we let e be the *empty heap* with $\mathsf{dom}(e) = \emptyset$. It is straightforward to verify that $\langle \text{Heaps}, \circ, \{e\}\rangle$ is a partial functional BBI-model.

▶ **Definition 2.5.** Let $M = \langle W, \circ, E\rangle$ be a BBI-model. A *valuation* for M is a function $\rho : \mathcal{V} \rightarrow \mathcal{P}(W)$ assigning to each proposition P a set $\rho(P) \subseteq W$. Given a valuation ρ for M, a $w \in W$ and a BBI-formula A, we define the forcing relation $w \models_\rho A$ by induction on A:

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

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

▶ **Theorem 2.6** ([11]). *A BBI-formula is BBI-valid if and only if it is BBI-provable.*

2.2 Classical BI

▶ **Definition 2.7.** *CBI-formulas* are defined as BBI-formulas (Defn. 2.1), except that they may also contain the "multiplicative falsum" constant $\bot^*$. We write $\sim A$ as an abbreviation for $A \twoheadrightarrow \bot^*$, and $A \,⅋\, B$ as an abbreviation for $\sim(\sim A * \sim B)$.

▶ **Definition 2.8.** Provability in CBI is defined as provability in the Hilbert system for BBI (Defn. 2.2) extended with the "double negation elimination" axiom, $\sim\sim A \vdash A$.

▶ **Definition 2.9.** A *CBI-model* is given by a tuple $\langle W, \circ, E, U\rangle$, where $\langle W, \circ, E\rangle$ is a BBI-model (see Defn. 2.3), $U \subseteq W$, and for each $w \in W$, there is a unique $-w \in W$ (the "dual" of w) satisfying $(w \circ -w) \cap U \neq \emptyset$.

Given a CBI-model $\langle W, \circ, E, U\rangle$, the condition in Defn. 2.9 induces a function $- : W \to W$ sending w to $-w$, and necessarily $--w = w$ for any $w \in W$ (see [4]). Moreover, extending $-$ pointwise to sets, it is easy to show that $-E = U$. Therefore, intuitively, $-$ should be understood as a sort of "inverse" function on worlds [4]. E.g., every Abelian group is trivially a CBI-model, with $-w$ the group inverse of w.

▶ **Definition 2.10.** A valuation for a CBI-model and satisfaction $w \models_\rho A$ of a CBI-formula A by the world w and valuation ρ are defined as for BBI (Defn. 2.5), except that we add the following clause for satisfaction of the multiplicative falsum: $w \models_\rho \bot^* \;\Leftrightarrow\; w \notin U$.

It is then straightforward to derive the following satisfaction clauses for $\sim$ and ⅋:

$$\begin{array}{rcl} w \models_\rho \sim A & \Leftrightarrow & -w \not\models_\rho A \\ w \models_\rho A \,⅋\, B & \Leftrightarrow & \forall w_1, w_2 \in W.\ \text{if } w \in -(-w_1 \circ -w_2) \text{ then } w_1 \models_\rho A \text{ or } w_2 \models_\rho B \end{array}$$

▶ **Theorem 2.11** ([4, 3]). *A CBI-formula is CBI-valid if and only if it is CBI-provable.*

Unfortunately, CBI cannot be used to reason about heap-like memory models:

▶ **Proposition 2.12.** *Given the heap model* $\langle \text{Heaps}, \circ, \{e\}\rangle$ *of BBI defined in Example 2.4, there is no set* $U \subseteq \text{Heaps}$ *such that* $\langle \text{Heaps}, \circ, \{e\}, U\rangle$ *is a CBI-model.*

Proof. Suppose for contradiction that such a U exists. By the remark following Defn. 2.9, we have $U = -\{e\} = \{-e\}$. Note that $-e \in \text{Heaps}$ and thus $\mathsf{dom}(-e)$ is finite. Let h be a heap with $\mathsf{dom}(h) \supset \mathsf{dom}(-e)$ (there are infinitely many such h). Then there exists a heap $-h$ such that $h \circ -h = -e$ by the CBI-axiom, but it is clear that there is no such heap. ◀

▶ **Theorem 2.13** ([4]). *CBI is not conservative over BBI, i.e., there are BBI-formulas that are CBI-valid but not BBI-valid.*

3 BiBBI: Sub-classical Boolean bunched logic

In this section we introduce our *sub-classical* Boolean bunched logic, BiBBI, which extends BBI with multiplicative disjunction ⅋, together with its adjoint co-implication $\backslash^*$ ("magic slash") and the multiplicative falsum $\bot^*$. We adopt the "Bi" prefix in BiBBI to remind ourselves that, like in FILL [16], we have two families of multiplicative connectives, $(*, -\!\!*, \top^*)$ and $(\mathbin{\check{\vee}}^*, \setminus^*, \bot^*)$, that are not however connected by De Morgan equivalences.

First, we present a basic characterisation of Kripke validity for BiBBI-formulas and an associated notion of basic provability. Then, we consider a range of variants of the basic logic obtained by adding various logical laws from FILL (see Figure 1), which we regard as a sort of "logical buffet" from which we can pick and choose the principles we wish to include. (Commutativity of $\mathbin{\check{\vee}}^*$ is considered a basic principle for technical convenience: a non-commutative $\mathbin{\check{\vee}}^*$ naturally leads to both $\setminus^*$ and $\bot^*$ splitting into two connectives.)

Our choice of models and interpretation achieves several complementary objectives:

1. BiBBI extends BBI and, furthermore, when a suitable "classicality" axiom is added to BiBBI, it collapses into CBI (see Prop. 3.9). Thus, the variants of BiBBI can be seen as intermediate logics between BBI and CBI.
2. We interpret multiplicative disjunction $\mathbin{\check{\vee}}^*$ in BiBBI as a natural dual of multiplicative conjunction $*$, in that $\mathbin{\check{\vee}}^*$ can be read as a binary *box modality* in modal logic [2], while $*$ can be read as a binary *diamond modality*.
3. For each natural logical principle of FILL governing $\mathbin{\check{\vee}}^*$, $\setminus^*$ and $\bot^*$, one can write down an equivalent first-order condition on BiBBI-models (see Figure 1).
4. Finally, for *any* variant of BiBBI obtained by taking some combination of logical axioms from Figure 1, we achieve soundness and completeness for that variant with respect to the associated class of models.

▶ **Definition 3.1.** A *BiBBI-formula* is defined as a BBI-formula (Defn. 2.1), except that it may also contain the multiplicative constant $\bot^*$, and the binary multiplicative connectives $\setminus^*$ and $\mathbin{\check{\vee}}^*$. As in CBI, we write $\sim\! A$ as an abbreviation for $A -\!\!* \bot^*$.

▶ **Definition 3.2.** A *basic BiBBI-model* is a tuple of the form $\langle W, \circ, E, \triangledown, U\rangle$, where $\langle W, \circ, E\rangle$ is a BBI-model, $U \subseteq W$ and $\triangledown \colon W \times W \to \mathcal{P}(W)$ is commutative. We extend $\triangledown$ pointwise to sets in a similar manner to $\circ$: $W_1 \triangledown W_2 = \bigcup_{w_1 \in W_1, w_2 \in W_2} w_1 \triangledown w_2$.

A valuation for a basic BiBBI-model $M = \langle W, \circ, E, \triangledown, U\rangle$ is defined as in Defn. 2.5. Satisfaction $w \models_\rho A$ of a BiBBI-formula A by the valuation ρ and world w is given by extending the forcing relation in Defn. 2.5 as follows:

$$\begin{array}{rcl} w \models_\rho \bot^* & \Leftrightarrow & w \notin U \\ w \models_\rho A \mathbin{\check{\vee}}^* B & \Leftrightarrow & \forall w_1, w_2 \in W.\ \text{if } w \in w_1 \triangledown w_2 \text{ then } w_1 \models_\rho A \text{ or } w_2 \models_\rho B \\ w \models_\rho A \setminus^* B & \Leftrightarrow & \exists w', w'' \in W.\ w'' \in w' \triangledown w \text{ and } w'' \models_\rho A \text{ and } w' \not\models_\rho B \end{array}$$

Similarly to BBI and CBI (see Section 2), a BiBBI-formula A is *valid in M* if $w \models_\rho A$ for all $w \in W$ and valuations ρ, and *BiBBI-valid* if it is valid in all BiBBI-models.

Intuitively, the binary operation $\triangledown$ and set U in a BiBBI-model $\langle W, \circ, E, \triangledown, U\rangle$ are used to interpret the connectives $\mathbin{\check{\vee}}^*$, $\setminus^*$ and $\bot^*$ in a way analogous to the use of $\circ$ and E to interpret $*$, $-\!\!*$ and $\top^*$. However, the analogy is not necessarily exact since, depending on the variant of BiBBI we consider, $\triangledown$ and U may exhibit quite different properties to $\circ$ and E. (For example, $\triangledown$ might fail to be associative.)

We note that the connective $\setminus^*$ was not present in the original formulation of FILL, although Clouston et al. [9] recently showed that its addition to FILL is conservative. Here, observe that $\setminus^*$ is interpreted as the natural adjoint of $\mathbin{\check{\vee}}^*$ in basic BiBBI-models.

Principle	**Axiom** $\mathcal{A}$	**Frame condition** $\mathcal{F}(\mathcal{A})$
Associativity	$A \bigtriangledown\!\!\!\!{}^{*}\, (B \bigtriangledown\!\!\!\!{}^{*}\, C) \vdash (A \bigtriangledown\!\!\!\!{}^{*}\, B) \bigtriangledown\!\!\!\!{}^{*}\, C$	$w_1 \triangledown (w_2 \triangledown w_3) = (w_1 \triangledown w_2) \triangledown w_3$
Unit weakening	$A \vdash A \bigtriangledown\!\!\!\!{}^{*}\, \bot^*$	$w \triangledown U \subseteq \{w\}$
Unit contraction	$A \bigtriangledown\!\!\!\!{}^{*}\, \bot^* \vdash A$	$w \in w \triangledown U$
Contraction	$A \bigtriangledown\!\!\!\!{}^{*}\, A \vdash A$	$w \in w \triangledown w$
Weak distribution	$A * (B \bigtriangledown\!\!\!\!{}^{*}\, C) \vdash (A * B) \bigtriangledown\!\!\!\!{}^{*}\, C$	if $(x_1 \circ x_2) \cap (y_1 \triangledown y_2) \neq \emptyset$ then $\exists w.\ y_1 \in x_1 \circ w$ and $x_2 \in w \triangledown y_2$
Classicality	$\sim\sim A \vdash A$	$\exists! -w.\ (w \circ -w) \cap U \neq \emptyset$

Figure 1 Optional axioms of BiBBI and the corresponding first-order frame conditions (we suppress outermost universal quantifiers over the model domain).

▶ **Definition 3.3.** *Provability for basic BiBBI* is given by extending the proof system for BBI (see Defn. 2.2) with the following axioms and inference rules:

Monotonicity:

$$\frac{A_1 \vdash B_1 \quad A_2 \vdash B_2}{A_1 \bigtriangledown\!\!\!\!{}^{*}\, A_2 \vdash B_1 \bigtriangledown\!\!\!\!{}^{*}\, B_2}$$

Residuation:

$$\frac{A \vdash B \bigtriangledown\!\!\!\!{}^{*}\, C}{A \setminus\!\!{}^{*}\, B \vdash C} \qquad \frac{A \setminus\!\!{}^{*}\, B \vdash C}{A \vdash B \bigtriangledown\!\!\!\!{}^{*}\, C}$$

Commutativity:

$$A \bigtriangledown\!\!\!\!{}^{*}\, B \vdash B \bigtriangledown\!\!\!\!{}^{*}\, A$$

▶ **Theorem 3.4.** *If a formula A is provable for basic BiBBI (Defn. 3.3) then it is valid in all basic BiBBI-models.*

Proof (sketch). By soundness for standard BBI (Theorem 2.6) it suffices to show that the axioms and rules in Defn. 3.3 preserve validity in any basic BiBBI-model. ◀

▶ **Definition 3.5.** A *variant* of BiBBI is obtained by adding, for any combination of "principles" from Figure 1, (a) the logical axiom $\mathcal{A}$ for that principle to the basic BiBBI proof system in Defn. 3.3, and (b) the frame condition $\mathcal{F}(\mathcal{A})$ for that principle as an additional condition on the basic BiBBI-models in Defn. 3.2.

We investigate the variants of BiBBI and their models more closely in Section 4. For now, we just show that the correspondences laid out in Figure 1 are exact.

▶ **Theorem 3.6.** *For each principle in Figure 1, the axiom $\mathcal{A}$ is valid in a basic BiBBI-model M if and only if M satisfies the corresponding frame condition $\mathcal{F}(\mathcal{A})$.*

Proof (sketch). Let $M = \langle W, \circ, E, \triangledown, U \rangle$ be a basic BiBBI-model. We distinguish a case for each principle from Figure 1. Here we just show the most interesting cases: weak distribution and classicality.

Weak distribution: ($\Leftarrow$) Assuming that the weak distribution frame condition holds in M, we have to show that $A * (B \bigtriangledown\!\!\!\!{}^{*}\, C) \vdash (A * B) \bigtriangledown\!\!\!\!{}^{*}\, C$ is valid in M. So, given $w \models_\rho A * (B \bigtriangledown\!\!\!\!{}^{*}\, C)$, we must show $w \models_\rho (A * B) \bigtriangledown\!\!\!\!{}^{*}\, C$. This means showing, assuming $w \in w_1 \triangledown w_2$, that $w_1 \models_\rho A * B$ or $w_2 \models_\rho C$. Since we have $w \models_\rho A * (B \bigtriangledown\!\!\!\!{}^{*}\, C)$, we have $w \in x_1 \circ x_2$ where $x_1 \models_\rho A$ and $x_2 \models_\rho B \bigtriangledown\!\!\!\!{}^{*}\, C$. Thus we have $(x_1 \circ x_2) \cap (w_1 \triangledown w_2) \neq \emptyset$, so by the weak distribution property there exists $y \in W$ such that $w_1 \in x_1 \circ y$ and $x_2 \in y \triangledown w_2$. Now, since $x_2 \in y \triangledown w_2$ and $x_2 \models_\rho B \bigtriangledown\!\!\!\!{}^{*}\, C$ we have $y \models_\rho B$ or $w_2 \models_\rho C$. If $w_2 \models_\rho C$, we are done. If not, we have $w_1 \in x_1 \circ y$ and $x_1 \models_\rho A$ and $y \models_\rho B$, i.e., $w_1 \models_\rho A * B$ as required.

($\Rightarrow$) Assuming that $A * (B \bigtriangledown\!\!\!\!{}^{*}\, C) \vdash (A * B) \bigtriangledown\!\!\!\!{}^{*}\, C$ is valid in M, we have to show that the weak distribution frame condition holds in M. That is, supposing $z \in (x_1 \circ x_2) \cap (y_1 \triangledown y_2)$, we need a $w \in W$ such that $y_1 \in x_1 \circ w$ and $x_2 \in w \triangledown y_2$. Let A, B, C be propositional variables and define a valuation ρ for M by

$$\rho(A) = \{x_1\}\ , \qquad \rho(B) = \{w \in W \mid x_2 \in w \triangledown y_2\}\ , \quad \text{and} \quad \rho(C) = W \setminus \{y_2\}\ .$$

We claim that $x_2 \models_\rho B \,\check{\triangledown}\, C$. To see this, let $x_2 \in w_1 \triangledown w_2$. By construction of ρ, if $w_2 \not\models_\rho C$ then $w_2 = y_2$ and hence $w_1 \models_\rho B$. Thus either $w_1 \models_\rho B$ or $w_2 \models_\rho C$ as required. Now, since $z \in x_1 \circ x_2$, with $x_1 \models_\rho A$ and $x_2 \models_\rho B \,\check{\triangledown}\, C$ by the above, we obtain $z \models_\rho A * (B \,\check{\triangledown}\, C)$. Since the weak distribution axiom is valid in M, we get $z \models_\rho (A * B) \,\check{\triangledown}\, C$. Then, as $z \models_\rho (A * B) \,\check{\triangledown}\, C$ and $z \in y_1 \triangledown y_2$ but $y_2 \not\models_\rho C$, we must have $y_1 \models_\rho A * B$. This means that there exist $u, w \in W$ with $y_1 \in u \circ w$ and $u \models_\rho A$ and $w \models_\rho B$. By definition of ρ, this means that $y_1 \in x_1 \circ w$ and $x_2 \in w \triangledown y_2$, as required.

Classicality: ($\Leftarrow$) Assuming the classicality condition, i.e. the CBI-model axiom, holds in M, we have to show that $\sim\sim A \vdash A$ is valid. Assume that $w \models_\rho \sim\sim A$. Using the clause for satisfaction of $\sim$ given in Section 2, we have $--w \models_\rho A$, and thus immediately $w \models_\rho A$ as required, using the fact (also from Section 2) that $--w = w$.

($\Rightarrow$) Assuming that $\sim\sim A \vdash A$ is valid in M, we have to show that, for any $w \in W$, there is a unique $w' \in W$ such that $(w \circ w') \cap U \neq \emptyset$. Let A be a propositional variable and define a valuation ρ for M by $\rho(A) = W \setminus \{w\}$. By construction, $w \not\models_\rho A$, so using the main assumption we have $w \not\models_\rho (A \mathrel{-\!\!*} \bot^*) \mathrel{-\!\!*} \bot^*$. Thus, there exist $w', w'' \in W$ such that $w'' \in w \circ w'$ and $w' \models_\rho A \mathrel{-\!\!*} \bot^*$ but $w'' \not\models_\rho \bot^*$, i.e. $w'' \in U$. That is, there exists an $-w = w' \in W$ such that $(w \circ -w) \cap U \neq \emptyset$.
It just remains to show that $-w$ is unique. Write $\mathrm{Co}(w)$ for the set of all w' such that $(w \circ w') \cap U \neq \emptyset$, and extend Co pointwise to sets as usual. Note that, by the above, $\mathrm{Co}(w)$ is nonempty. First we show that $\mathrm{Co}(\mathrm{Co}(w)) \subseteq \{w\}$. Define a new valuation ρ' for M by $\rho'(A) = \{w\}$, so that $w \models_{\rho'} A$ by construction. Since $A \vdash \sim\sim A$ is already provable in BBI, we have $w \models_{\rho'} (A \mathrel{-\!\!*} \bot^*) \mathrel{-\!\!*} \bot^*$. It is easy to show that this means that $w' \models_{\rho'} A$ for all $w' \in \mathrm{Co}(\mathrm{Co}(w))$, i.e., $\mathrm{Co}(\mathrm{Co}(w)) \subseteq \{w\}$ as required. Furthermore, letting $-w \in \mathrm{Co}(w)$, we have $(w \circ -w) \cap U \neq \emptyset$ and hence $(-w \circ w) \cap U \neq \emptyset$, i.e., $w \in \mathrm{Co}(\mathrm{Co}(w))$. Hence $\mathrm{Co}(\mathrm{Co}(w)) = \{w\}$. It is easy to see that $\mathrm{Co}(w)$ must then be a singleton set: if $w_1, w_2 \in \mathrm{Co}(w)$ then $\mathrm{Co}(w_1), \mathrm{Co}(w_2) \subseteq \mathrm{Co}(\mathrm{Co}(w)) = \{w\}$. Hence $\mathrm{Co}(w_1) = \mathrm{Co}(w_2) = \{w\}$, and so $\mathrm{Co}(\mathrm{Co}(w_1)) = \mathrm{Co}(\mathrm{Co}(w_2))$, i.e. $w_1 = w_2$ as required. This completes the proof. ◀

▶ **Corollary 3.7** (Soundness). *If a formula is provable in some variant of BiBBI then it is valid in that variant.*

Proof. Follows immediately from Theorems 3.4 and 3.6. ◀

We also have the converse completeness result:

▶ **Theorem 3.8** (Completeness). *If a BiBBI-formula is valid in some variant of BiBBI then it is provable in that variant.*

We defer the detailed proof of Theorem 3.8 until Section 5.

Turning to proof theory, we can reformulate the family of Hilbert-style proof systems above for BiBBI and its variants as a *display calculus* having the cut-elimination property, where each variant property in Figure 1 is captured by an optional structural rule in the calculus. We present our display calculus for BiBBI in Section 6.

To conclude this section, we show that CBI can be seen as the variant of BiBBI obeying the "classicality" axiom in Figure 1.

▶ **Proposition 3.9.** *BiBBI and CBI are related by the following:*

1. *For any BiBBI-model* $\langle W, \circ, E, \triangledown, U\rangle$ *satisfying the classicality axiom, the tuple* $\langle W, \circ, E, U\rangle$ *is a CBI-model.*
2. *If* $\langle W, \circ, E, U\rangle$ *is a CBI-model and we define* $w_1 \triangledown w_2 = -(-w_1 \circ -w_2)$*, then the tuple* $\langle W, \circ, E, \triangledown, U\rangle$ *is a BiBBI-model satisfying all axioms but contraction in Figure 1.*
3. *When CBI-models are identified with BiBBI-models as above, CBI-validity coincides with validity in the variant of BiBBI satisfying all properties but contraction in Figure 1.*

Proof. Part 1 of the proposition is immediate by construction. For part 2, let $\langle W, \circ, E, U\rangle$ be a CBI-model. It is immediate that $\langle W, \circ, E, \triangledown, U\rangle$ is a basic BiBBI-model. We have to check that $\langle W, \circ, E, \triangledown, U\rangle$ satisfies the required frame conditions. Classicality is exactly the CBI-model axiom, so is trivially satisfied (and consequently we have $--w = w$ for any $w \in W$ and $-E = U$). For associativity, we check:

$$\begin{array}{rcll} w_1 \triangledown (w_2 \triangledown w_3) & = & -(-w_1 \circ --(-w_2 \circ -w_3)) & \\ & = & -(-w_1 \circ (-w_2 \circ -w_3)) & (\text{since } --X = X) \\ & = & -((-w_1 \circ -w_2) \circ -w_3) & (\text{by associativity of } \circ) \\ & = & -(--(-w_1 \circ -w_2) \circ -w_3) & (\text{since } --X = X) \\ & = & (w_1 \triangledown w_2) \triangledown w_3 & \end{array}$$

For the unit axioms, we can similarly check that $U \triangledown w = \{w\}$. Finally, we must verify the weak distribution condition. Suppose $(x_1 \circ x_2) \cap (y_1 \triangledown y_2) \neq \emptyset$. That is, for some $z \in x_1 \circ x_2$ we have $z \in -(-y_1 \circ -y_2)$, i.e. $-z \in -y_1 \circ -y_2$, which is again equivalent (see [4]) to $y_1 \in z \circ -y_2$. Putting everything together and using associativity of $\circ$, we get $y_1 \in x_1 \circ (x_2 \circ -y_2)$. Thus, for some $w \in x_2 \circ -y_2$, we have $y_1 \in x_1 \circ w$. But, using the same properties as before, $w \in x_2 \circ -y_2$ is equivalent to $-x_2 \in -w \circ -y_2$ and then to $x_2 \in -(-w \circ -y_2)$, i.e. $x_2 \in w \triangledown y_2$ as required. This completes the verification.

Finally, for part 3, just observe that the clauses for satisfaction of $\bot^*$ coincide in the forcing relations for BiBBI and CBI, and that by inserting the definition of $\triangledown$ into BiBBI's clause for $\mathbin{\overset{*}{\vee}}$, we obtain exactly the usual CBI clause for $\mathbin{\overset{*}{\vee}}$. ◀

4 General constructions for BiBBI-models

In this section, we investigate the models of our variants of BiBBI, and present some general constructions for BiBBI-models, chiefly based on the heap-like models of BBI.

We begin with some simple constructions yielding conservativity results. Let $\langle W, \circ, E\rangle$ be a BBI-model. First, define $w \triangledown_= w' = \{w\}$ if $w = w'$, and $w \triangledown_= w' = \emptyset$ otherwise. Then $\langle W, \circ, E, \triangledown_=, W\rangle$ is easily seen to be a BiBBI-model satisfying associativity, unit weakening, unit contraction and contraction. Second, defining $w \triangledown_0 w' \stackrel{\text{def}}{=} \emptyset$ for all $w, w' \in W$, we have that $\langle W, \circ, E, \triangledown_0, U\rangle$ (for any $U \subseteq W$) is a BiBBI-model satisfying associativity, unit weakening and weak distribution. Consequently, we have:

▶ **Proposition 4.1.** *The variants of BiBBI given by: (a) associativity, unit weakening, unit contraction and contraction; and (b) associativity, unit weakening and weak distribution, are both* conservative *over BBI. That is, any BBI-formula valid in one of these variants is also BBI-valid.*

However, neither of the previous model constructions is very satisfying. In the first type, taking $\triangledown$ to be $\triangledown_=$, $A \mathbin{\overset{*}{\vee}} B$ simply becomes $A \vee B$. Moreover, as weak distribution does not hold in general, the $(*, -\!\!*, \top^*)$ and $(\mathbin{\overset{*}{\vee}}, \mathbin{\overset{*}{\setminus}}, \bot^*)$ fragments of the logic are essentially disjoint; we are inclined to regard the variants of BiBBI without weak distribution as being less interesting. On the other hand, under the second construction with $\triangledown$ being $\triangledown_0$, weak distribution does hold (trivially), but $A \mathbin{\check{\vee}} B$ collapses into $\top$, which is even less interesting!

An immediate question is therefore whether there are BiBBI-models with weak distribution in which $\triangledown$ has a non-trivial interpretation. Our interest here is strictly in *sub-classical* models, i.e. those in which classicality does not hold, since classical models fall under the rubric of CBI, in which $w_1 \triangledown w_2$ should be read as $-(-w_1 \circ -w_2)$, cf. Proposition 3.9. We explore this question, and related ones, in the next two subsections. A second question is whether conservativity extends to the other sub-classical variants of BiBBI (e.g. the variant with all sub-classical properties from Figure 1). Our next result suggests that this is unlikely.

▶ **Definition 4.2.** A partial functional BBI-model $\langle W, \circ, E\rangle$:
- is *cancellative* if $w \circ w_1 = w \circ w_2 \neq \emptyset$ implies $w_1 = w_2$;
- is *extensible* if for all $w \in W$ there exists a $w' \in W \setminus E$ such that $w \circ w'$ is defined;
- has *indivisible units* if $w_1 \circ w_2 \in E$ implies $w_1, w_2 \in E$.

Note that the heap model of Example 2.4 satisfies all three properties above, as does, e.g., the total monoid $\langle \mathbb{N}, +, \{0\}\rangle$.

▶ **Proposition 4.3.** *Let $\langle W, \circ, E\rangle$ be a partial functional BBI-model that is cancellative, extensible and has indivisible units, as in Defn. 4.2. There does not exist a BiBBI-model of the form $\langle W, \circ, E, \triangledown, U\rangle$ satisfying weak distribution, unit weakening and unit contraction.*

Proof. Suppose for contradiction that $\langle W, \circ, E, \triangledown, U\rangle$ does exist. By unit contraction, U must be nonempty, so let $u \in U$. By extensibility, there is a $y \notin E$ such that $y \circ u$ is defined. By unit contraction, there exists $u' \in U$ such that $y \circ u \in (y \circ u) \triangledown u'$. Thus, by the weak distribution law, there exists $v \in W$ such that $y \circ u = y \circ v$ and $u \in v \triangledown u'$. By cancellativity, we obtain $v = u$ and thus $u \in u \triangledown u'$. By unit weakening and commutativity of $\triangledown$, we obtain $\{u\} = u \triangledown u' \subseteq \{u'\}$, and thus $u = u'$.

Now, since $y \circ u \in (y \circ u) \triangledown u'$, using $u = u'$ and the commutativity of $\triangledown$, we have $y \circ u \in u \triangledown (y \circ u)$. Then, by the standard unit law for BBI, there exists $e \in E$ such that $(y \circ u) \circ e \in u \triangledown (y \circ u)$. Thus, by weak distribution, there exists $w \in W$ such that $u = (y \circ u) \circ w$. As e is a unit for $y \circ u$, it is also a unit for u, so we have $e \circ u = (y \circ w) \circ u$. Hence, by cancellativity, $y \circ w = e \in E$ and so by the indivisible units property we have $y \in E$. But we already know $y \notin E$, contradiction. ◀

Proposition 4.3 demonstrates that in the class of BBI-models given by Defn. 4.2, which includes many standard examples, we are forced to choose between weak distribution and (at least one direction of) the unit law $A \mathbin{\check{\vee}} \bot^* \equiv A$ when extending to a BiBBI-model. A BBI-formula whose validity implies membership of this class would yield nonconservativity of the BiBBI fragment with both weak distribution and unit weakening / contraction. Unfortunately, we have not yet been able to find such a formula. (We remark that the combination of weak distribution and unit contraction is particularly interesting, as it yields a multiplicative analogue of the usual *disjunctive syllogism*: $A * ({\sim}A \mathbin{\check{\vee}} B) \vdash B$.)

The next two subsections present general constructions extending (certain types of partial functional) BBI-models to BiBBI-models obeying the weak distribution law.

4.1 Intersection in BBI-models

Our first approach to constructing BiBBI-models from BBI-models is to interpret $\triangledown$ as an "intersection-like" operator on worlds. This construction yields BiBBI-models with the contraction and weak distribution properties, but in general no others (Proposition 4.7).

As a motivating example, there are two natural ways one could go about defining intersection in the heap model of Example 2.4, depending on how one deals with *incompatibility*:

▶ **Example 4.4** (Heap intersections). We define two binary intersection operations $\cap_1$ and $\cap_2$ on heaps by:

$$(h_1 \cap_1 h_2)(\ell) \stackrel{\text{def}}{=} \begin{cases} h_1(\ell) & \text{if } \ell \in \mathsf{dom}(h_1) \cap \mathsf{dom}(h_2) \text{ and } h_1(\ell) = h_2(\ell) \\ \text{undefined} & \text{otherwise} \end{cases}$$

$$h_1 \cap_2 h_2 \stackrel{\text{def}}{=} \begin{cases} h_1 \cap_1 h_2 & \text{if } h_1(\ell) = h_2(\ell) \text{ for all } \ell \in \mathsf{dom}(h_1) \cap \mathsf{dom}(h_2) \\ \text{undefined} & \text{otherwise} \end{cases}$$

The first intersection silently discards incompatible *parts* of heaps, while the second intersection requires the heaps to be fully compatible. Consequently, $\cap_1$ is associative, while $\cap_2$ is not. We note that neither $\cap_1$ nor $\cap_2$ has a natural set of units $U \subseteq \text{Heaps}$, in the sense that $h \cap_i U = \{h\}$ for all heaps h.

▶ **Proposition 4.5.** *Let $\langle \text{Heaps}, \circ, \{e\} \rangle$ be the heap model of Example 2.4, and let $\cap_1$ and $\cap_2$ be the heap intersection operations defined in Example 4.4. Then, for any $U \subseteq \text{Heaps}$, both $\langle \text{Heaps}, \circ, \{e\}, \cap_1, U \rangle$ and $\langle \text{Heaps}, \circ, \{e\}, \cap_2, U \rangle$ are BiBBI-models satisfying contraction and weak distribution (and the first also satisfies associativity).*

Unit contraction or unit weakening can easily be obtained in the above models by suitable choices of U, but, according to Prop. 4.3, it is impossible to obtain both simultaneously.

From now on, to simplify notation, and because most models of separation logic in the literature satisfy this constraint, we treat only partial functional BBI-models. Using associativity of $\circ$, we write $w_1 \sharp \ldots \sharp w_n$ to mean that $w_1 \circ \ldots \circ w_n$ is defined (i.e., non-empty). Then, we can extend Proposition 4.5 to arbitrary partial functional BBI-models, using a generalised version of the heap intersection $\cap_2$.

▶ **Definition 4.6.** Let $\langle W, \circ, E \rangle$ be a partial functional BBI-model, and define the operation $\triangledown_\cap \colon W \times W \to \mathcal{P}(W)$ by

$$w_1 \triangledown_\cap w_2 = \{x \mid \exists x_1, x_2 \in W.\ w_1 = x \circ x_1 \text{ and } w_2 = x \circ x_2 \text{ and } x \sharp x_1 \sharp x_2\}.$$

In the heap model, $h_1 \triangledown_\cap h_2$ is exactly $h_1 \cap_2 h_2$, while in $\langle \mathbb{N}, +, \{0\} \rangle$ we have $n \triangledown_\cap m = \{k \mid n, m \geq k\}$. Note that $\triangledown_\cap$ is neither a partial function nor associative, in general.

▶ **Proposition 4.7.** *For any partial functional BBI-model $M = \langle W, \circ, E \rangle$, and any $U \subseteq W$, we have that $\langle W, \circ, E, \triangledown_\cap, U \rangle$ is a BiBBI-model satisfying contraction and weak distribution.*

Proof. Since M is a BBI-model and $\triangledown_\cap$ is commutative by construction, $\langle W, \circ, E, \triangledown_\cap, U \rangle$ is a basic BiBBI-model. To check contraction, let $w \in W$; we must show that $w \in w \triangledown_\cap w$. This follows from the fact that, since M is a BBI-model, there is an $e \in E$ such that $w \circ e = w$, and thus $w \sharp e \sharp e$.

It remains to verify the weak distribution condition. That is, assuming $(x_1 \circ x_2) \cap (y_1 \triangledown_\cap y_2) \neq \emptyset$, we require to find $w \in W$ such that $y_1 = x_1 \circ w$ and $x_2 \in w \triangledown_\cap y_2$. By assumption, we have $x_1 \circ x_2 \in y_1 \triangledown_\cap y_2$. By definition of $\triangledown_\cap$ there are z_1 and z_2 such that $y_1 = x_1 \circ x_2 \circ z_1$ and $y_2 = x_1 \circ x_2 \circ z_2$ and $(x_1 \circ x_2) \sharp z_1 \sharp z_2$. Now, letting $w = x_2 \circ z_1$, we immediately have $y_1 = x_1 \circ w$. To see that $x_2 \in w \triangledown_\cap y_2$, we need $x', x'' \in W$ such that $w = x_2 \circ x'$ and $y_2 = x_2 \circ x''$ and $x_2 \sharp x' \sharp x''$. Choosing $x' = z_1$ and $x'' = x_1 \circ z_2$, we immediately have $w = x_2 \circ z_1$, and $y_2 = x_2 \circ x_1 \circ z_2$ by associativity. Finally, we must check $x_2 \sharp z_1 \sharp (x_1 \circ z_2)$, which follows by associativity from $(x_1 \circ x_2) \sharp z_1 \sharp z_2$. ◀

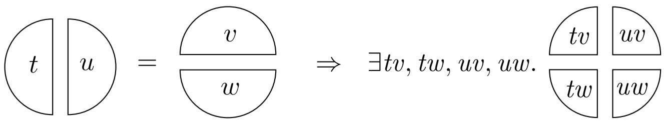
4.2 Intersection in BBI-models with environments

We now define our second general construction, based upon the one in the previous section, for constructing BiBBI-models obeying weak distribution, associativity, contraction *and* both unit laws. We require that the underlying BBI-model obeys the *cross-split* and *disjointness* properties typically encountered in heap-like models of separation logic [10, 6]:

▶ **Definition 4.8.** A partial functional BBI-model $M = \langle W, \circ, E\rangle$ has the *cross-split property* if for any $t, u, v, w \in W$ such that $t \circ u = v \circ w$, there exist tv, tw, uv, uw such that

$$t = tv \circ tw,\ \ u = uv \circ uw,\ \ v = tv \circ uv,\ \text{ and } w = tw \circ uw.$$

Diagrammatically, this can be thought of in the following way:



M has the *disjointness* property if $w \sharp w$ implies $w \in E$.

We remark that, again, the standard heap model of Example 2.4 has both the cross-split and the disjointness property. The monoid $(\mathbb{N}, +, \{0\})$ does not satisfy disjointness (because $+$ is a total operation), but it does have the cross split property: Given $t + u = v + w$, simply take $tv = \min(t, v)$, $uw = \min(u, w)$, $tw = t - tv$ and $uv = u - uw$.

Given a BBI-model with the above properties, we construct a BiBBI-model $\bar{M} = \langle \bar{W}, \bar{\circ}, \bar{E}, \bar{\triangledown}, D\rangle$, where each world in $\bar{W}$ consists of a "local" world $w \in W$ paired with a larger "environment" $x \in W$ such that $x = w \circ w'$ for some w'. On the "local" part of each world, $\bar{\circ}$ and $\bar{\triangledown}$ behave as $\circ$ and $\triangledown_\cap$, respectively. On the "environment" part of each world, $\bar{\circ}$ and $\bar{\triangledown}$ behave as a *union* operation $\cup$ (as defined below) and the identity, respectively.

▶ **Definition 4.9.** Given a partial functional BBI-model $\langle W, \circ, E\rangle$, we define the *union* operation, $\cup : W \times W \to \mathcal{P}(W)$, by

$$w_1 \cup w_2 = \{y \circ y_1 \circ y_2 \mid w_1 = y \circ y_1 \text{ and } w_2 = y \circ y_2\}\ .$$

We lift $\cup$ to $\mathcal{P}(W) \times \mathcal{P}(W) \to \mathcal{P}(W)$ in the usual way: $W_1 \cup W_2 = \bigcup_{w_1 \in W_1, w_2 \in W_2} w_1 \cup w_2$.

For our purposes we shall require $\cup$ to be associative, which is not necessarily the case for arbitrary partial functional BBI-models.

▶ **Lemma 4.10.** *If a partial functional BBI-model $\langle W, \circ, E\rangle$ has the cross-split property, then $\cup$ in Definition 4.9 is associative. Moreover, if $w = w_1 \circ w_2$, then $w \in w \cup w_1$.*

▶ **Definition 4.11.** Let $M = \langle W, \circ, E\rangle$ be a partial functional BBI-model. We define $\bar{M} = \langle \bar{W}, \bar{\circ}, \bar{E}, \bar{\triangledown}, D\rangle$ as follows:

$$\bar{W} = \{(w, x) \mid \exists w'.\ x = w \circ w'\} \qquad \bar{E} = \{(e, e) \mid e \in E\}$$

$$(w, x)\ \bar{\circ}\ (w', x') = \{(w \circ w', x'') \mid x'' \in x \cup x'\} \qquad D = \{(w, w) \mid w \in W\}$$

$$(w, x)\ \bar{\triangledown}\ (w', x') = \begin{cases} \{(w'', x) \mid w'' \in w \triangledown_\cap w'\} & \text{if } x = x' \\ \emptyset & \text{otherwise} \end{cases}$$

Instantiating M in the above definition with the heap model of Example 2.4, the set $\bar{W}$ pairs every heap with a larger heap that extends it, which can be thought of as pairing a local part of memory "owned" by a program with an "environment" reflecting the wider machine state.

Our main result about $\bar{M}$, stated as Theorem 4.13, is that, if M has the cross-split and the disjointness properties, then $\bar{M}$ is a BiBBI-model satisfying *all* the properties of Figure 1 (except classicality). The following lemma groups together a number of intermediary results used in the proof of this theorem.

▶ **Lemma 4.12.** *Suppose that $M = \langle W, \circ, E\rangle$ is partial functional and has the cross-split and disjointness properties, and let $\bar{M} = \langle \bar{W}, \bar{\circ}, \bar{E}, \bar{\triangledown}, D\rangle$ be as in Definition 4.11. All of the following hold:*

1. *For all $(w_1, x), (w_2, x) \in \bar{W}$, we have $w_1 \triangledown_\cap w_2$ a singleton set (and we typically drop the set brackets). Consequently, $\bar{\triangledown}$ is a partial function on $\bar{W} \times \bar{W}$.*
2. *If $(w, x), (w_1 \circ w_2, x) \in \bar{W}$ with $w \sharp w_1$ and $w \sharp w_2$, then $(w \circ w_1 \circ w_2, x) \in \bar{W}$.*
3. *For all $(w, x), (w_1 \circ w_2, x) \in \bar{W}$, we have $w \triangledown_\cap (w_1 \circ w_2) = (w \triangledown_\cap w_1) \circ (w \triangledown_\cap w_2)$.*

Proof (sketch). Each part of the lemma is proved directly; the proofs rely heavily on the disjointness and cross-split properties of M. ◀

▶ **Theorem 4.13.** *Given a partial functional BBI-model M with the cross-split and disjointness properties, $\bar{M}$ is a BiBBI-model with all the properties of Figure 1 except classicality.*

Proof (sketch). We check that $\bar{M}$ satisfies all properties of basic BiBBI-models, and all relevant properties from Figure 1, of which the most difficult case is, interestingly enough, the associativity of $\bar{\triangledown}$. The verifications rely heavily on Lemmas 4.10 and 4.12. ◀

5 Completeness of BiBBI

This section presents our proof of completeness for (variants of) BiBBI, stated earlier as Theorem 3.8. Our approach follows the basic pattern previously employed in the literature for BBI [8] and for CBI [4]: we translate a given variant of BiBBI into modal logic, and appeal to Sahlqvist's well known completeness result (see e.g. [2]). Here, unsurprisingly, the weak distribution law of BiBBI presents the greatest technical obstacles to this approach.

We begin by recalling the standard definitions, from [2], of validity and provability in normal modal logic over a suitably chosen signature (a.k.a. "modal similarity type").

▶ **Definition 5.1.** A *modal logic formula* is built from propositional variables using the classical connectives, 0-ary modalities $\top^*$ and $\mathbf{U}$, and binary modalities $*, -\!\circ, \triangledown$ and $\leftarrow$.

▶ **Definition 5.2.** A *modal frame* is given by a tuple of the form $\langle W, \circ, -\!\circ, \triangledown, \leftarrow, E, U\rangle$, where $\circ$, $-\!\circ$, $\triangledown$, and $\leftarrow$ all have type $W \times W \to \mathcal{P}(W)$, and $E, U \subseteq W$.

A valuation for a modal frame $M = \langle W, \ldots\rangle$ is as usual given by a function $\rho : \mathcal{V} \to \mathcal{P}(W)$. The forcing relation $w \models_\rho A$ is defined by induction on A in the standard way in modal logic, i.e. as for BBI in the case of propositional variables and classical connectives, with the following clauses for the modalities:

$$
\begin{aligned}
w \models_\rho \top^* &\iff w \in E \\
w \models_\rho \mathbf{U} &\iff w \in U \\
w \models_\rho A * B &\iff \exists w_1, w_2 \in W.\ w \in w_1 \circ w_2 \text{ and } w_1 \models_\rho A \text{ and } w_2 \models_\rho B \\
w \models_\rho A -\!\circ B &\iff \exists w_1, w_2 \in W.\ w \in w_1 -\!\circ w_2 \text{ and } w_1 \models_\rho A \text{ and } w_2 \models_\rho B \\
w \models_\rho A \triangledown B &\iff \exists w_1, w_2 \in W.\ w \in w_1 \triangledown w_2 \text{ and } w_1 \models_\rho A \text{ and } w_2 \models_\rho B \\
w \models_\rho A \leftarrow B &\iff \exists w_1, w_2 \in W.\ w \in w_1 \leftarrow w_2 \text{ and } w_1 \models_\rho A \text{ and } w_2 \models_\rho B
\end{aligned}
$$

As usual, A is *valid* in M iff we have $w \models_\rho A$ for all $w \in W$ and valuations ρ.

Each of the binary functions $\circ, \multimap, \triangledown, \multimapinv\!\!: W \times W \to \mathcal{P}(W)$ in a modal frame can be equivalently seen as a ternary relation over W (as is standard in modal logic). The corresponding modalities are each interpreted as a standard binary "diamond" modality.

▶ **Definition 5.3.** The *normal modal logic* $\mathbf{ML}_{\mathrm{BiBBI}}$ for the signature $(\top^*, \mathbf{U}, *, \multimap, \triangledown, \multimapinv)$ is given by extending a standard Hilbert system for classical logic with the following axioms and rules, for all $\otimes \in \{*, \multimap, \triangledown, \multimapinv\}$:

$$\begin{array}{l} \bot \otimes A \vdash \bot \text{ and } A \otimes \bot \vdash \bot \\ (A \vee B) \otimes C \vdash (A \otimes C) \vee (B \otimes C) \\ A \otimes (B \vee C) \vdash (A \otimes B) \vee (A \otimes C) \end{array} \qquad \frac{A_1 \vdash A_2 \quad B_1 \vdash B_2}{A_1 \otimes B_1 \vdash A_2 \otimes B_2}$$

Next, we recall the Sahlqvist completeness result for normal modal logics augmented with suitably well-behaved axioms, called *Sahlqvist formulas*. In fact, we only require so-called "very simple" Sahlqvist formulas for our completeness result.

▶ **Definition 5.4.** A *very simple Sahlqvist antecedent* (over the signature $(\top^*, \mathbf{U}, *, \multimap, \triangledown, \multimapinv)$) is given by the grammar: $S ::= P \mid \top \mid \bot \mid S \wedge S \mid \top^* \mid \mathbf{U} \mid S * S \mid S \multimap S \mid S \triangledown S \mid S \multimapinv S$. A *very simple Sahlqvist formula* is an implication $A \vdash B$, where A is a very simple Sahlqvist antecedent and B is a *positive* modal logic formula (i.e., every propositional variable occurs within the scope of an even number of negations).

▶ **Theorem 5.5** (Sahlqvist [2]). *If a modal logic formula is valid in the set of all modal frames satisfying a set $\mathcal{A}$ of very simple Sahlqvist formulas, then it is provable in $\mathbf{ML}_{BiBBI} + \mathcal{A}$.*

We now define a set of Sahlqvist formulas that collectively capture all variants of BiBBI.

▶ **Definition 5.6.** For a given variant of BiBBI, define the set $\mathcal{A}_{\mathrm{BiBBI}}$ of very simple Sahlqvist formulas as follows:

(1)	$A \wedge (B * C) \vdash (B \wedge (C \multimap A)) * \top$	(Assoc.)	$A \triangledown (B \triangledown C) \vdash (A \triangledown B) \triangledown C$
(2)	$A \wedge (B \multimap C) \vdash \top \multimap (C \wedge (A * B))$	(Unit weak.)	$A \triangledown \mathbf{U} \vdash A$
(3)	$A \wedge (B \triangledown C) \vdash \top \triangledown (C \wedge (A \multimapinv B))$	(Unit contr.)	$A \vdash A \triangledown \mathbf{U}$
(4)	$A \wedge (B \multimapinv C) \vdash (B \wedge (C \triangledown A)) \multimapinv \top$	(Contr.)	$A \vdash A \triangledown A$
(5)	$A * B \vdash B * A$	(Weak distr.)	$(A * B) \wedge (C \triangledown D) \vdash$
(6)	$A \triangledown B \vdash B \triangledown A$		$(A \wedge ((B \multimapinv D) \multimap C)) * \top$
(7)	$A * (B * C) \vdash (A * B) * C$	(Classicality)	$(A \multimap \mathbf{U}) \multimap \mathbf{U} \vdash A$ and
(8)	$A * \top^* \vdash A$ and $A \vdash A * \top^*$		$A \vdash (A \multimap \mathbf{U}) \multimap \mathbf{U}$

where A, B, C, D are considered here to be propositional variables, and the named axioms are included in $\mathcal{A}_{\mathrm{BiBBI}}$ iff the BiBBI variant includes the corresponding property in Figure 1.

▶ **Lemma 5.7.** *Let $M = \langle W, \circ, \multimap, \triangledown, \multimapinv, E, U\rangle$ be a modal frame satisfying axioms* (1)–(4) *of $\mathcal{A}_{BiBBI}$ in Definition 5.6. Then we have, for any $w, w_1, w_2 \in W$:*

$$w \in w_1 \multimap w_2 \quad \Leftrightarrow \quad w_2 \in w \circ w_1 \text{ and } w \in w_1 \multimapinv w_2 \quad \Leftrightarrow \quad w_1 \in w_2 \triangledown w \ .$$

Given a modal frame $M = \langle W, \circ, \multimap, \triangledown, \multimapinv, E, U\rangle$, we write $\ulcorner M \urcorner$ for $\langle W, \circ, E, \triangledown, U\rangle$.

▶ **Lemma 5.8.** *Let $M = \langle W, \circ, \multimap, \triangledown, \multimapinv, E, U\rangle$ be a modal frame satisfying the set $\mathcal{A}_{BiBBI}$ of axioms corresponding to a BiBBI variant, as given by Definition 5.6. Then $\ulcorner M \urcorner$ is a BiBBI-model for that variant.*

Proof (sketch). First, $\ulcorner M \urcorner$ is a basic BiBBI-model, since it satisfies axioms (5)–(8) in Defn. 5.6. We just show that if an optional Sahlqvist axiom from Defn. 5.6 is valid in M, then M satisfies the corresponding frame property in Figure 1 (and thus $\ulcorner M \urcorner$ does too).

We just show the case of weak distribution here. Assume the weak distribution axiom of Definition 5.6 is valid in M and suppose that $(x_1 \circ x_2) \cap (y_1 \triangledown y_2) \neq \emptyset$. That is, we have $z \in (x_1 \circ x_2) \cap (y_1 \triangledown y_2)$ for some $z \in W$. We require to find a $w \in W$ such that $y_1 \in x_1 \circ w$ and $x_2 \in w \triangledown y_2$. Define a valuation ρ for M by $\rho(A) = \{x_1\}$, $\rho(B) = \{x_2\}$, $\rho(C) = \{y_1\}$ and $\rho(D) = \{y_2\}$. By construction, $z \models_\rho (A * B) \wedge (C \triangledown D)$. Since the weak distribution axiom is valid in M, we have that $z \models_\rho (A \wedge ((B \multimapinv D) \multimap C)) * \top$. That is, for some z' we have $z' \models_\rho A \wedge ((B \multimapinv D) \multimap C)$. Since $z' \models_\rho A$, we get $z' = x_1$ and so $x_1 \models_\rho (B \multimapinv D) \multimap C$. As M satisfies axioms (1)–(4) by assumption, we can apply Lemma 5.7 to obtain w, w' such that $w' \in x_1 \circ w$ and $w \models_\rho B \multimapinv D$ and $w' \models_\rho C$. As $w' \models_\rho C$, we have $y_1 \in x_1 \circ w$. Using Lemma 5.7 and commutativity of $\triangledown$ (forced by the validity of axiom (6) in M), we obtain from $w \models_\rho B \multimapinv D$ that there exist w', w'' with $w'' \in w \triangledown w'$ and $w'' \models_\rho B$ and $w' \models_\rho D$. This means exactly that $x_2 \in w \triangledown y_2$ as required. This completes the proof. ◀

▶ **Definition 5.9.** We define a translation $t(-)$ from BiBBI-formulas to modal logic formulas, and a symmetric translation $u(-)$ in the opposite direction, by

$$
\begin{array}{rcl@{\qquad}rcl}
t(\phi) & = & \phi & u(\phi) & = & \phi \\
t(\bot^*) & = & \neg\mathbf{U} & u(\mathbf{U}) & = & \neg\bot^* \\
t(\neg A) & = & \neg t(A) & u(\neg A) & = & \neg u(A) \\
t(A \mathbin{?} B) & = & t(A) \mathbin{?} t(B) & u(A \mathbin{?} B) & = & u(A) \mathbin{?} u(B) \\
t(A \mathrel{-\!\!*} B) & = & \neg(t(A) \multimap \neg t(B)) & u(A \multimap B) & = & \neg(u(A) \mathrel{-\!\!*} \neg u(B)) \\
t(A \mathbin{\overset{*}{\triangledown}} B) & = & \neg(\neg t(A) \triangledown \neg t(B)) & u(A \triangledown B) & = & \neg(\neg u(A) \mathbin{\overset{*}{\triangledown}} \neg u(B)) \\
t(A \mathbin{\setminus^*} B) & = & t(A) \multimapinv \neg t(B) & u(A \multimapinv B) & = & u(A) \mathbin{\setminus^*} \neg u(B)
\end{array}
$$

where $\phi \in \{P, \top, \bot, \top^*\}$ and $? \in \{\wedge, \vee, \rightarrow, *\}$.

▶ **Lemma 5.10.** *If A is valid in some variant of BiBBI, then $t(A)$ is valid in the class of modal frames satisfying the corresponding Sahlqvist axioms $\mathcal{A}_{BiBBI}$ given by Definition 5.6.*

Proof (sketch). Let $M = \langle W, \circ, \multimap, \triangledown, \multimapinv, E, U \rangle$ be a modal frame satisfying the axioms $\mathcal{A}_{\mathrm{BiBBI}}$. By Lemma 5.8, $\ulcorner M \urcorner$ is a BiBBI-model for the variant of BiBBI determined by $\mathcal{A}_{\mathrm{BiBBI}}$, and thus A is valid in $\ulcorner M \urcorner$. We require to show that $t(A)$ is valid in M, which follows by establishing the bi-implication $w \models_\rho A$ (in $\ulcorner M \urcorner$) $\Leftrightarrow$ $w \models_\rho t(A)$ (in M), for all $w \in W$ and valuations ρ. This bi-implication follows by structural induction on A, making use of Lemma 5.7 for the cases $A = B \mathrel{-\!\!*} C$ and $A = B \mathbin{\setminus^*} C$. ◀

▶ **Lemma 5.11.** *If B is provable in $\mathbf{ML}_{BiBBI} + \mathcal{A}_{BiBBI}$, then $u(B)$ is provable in the corresponding variant of BiBBI.*

Proof (sketch). We have to show that all the axioms and rules of normal modal logic (Defn. 5.3) and all the $\mathcal{A}_{\mathrm{BiBBI}}$ axioms (Defn. 5.6) are derivable in the appropriate variant of BiBBI under the translation $u(-)$. For example, in the case of the Sahlqvist axiom for weak distribution from Defn. 5.6, we need to derive the following in BiBBI with weak distribution:

$$(u(A) * u(B)) \wedge \neg(\neg u(C) \mathbin{\overset{*}{\triangledown}} \neg u(D)) \vdash (u(A) \wedge \neg((u(B) \mathbin{\setminus^*} \neg u(D)) \mathrel{-\!\!*} \neg u(C)) * \top$$

The required derivations are often tedious and sometimes tricky: see [5] for details. ◀

▶ **Lemma 5.12.** *If $u(t(A))$ is provable in some variant of BiBBI then so is A.*

Proof (sketch). By structural induction on A. ◀

We may now finally prove our completeness result:

Proof of Theorem 3.8. Suppose A is valid in some BiBBI variant. By Lemma 5.10, $t(A)$ is then valid in the class of modal frames satisfying the Sahlqvist formulas $\mathcal{A}_{\mathrm{BiBBI}}$ given by Defn. 5.6. By Theorem 5.5, $t(A)$ is provable in $\mathbf{ML}_{\mathrm{BiBBI}} + \mathcal{A}_{\mathrm{BiBBI}}$. Thus, by Lemma 5.11, $u(t(A))$ is provable in the corresponding variant of BiBBI. By Lemma 5.12, A is then provable in this BiBBI variant as required. ◀

6 Proof theory

In this section, we construct a cut-eliminating *display calculus* (cf. [1, 4, 3]) for BiBBI by combining a display calculus for classical logic with the display calculus for the multiplicative fragment of FILL given by Clouston et al [9]. Particular variants of BiBBI are handled via the inclusion or otherwise of optional structural rules.

▶ **Definition 6.1.** *Structures* are given by the following grammar, where F ranges over BiBBI-formulas: $X ::= F \mid \varnothing \mid \sharp X \mid X;X \mid X,X \mid X:X$. If X and Y are structures then $X \vdash Y$ is a *consecution.*

▶ **Definition 6.2.** For any structure Z we define the BiBBI-formulas Ψ_Z and Υ_Z by mutual structural induction:

$$
\begin{array}{rcl@{\qquad}rcl}
\Psi_F & = & F & \Upsilon_F & = & F \\
\Psi_\varnothing & = & \top^* & \Upsilon_\varnothing & = & \bot^* \\
\Psi_{\sharp X} & = & \neg \Upsilon_X & \Upsilon_{\sharp X} & = & \neg \Psi_X \\
\Psi_{X;Y} & = & \Psi_X \wedge \Psi_Y & \Upsilon_{X;Y} & = & \Upsilon_X \vee \Upsilon_Y \\
\Psi_{X,Y} & = & \Psi_X * \Psi_Y & \Upsilon_{X,Y} & = & \Psi_X \mathrel{-\!\!*} \Upsilon_Y \\
\Psi_{X:Y} & = & \Psi_X \setminus^{*} \Upsilon_Y & \Upsilon_{X:Y} & = & \Upsilon_X \overset{*}{\vee} \Upsilon_Y
\end{array}
$$

Validity of the consecution $X \vdash Y$ (in a BiBBI variant) is then interpreted as validity of the formula $\Psi_X \vdash \Upsilon_Y$.

We give our display calculus $\mathrm{DL}_{\mathrm{BiBBI}}$ for BiBBI in Figure 2. As usual, we give a set of *display postulates* written as a binary relation $<>_D$ on consecutions, and let *display-equivalence*, $\equiv_D$, be the reflexive-transitive closure of $<>_D$. Then, for any substructure occurrence Z in a consecution C, we can "display" Z as the entire antecedent or consequent as appropriate: that is, either $C \equiv_D Z \vdash X$ or $C \equiv_D X \vdash Z$ for some structure X (depending on whether Z occurs positively or negatively in C). For further details see e.g. [3].

The "variant" structural rules are included in $\mathrm{DL}_{\mathrm{BiBBI}}$ only when we wish to consider particular variants of BiBBI. From left to right in Figure 2, the variant structural rules correspond respectively to: associativity; unit weakening; unit contraction; contraction; and weak distribution.

▶ **Lemma 6.3.** *For any structure X, both $X \vdash \Psi_X$ and $\Upsilon_X \vdash X$ are provable in DL_{BiBBI}.*

Proof (sketch). Structural induction on X. ◀

▶ **Theorem 6.4.** *$X \vdash Y$ is provable in a variant of DL_{BiBBI} if and only it is valid in the corresponding variant of BiBBI.*

Proof (sketch). For soundness, one just verifies directly that each rule of Figure 2 preserves validity, a straightforward exercise. For completeness, assume that $X \vdash Y$ is valid, i.e. that $\Psi_X \vdash \Upsilon_Y$ is a valid formula. By Theorem 3.8, $\Psi_X \vdash \Upsilon_Y$ is provable in the Hilbert system for (the required variant of) BiBBI. It is easy to show that the corresponding variant of $\mathrm{DL}_{\mathrm{BiBBI}}$ can derive all principles of the Hilbert system, and thus $\Psi_X \vdash \Upsilon_Y$ is provable in $\mathrm{DL}_{\mathrm{BiBBI}}$. Then, using (Cut) and Lemma 6.3, we can prove $X \vdash Y$ in $\mathrm{DL}_{\mathrm{BiBBI}}$ as required. ◀

Display postulates:

$$X;Y \vdash Z \;<>_D\; X \vdash \sharp Y;Z \;<>_D\; Y;X \vdash Z$$
$$X \vdash Y;Z \;<>_D\; X;\sharp Y \vdash Z \;<>_D\; X \vdash Z;Y$$
$$X \vdash Y \;<>_D\; \sharp Y \vdash \sharp X \;<>_D\; \sharp\sharp X \vdash Y$$

$$X,Y \vdash Z \;<>_D\; X \vdash Y,Z \;<>_D\; Y,X \vdash Z$$
$$X \vdash Y : Z \;<>_D\; X : Y \vdash Z \;<>_D\; X \vdash Z : Y$$

Identity rules:

$$\frac{}{P \vdash P}\,(\text{Id}) \qquad \frac{X \vdash F \quad F \vdash Y}{X \vdash Y}\,(\text{Cut}) \qquad \frac{X' \vdash Y'}{X \vdash Y}\; X \vdash Y \equiv_D X' \vdash Y' \;\;(\equiv_D)$$

Logical rules:

$$\frac{}{\bot \vdash X}\,(\bot\text{L}) \qquad \frac{\sharp F \vdash X}{\neg F \vdash X}\,(\neg\text{L}) \qquad \frac{F;G \vdash X}{F \wedge G \vdash X}\,(\wedge\text{L}) \qquad \frac{F \vdash X \quad G \vdash X}{F \vee G \vdash X}\,(\vee\text{L}) \qquad \frac{X \vdash F \quad G \vdash Y}{F \rightarrow G \vdash \sharp X;Y}\,(\rightarrow\text{L})$$

$$\frac{}{X \vdash \top}\,(\top\text{R}) \qquad \frac{X \vdash \sharp F}{X \vdash \neg F}\,(\neg\text{R}) \qquad \frac{X \vdash F \quad X \vdash G}{X \vdash F \wedge G}\,(\wedge\text{R}) \qquad \frac{X \vdash F;G}{X \vdash F \vee G}\,(\vee\text{R}) \qquad \frac{X;F \vdash G}{X \vdash F \rightarrow G}\,(\rightarrow\text{R})$$

$$\frac{\varnothing \vdash X}{\top^* \vdash X}\,(\top^*\text{L}) \qquad \frac{F,G \vdash X}{F * G \vdash X}\,(*\text{L}) \qquad \frac{X \vdash F \quad G \vdash Y}{F \mathrel{-\!\!*} G \vdash X,Y}\,(-\!\!*\text{L}) \qquad \frac{}{\bot^* \vdash \varnothing}\,(\bot^*\text{L}) \qquad \frac{F \vdash X \quad G \vdash Y}{F \stackrel{*}{\vee} G \vdash X : Y}\,(\stackrel{*}{\vee}\text{L})$$

$$\frac{}{\varnothing \vdash \top^*}\,(\top^*\text{R}) \qquad \frac{X \vdash F \quad Y \vdash G}{X,Y \vdash F * G}\,(*\text{R}) \qquad \frac{X,F \vdash G}{X \vdash F \mathrel{-\!\!*} G}\,(-\!\!*\text{R}) \qquad \frac{X \vdash \varnothing}{X \vdash \bot^*}\,(\bot^*\text{R}) \qquad \frac{X \vdash F : G}{X \vdash F \stackrel{*}{\vee} G}\,(\stackrel{*}{\vee}\text{R})$$

$$\frac{F : G \vdash X}{F \setminus^* G \vdash X}\,(\setminus^*\text{L}) \qquad \frac{X \vdash F \quad G \vdash Y}{X : Y \vdash F \setminus^* G}\,(\setminus^*\text{R})$$

Structural rules:

$$\frac{X \vdash Z}{X;Y \vdash Z}\,(\text{Wk}) \qquad \frac{X;X \vdash Z}{X \vdash Z}\,(\text{Ctr}) \qquad \frac{W,(X,Y) \vdash Z}{(W,X),Y \vdash Z}\,(*\text{A}) \qquad \frac{X \vdash Y}{\varnothing, X \vdash Y}\,(\varnothing\text{WkL}) \qquad \frac{\varnothing, X \vdash Y}{X \vdash Y}\,(\varnothing\text{CtrL})$$

Variant structural rules:

$$\frac{W \vdash (X : Y) : Z}{W \vdash X : (Y : Z)}\,(\stackrel{*}{\vee}\text{A}) \qquad \frac{X \vdash Y}{X \vdash Y : \varnothing}\,(\varnothing\text{WkR}) \qquad \frac{X \vdash Y : \varnothing}{X \vdash Y}\,(\varnothing\text{CtrR}) \qquad \frac{X \vdash Y : Y}{X \vdash Y}\,(\stackrel{*}{\vee}\text{Ctr})$$

$$\frac{W,(X : Y) \vdash Z}{(W,X) : Y \vdash Z}\,(\text{WDist})$$

Figure 2 The proof rules of DL_{BiBBI}. W, X, Y, Z range over structures, F, G range over BiBBI-formulas and P ranges over $\mathcal{V}$.

▶ **Theorem 6.5.** *Any* DL_{BiBBI} *proof of* $X \vdash Y$ *can be transformed into a proof of* $X \vdash Y$ *without (Cut).*

Proof (sketch). We just verify that the proof rules of $\mathrm{DL}_{\mathrm{BiBBI}}$ collectively satisfy Belnap's well known cut-elimination conditions (C2)–(C8) [1]. The verification is straightforward, and similar to the one carried out in [3]. ◀

7 Conclusions

In this paper, we study "sub-classical" bunched logics between BBI and CBI, where a multiplicative "disjunction family" of connectives, ($\overset{*}{\vee}$, $\setminus^{*}$, $\bot^{*}$), exists alongside the usual "conjunction family" ($*, -\!*, \top^{*}$). The two families are dual to one another in an intuitionistic sense: $*$ and $\overset{*}{\vee}$ are related, if at all, not by De Morgan equivalence but by the *weak distribution* law, $A * (B \overset{*}{\vee} C) \vdash (A * B) \overset{*}{\vee} C$. From the point of view of linear logic, the variants of our BiBBI can be seen as free combinations of classical logic with various multiplicative fragments of Hyland and de Paiva's FILL [16].

We have given a Kripke frame semantics for our logic(s) in which various logical axioms of FILL have natural semantic correspondents as first-order conditions on BiBBI-models (cf. Figure 1). We provide a completeness proof for this semantics, based on the Sahlqvist completeness theorem for modal logic, and moreover we obtain completeness for *any* variant of BiBBI given by a choice of logical principles from Figure 1.

Investigating the models of our sub-classical bunched logics in more detail, we find that heap-like models of BiBBI, as used in separation logic, can be obtained by interpreting $\overset{*}{\vee}$ using natural notions of heap *intersection*. (This stands in contrast to the situation for classical bunched logic CBI, of which heaps are not models.) In such models, the above weak distribution law holds, but this unavoidably comes at the expense of the unit law $A \overset{*}{\vee} \bot^{*} \equiv A$ (see Prop. 4.3). However, this is not true of all interesting models of BiBBI; we show how to turn sufficiently well-behaved BBI-models (such as the heap model) into more complex BiBBI-models in which both weak distribution and the unit law hold, based on pairing every world in the original model with a larger "environment" (Theorem 4.13).

We are cautiously optimistic that the disjunctive machinery of BiBBI might usefully be applied to program verification based on separation logic. As in linear logic, it seems more difficult to reason intuitively using multiplicative disjunction than using multiplicative conjunction. However, the fact that disjunction can be interpreted using natural heap intersection operations, which are closely related to the union operation used to reason about algorithms with complex sharing [15, 12], leads us to hope that such intuitions are within reach. We hope to explore this direction further in future work.

References

1. Nuel D. Belnap, Jr. Display logic. *Journal of Philosophical Logic*, 11:375–417, 1982.
2. Patrick Blackburn, Maarten de Rijke, and Yde Venema. *Modal Logic*. Cambridge University Press, 2001.
3. James Brotherston. Bunched logics displayed. *Studia Logica*, 100(6):1223–1254, 2012.
4. James Brotherston and Cristiano Calcagno. Classical BI: Its semantics and proof theory. *Logical Methods in Computer Science*, 6(3), 2010.
5. James Brotherston and Jules Villard. Bi-intuitionistic boolean bunched logic. Technical Report RN/14/06, University College London, 2014.
6. James Brotherston and Jules Villard. Parametric completeness for separation theories. In *Proc. POPL-41*, pages 453–464. ACM, 2014.

7 Cristiano Calcagno, Dino Distefano, Peter O'Hearn, and Hongseok Yang. Compositional shape analysis by means of bi-abduction. *Journal of the ACM*, 58(6), December 2011.

8 Cristiano Calcagno, Philippa Gardner, and Uri Zarfaty. Context logic as modal logic: Completeness and parametric inexpressivity. In *Proc. POPL-34*, pages 123–134. ACM, 2007.

9 Ranald Clouston, Jeremy Dawson, Rajeev Goré, and Alwen Tiu. Annotation-free sequent calculi for full intuitionistic linear logic. In *Proc. CSL-22*, pages 197–214. Dagstuhl, 2013.

10 Robert Dockins, Aquinas Hobor, and Andrew W. Appel. A fresh look at separation algebras and share accounting. In *Proc. APLAS-7*, pages 161–177. Springer, 2009.

11 Didier Galmiche and Dominique Larchey-Wendling. Expressivity properties of Boolean BI through relational models. In *Proc. FSTTCS-26*, pages 357–368. Springer, 2006.

12 Philippa Gardner, Sergio Maffeis, and Gareth David Smith. Towards a program logic for JavaScript. In *Proc. POPL-39*, pages 31–44, 2012.

13 Jean-Yves Girard and Yves Lafont. Linear logic and lazy computation. In *Proc. TAPSOFT*, pages 52–66. Springer-Verlag, 1987.

14 Alexey Gotsman, Byron Cook, Matthew Parkinson, and Viktor Vafeiadis. Proving that non-blocking algorithms don't block. In *Proc. POPL-36*, pages 16–28. ACM, 2009.

15 Aquinas Hobor and Jules Villard. The ramifications of sharing in data structures. In *Proc. POPL-40*, pages 523–536. ACM, 2013.

16 Martin Hyland and Valeria de Paiva. Full intuitionistic linear logic (extended abstract). *Annals of Pure and Applied Logic*, 64(3):273—291, 1993.

17 Samin Ishtiaq and Peter W. O'Hearn. BI as an assertion language for mutable data structures. In *Proc. POPL-28*, pages 14–26. ACM, 2001.

18 Peter W. O'Hearn and David J. Pym. The logic of bunched implications. *Bulletin of Symbolic Logic*, 5(2):215–244, 1999.

19 David Pym. *The Semantics and Proof Theory of the Logic of Bunched Implications.* Applied Logic Series. Kluwer, 2002.

20 David Pym, Peter O'Hearn, and Hongseok Yang. Possible worlds and resources: The semantics of BI. *Theor. Comp. Sci.*, 315(1):257–305, 2004.

21 John C. Reynolds. Separation logic: A logic for shared mutable data structures. In *Proc. LICS-17*, pages 55–74. IEEE, 2002.

22 H. Yang, O. Lee, J. Berdine, C. Calcagno, B. Cook, D. Distefano, and P. O'Hearn. Scalable shape analysis for systems code. In *Proc. CAV-20*, pages 385–398. Springer, 2008.