Classical BI

(A Logic for Reasoning about Dualising Resources)

James Brotherston [*]   Cristiano Calcagno [†]

Dept. of Computing, Imperial College London, UK
{jbrother,ccris}@doc.ic.ac.uk

Abstract

We show how to extend O'Hearn and Pym's logic of bunched implications, BI, to classical BI (CBI), in which both the additive and the multiplicative connectives behave classically. Specifically, CBI is a non-conservative extension of (propositional) Boolean BI that includes multiplicative versions of falsity, negation and disjunction. We give an algebraic semantics for CBI that leads us naturally to consider resource models of CBI in which every resource has a unique dual. We then give a cut-eliminating proof system for CBI, based on Belnap's display logic, and demonstrate soundness and completeness of this proof system with respect to our semantics.

Categories and Subject Descriptors F.4.1 [*Mathematical Logic and Formal Languages*]: Mathematical Logic—model theory, proof theory, computational logic

General Terms Theory, verification, languages

Keywords Classical BI, display logic, semantics, resource models, completeness, cut-elimination, bunched implications

1. Introduction

The *logic of bunched implications* (BI), due to O'Hearn and Pym [24], is a substructural logic suitable for reasoning about domains that incorporate a notion of *resource* [27]. Its best-known application in computer science is *separation logic*, which is a Hoare logic for reasoning about imperative, pointer-manipulating programs [29]. Semantically, BI arises by considering cartesian doubly closed categories (i.e. categories with one cartesian closed structure and one symmetric monoidal closed structure) [26]. This view gives rise to the following propositional connectives[1] for BI:

Additive:	$\top$	$\bot$	$\neg$	$\wedge$	$\vee$	$\rightarrow$
Multiplicative:	$\top^*$			$*$		$-\!\!*$

The interpretation of BI in models based upon the aforementioned categories is necessarily intuitionistic. By instead using the algebraic semantics of BI, in which the multiplicatives are modelled using (partially ordered) commutative monoids, the additive connectives can be interpreted either classically or intuitionistically according to preference [27, 26]. When the additives are interpreted classically the resulting logic is known as *Boolean* BI [26], also written BBI. The pure part of separation logic is essentially obtained by considering a particular model of BBI, based on a monoid of heaps [22]. In this paper, we show how to extend BBI to *classical* BI, also written CBI, in which both the additives and the multiplicatives are treated classically. Specifically, CBI includes the multiplicative analogues of additive falsity, negation and disjunction, which are absent in BBI. We consider CBI both from the model-theoretic and the proof-theoretic perspective.

Model-theoretic perspective: From the point of view of computer science, perhaps the most natural semantics for BBI is its algebraic semantics based on relational commutative monoids [17], which can be understood as an abstract representation of resource [16]. In such models, of which the separation logic heap model is one instance, BBI-formulas have a natural declarative reading as statements about resources (i.e. monoid elements). Thus the multiplicative unit $\top^*$ denotes the empty resource (i.e. the monoid identity element) and a multiplicative conjunction $F * G$ of two formulas denotes a division of resource, via the monoid operation, into two components satisfying respectively F and G. The multiplicative implication $-\!\!*$ functions as a right-adjoint of $*$, so that $(F * G) \rightarrow H$ and $F \rightarrow (G -\!\!* H)$ are semantically equivalent.

It has hitherto been somewhat unclear how to give similarly declarative readings to multiplicative falsity $\bot^*$ and multiplicative negation $\sim$ (with multiplicative disjunction $\mathbin{\vee\!\!\!\!*}$ then being obtained as the de Morgan dual of $*$ with respect to $\sim$). In Section 2 we provide a solution to this problem by giving an algebraic semantics for CBI which provides sufficient structure to admit a declarative interpretation of the full set of multiplicative connectives. Our CBI-models are obtained by imposing extra conditions on the usual relational commutative monoid models of BBI, the main requirement being the presence of an involution operation on monoid elements. The natural reading of this requirement in terms of resources is that every resource in our models must have a unique dual. In fact, all Abelian groups are special instances of our models, in which the dual of an element is its group inverse.

The resulting interpretations of multiplicative falsity, negation and disjunction in our models are similar to those employed in relevant logic (see e.g. [28, 15]). For example, the interpretation of multiplicative negation is obtained by combining the model involution and the additive negation. These interpretations, which at first sight may seem unusual, are justified by the desired semantic equivalences between formulas. For example, under our interpretation $F -\!\!* G$ is semantically equivalent to $\sim F \mathbin{\vee\!\!\!\!*} G$.

[*] Research supported by EPSRC grant EP/E002536/1.

[†] Research supported by an EPSRC Advanced Fellowship.

[1] Note that, for purposes of notational consistency with multiplicative falsity $\bot^*$, we write $\top^*$ rather than the usual I for the multiplicative unit of $*$.

POPL'09, January 18–24, 2009, Savannah, Georgia, USA.
Copyright © 2009 ACM 978-1-60558-379-2/09/01...$5.00

Proof-theoretic perspective: In BI, the presence of the two implications $\rightarrow$ and $\multimap\!\!*$ gives rise to two context-forming operations ';' and ',' which correspond to the conjunctions $\wedge$ and $*$ at the meta-level. This situation is exemplified by the following (intuitionistic) sequent calculus right-introduction rules for the implications:

$$\frac{\Gamma; F_1 \vdash F_2}{\Gamma \vdash F_1 \rightarrow F_2}\,(\rightarrow\text{R}) \qquad \frac{\Gamma, F_1 \vdash F_2}{\Gamma \vdash F_1 \mathrel{-\!\!*} F_2}\,(\mathrel{-\!\!*}\text{R})$$

Accordingly, the contexts Γ on the left-hand side of the sequents in the rules above are not sets or sequences, as in standard sequent calculi, but rather *bunches*: trees whose leaves are formulas and whose internal nodes are either ';' or ',' denoting respectively additive and multiplicative combinations of assumptions. The crucial difference between the two operations is that weakening and contraction are possible for ';' but not for ','. Since BI is an intuitionistic logic, bunches arise only on the left-hand side of sequents, with a single formula on the right. For CBI, a natural approach from a proof-theoretic perspective would be to consider a full two-sided sequent calculus in which ';' and ',' in bunches on the right of sequents correspond to the two disjunctions at the meta-level. One would then expect the additive and multiplicative negations to have the effect of "swapping sides" with respect to ';' and ',' respectively:

$$\frac{\Gamma \vdash F; \Delta}{\Gamma; \neg F \vdash \Delta}\,(\neg\text{L}) \qquad \frac{\Gamma, F \vdash \Delta}{\Gamma \vdash {\sim}F, \Delta}\,({\sim}\text{R})$$

with ($\neg$R) and (${\sim}$L) being symmetric, and with rules for multiplicative disjunction $\overset{*}{\vee}$ dual to those for $*$. Unfortunately, it is not obvious how to formulate such a sequent calculus that admits cut-elimination (see [6, 26] for some discussion of the difficulties), or a similar natural deduction system satisfying normalisation[2].

In Section 4, we address this rather unsatisfactory situation by formulating a *display calculus* proof system for CBI that satisfies cut-elimination, with an attendant subformula property for cut-free proofs. Our system, $\mathrm{DL}_{\mathrm{CBI}}$, is based on Belnap's *display logic*, which is a generalised Gentzen-style system that can be instantiated to a wide class of logics simply by choosing families of connectives and the structural rules governing those families [1]. The power of display logic comes from its generic structural principles, which are sufficient to guarantee certain desirable proof-theoretic properties, more or less independently of the particular choice of connective families and structural rules. As well as satisfying cut-elimination, our system $\mathrm{DL}_{\mathrm{CBI}}$ is sound and complete with respect to our algebraic semantics for CBI. The proofs of soundness and completeness constitute one of the main technical contributions of this paper, and are presented in Section 5. First, we define an extension of the usual sequent calculus for BBI by axioms that capture the behaviour of the involution in our models. Using techniques from modal logic, we show that this extended sequent calculus, LBI^+, is sound and complete with respect to validity in our models. (However, LBI^+ does not contain primitive introduction rules for every connective of CBI, nor does it satisfy cut elimination.) Soundness and completeness for $\mathrm{DL}_{\mathrm{CBI}}$ then follows by proving admissibility of $\mathrm{DL}_{\mathrm{CBI}}$ in LBI^+ under a suitable embedding, and vice versa.

Applications: (B)BI, and in particular its resource semantics, has found application in several areas of computer science, including polymorphic abstraction [12], type systems for reference update and disposal [2], context logic for tree update [8] and, most ubiquitously, separation logic [29] which forms the basis of many contemporary approaches to reasoning about pointer programs (recent examples include [25, 11, 10]).

We demonstrate that CBI is a non-conservative extension of BBI. Unfortunately, this appears to rule out the naive use of CBI for reasoning directly about some BBI-models such as the separation logic heap model, which is not a CBI-model. On the other hand, non-conservativity indicates that CBI is genuinely different in character to BBI — thus of intrinsic technical interest — and can reasonably be expected to have different applications. In Section 3 we consider a range of example CBI-models drawn from quite disparate areas of mathematics and computer science, including bit arithmetic, regular languages, money and a generalised heap model. In Section 6 we suggest some directions for future applications of CBI, as well as discussing related work.

Due to space limitations, we have abbreviated or omitted some proofs of the results in this paper. Full proofs can be found in an associated technical report [5].

2. Syntax and algebraic semantics of CBI

In this section we define CBI, the fully classical version of BBI featuring additive and multiplicative versions of all the usual propositional connectives (cf. [26]). We give a class of algebraic models for CBI, and show how to interpret CBI-formulas in these models.

Our CBI-models are based on the relational commutative monoids used to model BBI [17, 8]. In fact, they are special cases of these monoids, containing extra structure: an involution operation '$-$' on elements and a distinguished element[3] ∞ that characterises the result of combining an element with its dual under involution. In particular, our models include as instances all Abelian groups.

Note that we write $\mathcal{P}(X)$ for the powerset of a set X.

Definition 2.1 (CBI-*model*)**.** A CBI-*model* is given by a tuple $\langle R, \circ, e, -, \infty\rangle$, where $\circ : R \times R \rightarrow \mathcal{P}(R)$, $e \in R$, $- : R \rightarrow \mathcal{P}(R)$, and $\infty \subseteq R$ such that:

1. $\circ$ is commutative and associative, with $x \circ e = \{x\}$
2. $-x = \{y \in R \mid x \circ y \cap \infty \neq \emptyset\}$
3. $- - x = \{x\}$

We extend $-$ and $\circ$ to $\mathcal{P}(R)$ and $\mathcal{P}(R) \times \mathcal{P}(R)$ respectively by: $-X =_{\text{def}} \bigcup_{x \in X} -x$ and $X \circ Y =_{\text{def}} \bigcup_{x \in X, y \in Y} x \circ y$. Associativity of $\circ$ is understood with respect to this extension.

We remark that if $\langle R, \circ, e, -, \infty\rangle$ is a CBI-model then $\langle R, \circ, e\rangle$ is a BBI-model, i.e. a relational commutative monoid.

Proposition 2.2. *If $\langle R, \circ, e, -, \infty\rangle$ is a* CBI-*model then:*

1. *$\forall x \in R.\ -x$ is a singleton set;*
2. *$-e = \infty$;*
3. *$\forall x \in R.\ x \circ -x \supseteq \infty$;*
4. *$\forall X \subseteq R.\ R \setminus (-X) = -(R \setminus X)$.*

Proof. 1. By contradiction. If $-x = \emptyset$ then $--x = \bigcup_{y \in -x} -y = \emptyset$, which contradicts $--x = \{x\}$. If $x_1, x_2 \in -x$ with $x_1 \neq x_2$, then $-x_1 \cup -x_2 \subseteq --x$. Also, $-x_1 \neq -x_2$, otherwise we would have $\{x_1\} = --x_1 = --x_2 = \{x_2\}$ and thus $x_1 = x_2$. Since $-x_1$ and $-x_2$ have cardinality > 0 (see above), $--x$ must have cardinality > 1, which contradicts $--x = \{x\}$.

2. We have:

$$\begin{array}{rcl} -e & = & \{y \in R \mid e \circ y \cap \infty \neq \emptyset\} \\ & = & \{y \in R \mid \{y\} \cap \infty \neq \emptyset\} \\ & = & \{y \in R \mid y \in \infty\} \\ & = & \infty \end{array}$$

[2] To our knowledge, there are no existing such calculi even for BBI, though Pym and O'Hearn have given systems of both types for BI [26, 24]

[3] For technical convenience, we actually define ∞ to be a set of elements, but the conditions defining our models force ∞ to be a singleton set. See Convention 2.3.

3. Using part 1, first write $-x = \{x'\}$. Then $\{x'\} = \{y \in R \mid x \circ y \cap \infty \neq \emptyset\}$, so $x \circ x' \cap \infty = x \circ -x \cap \infty$ is nonempty. By parts 1 and 2, $\infty = -e$ is a singleton set, so we must have $x \circ -x \supseteq \infty$ as required.
4. ($\subseteq$) Suppose $x \in R \setminus -X$, i.e. $x \notin -X = \bigcup_{y \in X} -y$, so $x \notin -y$ for any $y \in X$. Also, using part 1, we have $x \in --x = -\{z\} = -z$ for some z. We must have $z \notin X$, so $x \in \bigcup_{z \notin X} -z = \bigcup_{z \in R \setminus X} -z = -(R \setminus X)$ as required.
($\supseteq$) Suppose $x \in -(R \setminus X)$, i.e. $x \in -y$ for some $y \notin X$. Note that we cannot have $x \in -z$ for any $z \in X$, otherwise by part 1 we have $-y = -z = \{x\}$ and thus $\{y\} = --y = --z = \{z\}$, so $y = z$, which is a contradiction. Thus $x \notin \bigcup_{z \in X} -z = -X$, i.e. $x \in R \setminus -X$ as required.

□

Parts 1 and 2 of Proposition 2.2 justify the following convention.

Convention 2.3. Given a CBI-model $\langle R, \circ, e, -, \infty \rangle$, for any $x \in R$ the notation $-x$ is henceforth to be understood as the unique element $z \in R$ such that $-x = \{z\}$. Similarly, ∞ is to be understood as the unique $z \in R$ such that $\infty = \{z\}$.

If $\langle R, \circ, e, -, \infty \rangle$ is a CBI-model and the cardinality of $x \circ y$ is ≤ 1 for all $x, y \in R$, then we understand $\circ$ as a partial function $R \times R \rightharpoonup R$ in the obvious way.

Proposition 2.4. *Let $\langle R, \circ, e, -, \infty \rangle$ be a* CBI-*model with $\circ$ a partial function. If $\infty = e$ then $\circ$ is in fact a total function and $\langle R, \circ, e, - \rangle$ is an Abelian group.*

Proof. First note that by part 3 of Proposition 2.2 and the fact that $\circ$ is a partial function, we have $-x \circ x = \infty = e$ for all $x \in R$. Now, to see that $x \circ y$ is defined for any $x, y \in R$, observe that $-x \circ (x \circ y) = (-x \circ x) \circ y = e \circ y = y$. Thus $-x \circ (x \circ y)$ is defined, which can only be the case if $x \circ y$ is defined.

To see that $\langle R, \circ, e, - \rangle$ is an Abelian group, we first observe that $\langle R, \circ, e \rangle$ is already a partial commutative monoid by the conditions imposed on $\circ$ by the definition of CBI-models (Defn. 2.1). Furthermore, $\circ$ is a total function by the above, and $-x$ is the unique inverse of x for any $x \in R$, since $-x \circ x = e$ and $y \circ x = e$ implies $-x = (y \circ x) \circ -x = y \circ (x \circ -x) = y$. □

We now define the syntax of CBI, and give the interpretation of its connectives in terms of our CBI-models. We assume a fixed set $\mathcal{V}$ of propositional variables.

Definition 2.5 (CBI-formula)**.** *Formulas* of CBI are given by the following grammar:

$$\begin{array}{rl} F ::= & P \mid \top \mid \bot \mid \neg F \mid F \wedge F \mid F \vee F \mid F \rightarrow F \mid \\ & \top^* \mid \bot^* \mid {\sim}F \mid F * F \mid F \mathbin{\overset{*}{\vee}} F \mid F \mathrel{-\!\!*} F \end{array}$$

where P ranges over $\mathcal{V}$.

CBI-formulas extend (B)BI-formulas with a multiplicative falsity $\bot^*$, negation $\sim$ and disjunction $\mathbin{\overset{*}{\vee}}$. Now in order to define the interpretation of CBI-formulas in a CBI-model $M = \langle R, \circ, e, -, \infty \rangle$, we need as usual an *environment for M*, which is a function $\rho : \mathcal{V} \rightarrow R$ interpreting propositional variables as true or false in a given "resource state" $r \in R$. We can then define a satisfaction or "forcing" relation interpreting formulas relative to model elements.

Definition 2.6 (CBI satisfaction relation)**.** Let $M = \langle R, \circ, e, -, \infty \rangle$ be a CBI-model and let ρ be an environment for M. Then, for any CBI-formula F and $r \in R$, define the *satisfaction relation* $r \models F$ by induction on the structure of F as follows:

$$\begin{array}{rcl}
r \models P & \Leftrightarrow & r \in \rho(P) \\
r \models \top & \Leftrightarrow & \text{always} \\
r \models \bot & \Leftrightarrow & \text{never} \\
r \models \neg F & \Leftrightarrow & r \not\models F \\
r \models F_1 \wedge F_2 & \Leftrightarrow & r \models F_1 \text{ and } r \models F_2 \\
r \models F_1 \vee F_2 & \Leftrightarrow & r \models F_1 \text{ or } r \models F_2 \\
r \models F_1 \rightarrow F_2 & \Leftrightarrow & r \models F_1 \text{ implies } r \models F_2 \\
r \models \top^* & \Leftrightarrow & r = e \\
r \models \bot^* & \Leftrightarrow & r \neq \infty \\
r \models {\sim}F & \Leftrightarrow & -r \not\models F \\
r \models F_1 * F_2 & \Leftrightarrow & \exists r_1, r_2.\ r \in r_1 \circ r_2 \text{ and } r_1 \models F_1 \\
 & & \text{and } r_2 \models F_2 \\
r \models F_1 \mathbin{\overset{*}{\vee}} F_2 & \Leftrightarrow & \forall r_1, r_2.\ -r \in r_1 \circ r_2 \text{ implies} \\
 & & -r_1 \models F_1 \text{ or } -r_2 \models F_2 \\
r \models F_1 \mathrel{-\!\!*} F_2 & \Leftrightarrow & \forall r', r''.\ r'' \in r \circ r' \text{ and } r' \models F_1 \\
 & & \text{implies } r'' \models F_2
\end{array}$$

Note that $r \models F$ should be read informally as: "F is true in resource state r (in the model M and under environment ρ)".

We remark that the satisfaction relation for CBI is just an extension of the standard satisfaction relation for BBI with the clauses for $\bot^*$, $\sim$ and $\mathbin{\overset{*}{\vee}}$.

Perhaps surprisingly, multiplicative falsity $\bot^*$ and multiplicative negation ${\sim}F$ are not interpreted in $\langle R, \circ, e, -, \infty \rangle$ as the model element ∞ and the set $-F = \{r \mid -r \models F\}$ respectively, but rather as $R \setminus \{\infty\}$ and $R \setminus -F$. These interpretations, which essentially embed an additive negation inside the multiplicative connectives, ensure that the expected semantic equivalences hold between formulas. For example, ${\sim}F$ and $F \mathrel{-\!\!*} \bot^*$ are semantically equivalent under our interpretation, but they are not if ${\sim}F$ and $\bot^*$ are interpreted as $-F$ and ∞ respectively. As expected, multiplicative disjunction $\mathbin{\overset{*}{\vee}}$ is interpreted as the de Morgan dual of $*$ with respect to $\sim$.

We say that a CBI-formula F is *true* in a CBI-model $M = \langle R, \circ, e, -, \infty \rangle$ iff $r \models F$ for any environment for M and for all $r \in R$. Truth of a BBI-formula in a BBI-model is similar.

Lemma 2.7 (CBI equivalences)**.** *For any* CBI-*model M, the following semantic equivalences $F = G$ hold in the sense that F is true in M iff G is true in M:*

$$\begin{array}{rclcrcl}
{\sim}\top & = & \bot & & F \mathbin{\overset{*}{\vee}} G & = & {\sim}({\sim}F * {\sim}G) \\
{\sim}\top^* & = & \bot^* & & F \mathrel{-\!\!*} G & = & {\sim}F \mathbin{\overset{*}{\vee}} G \\
{\sim}{\sim}F & = & F & & F \mathrel{-\!\!*} G & = & {\sim}G \mathrel{-\!\!*} {\sim}F \\
\neg{\sim}F & = & {\sim}\neg F & & F \mathrel{-\!\!*} \bot^* & = & {\sim}F \\
F * {\sim}F & = & \bot^* & & F \mathbin{\overset{*}{\vee}} \bot^* & = & F
\end{array}$$

In the following, we call a formula F a *theorem* of CBI if it is true in every CBI-model, and similarly for BBI. Our next result establishes that CBI is a stronger logic than BBI in the sense that it has more theorems.

Proposition 2.8 (Non-conservative extensionality)**.** CBI *is a non-conservative extension of* BBI. *That is, all theorems of* BBI *are theorems of* CBI, *but the converse does not hold (even when restricted to* BBI-*formulas).*

Proof. (Sketch) To see that CBI is an extension of BBI, we just observe that any CBI-model is in particular a BBI-model, since the latter are just relational commutative monoids.

Now let P be a propositional variable and let I and J be abbreviations for BBI-formulas defined as follows:

$$\begin{array}{rcl}
I & =_{\text{def}} & \neg\top^* \mathrel{-\!\!*} \bot \\
J & =_{\text{def}} & \top * (\top^* \wedge \neg(P \mathrel{-\!\!*} \neg I))
\end{array}$$

Using the definition of satisfaction above, the formula I can be satisfied only by "nonextensible" elements of a model, i.e. those elements r such that $r \circ r' = \emptyset$ for all $r' \neq e$. Similarly, the formula J expresses the existence of some element r such that $r \models P$ and r is nonextensible. In CBI-models, only ∞ can possibly be nonextensible since $r \circ -r \neq \emptyset$ for all r by Proposition 2.2, and ∞ is the unique element r satisfying $-r = e$. Thus, in CBI-models, if $r \models I$ and $r \models J$ then $r = \infty$ and $\infty \models P$, so $I \wedge J \rightarrow P$ is a theorem of CBI. However, it is not a theorem of BBI, since one can easily construct a partial or relational commutative monoid with two distinct nonextensible elements. □

3. Examples of CBI-models

We now turn to some concrete examples of CBI-models. In all of our examples, the monoid operation $\circ$ is a partial function rather than a relation.

Example 3.1 (Personal finance)**.** This example builds on the "vending machine" model for BI given by Pym, O'Hearn and Yang [27], which itself was inspired by Girard's well-known "Marlboro and Camel" illustration of linear logic [18].

Let $\langle \mathbb{Z}, +, 0, - \rangle$ be the Abelian group of integers under addition with identity 0, where $-$ is the usual unary minus. This group is a CBI-model by Proposition 2.4. The elements of this model can be understood as financial resources, i.e money (which we shall measure in pounds sterling, £), with positive and negative integers representing respectively *credit* and *debt*. We read the CBI-satisfaction relation $\pounds m \models F$ informally as "$\pounds m$ is enough to make F true", and show how to read some example CBI-formulas according to this interpretation.

Let C and W be atomic formulas denoting respectively the ability to buy cigarettes costing £5 and whisky costing £20[4], so that we have $\pounds m \models C \Leftrightarrow m \geq 5$ and $\pounds m \models W \Leftrightarrow m \geq 20$. Then, as is also the case in BBI, the formula $C \wedge W$ denotes the ability to buy cigarettes and the ability to buy whisky (but not necessarily to buy both together):

$$\begin{array}{lcl} \pounds m \models C \wedge W & \Leftrightarrow & \pounds m \models C \text{ and } \pounds m \models W \\ & \Leftrightarrow & m \geq 20 \end{array}$$

In contrast, the formula $C * W$ denotes the ability to buy both cigarettes and whisky together:

$$\begin{array}{lcl} \pounds m \models C * W & \Leftrightarrow & \exists m_1, m_2 \in \mathbb{Z}.\ \pounds m = \pounds m_1 + \pounds m_2 \text{ and} \\ & & \pounds m_1 \models C \text{ and } \pounds m_2 \models W \\ & \Leftrightarrow & m \geq 25 \end{array}$$

Again, as in BBI, the multiplicative implication $C \mathrel{-\!\!*} W$ denotes the fact that if one acquires enough money to buy cigarettes then the resulting balance of funds is sufficient to buy whisky:

$$\begin{array}{lcl} \pounds m \models C \mathrel{-\!\!*} W & \Leftrightarrow & \forall m' \in \mathbb{Z}.\ \pounds m' \models C \text{ implies} \\ & & \pounds m + \pounds m' \models W \\ & \Leftrightarrow & m \geq 15 \end{array}$$

What about the "new" multiplicative connectives of CBI? We have $\pounds m \models \bot^* \Leftrightarrow m \neq 0$, so that $\bot^*$ simply denotes the fact that one has either some credit or some debt. Now consider the formula $\sim C$. We have:

$$\pounds m \models \sim C \ \Leftrightarrow\ -\pounds m \not\models C \ \Leftrightarrow\ -m < 5 \ \Leftrightarrow\ m > -5$$

So $\sim C$ denotes the fact that one's debt, if any, is strictly less than the price of a pack of cigarettes. As for the multiplicative disjunction, $C \mathbin{\overset{*}{\vee}} W$, we have:

$$\begin{array}{lcl} \pounds m \models C \mathbin{\overset{*}{\vee}} W & \Leftrightarrow & \forall m_1, m_2.\ -\pounds m = \pounds m_1 + \pounds m_2 \\ & & \text{implies } -\pounds m_1 \models C \text{ or } -\pounds m_2 \models W \\ & \Leftrightarrow & m \geq 24 \end{array}$$

It is not immediately obvious how to read this formula informally. However, observing that $C \mathbin{\overset{*}{\vee}} W$ is semantically equivalent to $\sim C \mathrel{-\!\!*} W$ and to $\sim W \mathrel{-\!\!*} C$, the meaning becomes perfectly clear: if one spends less than the price of a pack of cigarettes, then one will still have enough money to buy whisky, and vice versa.

In our remaining examples, we just show how to construct a CBI-model, and leave the interpretation of CBI-formulas inside these models as an exercise for interested readers.

Example 3.2 (Regular languages)**.** Let Σ be an alphabet and let $\mathcal{L}(\Sigma)$ denote the set of regular languages over Σ. Let ϵ be the empty language and let $+$ denote disjoint union of languages (so that $L_1 + L_2$ is undefined if $L_1 \cap L_2 \neq \emptyset$). It is readily seen that $\langle \mathcal{L}(\Sigma), +, \epsilon \rangle$ is a partial commutative monoid. We observe that for any regular language L, its complement $\overline{L} = \Sigma \setminus L$ is the unique regular language such that $L + \overline{L} = \Sigma$. Thus $\langle \mathcal{L}(\Sigma), +, \epsilon, \overline{\cdot}, \Sigma \rangle$ is a CBI-model. Note that the same model construction works if one takes as the domain the set of all languages over Σ, rather than just the regular languages.

Example 3.3 (Bit arithmetic)**.** Let $n \in \mathbb{N}$ and observe that an n-bit binary number can be represented as an element of the set $\{0,1\}^n$. Let XOR and NOT be the usual logical operations on binary numbers. Then the following is a CBI-model:

$$\langle \{0,1\}^n, \text{XOR}, \{0\}^n, \text{NOT}, \{1\}^n \rangle$$

In this model, the resources e and ∞ are the n-bit representations of 0 and $2^n - 1$ respectively.

Example 3.4 (Action communication)**.** Let A be any set of objects (to be understood as CCS-style "actions") and define the set $\overline{A} = \{\overline{a} \mid a \in A\}$ to be disjoint from A. Then the following tuple is a CBI-model:

$$\langle A \cup \overline{A} \cup \{0, \tau\}, \cdot \mid \cdot\,, 0, \overline{\cdot}, \tau \rangle$$

where $0, \tau \notin A \cup \overline{A}$, the operation $\overline{\cdot}$ is extended to $A \cup \overline{A} \cup \{0, \tau\}$ by $\overline{0} =_{\text{def}} \tau$ and $\overline{\overline{a}} =_{\text{def}} a$ and $\cdot \mid \cdot$ is a commutative binary operation defined as follows:

$$\begin{array}{lcl} a \mid 0 & =_{\text{def}} & a \\ a \mid \overline{a} & =_{\text{def}} & \tau \\ a \mid b & =_{\text{def}} & \text{undefined for } b \notin \{0, \overline{a}\} \end{array}$$

Note that $\langle A \cup \overline{A} \cup \{0, \tau\}, \cdot|\cdot\,, 0 \rangle$ is a partial commutative monoid. The operation $\cdot \mid \cdot$ models a very simplistic version of communication between actions: communication with the empty action 0 has no effect, communication between a pair of dual actions a and $\overline{a}$ (which may be read, e.g., as "send a" and "receive a") results in the "successful communication" action τ, and all other communications are disallowed.

The following example shows that, when the monoidal structure of a CBI-model is fixed, the choice of ∞ is not unique in general.

Example 3.5 (Integer modulo arithmetic)**.** Consider the monoid $\langle \mathbb{Z}_n, +_n, 0 \rangle$, where $\mathbb{Z}_n$ is the set of integers modulo n, and $+_n$ is addition modulo n. We can form a CBI-model from this monoid by choosing, for any $m \in \mathbb{Z}_n$, $\infty =_{\text{def}} m$ and $-k =_{\text{def}} m -_n k$ (where $-_n$ is subtraction modulo n).

Example 3.6 (Syntactic models)**.** Given an arbitrary monoid $\langle R, \circ, e \rangle$, we give a syntactic construction to generate a CBI-model $\langle R', \circ', e', -', \infty' \rangle$. Consider the set T of terms given by the grammar:

$$t \in T ::= r \in R \mid \infty \mid t \cdot t \mid -t$$

and let $\approx$ be the least congruence such that: $r_1 \cdot r_2 \approx r$ when $r_1 \circ r_2 = r$; $t_1 \cdot t_2 \approx t_2 \cdot t_1$; $t_1 \cdot (t_2 \cdot t_3) \approx (t_1 \cdot t_2) \cdot t_3$; $- - t \approx t$; $t \cdot (-t) \approx \infty$, and $t_1 \approx -t_2$ whenever $t_1 \circ t_2 \approx \infty$. Write $T/\!\approx$ for the quotient of T by the relation $\approx$, and $[t]$ for

[4] Prices roughly correct at time of going to press.

the equivalence class of t. The required CBI-model is obtained by defining $R' =_{\text{def}} T/\approx$, $\circ'([t_1],[t_2]) =_{\text{def}} [t_1 \circ t_2]$, $e' =_{\text{def}} [e]$, $-'(t) =_{\text{def}} [-t]$, and $\infty' =_{\text{def}} [\infty]$.

Example 3.7 (Generalised heaps)**.** A natural question is whether BBI models used in separation logic are also CBI-models. Consider the partial commutative monoid $\langle H, \circ, e\rangle$, where $H =_{\text{def}} \mathbb{Z}_{>0} \rightharpoonup \mathbb{Z}$ is the set of partial functions from positive integers to integers, $\circ$ is disjoint union of the graph of functions, and e is the function with empty domain. Unfortunately, no choice of ∞ gives rise to a CBI-model. However, it is possible to embed the heap monoid into a more general structure $\langle H', \circ', e'\rangle$, where $H' =_{\text{def}} \mathcal{P}(\mathbb{Z}_{>0} \times \mathbb{Z})$ is the set of relations instead of partial functions, $\circ$ is disjoint union, and e is the empty relation. A CBI-model is then obtained by setting $\infty =_{\text{def}} \mathbb{Z}_{>0} \times \mathbb{Z}$, and $-r =_{\text{def}} (\mathbb{Z}_{>0} \times \mathbb{Z}) \setminus r$.

Example 3.8 (Heaps with fractional permissions)**.** As a final example, we consider a heap monoid with fractional permissions [4] $\langle H_p, \circ_p, e_p\rangle$, where $H_p =_{\text{def}} \mathbb{Z}_{>0} \rightharpoonup \mathbb{Z} \times (0,1]$ consists of functions which in addition return a permission in the real interval $(0, 1]$, and $\circ$ is defined on functions with overlapping domains using a partial composition function $\oplus : (\mathbb{Z}\times(0,1])\times(\mathbb{Z}\times(0,1]) \rightharpoonup (\mathbb{Z}\times(0,1])$ such that $\oplus((v_1,p_1),(v_2,p_2))$ is defined if and only if $v_1 = v_2$ and $p_1 + p_2 \leq 1$, and returns $(v_1, p_1 + p_2)$. The unit e_p is again the function with empty domain. In analogy with our approach to ordinary heaps in the previous example, we define a more general structure $\langle H'_p, \circ'_p, e'_p\rangle$, where $H'_p =_{\text{def}} \mathbb{Z}_{>0} \times \mathbb{Z} \to [0,1]$ is the set of *total* functions, and $\circ'_p$ is defined point-wise using $+ : [0,1]\times[0,1] \rightharpoonup [0,1]$, which is ordinary addition restricted to be defined only when the result is ≤ 1. The function e'_p maps everything to 0. A CBI-model is then obtained by setting ∞ as mapping everything to 1, and $-r =_{\text{def}} \{(l, v, 1-p) \mid (l, v, p) \in r\}$. Observe that, in this case, the general model is in a way simpler, and that the $-$ operation returns the complement of the permissions.

4. $\mathrm{DL}_{\mathrm{CBI}}$: a display calculus proof system for CBI

In this section, we present $\mathrm{DL}_{\mathrm{CBI}}$, a display calculus proof system for CBI based on Belnap's *display logic* [1]. $\mathrm{DL}_{\mathrm{CBI}}$ can be seen as a particular instantiation of display logic to CBI, in much the same style as Goré's display systems for other substructural logics [20]. Our display calculus satisfies cut-elimination, and is sound and complete with respect to our CBI-models.

The proof judgements of $\mathrm{DL}_{\mathrm{CBI}}$, called consecutions, are built from structures which generalise the bunches used in existing proof systems for (B)BI (cf. [26]).

Definition 4.1 (Structure / consecution)**.** A $\mathrm{DL}_{\mathrm{CBI}}$-*structure* X is constructed according to the following grammar:

$$X ::= F \mid \emptyset \mid \sharp X \mid X;X \mid \varnothing \mid \flat X \mid X,X$$

where F ranges over CBI-formulas. If X and Y are structures then $X \vdash Y$ is said to be a *consecution*.

The following definition gives the semantic interpretation of our consecutions, and extends the notion of validity for CBI formulas given in Section 2.

Structural connectives

Additive family:	$\emptyset$	$\sharp$	;
Multiplicative family:	$\varnothing$	$\flat$	,
Arity:	0	1	2

Formula connectives

Additive family:	$\top$	$\bot$	$\neg$	$\wedge$	$\vee$	$\to$
Multiplicative family:	$\top^*$	$\bot^*$	$\sim$	$*$	$\mathbin{\vee\!\!\!\!\!*}$	$\mathbin{-\!\!*}$
Arity:	0	0	1	2	2	2

Figure 1. The connective families of $\mathrm{DL}_{\mathrm{CBI}}$.

Definition 4.2 (Validity in $\mathrm{DL}_{\mathrm{CBI}}$)**.** For any structure X we mutually define two formulas Ψ_X and Υ_X by induction on the structure of X as follows:

$$\begin{array}{rcl@{\qquad}rcl}
\Psi_F & = & F & \Upsilon_F & = & F \\
\Psi_\emptyset & = & \top & \Upsilon_\emptyset & = & \bot \\
\Psi_{\sharp X} & = & \neg\Upsilon_X & \Upsilon_{\sharp X} & = & \neg\Psi_X \\
\Psi_{X_1;X_2} & = & \Psi_{X_1} \wedge \Psi_{X_2} & \Upsilon_{X_1;X_2} & = & \Upsilon_{X_1} \vee \Upsilon_{X_2} \\
\Psi_\varnothing & = & \top^* & \Upsilon_\varnothing & = & \bot^* \\
\Psi_{\flat X} & = & \sim\Upsilon_X & \Upsilon_{\flat X} & = & \sim\Psi_X \\
\Psi_{X_1,X_2} & = & \Psi_{X_1} * \Psi_{X_2} & \Upsilon_{X_1,X_2} & = & \Upsilon_{X_1} \mathbin{\vee\!\!\!\!\!*} \Upsilon_{X_2}
\end{array}$$

A consecution $X \vdash Y$ is said to be *true* in a CBI-model $M = \langle R, \circ, e, -, \infty\rangle$ if for any environment ρ for M and for all $r \in R$, we have $r \models \Psi_X$ implies $r \models \Upsilon_Y$. $X \vdash Y$ is said to be *valid* if it is true in all CBI-models.

We can divide the structural and logical connectives of $\mathrm{DL}_{\mathrm{CBI}}$ into an additive family and a multiplicative family, as illustrated in Figure 1. In Belnap's display logic, an arbitrary number of families of connectives may be involved; the structural connectives are fixed for each family while the logical connectives may be chosen from a given set. Then, for each family, display logic posits certain bidirectional proof rules called *display postulates*, involving only the structural connectives of the family. The purpose of the display postulates is to allow consecutions to be shuffled so as to "display" any structure occurrence therein as the entire left- or right-hand side of a consecution (according to the original position of the structure in the consecution). The logical introduction rules for formulas are similarly prescribed for each connective family, with only the structural rules governing the family chosen freely.

We give the display postulates for $\mathrm{DL}_{\mathrm{CBI}}$ in Figure 2. These are Belnap's original postulates instantiated to our connective families, though other formulations are possible (see e.g. [19]). Note that we write a rule with a double line to indicate that it is invertible, i.e., that the roles of premise and conclusion may be reversed. A figure with three consecutions separated by two double lines is used to abbreviate two invertible rules in the obvious way. Two consecutions are said to be *display-equivalent* if there is a derivation of one from the other using only the display postulates.

Definition 4.3 (Antecedent part / consequent part)**.** A structure W is said to be a *part* of another structure Z if W is a substructure of Z (in the obvious sense). W is said to be a *positive part* of Z if W occurs inside an even number of occurrences of $\sharp$ and $\flat$ in Z, and a *negative part* of Z otherwise.

A structure W is said to be an *antecedent part* of a consecution $X \vdash Y$ if it is a positive part of X or a negative part of Y. W is said to be a *consequent part* of $X \vdash Y$ if it is a negative part of X or a positive part of Y.

The following theorem describes the fundamental property of display logic: the ability to "display" structures occurring in a consecution by rearranging it using the display postulates.

Additive family:

$$\begin{array}{c} X;Y \vdash Z \\ \hline\hline X \vdash \sharp Y; Z \end{array}\ (\text{AD1}) \qquad \begin{array}{c} X \vdash Y;Z \\ \hline\hline X;\sharp Y \vdash Z \\ \hline\hline X \vdash Z;Y \end{array}\ \begin{array}{l}(\text{AD2a})\\ \\ (\text{AD2b})\end{array} \qquad \begin{array}{c} X \vdash Y \\ \hline\hline \sharp Y \vdash \sharp X \\ \hline\hline \sharp\sharp X \vdash Y \end{array}\ \begin{array}{l}(\text{AD3a})\\ \\ (\text{AD3b})\end{array}$$

Multiplicative family:

$$\begin{array}{c} X,Y \vdash Z \\ \hline\hline X \vdash \flat Y, Z \end{array}\ (\text{MD1}) \qquad \begin{array}{c} X \vdash Y,Z \\ \hline\hline X,\flat Y \vdash Z \\ \hline\hline X \vdash Z,Y \end{array}\ \begin{array}{l}(\text{MD2a})\\ \\ (\text{MD2b})\end{array} \qquad \begin{array}{c} X \vdash Y \\ \hline\hline \flat Y \vdash \flat X \\ \hline\hline \flat\flat X \vdash Y \end{array}\ \begin{array}{l}(\text{MD3a})\\ \\ (\text{MD3b})\end{array}$$

Figure 2. The display postulates for $\mathrm{DL}_{\mathrm{CBI}}$.

Theorem 4.4 (Display theorem (Belnap [1])). *For any antecedent part W of a consecution $X \vdash Y$ there exists a structure Z such that $W \vdash Z$ is display-equivalent to $X \vdash Y$. Similarly, for any consequent part W of $X \vdash Y$ there exists a structure Z such that $Z \vdash W$ is display-equivalent to $X \vdash Y$.*

We note that the display theorem holds even when connectives from different families occur in the same consecution.

Example 4.5. The antecedent part Y of the consecution $\flat(X, \sharp Y) \vdash Z; \flat W$ can be displayed as follows:

$$\begin{array}{cl} \flat(X,\sharp Y) \vdash Z;\flat W & \\ \hline \flat(Z;\flat W) \vdash \flat\flat(X,\sharp Y) & (\text{MD3a}) \\ \hline \flat\flat\flat(Z;\flat W) \vdash \flat\flat(X,\sharp Y) & (\text{MD3a,b}) \\ \hline \flat(X,\sharp Y) \vdash \flat\flat(Z;\flat W) & (\text{MD3a}) \\ \hline \flat(Z;\flat W) \vdash X,\sharp Y & (\text{MD3a}) \\ \hline \flat(Z;\flat W),\flat X \vdash \sharp Y & (\text{MD2b}) \\ \hline \sharp\sharp Y \vdash \sharp(\flat(Z;\flat W),\flat X) & (\text{AD3a}) \\ \hline Y \vdash \sharp(\flat(Z;\flat W),\flat X) & (\text{AD3a,b}) \end{array}$$

The logical rules for $\mathrm{DL}_{\mathrm{CBI}}$, given in Figure 3, follow the familiar division between left and right introduction rules (plus the identity axiom and a cut rule). Again, these are the instantiations of the standard display logic rules to the connective families we consider for CBI. The structural rules of $\mathrm{DL}_{\mathrm{CBI}}$ are given in Figure 4. These implement associativity, commutativity and unitary laws for ';' and ',' on both sides of consecutions, plus weakening and contraction for the additive combination ';'.

The identity axiom of $\mathrm{DL}_{\mathrm{CBI}}$ is postulated only for propositional variables[5], but can be recovered for arbitrary formulas.

Proposition 4.6. *$F \vdash F$ is $\mathrm{DL}_{\mathrm{CBI}}$-provable for all formulas F.*

Proof. By structural induction on F. □

Theorem 4.7 (Cut-elimination). *If a consecution $X \vdash Y$ is provable in $\mathrm{DL}_{\mathrm{CBI}}$ then it is also provable without the use of (Cut).*

Proof. By inspection, our proof rules satisfy the 8 conditions shown by Belnap in [1] to be sufficient for cut-elimination to hold. See [5] for details of the conditions and their verification. □

The following corollary of Theorem 4.7 uses the notion of a *subformula* of a CBI-formula, defined in the usual way.

Identity rules:

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

Additive family:

$$\frac{\emptyset \vdash X}{\top \vdash X}\ (\top\text{L}) \qquad \frac{}{\emptyset \vdash \top}\ (\top\text{R})$$

$$\frac{}{\bot \vdash \emptyset}\ (\bot\text{L}) \qquad \frac{X \vdash \emptyset}{X \vdash \bot}\ (\bot\text{R})$$

$$\frac{\sharp F \vdash X}{\neg F \vdash X}\ (\neg\text{L}) \qquad \frac{X \vdash \sharp F}{X \vdash \neg F}\ (\neg\text{R})$$

$$\frac{F;G \vdash X}{F \wedge G \vdash X}\ (\wedge\text{L}) \qquad \frac{X \vdash F \quad Y \vdash G}{X;Y \vdash F \wedge G}\ (\wedge\text{R})$$

$$\frac{F \vdash X \quad G \vdash Y}{F \vee G \vdash X;Y}\ (\vee\text{L}) \qquad \frac{X \vdash F;G}{X \vdash F \vee G}\ (\vee\text{R})$$

$$\frac{X \vdash F \quad G \vdash Y}{F \to G \vdash \sharp X;Y}\ (\to\text{L}) \qquad \frac{X;F \vdash G}{X \vdash F \to G}\ (\to\text{R})$$

Multiplicative family:

$$\frac{\varnothing \vdash X}{\top^* \vdash X}\ (\top^*\text{L}) \qquad \frac{}{\varnothing \vdash \top^*}\ (\top^*\text{R})$$

$$\frac{}{\bot^* \vdash \varnothing}\ (\bot^*\text{L}) \qquad \frac{X \vdash \varnothing}{X \vdash \bot^*}\ (\bot^*\text{R})$$

$$\frac{\flat F \vdash X}{\sim F \vdash X}\ (\sim\text{L}) \qquad \frac{X \vdash \flat F}{X \vdash \sim F}\ (\sim\text{R})$$

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

$$\frac{F \vdash X \quad G \vdash Y}{F \mathbin{\vee\!\!\!\!*} G \vdash X,Y}\ (\vee\!\!\!\!*\text{L}) \qquad \frac{X \vdash F,G}{X \vdash F \mathbin{\vee\!\!\!\!*} G}\ (\vee\!\!\!\!*\text{R})$$

$$\frac{X \vdash F \quad G \vdash Y}{F \mathrel{-\!\!*} G \vdash \flat X,Y}\ (-\!\!*\text{L}) \qquad \frac{X,F \vdash G}{X \vdash F \mathrel{-\!\!*} G}\ (-\!\!*\text{R})$$

Figure 3. Logical rules for $\mathrm{DL}_{\mathrm{CBI}}$. Note that X, Y range over structures, F, G range over CBI-formulas and P ranges over $\mathcal{V}$.

[5] This simplifies the proof of cut-elimination for $\mathrm{DL}_{\mathrm{CBI}}$.

Additive family:

$$\begin{array}{c} W;(X;Y)\vdash Z \\ \hline\hline (W;X);Y\vdash Z \end{array}\,(\text{AAL}) \qquad \begin{array}{c} W\vdash (X;Y);Z \\ \hline\hline W\vdash X;(Y;Z) \end{array}\,(\text{AAR})$$

$$\dfrac{X;Y\vdash Z}{Y;X\vdash Z}\,(\text{ACL}) \qquad \dfrac{X\vdash Y;Z}{X\vdash Z;Y}\,(\text{ACR})$$

$$\begin{array}{c} \emptyset;X\vdash Y \\ \hline\hline X\vdash Y \end{array}\,(\text{AIL}) \qquad \begin{array}{c} X\vdash Y;\emptyset \\ \hline\hline X\vdash Y \end{array}\,(\text{AIR})$$

$$\dfrac{X\vdash Z}{X;Y\vdash Z}\,(\text{WkL}) \qquad \dfrac{X\vdash Z}{X\vdash Y;Z}\,(\text{WkR})$$

$$\dfrac{X;X\vdash Z}{X\vdash Z}\,(\text{CtrL}) \qquad \dfrac{X\vdash Z;Z}{X\vdash Z}\,(\text{CtrR})$$

Multiplicative family:

$$\begin{array}{c} W,(X,Y)\vdash Z \\ \hline\hline (W,X),Y\vdash Z \end{array}\,(\text{MAL}) \qquad \begin{array}{c} W\vdash (X,Y),Z \\ \hline\hline W\vdash X,(Y,Z) \end{array}\,(\text{MAR})$$

$$\dfrac{X,Y\vdash Z}{Y,X\vdash Z}\,(\text{MCL}) \qquad \dfrac{X\vdash Y,Z}{X\vdash Z,Y}\,(\text{MCR})$$

$$\begin{array}{c} \varnothing,X\vdash Y \\ \hline\hline X\vdash Y \end{array}\,(\text{MIL}) \qquad \begin{array}{c} X\vdash Y,\varnothing \\ \hline\hline X\vdash Y \end{array}\,(\text{MIR})$$

Figure 4. Structural rules for $\mathrm{DL}_{\mathrm{CBI}}$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\begin{array}{c}\text{(Proposition 4.6)}\\ \vdots \\ F\vdash F\end{array}}{\sharp F\vdash \sharp F}\,(\mathrm{D}\equiv)}{\sharp F\vdash \neg F}\,(\neg\mathrm{R})}{\flat\neg F\vdash \flat\sharp F}\,(\mathrm{D}\equiv)}{\sim\neg F\vdash \flat\sharp F}\,(\sim\mathrm{L})}{\sim\neg F;\sim F\vdash \flat\sharp F}\,(\mathrm{WkL})}{\flat F\vdash \flat\sharp\flat(\sim\neg F;\sim F)}\,(\mathrm{D}\equiv)}{\sim F\vdash \flat\sharp\flat(\sim\neg F;\sim F)}\,(\sim\mathrm{L})}{\sim\neg F;\sim F\vdash \flat\sharp\flat(\sim\neg F;\sim F)}\,(\mathrm{WkL})}{\sharp\flat(\sim\neg F;\sim F)\vdash \flat(\sim\neg F;\sim F)}\,(\mathrm{D}\equiv)}{\flat\emptyset;\sharp\flat(\sim\neg F;\sim F)\vdash \flat(\sim\neg F;\sim F)}\,(\mathrm{WkL})}{\flat\emptyset\vdash \flat(\sim\neg F;\sim F);\flat(\sim\neg F;\sim F)}\,(\mathrm{D}\equiv)}{\flat\emptyset\vdash \flat(\sim\neg F;\sim F)}\,(\mathrm{CtrR})}{\sim\neg F\vdash \sharp\sim F;\emptyset}\,(\mathrm{D}\equiv)}{\sim\neg F\vdash \sharp\sim F}\,(\mathrm{AIR})}{\sim\neg F\vdash \neg\sim F}\,(\neg\mathrm{R})$$

Figure 5. A cut-free $\mathrm{DL}_{\mathrm{CBI}}$ proof of $\sim\neg F \vdash \neg\sim F$. The rule symbol $(\mathrm{D}\equiv)$ denotes the use of a display-equivalence.

Corollary 4.8 (Subformula property)**.** *If $X \vdash Y$ is $\mathrm{DL}_{\mathrm{CBI}}$-provable then there is a $\mathrm{DL}_{\mathrm{CBI}}$ proof of $X \vdash Y$ in which every formula occurrence is a subformula of a formula occurring in $X \vdash Y$.*

Proof. If $X \vdash Y$ is provable then it has a cut-free proof by Theorem 4.7. By inspection of the $\mathrm{DL}_{\mathrm{CBI}}$ rules, no rule instance in this proof can have in its premises any formula that is not a subformula of a formula occurring in its conclusion. Thus a cut-free proof of $X \vdash Y$ cannot contain any formulas which are not subformulas of formulas in $X \vdash Y$. □

Corollary 4.9 (Consistency)**.** *The consecution $\emptyset \vdash \emptyset$ is not provable in $\mathrm{DL}_{\mathrm{CBI}}$.*

Proof. If $\emptyset \vdash \emptyset$ were $\mathrm{DL}_{\mathrm{CBI}}$-provable then, by the subformula property (Corollary 4.8) there is a proof of $\emptyset \vdash \emptyset$ containing no formula occurrences anywhere. But every axiom of $\mathrm{DL}_{\mathrm{CBI}}$ contains a formula occurrence. □

Our main technical results concerning $\mathrm{DL}_{\mathrm{CBI}}$ are the following.

Theorem 4.10 (Soundness of $\mathrm{DL}_{\mathrm{CBI}}$)**.** *If there is a $\mathrm{DL}_{\mathrm{CBI}}$ proof of $X \vdash Y$ then $X \vdash Y$ is valid.*

Theorem 4.11 (Completeness of $\mathrm{DL}_{\mathrm{CBI}}$)**.** *If $X \vdash Y$ is valid then there is a $\mathrm{DL}_{\mathrm{CBI}}$ proof of $X \vdash Y$.*

We give the proofs of Theorems 4.10 and 4.11 in Section 5.

We remark that, although cut-free proofs in $\mathrm{DL}_{\mathrm{CBI}}$ enjoy the subformula property, cut-free proof search in our system is still rather non-deterministic due to the presence of the display postulates and structural rules. In Figure 5 we give a sample cut-free proof of the consecution $\sim\neg F \vdash \neg\sim F$, which illustrates this phenomenon. The applications of the display-equivalences are required in order to apply the logical rules, as one would expect, but the proof also makes seemingly essential use of contraction, weakening and a unitary law. It is not obvious to us whether the use of such structural rules can be eliminated by suitable reformulations of the logical rules. (We note that the need to manipulate the structure of bunches poses a similar problem for proof search in sequent calculus systems for BI [14].)

5. Soundness and completeness proofs for $\mathrm{DL}_{\mathrm{CBI}}$

In this section we give the proofs of soundness and completeness of our display calculus $\mathrm{DL}_{\mathrm{CBI}}$ with respect to validity in CBI-models. First, we define in Section 5.1 an extension LBI^{+} of a sequent calculus proof system for BBI. In this extension, the element ∞ and the involution '$-$' in CBI-models are represented directly. We demonstrate soundness and completeness of LBI^{+} with respect to CBI-models. Our proof of completeness uses techniques from modal logic, similar to those employed in [8], and is presented in Section 5.2. Then, in Section 5.3, we prove admissibility of the $\mathrm{DL}_{\mathrm{CBI}}$ rules in LBI^{+} under a suitable translation, and vice versa. Soundness and completeness of $\mathrm{DL}_{\mathrm{CBI}}$ then follows from the soundness and completeness of LBI^{+}.

5.1 LBI^{+}: a sequent calculus for CBI

In this section we define a simple extension BI^{+} of BBI, and a corresponding sequent calculus system, LBI^{+}, which is sound and complete with respect to CBI-models.

Formulas of BI^+ are given by the following grammar:

$$\begin{array}{rl} F ::= & P \mid \top \mid \bot \mid F \wedge F \mid F \vee F \mid F \to F \mid \\ & \top^* \mid F * F \mid F \mathrel{-\!\!*} F \mid \bowtie \end{array}$$

where P ranges over the propositional variables $\mathcal{V}$. These are exactly the formulas of BI plus the new atomic formula $\bowtie$. We also use the following abbreviations[6]:

$$\begin{array}{lll} \neg F & =_{\text{def}} & F \to \bot \\ -F & =_{\text{def}} & \neg(F \mathrel{-\!\!*} \neg\bowtie) \end{array}$$

Given a CBI-model $M = \langle R, \circ, e, -, \infty \rangle$ and an environment ρ for M, satisfaction of a BI^+-formula F by a resource state $r \in R$ is then given by the relation $r \models F$ for CBI-formulas (cf. Definition 2.6) plus the following clause for the formula $\bowtie$:

$$r \models \bowtie \quad \Leftrightarrow \quad r = \infty$$

Lemma 5.1.1. *Let $M = \langle R, \circ, e, -, \infty \rangle$ be a* CBI*-model and let ρ be an environment for M. For any $r \in R$ and formula F we have $r \models -F$ iff $-r \models F$.*

Proof. We have by the definitions of $-F$ and of satisfaction:

$$\begin{array}{rll} r \models -F & \Leftrightarrow & r \models \neg(F \mathrel{-\!\!*} \neg\bowtie) \\ & \Leftrightarrow & r \not\models F \mathrel{-\!\!*} \neg\bowtie \\ & \Leftrightarrow & \exists r', r''.\ r'' \in r \circ r' \text{ and } r' \models F \text{ but } r'' \not\models \neg\bowtie \\ & \Leftrightarrow & \exists r', r''.\ r'' \in r \circ r' \text{ and } r' \models F \text{ and } r'' = \infty \\ & \Leftrightarrow & \exists r'.\ \infty \in r \circ r' \text{ and } r' \models F \\ & \Leftrightarrow & -r \models F \end{array}$$

Note that the final equivalence above is justified by the fact that $-r$ is the unique element of R satisfying $\infty \in r \circ -r$, which follows from Proposition 2.2. □

As is standard in BI, we write *sequents* of the form $\Gamma \vdash F$, where F is a BI^+-formula and Γ is a *bunch*, given by the following grammar:

$$\Gamma ::= F \mid \Gamma ; \Gamma \mid \Gamma , \Gamma$$

where F ranges over BI^+-formulas. Thus bunches are trees whose leaves are formulas and whose internal nodes are either ';' or ','.

We write $\Gamma(\Delta)$ for a bunch of which Δ is a distinguished subbunch (i.e. subtree), and in such cases write $\Gamma(\Delta')$ for the bunch obtained by replacing Δ by the bunch Δ' in $\Gamma(\Delta)$. In analogy to the use of sets in ordinary sequent calculus, and as is again standard for BI, we consider bunches up to *coherent equivalence*:

Definition 5.1.2 (Coherent equivalence)**.** $\equiv$ is the least relation on bunches satisfying commutative monoid equations for ';' and $\top$, and for ',' and $\top^*$, plus the rule of congruence: if $\Delta \equiv \Delta'$ then $\Gamma(\Delta) \equiv \Gamma(\Delta')$.

We remark that a BI^+ sequent is a special case of a $\mathrm{DL}_{\mathrm{CBI}}$ consecution, modulo possible occurrences of the formula $\bowtie$, so that the notion of validity for $\mathrm{DL}_{\mathrm{CBI}}$ consecutions (cf. Definition 4.2) transfers straightforwardly to BI^+ sequents. That is, a sequent $\Gamma \vdash F$ is valid iff for any CBI-model $M = \langle R, \circ, e, -, \infty \rangle$, any environment ρ for M and all $r \in R$, we have $r \models \Psi_\Gamma$ implies $r \models F$, where Ψ_- is the function given in Definition 4.2 that replaces occurrences of ';' and ',' in a bunch by $\wedge$ and $*$ respectively. This definition of validity coincides with the standard one for BBI, when restricted to BBI-formulas.

We give the rules of a sequent calculus proof system LBI^+ for BI^+ in Figure 6. Its rules extend the rules of the usual sequent calculus for BI (cf. [26, 16]) with the double negation axiom needed for BBI, and two further axioms that directly reflect the fact that $-$ behaves as an involution in our models.

Structural rules:

$$\frac{}{F \vdash F}\,(\text{Id}) \qquad \frac{\Gamma(\Delta) \vdash F}{\Gamma(\Delta;\Delta') \vdash F}\,(\text{Weak}) \qquad \frac{\Gamma(\Delta;\Delta) \vdash F}{\Gamma(\Delta) \vdash F}\,(\text{Contr})$$

$$\frac{\Gamma' \vdash F}{\Gamma \vdash F}\,\Gamma \equiv \Gamma'\ (\text{Equiv}) \qquad \frac{\Delta \vdash G \quad \Gamma(G) \vdash F}{\Gamma(\Delta) \vdash F}\,(\text{Cut})$$

Propositional rules:

$$\frac{}{\Gamma(\bot) \vdash F}\,(\bot\text{L}) \qquad \frac{}{\Gamma \vdash \top}\,(\top\text{R})$$

$$\frac{\Gamma(F_1;F_2) \vdash F}{\Gamma(F_1 \wedge F_2) \vdash F}\,(\wedge\text{L}) \qquad \frac{\Gamma \vdash F_1 \quad \Gamma \vdash F_2}{\Gamma \vdash F_1 \wedge F_2}\,(\wedge\text{R})$$

$$\frac{\Gamma(F_1) \vdash F \quad \Gamma(F_2) \vdash F}{\Gamma(F_1 \vee F_2) \vdash F}\,(\vee\text{L}) \qquad \frac{\Gamma \vdash F_i}{\Gamma \vdash F_1 \vee F_2}\ i \in \{1,2\}\ (\vee R_i)$$

$$\frac{\Delta \vdash F_1 \quad \Gamma(\Delta;F_2) \vdash F}{\Gamma(\Delta; F_1 \to F_2) \vdash F}\,(\to\text{L}) \qquad \frac{\Gamma; F_1 \vdash F_2}{\Gamma \vdash F_1 \to F_2}\,(\to\text{R})$$

$$\frac{\Gamma(F_1,F_2) \vdash F}{\Gamma(F_1 * F_2) \vdash F}\,(*\text{L}) \qquad \frac{\Gamma \vdash F_1 \quad \Delta \vdash F_2}{\Gamma, \Delta \vdash F_1 * F_2}\,(*\text{R})$$

$$\frac{\Delta \vdash F_1 \quad \Gamma(F_2) \vdash F}{\Gamma(\Delta, F_1 \mathrel{-\!\!*} F_2) \vdash F}\,(\mathrel{-\!\!*}\text{L}) \qquad \frac{\Gamma, F_1 \vdash F_2}{\Gamma \vdash F_1 \mathrel{-\!\!*} F_2}\,(\mathrel{-\!\!*}\text{R})$$

BI^+ **axioms:**

$$\frac{}{\neg\neg F \vdash F}\,(\text{DNE}) \qquad \frac{}{--F \vdash F}\,(\text{DIE}) \qquad \frac{}{F \vdash --F}\,(\text{DII})$$

Figure 6. The proof rules of LBI^+.

Proposition 5.1.3. LBI^+ *is sound with respect to* CBI*-models.*

Proof. As usual, soundness follows from the fact that the proof rules of LBI^+ preserve truth in CBI-models and every axiom (i.e. 0-premise rule) is valid. We note first that the rules of LBI^+ preserve truth in BBI-models and thus in CBI-models in particular. Thus it only remains to show that the BI^+ axioms are true in any CBI-model. Soundness of the axiom (DNE) follows from the fact that additive implication is interpreted classically in BI^+. For the axioms (DIE) and (DII), note that $r \models --F$ iff $--r \models F$ by Lemma 5.1.1. Soundness of these axioms then follows from the fact that $--r = r$ in CBI-models. □

5.2 Completeness of LBI^+

We now show completeness of LBI^+ with respect to CBI-models by appealing to a general theorem of modal logic due to Sahlqvist. The result is an adaptation of the analogous completeness result for BBI in [8].

We first define MBI^+ pre-models, which interpret the LBI^+ connectives as modalities.

Definition 5.2.1. An MBI^+ *pre-model* is a tuple $\langle R, \circ, \mathrel{-\!\!\bullet}, e, -, \infty \rangle$, where $\circ : R \times R \to \mathcal{P}(R)$, $\mathrel{-\!\!\bullet} : R \times R \to \mathcal{P}(R)$, $e \in R$,

[6] Since we will treat $\to$ and the other additives classically in BI^+, we could also take $\neg$ as primitive, but choose not to for technical convenience.

$- : R \to \mathcal{P}(R)$, and $\infty \subseteq R$. We extend $\circ$ and $-$ to $\mathcal{P}(R) \times \mathcal{P}(R)$ and $\mathcal{P}(R)$ respectively in the same manner as in Definition 2.1.

The satisfaction relation for BI^+-formulas in MBI^+ pre-models is defined exactly as the satisfaction relation given above for BI^+-formulas in CBI-models, except that the clause for formulas of the form $F \mathrel{-\!\!*} G$ is replaced by the following one:

$$r \models F_1 \mathrel{-\!\!*} F_2 \quad \Leftrightarrow \quad \forall r', r''.\, r \in r' \mathrel{-\!\!\bullet} r'' \text{ and } M, r' \models F_1 \text{ implies } M, r'' \not\models F_2$$

Then, given any set AX of axioms, we define *AX-models* to be the MBI^+ pre-models in which every axiom in AX holds.

Definition 5.2.2 (Modal Logic Formulas)**.** Modal logic formulas F are defined by the grammar:

$$F ::= \bot \mid P \mid F \wedge F \mid \neg F \mid \triangle(F_1, \ldots, F_n)$$

where $\triangle$ ranges over the modalities $\{e, -, \circ, \mathrel{-\!\!\bullet}, \infty\}$ (with the obvious arities) and P ranges over $\mathcal{V}$. We identify BI^+-formulas and modal logic formulas by implicitly applying the usual translation for additives, plus the abbreviations $\bowtie \, = \infty$, $\top^* = e$, $F_1 * F_2 = F_1 \circ F_2$ and $F_1 \mathrel{-\!\!*} F_2 = \neg(F_1 \mathrel{-\!\!\bullet} \neg F_2)$.

Definition 5.2.3 (Very Simple Sahlqvist Formulas)**.** A *very simple Sahlqvist antecedent* A is a formula given by the grammar:

$$A ::= \top \mid \bot \mid P \mid A \wedge A \mid \triangle(A_1, \ldots, A_n)$$

where $\triangle$ ranges over the modalities $\{e, -, \circ, \mathrel{-\!\!\bullet}, \infty\}$ and P ranges over $\mathcal{V}$. A *very simple Sahlqvist formula* is a formula of the form $A \Rightarrow F^+$, where A is a very simple Sahlqvist antecedent and F^+ is a modal logic formula which is *positive* in that no propositional variable P in F^+ may occur inside the scope of an odd number of occurrences of $\neg$.

Theorem 5.2.4 (Sahlqvist [3])**.** *For every axiom set AX consisting of very simple Sahlqvist formulas, the modal logic proof theory generated by AX is complete with respect to the class of AX-models.*

Definition 5.2.5 (BI^+-Axioms)**.** The axiom set AX_{BI^+} consists of the following very simple Sahlqvist formulas:

1. $e \circ F \Rightarrow F$
2. $F \Rightarrow e \circ F$
3. $F \circ G \Rightarrow G \circ F$
4. $(F \circ G) \circ H \Rightarrow F \circ (G \circ H)$
5. $F \circ (G \circ H) \Rightarrow (F \circ G) \circ H$
6. $G \wedge (H \circ F) \Rightarrow (H \wedge (F \mathrel{-\!\!\bullet} G)) \circ \top$
7. $H \wedge (F \mathrel{-\!\!\bullet} G) \Rightarrow \top \mathrel{-\!\!\bullet} (G \wedge (H \circ F))$
8. $- - F \Rightarrow F$
9. $F \Rightarrow - - F$
10. $-F \Rightarrow F \mathrel{-\!\!\bullet} \infty$
11. $F \mathrel{-\!\!\bullet} \infty \Rightarrow -F$

We write $\mathrm{LAX}_{\mathrm{BI}^+}$ for the modal logic proof theory generated by the AX_{BI^+} axioms.

Corollary 5.2.6. *LAX_{BI^+} is complete with respect to the class of AX_{BI^+} models.*

Lemma 5.2.7. *Let $\langle R, \circ, e, -, \infty \rangle$ be a tuple with the same types as in Definition 2.1, and extend $-$ and $\circ$ to $\mathcal{P}(R)$ and $\mathcal{P}(R) \times \mathcal{P}(R)$ respectively as in that definition. Then $\langle R, \circ, e, -, \infty \rangle$ is a* CBI-*model iff the following hold for all $X, Y, Z \in \mathcal{P}(R)$:*

1. *$X \circ Y = Y \circ X$ and $X \circ (Y \circ Z) = (X \circ Y) \circ Z$ and $\{e\} \circ X = X$*
2. *$-X = X \mathrel{-\!\!\bullet} \infty$*
3. *$--X = X$*

where $X \mathrel{-\!\!\bullet} Y =_{def} \{z \in R \mid \exists x \in X, y \in Y.\, y \in x \circ z\}$.

Proof. ($\Rightarrow$) The required properties follow straightforwardly from the corresponding conditions on CBI-models and the extension of $-$ and $\circ$ to sets of elements.
($\Leftarrow$) The conditions required for $\langle R, \circ, e, -, \infty \rangle$ to be a CBI-model follow from taking X, Y, Z to be singleton sets in the given conditions and noting that $-\{x\} = -x$ and $\{x\} \circ \{y\} = x \circ y$ for any $x, y \in R$. □

The following two propositions extend analogous results in [8]. Note that Ψ_Γ denotes the BI^+-formula constructed from a bunch Γ by Definition 4.2.

Proposition 5.2.8. *$\Gamma \vdash F$ is derivable in* LBI^+ *iff $\Psi_\Gamma \Rightarrow F$ is derivable in* $\mathrm{LAX}_{\mathrm{BI}^+}$.

Proposition 5.2.9. *$\Gamma \vdash F$ is valid with respect to classical BI-models iff $\Psi_\Gamma \Rightarrow F$ is valid with respect to AX_{BI^+}-models.*

The specific properties of $-$ and ∞ given by the AX_{BI^+} axioms are consequences of Lemma 5.2.7.

Theorem 5.2.10 (Completeness of LBI^+)**.** LBI^+ *is complete with respect to validity in* CBI-*models.*

Proof. If $\Gamma \vdash F$ is valid with respect to CBI-models then, by Proposition 5.2.9 $\Psi_\Gamma \Rightarrow F$ is valid with respect to AX_{BI^+}-models and thus provable in LAX_{BI^+} by Corollary 5.2.6. By Proposition 5.2.8, $\Gamma \vdash F$ is then provable in LBI^+ as required. □

5.3 Admissibility embeddings between $\mathrm{DL}_{\mathrm{CBI}}$ and LBI^+

Definition 5.3.1 (Embedding of $\mathrm{DL}_{\mathrm{CBI}}$ in LBI^+)**.** We define a function $\ulcorner - \urcorner$ from $\mathrm{DL}_{\mathrm{CBI}}$-formulas to BI^+-formulas by recursion on the structure of $\mathrm{DL}_{\mathrm{CBI}}$-formulas, as follows:

$$\begin{array}{rcll}
\ulcorner F \urcorner & = & F & \text{where } F \in \{P, \top, \bot, \top^*\} \\
\ulcorner F_1 \mathbin{?} F_2 \urcorner & = & \ulcorner F_1 \urcorner \mathbin{?} \ulcorner F_2 \urcorner & \text{where } ? \in \{\wedge, \vee, \to, *, \mathrel{-\!\!*}\} \\
\ulcorner \neg F \urcorner & = & \neg \ulcorner F \urcorner & \\
\ulcorner \bot^* \urcorner & = & \neg \bowtie & \\
\ulcorner {\sim} F \urcorner & = & \neg - \ulcorner F \urcorner & \\
\ulcorner F_1 \overset{*}{\vee} F_2 \urcorner & = & \neg - (\neg - \ulcorner F_1 \urcorner * \neg - \ulcorner F_2 \urcorner) &
\end{array}$$

where P in the first clause ranges over $\mathcal{V}$. We extend $\ulcorner - \urcorner$ to a function from $\mathrm{DL}_{\mathrm{CBI}}$ consecutions to BI^+ sequents by:

$$\ulcorner X \vdash Y \urcorner = \ulcorner \Psi_X \urcorner \vdash \ulcorner \Upsilon_Y \urcorner$$

where Ψ_- and Υ_- are the functions given in Definition 4.2. We call the function $\ulcorner - \urcorner$ the *embedding of* $\mathrm{DL}_{\mathrm{CBI}}$ *in* LBI^+.

Lemma 5.3.2. *A consecution $X \vdash Y$ is valid iff $\ulcorner X \vdash Y \urcorner$ is valid.*

Proof. (Sketch) We first show by structural induction on CBI-formulas F that $r \models F$ iff $r \models \ulcorner F \urcorner$. The main interesting case is $F = F_1 \overset{*}{\vee} F_2$, in which case we need to use Lemma 5.1.1 in order to establish the required equivalence. This result can then be straightforwardly lifted to consecutions $X \vdash Y$. □

We write $F \dashv\vdash G$ to mean that both $F \vdash G$ and $G \vdash F$ are derivable (in $\mathrm{DL}_{\mathrm{CBI}}$ or LBI^+), and call $F \dashv\vdash G$ a *derivable equivalence* (of $\mathrm{DL}_{\mathrm{CBI}}$ and LBI^+ respectively).

Lemma 5.3.3. *The following are derivable equivalences of* LBI^+*:*

1. $\neg - \neg - F \dashv\vdash F$
2. $\neg - (F * \neg - G) \dashv\vdash F \mathrel{-\!\!*} G$
3. $F \mathrel{-\!\!*} G \dashv\vdash \neg - G \mathrel{-\!\!*} \neg - F$
4. $F \dashv\vdash \neg - (\neg - F * \neg - \neg \bowtie)$

The following lemma says that we can rewrite formulas in BI^+ sequents according to derivable equivalences without affecting LBI^+-derivability.

Lemma 5.3.4. *Write $F(G)$ for a formula F of which G is a distinguished subformula occurrence, and when $F(G)$ is understood write $F(G')$ for the formula obtained by replacing G by G' in F. (This is analogous to the notation for bunches.)*

Now suppose that $A \dashv\vdash B$ is a derivable equivalence of LBI^+ (where A, B are BI^+-formulas). Then the following two proof rules are derivable in LBI^+:

$$\dfrac{\Gamma(F(A)) \vdash C}{\Gamma(F(B)) \vdash C}\,(\dashv\vdash L) \qquad \dfrac{\Gamma \vdash F(A)}{\Gamma \vdash F(B)}\,(\dashv\vdash R)$$

Proof. By considering the following two instances of (Cut):

$$\dfrac{F(B) \vdash F(A) \quad \Gamma(F(A)) \vdash C}{\Gamma(F(B)) \vdash C}\,\text{(Cut)}$$

$$\dfrac{\Gamma \vdash F(A) \quad F(A) \vdash F(B)}{\Gamma \vdash F(B)}\,\text{(Cut)}$$

it suffices to prove that $F(A) \vdash F(B)$ is derivable in LBI^+, whence it follows by symmetry that $F(B) \vdash F(A)$ is also derivable. If $F(A) = A$ then this is immediate by assumption. Otherwise A is a (distinguished) strict subformula occurrence in F and we proceed by an easy structural induction on F. □

Proposition 5.3.5. *The proof rules of $\mathrm{DL}_{\mathrm{CBI}}$ are admissible in LBI^+ under the embedding $\ulcorner - \urcorner$. That is, for any instance of a $\mathrm{DL}_{\mathrm{CBI}}$ rule, say:*

$$\dfrac{\{X_i \vdash Y_i \mid 1 \le i \le j\}}{X \vdash Y}\, j \in \{0,1,2\}$$

if $\ulcorner X_i \vdash Y_i \urcorner$ is derivable for all $1 \le i \le j$ then so is $\ulcorner X \vdash Y \urcorner$.

Proof. (Sketch) We distinguish a case for each proof rule of $\mathrm{DL}_{\mathrm{CBI}}$. Most of the cases are straightforward. The main interesting cases are the logical rules ($\overset{*}{\vee}$L) and ($-\!\!*$L), the structural rule (MIR) and the display postulates for the multiplicative family. These can be derived in LBI^+ under the embedding $\ulcorner - \urcorner$ with the aid of the rewrite rules given by Lemma 5.3.4 in conjunction with the derivable equivalences of Lemma 5.3.3. E.g., in the case of ($-\!\!*$L) we proceed as follows, using the rule symbol (=) to denote rewriting a sequent according to the definitions of Ψ_{-}, Υ_{-} and/or $\ulcorner - \urcorner$ (cf. Definitions 4.2 and 5.3.1).:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\begin{array}{c}\vdots\\ \ulcorner X \vdash F \urcorner\end{array}}{\ulcorner \Psi_X \urcorner \vdash \ulcorner \Upsilon_F \urcorner}\,(=)}{\ulcorner \Psi_X \urcorner \vdash \ulcorner F \urcorner}\,(=) \quad \dfrac{\dfrac{\begin{array}{c}\vdots\\ \ulcorner G \vdash Y \urcorner\end{array}}{\ulcorner \Psi_G \urcorner \vdash \ulcorner \Upsilon_Y \urcorner}\,(=)}{\ulcorner G \urcorner \vdash \ulcorner \Upsilon_Y \urcorner}\,(=)}{\ulcorner F \urcorner -\!\!* \ulcorner G \urcorner, \ulcorner \Psi_X \urcorner \vdash \ulcorner \Upsilon_Y \urcorner}\,(-\!\!*\mathrm{L})}{\ulcorner F \urcorner -\!\!* \ulcorner G \urcorner \vdash \ulcorner \Psi_X \urcorner -\!\!* \ulcorner \Upsilon_Y \urcorner}\,(-\!\!*\mathrm{R})}{\ulcorner F \urcorner -\!\!* \ulcorner G \urcorner \vdash \neg-(\ulcorner \Psi_X \urcorner * \neg-\ulcorner \Upsilon_Y \urcorner)}\,(\dashv\vdash\mathrm{R})}{\ulcorner F \urcorner -\!\!* \ulcorner G \urcorner \vdash \neg-(\neg-\neg-\ulcorner \Psi_X \urcorner * \neg-\ulcorner \Upsilon_Y \urcorner)}\,(\dashv\vdash\mathrm{R})}{\ulcorner F \urcorner -\!\!* \ulcorner G \urcorner \vdash \ulcorner \sim\Psi_X \overset{*}{\vee} \Upsilon_Y \urcorner}\,(=)}{\ulcorner \Psi_{F -\!\!* G} \urcorner \vdash \ulcorner \Upsilon_{\flat X, Y} \urcorner}\,(=)}{\ulcorner F -\!\!* G \vdash \flat X, Y \urcorner}\,(=)$$

□

We can now prove the soundness of $\mathrm{DL}_{\mathrm{CBI}}$ as follows.

Proof of Theorem 4.10. If $X \vdash Y$ is provable in $\mathrm{DL}_{\mathrm{CBI}}$ then $\ulcorner X \vdash Y \urcorner$ is provable in LBI^+ by Proposition 5.3.5, and thus is valid by the soundness of LBI^+ (Proposition 5.1.3), whence $X \vdash Y$ is valid by Lemma 5.3.2.

Definition 5.3.6 (Embedding of LBI^+ in $\mathrm{DL}_{\mathrm{CBI}}$)**.** We define a function $\llcorner - \lrcorner$ from BI^+ sequents to $\mathrm{DL}_{\mathrm{CBI}}$ consecutions by: $\llcorner \Gamma \vdash F \lrcorner$ is the consecution obtained by replacing every occurrence of the formula $\bowtie$ in $\Gamma \vdash F$ by the formula $\neg\bot^*$.

We remark that $\llcorner - \lrcorner$ can be defined recursively over BI^+ formulas and extended to LBI^+ sequents in a manner similar to that in Definition 5.3.1.

Lemma 5.3.7. *The following are all derivable equivalences of $\mathrm{DL}_{\mathrm{CBI}}$:*

1. $\neg\neg F \dashv\vdash F$
2. $\neg F \dashv\vdash F \to \bot$
3. $\sim F \dashv\vdash F -\!\!* \bot^*$
4. $\neg\sim F \dashv\vdash \sim\neg F$
5. $F_1 \overset{*}{\vee} F_2 \dashv\vdash \sim(\sim F_1 * \sim F_2)$

Proposition 5.3.8. *The proof rules of LBI^+ are admissible in $\mathrm{DL}_{\mathrm{CBI}}$ under the embedding $\llcorner - \lrcorner$. That is, for any instance of an LBI^+ rule, say:*

$$\dfrac{\{\Gamma_i \vdash F_i \mid 1 \le i \le j\}}{\Gamma \vdash F}\, j \in \{0,1,2\}$$

if $\llcorner \Gamma_i \vdash F_i \lrcorner$ is derivable for all $1 \le i \le j$ then so is $\llcorner \Gamma \vdash F \lrcorner$.

Proof. (Sketch) We distinguish a case for each proof rule of LBI^+. The main interesting cases are the rules that operate inside bunches. We observe that $\llcorner \Gamma \lrcorner$ is a structure for any bunch Γ and that, in particular, $\llcorner \Delta \lrcorner$ is always an antecedent part of $\llcorner \Gamma \lrcorner(\llcorner \Delta \lrcorner)$. By the display theorem (Theorem 4.4) we can display the sub-bunch on which the rule operates as the entire antecedent of a display-equivalent consecution. We can then apply the corresponding rule of $\mathrm{DL}_{\mathrm{CBI}}$ to this antecedent and then simply invert the display postulate steps used to display the antecedent to restore the original context. For example, in the case of (→L) we proceed as follows, writing (D≡) to denote the use of a display equivalence:

$$\dfrac{\dfrac{\dfrac{\dfrac{\llcorner \Delta \lrcorner \vdash \llcorner F_1 \lrcorner \qquad \dfrac{\dfrac{\dfrac{\llcorner \Gamma \lrcorner(\llcorner \Delta \lrcorner; \llcorner F_2 \lrcorner) \vdash \llcorner F \lrcorner}{\llcorner \Delta \lrcorner; \llcorner F_2 \lrcorner \vdash X}\,(\mathrm{D}\equiv)}{\llcorner F_2 \lrcorner; \llcorner \Delta \lrcorner \vdash X}\,(\mathrm{ACL})}{\llcorner F_2 \lrcorner \vdash \sharp\llcorner \Delta \lrcorner; X}\,(\mathrm{D}\equiv)}{\llcorner F_1 \lrcorner \to \llcorner F_2 \lrcorner \vdash \sharp\llcorner \Delta \lrcorner; \sharp\llcorner \Delta \lrcorner; X}\,(\to\mathrm{L})}{\llcorner \Delta \lrcorner; \llcorner \Delta \lrcorner \vdash \sharp(\llcorner F_1 \lrcorner \to \llcorner F_2 \lrcorner); X}\,(\mathrm{D}\equiv)}{\llcorner \Delta \lrcorner \vdash \sharp(\llcorner F_1 \lrcorner \to \llcorner F_2 \lrcorner); X}\,(\mathrm{CtrL})}{\dfrac{\llcorner \Delta \lrcorner; \llcorner F_1 \lrcorner \to \llcorner F_2 \lrcorner \vdash X}{\llcorner \Gamma \lrcorner(\llcorner \Delta \lrcorner; \llcorner F_1 \lrcorner \to \llcorner F_2 \lrcorner) \vdash \llcorner F \lrcorner}\,(\mathrm{D}\equiv)}\,(\mathrm{D}\equiv)$$

where X is a placeholder for the structure that results as the consequent from displaying Y in the consecution $\llcorner \Gamma \lrcorner(Y) \vdash \llcorner F \lrcorner$. □

Lemma 5.3.9. *If $\llcorner \ulcorner X \vdash Y \urcorner \lrcorner$ is $\mathrm{DL}_{\mathrm{CBI}}$-provable then so is $X \vdash Y$.*

Proof. (Sketch) The proof proceeds in three stages. First, we show by induction on CBI-formulas F that $F \dashv\vdash \llcorner \ulcorner F \urcorner \lrcorner$ is $\mathrm{DL}_{\mathrm{CBI}}$-provable, making use of the derivable equivalences given by Lemma 5.3.7 in the non-trivial cases. Second, we show by induction on $\mathrm{DL}_{\mathrm{CBI}}$-structures X that $X \vdash \Psi_X$ and $\Upsilon_X \vdash X$ are

$\mathrm{DL}_{\mathrm{CBI}}$-provable. Finally, we can construct a proof of $X \vdash Y$ using the given proof of $\llcorner\!\ulcorner X \vdash Y \urcorner\!\lrcorner = \llcorner\!\ulcorner \Psi_X \urcorner\!\lrcorner \vdash \llcorner\!\ulcorner \Upsilon_Y \urcorner\!\lrcorner$ using the first two stages together with (Cut):

$$\dfrac{\begin{array}{c}\text{(assumption)}\\ \vdots \\ \llcorner\!\ulcorner \Psi_X \urcorner\!\lrcorner \vdash \llcorner\!\ulcorner \Upsilon_Y \urcorner\!\lrcorner\end{array} \qquad \dfrac{\begin{array}{c}\text{(Stage 1)}\\ \vdots \\ \llcorner\!\ulcorner \Upsilon_Y \urcorner\!\lrcorner \vdash \Upsilon_Y\end{array} \quad \begin{array}{c}\text{(Stage 2)}\\ \vdots \\ \Upsilon_Y \vdash Y\end{array}}{\llcorner\!\ulcorner \Upsilon_Y \urcorner\!\lrcorner \vdash Y}\,\text{(Cut)}}{\begin{array}{c}\llcorner\!\ulcorner \Psi_X \urcorner\!\lrcorner \vdash Y \\ \vdots \\ \text{(contd. below)}\end{array}}\,\text{(Cut)}$$

$$\dfrac{\dfrac{\begin{array}{c}\text{(Stage 2)}\\ \vdots \\ X \vdash \Psi_X\end{array} \quad \begin{array}{c}\text{(Stage 1)}\\ \vdots \\ \Psi_X \vdash \llcorner\!\ulcorner \Psi_X \urcorner\!\lrcorner\end{array}}{X \vdash \llcorner\!\ulcorner \Psi_X \urcorner\!\lrcorner}\,\text{(Cut)} \qquad \begin{array}{c}\text{(contd. above)}\\ \vdots \\ \llcorner\!\ulcorner \Psi_X \urcorner\!\lrcorner \vdash Y\end{array}}{X \vdash Y}\,\text{(Cut)}$$

which completes the proof. □

We can now prove completeness for $\mathrm{DL}_{\mathrm{CBI}}$ as follows.

Proof of Theorem 4.11. If $X \vdash Y$ is valid then so is $\ulcorner X \vdash Y \urcorner$ by Lemma 5.3.2, which is then LBI^+-provable by Theorem 5.2.10. By Proposition 5.3.8, $\llcorner\!\ulcorner X \vdash Y \urcorner\!\lrcorner$ is then provable in $\mathrm{DL}_{\mathrm{CBI}}$, whence $X \vdash Y$ is also $\mathrm{DL}_{\mathrm{CBI}}$-provable by Lemma 5.3.9.

6. Related and future work

We consider related work, and directions for future work, from several perspectives.

Classical versions of* BI*: CBI as presented here is essentially a new logic, obtained as a nonconservative extension of BBI. However, a version of classical BI was previously proposed by Pym, who gave two-sided sequent calculus proof rules for the logic and discussed some of the obstacles to its further development — principally, the formulation of a suitable forcing semantics and cut-eliminating proof systems [26]. Pym also made the observation that a relevantist approach to multiplicative negation, which essentially is also our approach, is compatible with the other multiplicative connectives. However, the multiplicative falsity $\bot^*$ is absent in this treatment. Our models, with their crucial inclusion of the element ∞ and its relationship to the involution '$-$', provide precisely the structure necessary to interpret all the connectives (as evidenced by our soundness and completeness results).

Display calculi: Our display calculus $\mathrm{DL}_{\mathrm{CBI}}$ is an instance of Belnap's general display logic [1] and is in the same vein as display calculi by Goré for other substructural logics and relational algebras [19, 20]. In particular, cut-elimination for $\mathrm{DL}_{\mathrm{CBI}}$ is a consequence of Belnap's general cut-elimination theorem for display logic. Our main technical contribution is the soundness and completeness of $\mathrm{DL}_{\mathrm{CBI}}$ with respect to validity in our CBI-models. Moreover, the proofs of these theorems, which rely upon admissibility embeddings, make an explicit connection between proof in $\mathrm{DL}_{\mathrm{CBI}}$ and the intuitionistic style of proof in LBI^+, which is just the usual BI sequent calculus extended by three axioms. It should be noted, however, that even though cut-elimination in $\mathrm{DL}_{\mathrm{CBI}}$ entails a subformula property, proof search in this setting is nevertheless made daunting by the presence of the display postulates and structural rules, which can obviously lead to divergence if applied blindly. It thus remains of clear interest to formulate well-behaved sequent calculus or natural deduction proof systems for CBI, or to refine our display calculus further so as to eliminate structural inferences.

Classical linear logic: Readers may wonder about the relationship between CBI and classical linear logic (CLL), which also features a full set of propositional multiplicative connectives, and is a nonconservative extension of intuitionistic linear logic (ILL) [30]. The differences between the two are quite striking when comparing our money model of CBI (Example 3.1) with Girard's corresponding Marlboro / Camel example [18]. In particular, formulas in our model, including those involving multiplicative negation, are read as declarative statements about resources (i.e. money), whereas linear logic formulas in Girard's model are typically read as procedural statements about actions. Compared to CLL, CBI has the advantage of a simple, declarative notion of truth relative to resource, but this advantage appears to come at the expense of CLL's constructive interpretation of proofs.

Of course, the typical reading of BI departs from that of ILL in a similar way, and indeed it seems that the main differences between CBI and CLL are inherited from the differences between BI and ILL (see [24] for discussions of the latter). These differences are not merely conceptual, but are also manifested at the technical level of logical consequence. For example, $P \multimap Q \vdash P \to Q$ is a theorem of linear logic for any propositions P and Q, via the encoding of additive implication $P \to Q$ as $!P \multimap Q$, but $P \mathrel{-\!\!*} Q \vdash P \to Q$ is not a theorem of (any version of) BI. Similarly, distributivity of additive conjunction over additive disjunction holds in all versions of BI, but fails in linear logics. Finally, of course, there is only one negation in CLL, whereas there are two in CBI.

Interestingly, however, there is an intersection between our CBI-models and the CLL-models obtained from the *phase semantics* of classical linear logic [18]. A CBI-model $\langle R, \circ, e, -, \infty \rangle$ in which the monoid operation $\circ$ is a total function, rather than a relation, is a special instance of a phase space, used to provide a phase model of CLL. This can be seen by taking the linear logic "perp" $\bot$ to be the set $R \setminus \{\infty\}$, whence the linear negation $X^\bot$ on sets $X \subseteq R$ becomes $-X$. In the linear logic terminology, every subset X of R is then a "fact" in the sense that $(X^\bot)^\bot = --X = X$. It seems somewhat curious that there is a subclass of models where CBI and CLL agree, since known interesting phase models of linear logic are relatively few whereas there appear to be many interesting CBI-models (cf. Section 3). However, one can argue that this subclass is faithful to the spirit of neither logic. On the one hand, the restriction to a total monoid operation in CBI-models rules out many natural examples where resource combination is partial. On the other hand, it seems certain that the induced subclass of CLL phase models will be at odds with the coherence semantics of CLL proofs.

Application to program analysis: The main application of BBI so far has been the use of separation logic in program analysis. There are now several program analysis tools [9, 10, 13, 21, 23] which use logical and semantic properties of the heap model of BBI at their core. These tools often define a suitable fragment of separation logic with convenient algebraic properties, and use it in custom lightweight theorem provers and abstract domains. We suggest that our work on CBI could be taken up in two main directions. The first direction is theorem proving. Our display calculus $\mathrm{DL}_{\mathrm{CBI}}$ might form a basis for the design of new theorem provers, which could easily employ the powerful (and historically difficult to use) implication $\mathrel{-\!\!*}$ since, in CBI, it can be reexpressed using more primitive connectives. Moreover, the notion of negative resource might be employed in extended theorem proving questions, such as the frame inference problem $F \vdash G * X$ where the frame X is computed essentially by subtracting G from F. A similar problem is the bi-abduction question, which forms the basis of the compositional shape analysis in [7] and has the form $F * X \vdash G * Y$, interpreted as an obligation to find formulae to instantiate X and Y such that the implication holds. This question arises at program procedure call sites, where F is the procedure's precondition, G is the current precondition at the call point, X is the resource missing, and Y is the leftover resource. We speculate that such inferences could be explained in terms of an ordinary proof theory, providing that multiplicative negation is supported, as in CBI.

The second direction is the investigation of richer fragments and properties. The richer algebraic properties of CBI models might suggest new separation logic fragments, or new ways of manipulating the existing fragments. For example, in order to express invariants of traversal algorithms one needs to generalize a data structure predicate, such as *list(x)* for a 0-terminated linked list, to $lseg(x, y)$ for list segments from x to y. The latter can be obtained from *list(x)* by subtracting *list(y)*. It is conceivable that the notion of subtraction could be employed to convert automatically predicates describing whole data structures into predicates which describe partial data structures. Finally, new fragments could be obtained by studying appropriate generalizations of conjunctive and disjunctive normal forms to include both additive and multiplicative connectives.

CBI is presently very new, and our suggestions regarding its applications are necessarily somewhat speculative. However, the "dualising resource" semantics of CBI developed in this paper has already given rise to several example models which, though relatively simple in their present form, are suggestive of the applicability of CBI to more complex domains. For example, the money model presented in Section 3 extends easily to a CBI-model of portfolios of assets, which might potentially form the basis of a Hoare logic for financial transactions in the same way that the heap model of BBI underpins separation logic. Furthermore, our proof-theoretic results provide some hope that proof search in the logic can be tamed, thus opening the way for theorem proving tools based upon CBI. We hope that this paper represents a first step in these directions.

Acknowledgements

We extend special thanks to Peter O'Hearn and David Pym for many interesting and enlightening discussions which informed the present paper. We also thank Byron Cook, Ross Duncan, Philippa Gardner, Alex Simpson, and the members of the East London Massive for useful discussions and feedback.

References

[1] Nuel D. Belnap, Jr. Display logic. *Journal of Philosophical Logic*, 11:375–417, 1982.

[2] Josh Berdine and Peter O'Hearn. Strong update, disposal and encapsulation in bunched typing. In *Proceedings of MFPS*, ENTCS. Elsevier, 2006.

[3] Patrick Blackburn, Maarten de Rijke, and Yde Venema. *Modal Logic*. Cambridge University Press, 2001.

[4] R. Bornat, C. Calcagno, P. O'Hearn, and M. Parkinson. Permission accounting in separation logic. In *32nd POPL*, pp59–70, 2005.

[5] James Brotherston and Cristiano Calcagno. Algebraic models and complete proof calculi for classical BI. Technical Report 2008/7, Imperial College London, 2008. Available from `http://www.doc.ic.ac.uk/~jbrother`.

[6] James Brotherston and Cristiano Calcagno. Classical logic of bunched implications. In the informal proceedings of CL&C 2008, an ICALP satellite workshop; available from `http://www.doc.ic.ac.uk/~jbrother`, 2008.

[7] Cristiano Calcagno, Dino Distefano, Peter O'Hearn and Hongseok Yang. Compositional Shape Analysis by means of BI-Abduction. In *Proceedings of POPL-36*, 2009.

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

[9] Cristiano Calcagno, Matthew Parkinson, and Viktor Vafeiadis. Modular safety checking for fine-grained concurrency. In *SAS*, 2007.

[10] Bor-Yuh Evan Chang and Xavier Rival. Relational inductive shape analysis. In *Proceedings of POPL-35*, 2008.

[11] Wei-Ngan Chin, Cristina David, Huu Hai Nguyen, and Shengchao Qin. Enhancing modular OO verification with separation logic. In *Proceedings of POPL-35*, 2008.

[12] Matthew Collinson, David Pym, and Edmund Robinson. Bunched polymorphism. *Mathematical Structures in Computer Science*, 2009. To appear.

[13] D. Distefano and M. Parkinson. jStar: Towards Practical Verification for Java. In *OOPSLA*, 2008.

[14] Kevin Donnelly, Tyler Gibson, Neel Krishnaswami, Stephen Magill, and Sungwoo Park. The inverse method for the logic of bunched implications. In *Proceedings of LPAR 2004*, volume 3452 of *LNAI*, pages 466–480. Springer-Verlag, 2005.

[15] Michael Dunn. Star and perp: Two treatments of negation. *Philosophical Perspectives*, 7:331–357, 1993.

[16] D. Galmiche, D. Mery, and D. Pym. The semantics of BI and resource tableaux. *Mathematical Structures in Computer Science*, 15:1033–1088, 2005.

[17] Didier Galmiche and Dominique Larchey-Wendling. Expressivity properties of Boolean BI through relational models. In *Proceedings of FSTTCS*, 2006.

[18] Jean-Yves Girard. Linear logic: Its syntax and semantics. In J.-Y. Girard, Y. Lafont, and L. Regnier, editors, *Advances in Linear Logic*, pages 1–42. Cambridge University Press, 1995.

[19] Rajeev Goré. Cut-free display calculi for relation algebras. In *Proceedings of CSL'96*, volume 1258 of *LNCS*, pages 198–210, 1997.

[20] Rajeev Goré. Substructural logics on display. *Logic Journal of the IGPL*, 6(3):451–504, 1998.

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

[22] Samin Ishtiaq and Peter W. O'Hearn. BI as an assertion language for mutable data structures. In *Proceedings of POPL'01*, January 2001.

[23] H.H. Nguyen and W.-N. Chin. Enhancing program verification with lemmas. In *Proceedings of CAV*, 2008.

[24] P.W. O'Hearn and D. J. Pym. The logic of bunched implications. *Bulletin of Symbolic Logic*, 5(2):215–244, June 1999.

[25] Matthew Parkinson and Gavin Bierman. Separation logic, abstraction and inheritance. In *Proceedings of POPL-35*, 2008.

[26] David Pym. *The Semantics and Proof Theory of the Logic of Bunched Implications*. Applied Logic Series. Kluwer, 2002. Errata and remarks (Pym 2004) maintained at `http://www.cs.bath.ac.uk/~pym/reductive-logic-errata.html`.

[27] David Pym, Peter O'Hearn, and Hongseok Yang. Possible worlds and resources: The semantics of BI. *Theoretical Computer Science*, 315(1):257–305, 2004.

[28] S. Read. *Relevant Logic: A Philosophical Examination*. Basil Blackwell, 1987.

[29] John C. Reynolds. Separation logic: A logic for shared mutable data structures. In *Proceedings of 17th LICS*, 2002.

[30] Harold Schellinx. Some syntactical observations on linear logic. *Journal of Logic and Computation*, 1(4):537–559, 1991.