

CLASSICAL BI: ITS SEMANTICS AND PROOF THEORY

JAMES BROTHERSTON AND CRISTIANO CALCAGNO

Dept. of Computing, Imperial College London, UK
e-mail address: J.Brotherston@imperial.ac.uk

Dept. of Computing, Imperial College London, UK
e-mail address: ccris@doc.ic.ac.uk

ABSTRACT. We present Classical BI (CBI), a new addition to the family of bunched logics which originate in O’Hearn and Pym’s logic of bunched implications BI. CBI differs from existing bunched logics in that its multiplicative connectives behave classically rather than intuitionistically (including in particular a multiplicative version of classical negation). At the semantic level, CBI-formulas have the normal bunched logic reading as declarative statements about resources, but its resource models necessarily feature more structure than those for other bunched logics; principally, they satisfy the requirement that every resource has a unique dual. At the proof-theoretic level, a very natural formalism for CBI is provided by a display calculus *à la* Belnap, which can be seen as a generalisation of the bunched sequent calculus used for BI. In this paper we formulate the aforementioned model theory and proof theory for CBI, and prove some fundamental results about the logic, most notably completeness of the proof theory with respect to the semantics.

1. INTRODUCTION

Substructural logics, whose best-known varieties include linear logic, relevant logic and the Lambek calculus, are characterised by their restriction of the use of the so-called *structural* proof principles of classical logic [35]. These may be roughly characterised as those principles that are insensitive to the syntactic form of formulas, chiefly weakening (from premises A, B conclude A) and contraction (from premise A conclude A, A). For example, in linear logic, only formulas prefixed with a special “exponential” modality are subject to weakening and contraction, while in relevant logic it is usual for contraction but not weakening to be permitted.

A relatively new area of substructural logic, and one which has been receiving increasing attention amongst the logical and computer science research communities in recent years, is that of *bunched logic*. In bunched logic, the restriction on the use of structural proof principles is achieved by allowing the connectives of a standard “additive” propositional

1998 ACM Subject Classification: F.4.1 [Mathematical Logic and Formal Languages]: Mathematical Logic – model theory, proof theory, computational logic.

Key words and phrases: Classical BI, bunched logic, resource models, display logic, completeness.

Research supported by EPSRC grant EP/E002536/1 and an EPSRC postdoctoral fellowship.

Research supported by an EPSRC Advanced Fellowship.

logic, which admits weakening and contraction, to be freely combined with those of a second “multiplicative” propositional logic, which does not. Proof systems for bunched logic therefore employ two different operations for the meta-level combination of premises (akin to the comma in standard sequent calculus), one corresponding to each constituent logic. The arbitrary nesting of these operations gives rise to tree-like structures of premises called “bunches”, from which bunched logic derives its name. In contrast to linear logic, whose restricted treatment of additive connectives facilitates a natural constructive reading of proofs as computations [1], the unrestricted nature of the additives in bunched logic gives rise to a simple Tarski-style algebraic semantics in which formulas can be understood as declarative statements about *resource* [32]. This resource reading of the logic has found substantial application in computer science, most notably in the shape of *separation logic*, which is a Hoare logic based upon a bunched logic model of heap memory [36].

Although the main ideas necessary to develop bunched logic can retrospectively be seen to have been present in earlier work by others, it first emerged fairly recently with the introduction of BI, O’Hearn and Pym’s *logic of bunched implications* [28]. Semantically, BI can be seen to arise by considering the structure of cartesian doubly closed categories (i.e. categories with one cartesian closed structure and one symmetric monoidal closed structure) [31]. Concretely, such categories correspond to a combination of standard intuitionistic logic with multiplicative intuitionistic linear logic¹ (MILL), and thus one has the following propositional connectives² for BI:

$$\begin{array}{l} \text{Additive:} \quad \top \quad \perp \quad \neg \quad \wedge \quad \vee \quad \rightarrow \\ \text{Multiplicative:} \quad \top^* \quad \quad \quad * \quad \quad \quad -^* \end{array}$$

(where \neg is the intuitionistic negation defined by $\neg F = F \rightarrow \perp$). As well as the semantics based on the aforementioned categories, BI can be given an algebraic semantics: one simply requires that algebraic BI-models have both the Heyting algebra structure required to interpret intuitionistic logic, and the residuated commutative monoid structure required to interpret MILL. By requiring a Boolean algebra instead of the Heyting algebra in BI-models, one obtains the variant logic Boolean BI (BBI), which can be seen as a combination of classical logic and MILL [32, 31]. Most of the computer science applications of bunched logic, are in fact based on BBI rather than BI; for example, the heap model used in separation logic is a model of BBI [24].

A natural question from a logician’s standpoint is whether bunched logics exist in which the multiplicative connectives behave classically, rather than intuitionistically (and do not simply collapse into their additive equivalents). A computer scientist might also enquire whether such a logic could, like its siblings, be understood semantically in terms of resource. In this paper, we address these questions by presenting a new addition to the bunched logic family, which we call *Classical BI* (CBI), and whose additives and multiplicatives both behave classically. In particular, CBI features multiplicative analogues of the additive falsity, negation, and disjunction, which are absent in the other bunched logics. Thus CBI can be seen as a combination of classical logic and multiplicative classical linear logic (MLL). We examine CBI both from the model-theoretic and the proof-theoretic perspective, each of which we describe below.

¹We refer here to linear logic without the exponentials.

² \top^* , which is the unit of $*$, is often elsewhere written I .

Model-theoretic perspective: From the point of view of computer science, the main interest of bunched logic stems from its algebraic semantics based on relational commutative monoids, which can be understood as an abstract representation of resource [19, 20]. In such models, formulas of bunched logic 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 those resources which divide, via the monoid operation, into two component resources satisfying respectively F and G . The multiplicative implication \multimap then comes along naturally as the right-adjoint of the multiplicative conjunction $*$, so that $F \multimap G$ denotes those resources which satisfy G when combined with a resource satisfying F .

The difference between intuitionistic and classical logics can be seen as a matter of the differing strengths of their respective negations [30]. From this viewpoint the main obstacle to formulating a bunched logic like CBI is in giving a convincing account of classical multiplicative negation; multiplicative falsity can then be obtained as the negation of \top^* and multiplicative disjunction as the de Morgan dual of $*$. We show that multiplicative negation can be given a declarative resource reading just as for the usual bunched logic connectives, provided that we enrich the relational commutative monoid structure of BBI-models with an involutive operator (which interacts with the binary monoid operation in a suitable fashion). Thus every resource in a CBI-model is required to 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. Our interpretation of multiplicative negation \sim is then in the tradition of Routley’s interpretation of negation in relevant logic [37, 18]: a resource satisfies $\sim F$ iff its dual fails to satisfy F . This interpretation, which at first sight may seem unusual, is justified by the desired semantic equivalences between formulas. For example, under our interpretation $F \multimap G$ is semantically equivalent to $\sim F \multimap G$, where \multimap denotes the multiplicative disjunction.

In Section 2 we state the conditions on BBI-models qualifying them as CBI-models and examine some fundamental properties of these models. We then give the forcing semantics for CBI-formulas with respect to our models, and compare the resulting notion of validity with that for BBI. The most notable result is that CBI is a non-conservative extension of BBI, which indicates that CBI is intrinsically different in character to its bunched logic siblings, and justifies independent consideration.

Proof-theoretic perspective: The proof theory of BI (cf. [31, 28]) can be motivated by the observation that the presence of two implications \rightarrow and \multimap should give rise to two context-forming operations, which correspond to the conjunctions \wedge and $*$ at the meta-level. This situation is illustrated by the following (intuitionistic) sequent calculus right-introduction rules for the implications:

$$\frac{\Gamma; F_1 \vdash F_2}{\Gamma \vdash F_1 \rightarrow F_2} (\rightarrow R) \qquad \frac{\Gamma, F_1 \vdash F_2}{\Gamma \vdash F_1 \multimap F_2} (\multimap R)$$

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 semicolons or commas, denoting respectively additive and multiplicative combinations of assumptions. The crucial difference between the two operations is that weakening and contraction are possible for the additive semicolon but not for the multiplicative comma. Since BI is an intuitionistic logic (in both its additive and multiplicative components), bunches arise only on the left-hand side of sequents, with

a single formula on the right. In order to take into account the bunched contexts in BI sequents, the left-introduction rules for logical connectives are then formulated so as to apply at arbitrary positions within a bunch³. E.g., the left-introduction rules for the two implications are:

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

where $\Gamma(\Delta)$ denotes a bunch Γ with a distinguished sub-bunch occurrence Δ . In contrast, the right-introduction rules need take into account only the top level of bunches, as in the right-introduction rules above for the implications.

For a classical bunched logic like CBI, it would appear natural from a proof-theoretic perspective to consider a full two-sided sequent calculus in which semicolon and comma in bunches on the right of sequents correspond to the two disjunctions at the meta-level. Unfortunately, it is far from clear how to formulate such a sequent calculus that admits cut-elimination, or a similar natural deduction system satisfying normalisation⁴. The main problem lies in formulating suitable “bunched” rules for the logical connectives in the two-sided formalism, owing to the failure of various distribution properties in the logic (see [7, 31] for some discussion of the difficulties).

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, DL_{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 [2]. 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 DL_{CBI} is sound and complete with respect to our algebraic semantics for CBI. Soundness follows by showing directly that each of the proof rules preserves validity with respect to our models. The proof of completeness, which is presented in Section 5, is by reduction to a completeness result for modal logic due to Sahlqvist.

Applications: Bunched logic (especially BBI) and its resource semantics has found application in several areas of computer science, including polymorphic abstraction [15], type systems for reference update and disposal [3], context logic for tree update [11] and, most ubiquitously, separation logic [36] which forms the basis of many contemporary approaches to reasoning about pointer programs (recent examples include [29, 14, 13]).

Unfortunately, the fact that CBI is a non-conservative extension of BBI 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 can reasonably be expected to have different applications to those of other bunched logics. In Section 3 we consider a range of example CBI-models drawn from

³In this respect, the BI sequent calculus resembles calculi for *deep inference* [9]. However, deep inference calculi differ substantially from the BI calculus in that they also abandon the distinction between logical connectives and the meta-level structural connectives.

⁴To our knowledge, there are no existing such calculi even for BBI. However, our proof theory for CBI has been adapted to BBI by the first author [6].

quite disparate areas of mathematics and computer science, including bit arithmetic, regular languages, money, generalised heaps and fractional permissions. In Section 6 we suggest some directions for future applications of CBI, and discuss some related work.

This paper is a revised and expanded version of [8], including several new results. We have endeavoured to include detailed proofs where space permits.

2. SYNTAX AND ALGEBRAIC SEMANTICS OF CBI

In this section we define CBI, a fully classical bunched logic featuring additive and multiplicative versions of all the usual propositional connectives (cf. [31]). 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 [20, 11]. In fact, they are special cases of these monoids, containing extra structure: an involution operation ‘ $-$ ’ on elements and a distinguished element ∞ that characterises the result of combining an element with its involutive dual. In particular, the Abelian groups form a subclass of our models.

We first recall the standard models of BBI, and then give the extra conditions required for such models to also be models of CBI. Note that we write $\mathcal{P}(X)$ for the powerset of a set X .

Definition 2.1 (BBI-model). A BBI-*model* is a relational commutative monoid, i.e. a tuple $\langle R, \circ, e \rangle$, where $e \in R$ and $\circ : R \times R \rightarrow \mathcal{P}(R)$ are such that \circ is commutative and associative, with $r \circ e = \{r\}$ for all $r \in R$. Associativity of \circ is understood with respect to its pointwise extension to $\mathcal{P}(R) \times \mathcal{P}(R) \rightarrow \mathcal{P}(R)$, given by $X \circ Y =_{\text{def}} \bigcup_{x \in X, y \in Y} x \circ y$.

Of course, we could equally well represent \circ in a BBI-model as a true relation, i.e. a subset of $R \times R \times R$, rather than a function. However, the functional notation is perhaps the more natural one under a resource reading of BBI-models, in which \circ is understood as a (possibly non-deterministic) way of combining resources.

Definition 2.2 (CBI-model). A CBI-*model* is given by a tuple $\langle R, \circ, e, -, \infty \rangle$, where $\langle R, \circ, e \rangle$ is a BBI-model and $- : R \rightarrow R$ and $\infty \in R$ satisfy: $-x$ is the unique $y \in R$ such that $\infty \in x \circ y$. We extend $-$ pointwise to $\mathcal{P}(R) \rightarrow \mathcal{P}(R)$ by $-X =_{\text{def}} \bigcup_{x \in X} -x$.

We remark that, in our original definition of CBI-models [8], both ∞ and $-x$ for $x \in R$ were defined as subsets of R , rather than elements of R . However, under such circumstances both $-x$ and ∞ are forced to be singleton sets by the other conditions on CBI-models. Thus there is no loss of generality in requiring $-x$ and ∞ to be elements of R .

Proposition 2.3. If $\langle R, \circ, e, -, \infty \rangle$ is a CBI-model then:

- (1) $\forall x \in R. --x = x$;
- (2) $-e = \infty$;
- (3) $\forall X \subseteq R. R \setminus (-X) = -(R \setminus X)$;
- (4) $\forall x, y, z \in R. z \in x \circ y$ iff $-x \in y \circ -z$ iff $-y \in x \circ -z$.

Proof.

- (1) By definition of CBI-models, and using commutativity of \circ , we have $\infty \in -x \circ x$. However, again by definition, $--x$ is the unique $y \in R$ such that $\infty \in -x \circ y$. Thus we must have $--x = x$.

- (2) We have that $-e$ is the unique $y \in R$ such that $\infty \in e \circ y$. Since $\infty \in \{\infty\} = e \circ \infty$ by definition, we have $-e = \infty$.
- (3) (\subseteq) Suppose $x \in R \setminus -X$, i.e. $x \notin -X = \bigcup_{y \in X} -y$, so $x \neq -y$ for any $y \in X$. Then, since $x = --x$ by part 1, we must have $-x \notin X$, 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. $x = -y$ for some $y \notin X$. Note that we cannot have $x = -z$ for any $z \in X$, otherwise we have $-y = -z$ and thus $--y = --z$, so $y = z$ by part 1, which is a contradiction. Thus $x \notin \bigcup_{z \in X} -z = -X$, i.e. $x \in R \setminus -X$ as required.
- (4) We prove that the two bi-implications hold by showing three implications. Suppose first that $z \in x \circ y$. Using associativity of \circ , we have:

$$\infty \in z \circ -z \subseteq (x \circ y) \circ -z = x \circ (y \circ -z)$$

Since $-x$ is the unique $w \in R$ such that $\infty \in x \circ w$, we must have $-x \in y \circ -z$.

For the second implication, suppose that $-x \in y \circ -z$. By the first implication and part 1 above and commutativity of \circ , we then have as required:

$$-y \in -z \circ --x = --x \circ -z = x \circ -z$$

Finally, for the third implication, suppose that $-y \in x \circ -z$. Using the first and second implications together we obtain $--z \in y \circ --x$, i.e. $z \in x \circ y$ as required. This completes the proof. \square

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 $R \times R \rightarrow R$ in the obvious way.

Proposition 2.4. $\langle R, \circ, e, - \rangle$ is an Abelian group if and only if $\langle R, \circ, e, -, \infty \rangle$ is a CBI-model such that $\infty = e$ and \circ is a partial function.

Proof. (\Leftarrow) Let $\langle R, \circ, e, - \rangle$ be an Abelian group. We trivially have \circ a partial function since it is already a total function. To see that $\langle R, \circ, e \rangle$ is a BBI-model, we just note that \circ is associative and commutative and that e is the unit of \circ by the group axioms. By the uniqueness of group inverses, we then have that $-x$ is the unique y such that $e = \infty \in x \circ y$. Thus $\langle R, \circ, e, -, e \rangle$ is a CBI-model, as required.

(\Rightarrow) Let $\langle R, \circ, e, -, \infty \rangle$ be a CBI-model with $\infty = e$ and \circ a partial function. First note that, by the latter two facts, we have $-x \circ x = \infty = e$ for all $x \in R$. Now for any $x, y \in R$ we 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. Thus \circ is in fact a total function.

To see that $\langle R, \circ, e, - \rangle$ is an Abelian group, we first observe that, since \circ is a total function by the above, $\langle R, \circ, e \rangle$ is a total commutative monoid by the conditions imposed on BBI-models. The uniqueness of group inverses then follows immediately from the CBI-model conditions and the fact that $\infty = e$. \square

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:

$$F ::= P \mid \top \mid \perp \mid \neg F \mid F \wedge F \mid F \vee F \mid F \rightarrow F \mid \\ \top^* \mid \perp^* \mid \sim F \mid F * F \mid F \check{*} F \mid F -* F$$

where P ranges over \mathcal{V} . We treat the negations \neg and \sim as having greater precedence than the other connectives, and use parentheses to disambiguate where necessary. As usual, we write $F \leftrightarrow G$ as an abbreviation for $(F \rightarrow G) \wedge (G \rightarrow F)$.

We remark that the connectives of CBI-formulas are the standard connectives of BBI-formulas, plus a multiplicative falsity \perp^* , negation \sim and disjunction $\check{\vee}$. In order to define the interpretation of our formulas in a given model, we need as usual environments which interpret the propositional variables, and a satisfaction or “forcing” relation which interprets formulas as true or false relative to model elements in a given environment.

Definition 2.6 (Environment). An *environment* for either a CBI-model $\langle R, \circ, e, -, \infty \rangle$ or a BBI-model $\langle R, \circ, e \rangle$ is a function $\rho : \mathcal{V} \rightarrow \mathcal{P}(R)$ interpreting propositional variables as subsets of R . An environment for a model M will sometimes be called an *M-environment*.

Definition 2.7 (CBI satisfaction relation). Let $M = \langle R, \circ, e, -, \infty \rangle$ be a CBI-model. *Satisfaction* of a CBI-formula F by an M -environment ρ and an element $r \in R$ is denoted $r \models_{\rho} F$ and defined by structural induction on F as follows:

$$\begin{aligned}
 r \models_{\rho} P &\Leftrightarrow r \in \rho(P) \\
 r \models_{\rho} \top &\Leftrightarrow \text{always} \\
 r \models_{\rho} \perp &\Leftrightarrow \text{never} \\
 r \models_{\rho} \neg F &\Leftrightarrow r \not\models_{\rho} F \\
 r \models_{\rho} F_1 \wedge F_2 &\Leftrightarrow r \models_{\rho} F_1 \text{ and } r \models_{\rho} F_2 \\
 r \models_{\rho} F_1 \vee F_2 &\Leftrightarrow r \models_{\rho} F_1 \text{ or } r \models_{\rho} F_2 \\
 r \models_{\rho} F_1 \rightarrow F_2 &\Leftrightarrow r \models_{\rho} F_1 \text{ implies } r \models_{\rho} F_2 \\
 r \models_{\rho} \top^* &\Leftrightarrow r = e \\
 r \models_{\rho} \perp^* &\Leftrightarrow r \neq \infty \\
 r \models_{\rho} \sim F &\Leftrightarrow -r \not\models_{\rho} F \\
 r \models_{\rho} F_1 * F_2 &\Leftrightarrow \exists r_1, r_2 \in R. r \in r_1 \circ r_2 \text{ and } r_1 \models_{\rho} F_1 \text{ and } r_2 \models_{\rho} F_2 \\
 r \models_{\rho} F_1 \check{\vee} F_2 &\Leftrightarrow \forall r_1, r_2 \in R. -r \in r_1 \circ r_2 \text{ implies } -r_1 \models_{\rho} F_1 \text{ or } -r_2 \models_{\rho} F_2 \\
 r \models_{\rho} F_1 -* F_2 &\Leftrightarrow \forall r', r'' \in R. r'' \in r \circ r' \text{ and } r' \models_{\rho} F_1 \text{ implies } r'' \models_{\rho} F_2
 \end{aligned}$$

We remark that the above satisfaction relation for CBI is just an extension of the standard satisfaction relation for BBI with the clauses for \perp^* , \sim and $\check{\vee}$. The interpretations of \perp^* and $\check{\vee}$, however, may be regarded as being determined by the interpretation of the multiplicative negation \sim since, as we expect the classical relationships between multiplicative connectives to hold, we may simply define \perp^* to be $\sim \top^*$ and $F \check{\vee} G$ to be $\sim(\sim F * \sim G)$. The interpretation of \sim itself will not surprise readers familiar with relevant logics, since negation there is usually semantically defined by the clause:

$$x \models \sim A \Leftrightarrow x^* \not\models A$$

where x and x^* are points in a model related by the somewhat notorious “Routley star”, the philosophical interpretation of which has been the source of some angst for relevant logicians (see e.g. [34] for a discussion). In the setting of CBI, the involution operation ‘ $-$ ’ in a CBI-model plays the role of the Routley star. A more prosaic reason for our interpretation of \sim is that it yields the expected semantic equivalences between formulas, as opposed to, e.g., the superficially appealing definition $r \models_{\rho} \sim F \Leftrightarrow -r \models_{\rho} F$, which does not. For example, in analogy to ordinary classical logic, we would expect that $r \models_{\rho} F -* G$ iff $r \models_{\rho} \sim(F * \sim G)$. However, satisfaction of $-*$ involves universal quantification while satisfaction of $*$ involves existential quantification, strongly suggesting that the incorporation of a Boolean negation

into \sim is necessary to ensure such an outcome. One can also observe that the following is true in any CBI-model:

$$\begin{aligned} -r \models_{\rho} F &\Leftrightarrow \infty \in r \circ -r \text{ and } -r \models_{\rho} F \\ &\Leftrightarrow \exists r', r''. r'' \in r \circ r' \text{ and } r' \models_{\rho} F \text{ and } r'' = \infty \\ \text{i.e. } -r \not\models_{\rho} F &\Leftrightarrow \forall r', r''. r'' \in r \circ r' \text{ and } r' \models_{\rho} F \text{ implies } r'' \neq \infty \end{aligned}$$

One can then observe that by interpreting \perp^* and \sim as we do in Definition 2.7, we immediately obtain $r \models_{\rho} \sim F$ iff $r \models_{\rho} F \multimap \perp^*$, another desired equivalence.

Definition 2.8 (Formula validity). We say that a CBI-formula F is *true* in a CBI-model $M = \langle R, \circ, e, -, \infty \rangle$ iff $r \models_{\rho} F$ for any M -environment ρ and $r \in R$. F is said to be (CBI)-*valid* if it is true in all CBI-models.

Truth of BBI-formulas in BBI-models, and BBI-validity of formulas, is defined similarly.

Lemma 2.9 (CBI equivalences). The following formulas are all CBI-valid:

$$\begin{array}{ll} \sim \top \leftrightarrow \perp & F \checkmark G \leftrightarrow \sim(\sim F * \sim G) \\ \sim \top^* \leftrightarrow \perp^* & (F \multimap G) \leftrightarrow \sim F \checkmark G \\ \sim \sim F \leftrightarrow F & (F \multimap G) \leftrightarrow (\sim G \multimap \sim F) \\ \neg \sim F \leftrightarrow \sim \neg F & (F \multimap G) \leftrightarrow \sim(F * \sim G) \\ \sim F \leftrightarrow (F \multimap \perp) & F \checkmark \perp^* \leftrightarrow F \end{array}$$

Proof. We fix an arbitrary CBI-model M and M -environment ρ . For each of the equivalences $F \leftrightarrow G$ we require to show $r \models_{\rho} F \Leftrightarrow r \models_{\rho} G$. These follow directly from the definition of satisfaction, plus the properties of CBI-models given by Proposition 2.3. We show three of the cases in detail.

Case $(F \multimap G) \leftrightarrow \sim F \checkmark G$:

$$\begin{aligned} r \models_{\rho} \sim F \checkmark G &\Leftrightarrow \forall r_1, r_2 \in R. -r \in r_1 \circ r_2 \text{ implies } -r_1 \models_{\rho} \sim F \text{ or } -r_2 \models_{\rho} G \\ \text{(by Prop 2.3, pt. 1)} &\Leftrightarrow \forall r_1, r_2 \in R. -r \in r_1 \circ r_2 \text{ implies } r_1 \not\models_{\rho} F \text{ or } -r_2 \models_{\rho} G \\ &\Leftrightarrow \forall r_1, r_2 \in R. -r \in r_1 \circ r_2 \text{ and } r_1 \models_{\rho} F \text{ implies } -r_2 \models_{\rho} G \\ \text{(by Prop 2.3, pt. 1)} &\Leftrightarrow \forall r_1, r_2 \in R. -r \in r_1 \circ -r_2 \text{ and } r_1 \models_{\rho} F \text{ implies } r_2 \models_{\rho} G \\ \text{(by Prop 2.3, pt. 4)} &\Leftrightarrow \forall r_1, r_2 \in R. r_2 \in r \circ r_1 \text{ and } r_1 \models_{\rho} F \text{ implies } r_2 \models_{\rho} G \\ &\Leftrightarrow r \models_{\rho} F \multimap G \end{aligned}$$

Case $(F \multimap G) \leftrightarrow (\sim G \multimap \sim F)$:

$$\begin{aligned} r \models_{\rho} \sim G \multimap \sim F &\Leftrightarrow \forall r', r'' \in R. r'' \in r \circ r' \text{ and } r' \models_{\rho} \sim G \text{ implies } r'' \models_{\rho} \sim F \\ &\Leftrightarrow \forall r', r'' \in R. r'' \in r \circ r' \text{ and } -r' \not\models_{\rho} G \text{ implies } -r'' \not\models_{\rho} F \\ \text{(by Prop 2.3, pt. 1)} &\Leftrightarrow \forall r', r'' \in R. -r'' \in r \circ -r' \text{ and } r' \not\models_{\rho} G \text{ implies } r'' \not\models_{\rho} F \\ &\Leftrightarrow \forall r', r'' \in R. -r'' \in r \circ -r' \text{ and } r'' \models_{\rho} F \text{ implies } r' \models_{\rho} G \\ \text{(by Prop 2.3, pt. 4)} &\Leftrightarrow \forall r', r'' \in R. r' \in r \circ r'' \text{ and } r'' \models_{\rho} F \text{ implies } r' \models_{\rho} G \\ &\Leftrightarrow r \models_{\rho} F \multimap G \end{aligned}$$

Case $F \check{\vee} \perp^* \leftrightarrow F$:

$$\begin{aligned}
 r \models_{\rho} F \check{\vee} \perp^* &\Leftrightarrow \forall r_1, r_2 \in R. -r \in r_1 \circ r_2 \text{ implies } -r_1 \models_{\rho} F \text{ or } -r_2 \models_{\rho} \perp^* \\
 &\Leftrightarrow \forall r_1, r_2 \in R. -r \in r_1 \circ r_2 \text{ implies } -r_1 \models_{\rho} F \text{ or } -r_2 \neq \infty \\
 \text{(by Prop 2.3, pt. 2)} &\Leftrightarrow \forall r_1, r_2 \in R. -r \in r_1 \circ r_2 \text{ implies } -r_1 \models_{\rho} F \text{ or } r_2 \neq e \\
 &\Leftrightarrow \forall r_1 \in R. -r \in r_1 \circ e \text{ implies } -r_1 \models_{\rho} F \\
 &\Leftrightarrow \forall r_1 \in R. -r = r_1 \text{ implies } -r_1 \models_{\rho} F \\
 &\Leftrightarrow r \models_{\rho} F
 \end{aligned}$$

□

We remark that there is nevertheless one important classical equivalence whose multiplicative analogue does *not* hold in CBI in the strong sense of Lemma 2.9: the law of disjunctive middle, $\top^* \leftrightarrow F \check{\vee} \sim F$, which can be reexpressed (using the lemma) as the law of contradiction $\perp^* \leftrightarrow F * \sim F$. This equivalence certainly holds in one direction, since if $r \models_{\rho} F * \sim F$ then $r \in r_1 \circ r_2$, $r_1 \models_{\rho} F$ and $-r_2 \not\models_{\rho} F$, so r_1 is not $-r_2$ and thus $r \neq \infty$ by the CBI-model axiom, i.e. $r \models_{\rho} \perp^*$. The converse implication does not hold as, given $r \models_{\rho} \perp^*$ and some formula F , it clearly is not the case in general that $r \models_{\rho} F * \sim F$ (e.g., take $F = \perp$). However, the law does hold in the weak sense that \perp^* is true in a model M iff $F * \sim F$ is true in M . One direction of the implication follows by the argument above, and the other from the fact that \perp^* is never true in M (because it is not satisfied by ∞).

One might be tempted to think that, since the definition of satisfaction for CBI coincides with that of BBI when restricted to BBI-formulas, CBI and BBI might well be indistinguishable under such a restriction. Our next result establishes that this is by no means the case.

Proposition 2.10 (Non-conservative extensionality). CBI is a non-conservative extension of BBI. That is, every BBI-valid formula is also CBI-valid, but there is a BBI-formula that is CBI-valid but not BBI-valid.

Proof. To see that BBI-valid formulas are also CBI-valid, let $M = \langle R, \circ, e, -, \infty \rangle$ be a CBI-model, and let ρ be an M -environment. Thus $M' = \langle R, \circ, e \rangle$ is a BBI-model and ρ is an M' -environment. Then for any BBI-valid formula F we have $r \models_{\rho} F$ for all $r \in R$ with respect to M' since F is true in M' . Thus $r \models_{\rho} F$ for all $r \in R$ with respect to M (because the definition of satisfaction coincides in CBI and BBI for BBI-formulas) so F is true in M , and F is then CBI-valid since M was arbitrarily chosen.

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

$$\begin{aligned}
 I &=_{\text{def}} \neg \top^* -* \perp \\
 J &=_{\text{def}} \top^* (\top^* \wedge \neg(P -* \neg I))
 \end{aligned}$$

In a BBI-model $\langle R, \circ, e \rangle$, the formula I can be satisfied only by “nonextensible” elements of R , i.e. those elements $r \in R$ such that $r \circ r' = \emptyset$ for all $r' \neq e$:

$$\begin{aligned}
 r \models_{\rho} I &\Leftrightarrow \forall r', r'' \in R. r'' \in r \circ r' \text{ and } r' \models_{\rho} \neg \top^* \text{ implies } r'' \models_{\rho} \perp \\
 &\Leftrightarrow \forall r', r'' \in R. r'' \in r \circ r' \text{ implies } r' \not\models_{\rho} \neg \top^* \\
 &\Leftrightarrow \forall r', r'' \in R. r'' \in r \circ r' \text{ implies } r' = e \\
 &\Leftrightarrow \forall r' \in R. r' \neq e \text{ implies } r \circ r' = \emptyset
 \end{aligned}$$

The formula J is satisfied by an arbitrary element of R iff there exists *some* element of R that satisfies the proposition P and is nonextensible:

$$\begin{aligned}
r \models_\rho J &\Leftrightarrow \exists r_1, r_2 \in R. r \in r_1 \circ r_2 \text{ and } r_1 \models_\rho \top \text{ and } r_2 \models_\rho \top^* \wedge \neg(P \multimap \neg I) \\
&\Leftrightarrow \exists r_1, r_2 \in R. r \in r_1 \circ r_2 \text{ and } r_2 \models_\rho \top^* \text{ and } r_2 \not\models_\rho P \multimap \neg I \\
&\Leftrightarrow e \not\models_\rho P \multimap \neg I \\
&\Leftrightarrow \exists r', r'' \in R. r'' \in e \circ r' \text{ and } r' \models_\rho P \text{ but } r'' \not\models_\rho \neg I \\
&\Leftrightarrow \exists r' \in R. r' \in \rho(P) \text{ and } r' \models_\rho I
\end{aligned}$$

Note that in any CBI-model $\langle R, \circ, e, -, \infty \rangle$, for any $r \in R$ we have $r \circ -r \neq \emptyset$ since $\infty \in r \circ -r$ by definition. Since ∞ is the unique element $x \in R$ such that $-x = e$ by Proposition 2.3, it follows that if $r \models_\rho I$ then $r = \infty$. Thus, in CBI-models, if $r \models_\rho I$ and $r \models_\rho J$ then $r = \infty \in \rho(P)$, so the BBI-formula $I \wedge J \rightarrow P$ is CBI-valid.

To see that $I \wedge J \rightarrow P$ is not BBI-valid, consider the three-element model $\langle \{e, a, b\}, \circ, e \rangle$, where \circ is defined by: $e \circ x = x \circ e = \{x\}$ for all $x \in \{e, a, b\}$, and $x \circ y = \emptyset$ for all other $x, y \in \{e, a, b\}$. It is easy to verify that \circ is both commutative and associative and that e is a unit for \circ , so $\langle \{e, a, b\}, \circ, e \rangle$ is indeed a BBI-model. Now define an environment ρ for this model by $\rho(P) = \{a\}$. By the definition of \circ we have both $a \models_\rho I$ and $b \models_\rho I$ because a and b are both nonextensible in the model. Then we have $b \models_\rho I \wedge J$ but $b \not\models_\rho P$, so $I \wedge J \rightarrow P$ is false in this model and hence not BBI-valid. \square

The following proposition shows that, if we were to restrict our class of CBI-models to those in which the binary operation is a partial function rather than a relation, we would obtain a different notion of validity. In other words, CBI is sufficiently expressive to distinguish between partial functional and relational CBI-models.

Proposition 2.11 (Distinction of partial functional and relational CBI-models). CBI-validity does not coincide with validity in the class of partial functional CBI-models. That is, there is a CBI-formula that is not generally valid, but is true in every CBI-model $\langle R, \circ, e, -, \infty \rangle$ in which \circ is a partial function.

Proof. Let $P \in \mathcal{V}$ be a propositional variable and let K and L be abbreviations for CBI-formulas defined as follows:

$$\begin{aligned}
K &=_{\text{def}} \neg(\neg\perp^* \multimap \neg\top^*) \\
L &=_{\text{def}} \neg\perp^* \multimap \top^*
\end{aligned}$$

In a CBI-model $\langle R, \circ, e, -, \infty \rangle$, the formula K is satisfied by those model elements that can be extended by ∞ to obtain e :

$$\begin{aligned}
r \models_\rho K &\Leftrightarrow \exists r', r'' \in R. r'' \in r \circ r' \text{ and } r' \models_\rho \neg\perp^* \text{ but } r'' \not\models_\rho \neg\top^* \\
&\Leftrightarrow \exists r', r'' \in R. r'' \in r \circ r' \text{ and } r' = \infty \text{ and } r'' = e \\
&\Leftrightarrow e \in r \circ \infty
\end{aligned}$$

Similarly, the formula L is satisfied by those elements that, *whenever* they are extended by ∞ , always yield e :

$$\begin{aligned}
r \models_\rho L &\Leftrightarrow \forall r', r'' \in R. r'' \in r \circ r' \text{ and } r' \models_\rho \neg\perp^* \text{ implies } r'' \models_\rho \top^* \\
&\Leftrightarrow \forall r', r'' \in R. r'' \in r \circ r' \text{ and } r' = \infty \text{ implies } r'' = e \\
&\Leftrightarrow r \circ \infty = \{e\}
\end{aligned}$$

Let $M = \langle R, \circ, e, -, \infty \rangle$ be a CBI-model in which \circ is a partial function, let ρ be an M -environment and let $r \in R$. Suppose that $r \models_\rho K$, so that $e \in r \circ \infty$ by the above. Since \circ is a partial function, the cardinality of $r \circ \infty$ is at most 1, so we must have $r \circ \infty = \{e\}$,

i.e., $r \models_\rho L$. Thus the formula $K \rightarrow L$ is true in M , and so valid with respect to partial functional CBI-models.

To see that $K \rightarrow L$ is not generally valid, we must provide a CBI-model in which it is false. Consider the three-element model $\langle \{e, a, \infty\}, \circ, e, -, \infty \rangle$, where $-$ is defined by $-e = \infty, -a = a, -\infty = e$ and \circ is defined as follows:

$$\begin{aligned} e \circ x &= x \circ e = \{x\} \text{ for all } x \in \{e, a, \infty\} \\ a \circ a &= \{e, \infty\} \\ a \circ \infty &= \infty \circ a = \infty \circ \infty = \{e, a\} \end{aligned}$$

In this model e is a unit for \circ and \circ is commutative by construction. It can also easily be verified that \circ is associative (e.g., $a \circ (a \circ \infty) = \{e, a, \infty\} = (a \circ a) \circ \infty$) and that $-x$ is the unique element such that $\infty \in x \circ -x$ for all $x \in \{e, a, \infty\}$. Thus $\langle \{e, a, \infty\}, \circ, e, -, \infty \rangle$ is indeed a CBI-model (and we note that \circ is not a partial function). Now for any environment ρ we have $a \models_\rho K$ since $e \in a \circ \infty$, but $a \not\models_\rho L$ since $a \circ \infty \neq \{e\}$. Thus $K \rightarrow L$ is false in this model, and hence invalid. \square

The question of whether BBI-validity coincides for partial functional and relational BBI-models is still open. Our proof of Proposition 2.11 does not transfer straightforwardly to BBI because it crucially relies upon the fact that, in CBI, we can write down a formula $(\neg \perp^*)$ that is satisfied by exactly one model element (∞), which is not the unit e in general.

3. EXAMPLES OF CBI-MODELS

In this section we give some concrete examples of CBI-models, and some general constructions for forming new models. In many of our examples, the monoid operation \circ in the CBI-model is a partial function rather than a relation, and in these cases we treat it as such (i.e., by dropping the brackets on singleton sets).

Example 3.1 (Personal finance). This example builds on the “vending machine” model for BI given by Pym, O’Hearn and Yang [32], which itself was inspired by Girard’s well-known “Marlboro and Camel” illustration of linear logic [21].

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 can be understood as a CBI-model $\langle \mathbb{Z}, +, 0, -, 0 \rangle$ by Proposition 2.4. We view the elements of this model 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 $\mathcal{L}m \models_\rho F$ informally as “ $\mathcal{L}m$ 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, so that we have $\mathcal{L}m \models_\rho C \Leftrightarrow m \geq 5$ and $\mathcal{L}m \models_\rho W \Leftrightarrow m \geq 20$. Then the formula $C \wedge W$ denotes the ability to buy cigarettes and the ability to buy whisky (but not necessarily to buy both together):

$$\begin{aligned} \mathcal{L}m \models_\rho C \wedge W &\Leftrightarrow \mathcal{L}m \models_\rho C \text{ and } \mathcal{L}m \models_\rho W \\ &\Leftrightarrow m \geq 20 \end{aligned}$$

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

$$\begin{aligned} \mathcal{L}m \models_\rho C * W &\Leftrightarrow \exists m_1, m_2 \in \mathbb{Z}. \mathcal{L}m = \mathcal{L}m_1 + \mathcal{L}m_2 \text{ and } \mathcal{L}m_1 \models_\rho C \text{ and } \mathcal{L}m_2 \models_\rho W \\ &\Leftrightarrow m \geq 25 \end{aligned}$$

The multiplicative implication $C \multimap W$ denotes the fact that if one acquires enough money to buy cigarettes then the resulting balance of funds is sufficient to buy whisky:

$$\begin{aligned} \mathcal{L}m \models_{\rho} C \multimap W &\Leftrightarrow \forall m' \in \mathbb{Z}. \mathcal{L}m' \models_{\rho} C \text{ implies } \mathcal{L}m + \mathcal{L}m' \models_{\rho} W \\ &\Leftrightarrow m \geq 15 \end{aligned}$$

We remark that all of the above formulas are BBI-formulas, and so would be interpreted in exactly the same way in the BBI-model $\langle \mathbb{Z}, +, 0 \rangle$. Let us examine the multiplicative connectives that are particular to CBI. We have $\mathcal{L}m \models_{\rho} \perp^* \Leftrightarrow m \neq 0$, so that \perp^* simply denotes the fact that one has either some credit or some debt. (This is exactly the interpretation of the formula $\neg \top^*$, a collapse induced by the fact that e and ∞ coincide in the Abelian group model.) Now consider the formula $\sim C$. We have:

$$\mathcal{L}m \models_{\rho} \sim C \Leftrightarrow -\mathcal{L}m \not\models_{\rho} C \Leftrightarrow -m < 5 \Leftrightarrow m > -5$$

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, $C \dot{\vee} W$, we have:

$$\begin{aligned} \mathcal{L}m \models_{\rho} C \dot{\vee} W &\Leftrightarrow \forall m_1, m_2. -\mathcal{L}m = \mathcal{L}m_1 + \mathcal{L}m_2 \text{ implies } -\mathcal{L}m_1 \models_{\rho} C \text{ or } -\mathcal{L}m_2 \models_{\rho} W \\ &\Leftrightarrow m \geq 24 \end{aligned}$$

It is not immediately obvious how to read this formula informally. However, observing that $C \dot{\vee} W$ is semantically equivalent to $\sim C \multimap W$ and to $\sim W \multimap C$, 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 the 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 $\bar{L} = \Sigma \setminus L$ is the unique regular language such that $L + \bar{L} = \Sigma$. Thus $\langle \mathcal{L}(\Sigma), +, \epsilon, \bar{\cdot}, \Sigma \rangle$ 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 $\bar{A} = \{\bar{a} \mid a \in A\}$ to be disjoint from A . Then the following tuple is a CBI-model:

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

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

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

Note that $\langle A \cup \bar{A} \cup \{0, \tau\}, \cdot | \cdot, 0 \rangle$ is a partial commutative monoid. The operation $\cdot | \cdot$ 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 \bar{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 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 $H =_{\text{def}} \mathbb{Z}_{>0} \rightarrow \mathbb{Z}$ 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 $-r =_{\text{def}} (\mathbb{Z}_{>0} \times \mathbb{Z}) \setminus r$.

We now examine some more general ways of constructing CBI-models. Our first result gives a construction for extending BBI-models into CBI-models.

Proposition 3.8 (CBI-extension of BBI-models). Let $\langle R, \circ, e \rangle$ be a BBI-model and define a second, disjoint copy \bar{R} of R by $\bar{R} =_{\text{def}} \{\bar{r} \mid r \in R\}$. Define $-x = \bar{x}$ for all $x \in R$ and $-\bar{x} = x$ for all $x \in \bar{R}$. Finally, define the binary relation \oplus over $R \cup \bar{R}$ by the following:

$$\begin{aligned} (\oplus 1) \quad & z \in x \circ y \Rightarrow z \in x \oplus y \\ (\oplus 2) \quad & z \in x \circ y \Rightarrow \bar{y} \in x \oplus \bar{z} \cap \bar{z} \oplus x \end{aligned}$$

Then $\langle R \cup \bar{R}, \oplus, e, -, \bar{e} \rangle$ is a CBI-model.

Proof. We start by stating the following *elimination principle* for \oplus which follows directly from its introduction rules $(\oplus 1)$ and $(\oplus 2)$.

Elimination principle. If $z \in x \oplus y$ then the following hold:

- (1) $z \in R$ iff $x, y \in R$, and if $x, y, z \in R$ then $z \in x \circ y$.
- (2) $z \in \overline{R}$ iff either $x \in R$ and $y \in \overline{R}$, or $x \in \overline{R}$ and $y \in R$. Furthermore:
 - if $x \in R$ and $y, z \in \overline{R}$ then $y' \in x \circ z'$, where $\overline{y'} = y$ and $\overline{z'} = z$;
 - if $y \in R$ and $x, z \in \overline{R}$ then $x' \in z' \circ y$, where $\overline{x'} = x$ and $\overline{z'} = z$.

With this principle in place we carry out the main proof. First, we need to check that $\langle R \cup \overline{R}, \oplus, e \rangle$ is a BBI-model, i.e., that \oplus is commutative and associative, and satisfies $x \circ e = \{x\}$ for all $x \in R \cup \overline{R}$.

We tackle the last of these requirements first. Since $\langle R, \circ, e \rangle$ is a BBI-model we have $x \in x \circ e = e \circ x = \{x\}$ for all $x \in R$. Thus, for all $x \in R$, we have $x \in x \oplus e$ by $(\oplus 1)$ and $\overline{x} \in \overline{x} \oplus e$ by $(\oplus 2)$. That is, $x \in x \oplus e$ for all $x \in R \cup \overline{R}$. Now suppose $y \in x \oplus e$. Since $e \in R$, there are two cases to consider by the elimination principle. If both $x, y \in R$ then we have $y \in x \circ e = \{x\}$, thus $y = x$. Otherwise, both $x, y \in \overline{R}$ and $x' \in y' \circ e = \{y'\}$, where $\overline{x'} = x$ and $\overline{y'} = y$. Thus $x' = y'$ and, since $\overline{\cdot}$ is injective, $x = y$. So $x \oplus e = \{x\}$ for all $x \in R \cup \overline{R}$ as required.

To see that \oplus is commutative, let $z \in x \oplus y$, and consider the cases given by the elimination principle. First, suppose that all of $x, y, z \in R$ and $z \in x \circ y$. Since $\langle R, \circ, e \rangle$ is a BBI-model, \circ is commutative, so $z \in y \circ x$. Thus by $(\oplus 1)$ we have $z \in y \oplus x$. Next, suppose that $x \in R$, $y, z \in \overline{R}$ and $y' \in x \circ z'$, where $\overline{y'} = y$ and $\overline{z'} = z$. By $(\oplus 2)$ we then have $z \in y \oplus x$. The case where $y \in R$ and $x, z \in \overline{R}$ is symmetric. Thus $z \in x \oplus y$ implies $z \in y \oplus x$, so $x \oplus y = y \oplus x$ for any $x, y \in R \cup \overline{R}$, i.e. \oplus is commutative.

It remains to show that \oplus is associative, i.e. that $(x \oplus y) \oplus z = x \oplus (y \oplus z)$ for any $x, y, z \in R \cup \overline{R}$. We divide into cases as follows:

Case: at least two of x, y, z are in \overline{R} . The elimination principle implies that $x \oplus y = \emptyset$ whenever both $x, y \in \overline{R}$ and, furthermore, $z \in \overline{R}$ whenever $z \in x \oplus y$ and either $x \in \overline{R}$ or $y \in \overline{R}$. Combined with the pointwise extension of \oplus to sets of elements, this implies that $(x \oplus y) \oplus z = x \oplus (y \oplus z) = \emptyset$.

Case: none of x, y, z are in \overline{R} . The elimination principle implies that $(x \oplus y) \oplus z = (x \circ y) \circ z$ and $x \oplus (y \oplus z) = x \circ (y \circ z)$. We are then done since \circ is associative (because $\langle R, \circ, e \rangle$ is a BBI-model).

Case: exactly one of x, y, z is in \overline{R} . We show how to treat the case where $x \in \overline{R}$; the other cases are similar. We write $x = \overline{x'}$. Let $w \in (\overline{x'} \oplus y) \oplus z = \bigcup_{v \in \overline{x'} \oplus y} v \oplus z$. Thus $w \in v \oplus z$ for some $v \in \overline{x'} \oplus y$. By part 2 of the elimination principle, $v \in \overline{R}$ and $x' \in v' \circ y$, where $v = \overline{v'}$. Applying the same elimination principle to $w \in v' \oplus z$, we obtain that $w \in \overline{R}$ and $v' \in w' \circ z$, where $w = \overline{w'}$. Thus $x' \in \bigcup_{v' \in w' \circ z} v' \circ y = (w' \circ z) \circ y$. Since \circ is associative and commutative, $x' \in w' \circ (y \circ z)$. By (1), it is certainly the case that $y \circ z \subseteq y \oplus z$, whence we obtain $x' \in w' \circ (y \oplus z) = (y \oplus z) \circ w'$. Thus, by $(\oplus 2)$, we obtain $w \in x \oplus (y \oplus z)$.

As we have shown $w \in (x \oplus y) \oplus z$ implies $w \in x \oplus (y \oplus z)$, we conclude $(x \oplus y) \oplus z = x \oplus (y \oplus z)$, i.e. \oplus is associative as required. Thus $\langle R \cup \overline{R}, \oplus, e \rangle$ is indeed a BBI-model.

To see that $\langle R \cup \overline{R}, \oplus, e, -, \infty \rangle$ is a CBI-model, we just need to check that for any $x \in R \cup \overline{R}$, \overline{x} is the unique element such that $\infty = \overline{e} \in x \oplus \overline{x}$. Suppose first that $x \in R$. Since $x \circ e = \{x\}$ (because $\langle R, \circ, e \rangle$ is a BBI-model), we have $\overline{e} \in x \oplus \overline{x}$ by $(\oplus 2)$. So \overline{x} satisfies the equation. To see that it is unique, suppose that $\overline{e} \in x \oplus y$. By part 2 of the elimination principle, we must have $y = \overline{y'}$ and $y' \in x \circ e = \{x\}$. Thus $y' = x$ so $y = \overline{x}$ as

required. When $x \in \overline{R}$, we have $x = \overline{y}$ for some $y \in R$ and the reasoning is exactly dual to the case above, since \circ is commutative. This completes the proof. \square

We remark that the extension of BBI-models into CBI-models given by Proposition 3.8 may be viewed as being canonical in the sense that the construction is clearly injective (the original BBI-model M can be reobtained by restricting the constructed CBI-model to the domain of M).

Lemma 3.9 (Disjoint union of CBI-models). Let $\langle R_1, \circ_1, e_1, -_1, \infty_1 \rangle$ and $\langle R_2, \circ_2, e_2, -_2, \infty_2 \rangle$ be CBI-models such that R_1 and R_2 are disjoint and either $\infty_1 = e_1$ and $\infty_2 = e_2$ or ∞_1, ∞_2 are nonextensible, i.e. $\infty_1 \circ_1 x = \emptyset$ for all $x \neq e_1$ and $\infty_2 \circ_2 x = \emptyset$ for all $x \neq e_2$.

Let R be the set obtained by identifying e_1 with e_2 and ∞_1 with ∞_2 in $R_1 \cup R_2$, and write $e = e_1 = e_2$ and $\infty = \infty_1 = \infty_2$ for the elements obtained by this identification. Define $- = -_1 \cup -_2$ and $\circ = \circ_1 \cup \circ_2$. Then $\langle R, \circ, e, -, \infty \rangle$ is a CBI-model.

Proof. We start by observing that $-$ is indeed a function from R to R because R_1 and R_2 are assumed disjoint and, using Proposition 2.3, $-e_1 = \infty_1 = \infty_2 = -e_2$, and similarly $-\infty_1 = -\infty_2$.

We need to check that $\langle R, \circ, e \rangle$ is a BBI-model. The commutativity of \circ is immediate by the commutativity of \circ_1, \circ_2 and set union. Similarly, $x \circ e = \{x\}$ for all $x \in R$ because $e = e_1$ is a unit of \circ_1 and $e = e_2$ is a unit of \circ_2 . To see that \circ is associative, we let $x, y, z \in R$ and show that $x \circ (y \circ z) = (x \circ y) \circ z$ by case analysis.

Case: at least one of x, y, z is e . We are immediately done by the fact that e is a unit for \circ .

Case: at least one of x, y, z is ∞ . We may assume that none of x, y, z is e , since these possibilities are covered by the previous case, and so it follows by assumption that ∞_1 and ∞_2 are nonextensible. Consequently $\infty \circ x = \emptyset$ for all $x \neq e$, so $x \circ (y \circ z) = \emptyset = (x \circ y) \circ z$.

Case: all of $x, y, z \in R_1$. We may assume by the previous cases that none of x, y, z is either e or ∞ , so we have $x \circ (y \circ z) = x \circ_1 (y \circ_1 z)$ and $(x \circ y) \circ z = (x \circ_1 y) \circ_1 z$, whence we are done by the associativity of \circ_1 .

Case: all of $x, y, z \in R_2$. Similar to the case above.

Case: none of the above. We have $x \circ (y \circ z) = \emptyset = (x \circ y) \circ z$ since $x \circ y = \emptyset$ whenever $x \in R_1, y \in R_2$ and neither x nor y is e or ∞ . This covers all the cases, so \circ is indeed associative.

Now to see that $\langle R, \circ, e, -, \infty \rangle$ is a CBI-model, given $x \in R$ we need to show that $-x$ is the unique $y \in R$ such that $\infty \in x \circ y$. It is easily verified that $\infty \in x \circ -x$ for all $x \in R$. Now suppose that $\infty \in x \circ y = x \circ_1 y \cup x \circ_2 y$ for some $y \in R$. If $\infty \in x \circ_1 y$ then $y = -_1 x = -x$ as required. Similarly, if $\infty \in x \circ_2 y$ then $y = -_2 x = -x$. \square

We remark that the restrictions on ∞_1 and ∞_2 in Lemma 3.9 are needed in order to ensure the associativity of \circ . For example, if $x \in R_1$ and $y \in R_2$ and $x, y \neq e$ then $(x \circ y) \circ -y = \emptyset \circ -y = \emptyset$ while $x \circ (y \circ -y) \supseteq x \circ \infty = x \circ_1 \infty_1$, which is not empty in general.

Lemma 3.10 (Cartesian product of CBI-models). Let $\langle R_1, \circ_1, e_1, -_1, \infty_1 \rangle$ and $\langle R_2, \circ_2, e_2, -_2, \infty_2 \rangle$ be CBI-models. Define $- : R_1 \times R_2 \rightarrow R_1 \times R_2$ and $\circ : (R_1 \times R_2) \times (R_1 \times R_2) \rightarrow \mathcal{P}(R_1 \times R_2)$ by:

$$\begin{aligned} -(x_1, x_2) &= (-_1x_1, -_2x_2) \\ (x_1, x_2) \circ (y_1, y_2) &= \bigcup_{z_1 \in x_1 \circ_1 y_1, z_2 \in x_2 \circ_2 y_2} (z_1, z_2) \end{aligned}$$

Then $\langle R_1 \times R_2, \circ, (e_1, e_2), -, (\infty_1, \infty_2) \rangle$ is a CBI-model.

Proof. First we need to check that $\langle R_1 \times R_2, \circ, (e_1, e_2) \rangle$ is a BBI-model. To see that (e_1, e_2) is a unit for \circ we observe:

$$(e_1, e_2) \circ (x_1, x_2) = \bigcup_{z_1 \in e_1 \circ_1 x_1, z_2 \in e_2 \circ_2 x_2} (z_1, z_2) = \bigcup_{z_1 \in \{x_1\}, z_2 \in \{x_2\}} (z_1, z_2) = (x_1, x_2)$$

The commutativity of \circ follows in a similar fashion. To see that \circ is associative, let $(r_1, r_2) \in (x_1, x_2) \circ ((y_1, y_2) \circ (z_1, z_2))$, so that there is a $(w_1, w_2) \in (y_1, y_2) \circ (z_1, z_2)$ such that $(r_1, r_2) \in (x_1, x_2) \circ (w_1, w_2)$. Thus $w_1 \in y_1 \circ_1 z_1$ and $w_2 \in y_2 \circ_2 z_2$, and $r_1 \in x_1 \circ_1 w_1$ and $r_2 \in x_2 \circ_2 w_2$, so $r_1 \in x_1 \circ_1 (y_1 \circ_1 z_1)$ and $r_2 \in x_2 \circ_2 (y_2 \circ_2 z_2)$. By associativity of \circ_1 and \circ_2 , we then have $r_1 \in (x_1 \circ_1 y_1) \circ_1 z_1$ and $r_2 \in (x_2 \circ_2 y_2) \circ_2 z_2$. Thus $r_1 \in v_1 \circ_1 z_1$ for some $v_1 \in x_1 \circ_1 y_1$ and $r_2 \in v_2 \circ_2 z_2$ for some $v_2 \in x_2 \circ_2 y_2$. By definition of \circ we then have $(v_1, v_2) \in (x_1, x_2) \circ (y_1, y_2)$ and $(r_1, r_2) \in (v_1, v_2) \circ (z_1, z_2)$, so $(r_1, r_2) \in ((x_1, x_2) \circ (y_1, y_2)) \circ (z_1, z_2)$ as required.

To see that the required conditions on $-$ and (∞_1, ∞_2) are met, we observe that since $\infty_1 \in x_1 \circ_1 -_1x_1$ for all $x_1 \in R_1$ and $\infty_2 \in x_2 \circ_2 -_2x_2$ for all $x_2 \in R_2$, we have $(\infty_1, \infty_2) \in (x_1, x_2) \circ (-_1x_1, -_2x_2) = (x_1, x_2) \circ -(x_1, x_2)$ for all $(x_1, x_2) \in R_1 \times R_2$. Now if $(\infty_1, \infty_2) \in (x_1, x_2) \circ (y_1, y_2)$ then $\infty_1 \in x_1 \circ_1 y_1$ and $\infty_2 \in x_2 \circ_2 y_2$. Thus $y_1 = -_1x_1$ and $y_2 = -_2x_2$, so $(y_1, y_2) = (-_1x_1, -_2x_2) = -(x_1, x_2)$ as required. \square

Clearly, Lemma 3.10 generalises to give a construction for the Cartesian product of n CBI-models.

Lemma 3.11 (Maps into CBI-models). Let $\langle R, \circ, e, -, \infty \rangle$ be a CBI-model, let A be any set and define $e_A, \infty_A : A \rightarrow R$, $-_A : (A \rightarrow R) \rightarrow (A \rightarrow R)$ and $\circ_A : (A \rightarrow R) \times (A \rightarrow R) \rightarrow \mathcal{P}(A \rightarrow R)$ by:

$$\begin{aligned} e_A &= \lambda a. e \\ \infty_A &= \lambda a. \infty \\ -_A(f) &= \lambda a. -f(a) \\ f_1 \circ_A f_2 &= \{\lambda a. x \mid x \in f_1(a) \circ f_2(a)\} \end{aligned}$$

Then $\langle A \rightarrow R, \circ_A, e_A, -_A, \infty_A \rangle$ is a CBI-model.

Proof. First we need to check that $\langle A \rightarrow R, \circ_A, e_A \rangle$ is a BBI-model. We have:

$$\begin{aligned} f \circ_A e_A &= \{\lambda a. x \mid x \in f(a) \circ e_A(a)\} \\ &= \{\lambda a. x \mid x \in \{f(a)\}\} \\ &= \{\lambda a. f(a)\} \\ &= f \end{aligned}$$

so e_A is a unit for \circ_A . The commutativity of \circ_A follows similarly from the commutativity of \circ . To see that \circ_A is associative, note that we have:

$$\begin{aligned} f_1 \circ_A (f_2 \circ_A f_3) &= \{\lambda a. x \mid x \in f_1(a) \circ (f_2 \circ_A f_3)(a)\} \\ &= \{\lambda a. x \mid x \in f_1(a) \circ (f_2(a) \circ f_3(a))\} \\ &= \{\lambda a. x \mid x \in (f_1(a) \circ f_2(a)) \circ f_3(a)\} && \text{(since } \circ \text{ associative)} \\ &= \{\lambda a. x \mid x \in (f_1 \circ_A f_2)(a) \circ f_3(a)\} \\ &= (f_1 \circ_A f_2) \circ_A f_3 \end{aligned}$$

Finally, to see that $-_A$ and ∞_A meet the CBI-model condition, we proceed as follows:

$$\begin{aligned}
 \infty_A \in f \circ_A g &\Leftrightarrow \lambda a. \infty \in \{\lambda a. x \mid x \in f(a) \circ g(a)\} \\
 &\Leftrightarrow \infty \in f(a) \circ g(a) \text{ for all } a \in A \\
 &\Leftrightarrow g(a) = -f(a) \text{ for all } a \in A \quad (\text{since } \langle R, \circ, e, -, \infty \rangle \text{ a CBI-model}) \\
 &\Leftrightarrow g = \lambda a. -f(a) = -_A(f)
 \end{aligned}$$

This completes the verification. \square

We remark that Lemma 3.11 gives a canonical way of extending CBI-models to heap-like structures mapping elements of a set into model values. For example, our “money” model of Example 3.1 extends via Lemma 3.11 to a model of maps from a set to the integers, which can be understood as financial “asset portfolios” mapping identifiers (commodities) to integers (assets or liabilities). Such a model 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.

Example 3.12 (Deny-guarantee model). The *deny-guarantee* permissions employed by Dodds et al. [17] are elements of $\text{PermDG} = \text{Actions} \rightarrow \text{FractionDG}$, where Actions is a set of “actions” and $\text{FractionDG} = \{(deny, \pi) \mid \pi \in (0, 1)\} \cup \{(guar, \pi) \mid \pi \in (0, 1)\} \cup \{0, 1\}$. A partial binary function \oplus is defined on FractionDG by:

$$\begin{aligned}
 0 \oplus x = x \oplus 0 &= x \\
 (deny, \pi_1) \oplus (deny, \pi_2) &= \begin{cases} (deny, \pi_1 + \pi_2) & \text{if } \pi_1 + \pi_2 < 1 \\ 1 & \text{if } \pi_1 + \pi_2 = 1 \\ \text{undefined} & \text{otherwise} \end{cases} \\
 (guar, \pi_1) \oplus (guar, \pi_2) &= \begin{cases} (guar, \pi_1 + \pi_2) & \text{if } \pi_1 + \pi_2 < 1 \\ 1 & \text{if } \pi_1 + \pi_2 = 1 \\ \text{undefined} & \text{otherwise} \end{cases} \\
 1 \oplus x = x \oplus 1 &= \text{undefined for } x \neq 0
 \end{aligned}$$

The operation \oplus is lifted to PermDG by $(p_1 \oplus p_2)(a) = p_1(a) \oplus p_2(a)$. Next, define the involution $-$ on FractionDG by:

$$-0 = 1 \quad -(deny, \pi) = (deny, 1 - \pi) \quad -(guar, \pi) = (guar, 1 - \pi) \quad -1 = 0$$

and lift $-$ to PermDG by $(-p)(a) = -p(a)$. Finally, we lift 0 and 1 to PermDG by $0(a) = 0$ and $1(a) = 1$.

Then $\langle \text{PermDG}, \oplus, 0, -, 1 \rangle$ is a CBI-model. One can check this directly, but we can also reconstruct the model using our general constructions. First, one verifies easily that both the “deny fragment” and the “guarantee fragment” of FractionDG given by $\{(deny, \pi) \mid \pi \in (0, 1)\} \cup \{0, 1\}, \oplus, 0, -, 1$ and $\{(guar, \pi) \mid \pi \in (0, 1)\} \cup \{0, 1\}, \oplus, 0, -, 1$ are CBI-models. Noting that 1 is nonextensible in both models, we can apply Lemma 3.9 to obtain the disjoint union of these models, which is exactly the CBI-model $\langle \text{FractionDG}, \oplus, 0, -, 1 \rangle$. By applying Lemma 3.11 (taking A to be the set Actions) we then obtain the CBI-model $\langle \text{PermDG}, \oplus, 0, -, 1 \rangle$.

<i>Symbol</i>	<i>Arity</i>	<i>Antecedent meaning</i>	<i>Consequent meaning</i>
\emptyset	0	\top	\perp
\emptyset^*	0	\top^*	\perp^*
$\#$	1	\neg	\neg
\flat	1	\sim	\sim
$;$	2	\wedge	\vee
$,$	2	$*$	\forall^*

Figure 1: The structural connectives of DL_{CBI} .

4. DL_{CBI} : A DISPLAY CALCULUS PROOF SYSTEM FOR CBI

In this section, we present DL_{CBI} , a display calculus for CBI based on Belnap’s general *display logic* which provides a generic syntactic framework for formal proof in a very general class of logics [2]. Display calculi are akin to sequent calculi in that logical connectives are specified by a pair of introduction rules introducing the connective on the left and right of proof judgements respectively. However, the proof judgements of display calculi have a richer structure than an ordinary sequent, and a corresponding set of meta-level rules (called *display postulates*) for manipulating this structure. This ensures the characteristic, and very useful *display property* of display calculi: any proof judgement may be rearranged so that any given part of the judgement appears alone on one side of the turnstile (without loss of information). In addition to its conceptual elegance, this property ensures that cut-elimination holds for any display calculus whose structural rules obey a few easily verified conditions. Our display calculus DL_{CBI} indeed satisfies these conditions, and thus cut-elimination. Furthermore, it is sound and complete with respect to our CBI-models.

Belnap’s original formulation of display logic treats an arbitrary number of “families” of propositional connectives. The necessary structural connectives, display postulates and logical introduction rules are then ascribed automatically to each family, with only the structural rules governing the family chosen freely. For CBI, it is obvious that there are two complete families of propositional connectives, one additive and one multiplicative. Thus the formulation of DL_{CBI} can be viewed as arising more or less directly from Belnap’s general schema.

The proof judgements of DL_{CBI} , called consecutions, are built from structures which generalise the bunches used in existing proof systems for BI (cf. [31]).

Definition 4.1 (Structure / consecution). A DL_{CBI} -structure X is constructed according to the following grammar:

$$X ::= F \mid \emptyset \mid \#X \mid X; X \mid \emptyset^* \mid \flat X \mid X, X$$

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

Figure 1 gives a summary of the structural connectives of our display calculus and their semantic reading as antecedents (or premises) and consequents (or conclusions) in a consecution. However, the presence of the meta-level negations $\#$ and \flat in our structures leads to a subtler notion of antecedent and consequent parts of consecutions than the simple left-right division of sequent calculus. Informally, moving inside a meta-level negation flips the interpretation of its immediate substructure. For example, if $\#X$ or $\flat X$ is an antecedent

$$\begin{array}{ccc}
 \frac{X; Y \vdash Z}{\frac{\frac{\frac{}{}{}}{}}{}} \text{(AD1a)} & \frac{X \vdash Y; Z}{\frac{\frac{\frac{}{}{}}{}}{}} \text{(AD2a)} & \frac{X \vdash Y}{\frac{\frac{\frac{}{}{}}{}}{}} \text{(AD3a)} \\
 \frac{X; Y \vdash Z}{\frac{\frac{\frac{}{}{}}{}}{}} \text{(AD1b)} & \frac{X \vdash Y; Z}{\frac{\frac{\frac{}{}{}}{}}{}} \text{(AD2b)} & \frac{X \vdash Y}{\frac{\frac{\frac{}{}{}}{}}{}} \text{(AD3b)} \\
 \\
 \frac{X, Y \vdash Z}{\frac{\frac{\frac{}{}{}}{}}{}} \text{(MD1a)} & \frac{X \vdash Y, Z}{\frac{\frac{\frac{}{}{}}{}}{}} \text{(MD2a)} & \frac{X \vdash Y}{\frac{\frac{\frac{}{}{}}{}}{}} \text{(MD3a)} \\
 \frac{X, Y \vdash Z}{\frac{\frac{\frac{}{}{}}{}}{}} \text{(MD1b)} & \frac{X \vdash Y, Z}{\frac{\frac{\frac{}{}{}}{}}{}} \text{(MD2b)} & \frac{X \vdash Y}{\frac{\frac{\frac{}{}{}}{}}{}} \text{(MD3b)}
 \end{array}$$

 Figure 2: The display postulates for DL_{CBI} .

part then the substructure X should be considered a consequent part, and vice versa. This notion is made formal by the following definition.

Definition 4.2 (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 $\#$ 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 .

We can now give the formal interpretation of our consecutions, using a pair of mutually recursive functions to capture the dependency between antecedent and consequent interpretations.

Definition 4.3 (Validity in DL_{CBI}). For any structure X we mutually define two formulas Ψ_X and Υ_X by induction on the structure of X as follows:

$$\begin{array}{ll}
 \Psi_F = F & \Upsilon_F = F \\
 \Psi_\emptyset = \top & \Upsilon_\emptyset = \perp \\
 \Psi_{\#X} = \neg \Upsilon_X & \Upsilon_{\#X} = \neg \Psi_X \\
 \Psi_{X_1; X_2} = \Psi_{X_1} \wedge \Psi_{X_2} & \Upsilon_{X_1; X_2} = \Upsilon_{X_1} \vee \Upsilon_{X_2} \\
 \Psi_\emptyset = \top^* & \Upsilon_\emptyset = \perp^* \\
 \Psi_{\flat X} = \sim \Upsilon_X & \Upsilon_{\flat X} = \sim \Psi_X \\
 \Psi_{X_1, X_2} = \Psi_{X_1} * \Psi_{X_2} & \Upsilon_{X_1, X_2} = \Upsilon_{X_1} \checkmark \Upsilon_{X_2}
 \end{array}$$

A consecution $X \vdash Y$ is said to be *true* in a CBI-model M if the formula $\Psi_X \rightarrow \Upsilon_Y$ is true in M . $X \vdash Y$ is said to be *valid* if it is true in all CBI-models.

We write a proof rule with a double line between premise and conclusion 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.

Definition 4.4 (Display-equivalence). Two consecutions $X \vdash Y$ and $X' \vdash Y'$ are said to be *display-equivalent*, written $X \vdash Y \equiv_D X' \vdash Y'$, if there is a derivation of one from the other using only the *display postulates* given in Figure 2.

The display postulates for DL_{CBI} are essentially Belnap's original display postulates, instantiated (twice) to the additive and multiplicative connective families of CBI. The only

difference is that our postulates build commutativity of the comma and semicolon into the notion of display-equivalence, since in CBI both the conjunctions and both the disjunctions are commutative.

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.

Theorem 4.5 (Display theorem (Belnap [2])). For any antecedent part W of a consecution $X \vdash Y$ there exists a structure Z such that $W \vdash Z \equiv_D X \vdash Y$. Similarly, for any consequent part W of $X \vdash Y$ there exists a structure Z such that $Z \vdash W \equiv_D X \vdash Y$.

Proof. Essentially, one uses the display postulates to move any structure surrounding W to the opposite side of the consecution, or to eliminate any preceding occurrences of \sharp and \flat (note that for each possible position of W in $X \vdash Y$ there is a display postulate allowing the topmost level of structure above W to be moved away or eliminated). Moreover, each of the display postulates preserves antecedent and consequent parts of consecutions, so that W must end up on the correct side of the consecution at the end of this process. The details are straightforward. \square

Example 4.6. The antecedent part Y of the consecution $\flat(X, \sharp Y) \vdash Z; \flat W$ can be displayed as follows:

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

The proof rules of DL_{CBI} are given in Figure 3, and are divided into three distinct types. The identity rules consist of the usual identity axiom for propositional variables, a cut rule and a rule for display equivalence. The logical rules follow the division between left and right introduction rules familiar from sequent calculus. Both the identity rules and the logical rules are the standard ones for display logic, instantiated to the additive and multiplicative connective families of CBI. The structural rules of DL_{CBI} implement suitable associativity and unitary laws on both sides of consecutions, plus weakening and contraction for the (additive) semicolon.

The identity axiom of DL_{CBI} is postulated only for propositional variables⁵, but can be recovered for arbitrary formulas.

Proposition 4.7. $F \vdash F$ is DL_{CBI} -provable for all formulas F .

Proof. By structural induction on F . \square

⁵This slightly simplifies the proof of cut-elimination for DL_{CBI} .

Identity rules:

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

Logical rules:

$$\begin{array}{cccc} \frac{\emptyset \vdash X}{\top \vdash X} (\top\text{L}) & \frac{}{\emptyset \vdash \top} (\top\text{R}) & \frac{\emptyset \vdash X}{\top^* \vdash X} (\top^*\text{L}) & \frac{}{\emptyset \vdash \top^*} (\top^*\text{R}) \\ \frac{}{\perp \vdash \emptyset} (\perp\text{L}) & \frac{X \vdash \emptyset}{X \vdash \perp} (\perp\text{R}) & \frac{}{\perp^* \vdash \emptyset} (\perp^*\text{L}) & \frac{X \vdash \emptyset}{X \vdash \perp^*} (\perp^*\text{R}) \\ \frac{\sharp F \vdash X}{\neg F \vdash X} (\neg\text{L}) & \frac{X \vdash \sharp F}{X \vdash \neg F} (\neg\text{R}) & \frac{\flat F \vdash X}{\sim F \vdash X} (\sim\text{L}) & \frac{X \vdash \flat F}{X \vdash \sim F} (\sim\text{R}) \\ \frac{F; G \vdash X}{F \wedge G \vdash X} (\wedge\text{L}) & \frac{X \vdash F \quad Y \vdash G}{X; Y \vdash F \wedge G} (\wedge\text{R}) & \frac{F, G \vdash X}{F * G \vdash X} (*\text{L}) & \frac{X \vdash F \quad Y \vdash G}{X, Y \vdash F * G} (*\text{R}) \\ \frac{F \vdash X \quad G \vdash Y}{F \vee G \vdash X; Y} (\vee\text{L}) & \frac{X \vdash F; G}{X \vdash F \vee G} (\vee\text{R}) & \frac{F \vdash X \quad G \vdash Y}{F \check{\vee} G \vdash X, Y} (\check{\vee}\text{L}) & \frac{X \vdash F, G}{X \vdash F \check{\vee} G} (\check{\vee}\text{R}) \\ \frac{X \vdash F \quad G \vdash Y}{F \rightarrow G \vdash \sharp X; Y} (\rightarrow\text{L}) & \frac{X; F \vdash G}{X \vdash F \rightarrow G} (\rightarrow\text{R}) & \frac{X \vdash F \quad G \vdash Y}{F \multimap G \vdash \flat X, Y} (\multimap\text{L}) & \frac{X, F \vdash G}{X \vdash F \multimap G} (\multimap\text{R}) \end{array}$$

Structural rules:

$$\begin{array}{cccc} \frac{W; (X; Y) \vdash Z}{(W; X); Y \vdash Z} (\text{AAL}) & \frac{W \vdash (X; Y); Z}{W \vdash X; (Y; Z)} (\text{AAR}) & \frac{W, (X, Y) \vdash Z}{(W, X), Y \vdash Z} (\text{MAL}) & \frac{W \vdash (X, Y), Z}{W \vdash X, (Y, Z)} (\text{MAR}) \\ \frac{\emptyset; X \vdash Y}{X \vdash Y} (\emptyset\text{L}) & \frac{X \vdash Y; \emptyset}{X \vdash Y} (\emptyset\text{R}) & \frac{\emptyset, X \vdash Y}{X \vdash Y} (\emptyset\text{L}) & \frac{X \vdash Y, \emptyset}{X \vdash Y} (\emptyset\text{R}) \\ \frac{X \vdash Z}{X; Y \vdash Z} (\text{WkL}) & \frac{X \vdash Z}{X \vdash Y; Z} (\text{WkR}) & \frac{X; X \vdash Z}{X \vdash Z} (\text{CtrL}) & \frac{X \vdash Z; Z}{X \vdash Z} (\text{CtrR}) \end{array}$$

Figure 3: The proof rules of DL_{CBI} . W, X, Y, Z range over structures, F, G range over CBI-formulas and P ranges over \mathcal{V} .

Theorem 4.8 (Cut-elimination). If a consecution $X \vdash Y$ is provable in DL_{CBI} then it is also provable without the use of (Cut).

Proof. By inspection, the DL_{CBI} proof rules satisfy the conditions shown by Belnap in [2] to be sufficient for cut-elimination to hold. We state these conditions and indicate how they are verified in Appendix A. \square

$$\begin{array}{c}
\text{(Proposition 4.7)} \\
\vdots \\
\frac{F \vdash F}{\#F \vdash \#F} (\equiv_D) \\
\frac{\#F \vdash \#F}{\#F \vdash \neg F} (\neg R) \\
\frac{\#F \vdash \neg F}{b\neg F \vdash b\#F} (\equiv_D) \\
\frac{b\neg F \vdash b\#F}{\sim\neg F \vdash b\#F} (\sim L) \\
\frac{\sim\neg F \vdash b\#F}{\sim\neg F; \sim F \vdash b\#F} (\text{WkL}) \\
\frac{\sim\neg F; \sim F \vdash b\#F}{bF \vdash b\#b(\sim\neg F; \sim F)} (\equiv_D) \\
\frac{bF \vdash b\#b(\sim\neg F; \sim F)}{\sim F \vdash b\#b(\sim\neg F; \sim F)} (\sim L) \\
\frac{\sim F \vdash b\#b(\sim\neg F; \sim F)}{\sim\neg F; \sim F \vdash b\#b(\sim\neg F; \sim F)} (\text{WkL}) \\
\frac{\sim\neg F; \sim F \vdash b\#b(\sim\neg F; \sim F)}{\#b(\sim\neg F; \sim F) \vdash b(\sim\neg F; \sim F)} (\equiv_D) \\
\frac{\#b(\sim\neg F; \sim F) \vdash b(\sim\neg F; \sim F)}{b\emptyset; \#b(\sim\neg F; \sim F) \vdash b(\sim\neg F; \sim F)} (\text{WkL}) \\
\frac{b\emptyset; \#b(\sim\neg F; \sim F) \vdash b(\sim\neg F; \sim F)}{b\emptyset \vdash b(\sim\neg F; \sim F); b(\sim\neg F; \sim F)} (\equiv_D) \\
\frac{b\emptyset \vdash b(\sim\neg F; \sim F); b(\sim\neg F; \sim F)}{b\emptyset \vdash b(\sim\neg F; \sim F)} (\text{CtrR}) \\
\frac{b\emptyset \vdash b(\sim\neg F; \sim F)}{\sim\neg F \vdash \# \sim F; \emptyset} (\equiv_D) \\
\frac{\sim\neg F \vdash \# \sim F; \emptyset}{\sim\neg F \vdash \# \sim F} (\emptyset R) \\
\frac{\sim\neg F \vdash \# \sim F}{\sim\neg F \vdash \neg \sim F} (\neg R)
\end{array}$$

Figure 4: A cut-free DL_{CBI} proof of $\sim\neg F \vdash \neg\sim F$.

The following corollary of Theorem 4.8 uses the notion of a *subformula* of a CBI-formula, defined in the usual way.

Corollary 4.9 (Subformula property). If $X \vdash Y$ is DL_{CBI} -provable then there is a DL_{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 4.8. By inspection of the DL_{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 $X \vdash Y$. \square

Corollary 4.10 (Consistency). Neither $\emptyset \vdash \emptyset$ nor $\emptyset \vdash \emptyset$ is provable in DL_{CBI} .

Proof. If $\emptyset \vdash \emptyset$ were DL_{CBI} -provable then, by the subformula property (Corollary 4.9) there is a proof of $\emptyset \vdash \emptyset$ containing no formula occurrences anywhere. But every axiom of DL_{CBI} contains a formula occurrence, so this is impossible. The same reasoning also shows that $\emptyset \vdash \emptyset$ is not DL_{CBI} -provable. \square

Our main technical results concerning DL_{CBI} are the following.

Proposition 4.11 (Soundness). If $X \vdash Y$ is DL_{CBI} -provable then it is valid.

Proof. It suffices to show that, if the conclusion of an instance of a DL_{CBI} rule is false in some CBI-model $M = \langle R, \circ, e, -, \infty \rangle$, then some premise of the rule is also false in M . In the case of the display rule (\equiv_D), this property follows by establishing that each display postulate (cf. Figure 2) has the property. We show how to deal with some sample rule cases.

*Case ($-*L$).* Suppose the conclusion $F -* G \vdash \text{b}X, Y$ is false in M , so that for some $r \in R$ and M -environment ρ we have $r \models_\rho F -* G$ but $r \not\models_\rho \sim\Psi_X \dot{\vee} \Upsilon_Y$. Using Lemma 2.9, it follows from the latter that $r \not\models_\rho \Psi_X -* \Upsilon_Y$, i.e., there exist $r', r'' \in R$ such that $r'' \in r \circ r'$ and $r' \models_\rho \Psi_X$ but $r'' \not\models_\rho \Upsilon_Y$. Then there are two cases to consider. First, if we have $r' \not\models_\rho F$ then, since $r' \models_\rho \Psi_X$, the premise $X \vdash F$ is false in M and we are done. Otherwise, we have $r' \models_\rho F$, and since we have both $r \models_\rho F -* G$ and $r'' \in r \circ r'$ we must have $r'' \models_\rho G$. Thus we have $r'' \models_\rho G$ and $r'' \not\models_\rho \Upsilon_Y$, so the premise $G \vdash Y$ is false in M and we are done.

Case ($\dot{\vee}L$). Suppose the conclusion $F \dot{\vee} G \vdash X, Y$ is false in M , i.e. for some ρ and $r \in R$ we have $r \models_\rho F \dot{\vee} G$ but $r \not\models_\rho \Upsilon_X \dot{\vee} \Upsilon_Y$. By the definition of satisfaction, we obtain from the latter that there exist $r_1, r_2 \in R$ such that $-r \in r_1 \circ r_2$ but $-r_1 \not\models_\rho \Upsilon_X$ and $-r_2 \not\models_\rho \Upsilon_Y$. So, if $-r_1 \models_\rho F$ then the premise $F \vdash X$ is false in M and we are done. Otherwise, $-r_1 \not\models_\rho F$ and, since we also have $r \models_\rho F \dot{\vee} G$ and $-r \in r_1 \circ r_2$, it follows that $-r_2 \models_\rho G$. Thus the premise $G \vdash Y$ is false in M and we are done.

Case (MAR). We show how to treat one direction of the rule; the reverse direction is symmetric. Suppose the conclusion $W \vdash X, (Y, Z)$ is false in M , i.e. for some ρ and $r \in R$ we have $r \models_\rho \Psi_W$ but $r \not\models_\rho \Upsilon_X \dot{\vee} (\Upsilon_Y \dot{\vee} \Upsilon_Z)$. By applying the equivalences given in Lemma 2.9 we obtain from the latter that $r \not\models_\rho \sim(\sim\Upsilon_X * (\sim\Upsilon_Y * \sim\Upsilon_Z))$. By the definition of satisfaction for $*$ and the associativity of \circ this is clearly equivalent to $r \not\models_\rho \sim((\sim\Upsilon_X * \sim\Upsilon_Y) * \sim\Upsilon_Z)$, which by Lemma 2.9 is again equivalent to $r \not\models_\rho (\Upsilon_X \dot{\vee} \Upsilon_Y) \dot{\vee} \Upsilon_Z$. Thus the premise $W \vdash (X, Y), Z$ is false in M as required.

Case ($MD1a$). We show how to treat one direction of this display postulate; the reverse direction is symmetric. Suppose the conclusion $X \vdash \text{b}Y, Z$ is false in M , i.e. for some ρ and $r \in R$ we have $r \models_\rho \Psi_X$ but $r \not\models_\rho \sim\Psi_Y \dot{\vee} \Upsilon_Z$. By Lemma 2.9, the latter is equivalent to $r \not\models_\rho \Psi_Y -* \Upsilon_Z$. So there exist $r', r'' \in R$ such that $r'' \in r \circ r'$ and $r' \models_\rho \Psi_Y$ but $r'' \not\models_\rho \Upsilon_Z$. Thus we have $r'' \models_\rho \Psi_X * \Psi_Y$ but $r'' \not\models_\rho \Upsilon_Z$, i.e. the premise $X, Y \vdash Z$ is false in M as required. \square

Theorem 4.12 (Completeness of DL_{CBI}). If $X \vdash Y$ is valid then it is provable in DL_{CBI} .

We give the proof of Theorem 4.12 in Section 5.

We remark that, although cut-free proofs in DL_{CBI} enjoy the subformula property, cut-free proof search in our system is still highly non-deterministic due to the presence of the display postulates and structural rules. In Figure 4 we give a sample cut-free proof of the consecution $\sim\neg F \vdash \neg\sim F$, which illustrates the problems. The applications of display-equivalence 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 plausible that the explicit use of at least some of these structural rules can be eliminated by suitable reformulations of the logical rules. However, proof search in such a refined version of the display system would likely still be very difficult.

This difficulty is not in the least surprising since, by soundness and completeness, the proof search problem in DL_{CBI} is equivalent to the decidability of CBI, and decidability of

bunched logics is known to be a hard problem. Galmiche, Méry and Pym established the decidability of BI [19], but the decidability of BBI is still open at the time of writing despite considerable attention. It seems plausible that the decision problem for CBI is at least as hard as for BBI, since its richer structure seemingly entails a greater number of combinatorial possibilities to consider during proof search. (Unfortunately, the decidability of an arbitrary logic with a display calculus presentation has itself been shown to be undecidable by Kracht [26].)

5. COMPLETENESS OF DL_{CBI}

In this section we prove completeness of our display calculus DL_{CBI} with respect to validity in CBI-models. As in the case of the analogous result for BBI in [11], our result hinges on an appeal to a general theorem of modal logic due to Sahlqvist. However, we also require an extra layer of translation between proofs in modal logic and proofs in DL_{CBI} .

Our proof is divided into three main parts. First, we show that, via a translation from CBI-formulas to modal logic formulas, CBI-models can be regarded as modal logic models satisfying certain axioms. Second, we appeal to Sahlqvist to obtain a complete modal logic proof theory for this class of models. Finally, we show how to translate this modal logic proof theory into DL_{CBI} . Thus we obtain the DL_{CBI} -provability of any valid consecution.

5.1. CBI-models as modal logic models. We first define ML_{CBI} pre-models, which interpret the CBI-model operations (cf. Definition 2.2) as modalities.

Definition 5.1.1. An ML_{CBI} *pre-model* is a tuple $\langle R, \circ, \multimap, e, -, \infty \rangle$, where $\circ : R \times R \rightarrow \mathcal{P}(R)$, $\multimap : R \times R \rightarrow \mathcal{P}(R)$, $e \subseteq R$, $- : R \rightarrow \mathcal{P}(R)$, and $\infty \subseteq R$. We extend \circ and $-$ to $\mathcal{P}(R) \times \mathcal{P}(R) \rightarrow \mathcal{P}(R)$ and $\mathcal{P}(R) \rightarrow \mathcal{P}(R)$ respectively in the same manner as in Definition 2.2.

Definition 5.1.2 (Modal logic formulas). Modal logic formulas A are defined by the grammar:

$$A ::= P \mid \top \mid \perp \mid \neg A \mid A \wedge A \mid A \vee A \mid A \rightarrow A \mid e \mid \infty \mid -A \mid A \circ A \mid A \multimap A$$

where P ranges over \mathcal{V} . We remark that we read $e, \infty, -, \circ, \multimap$ as *modalities* (with the obvious arities obtained by analogy to CBI-models). We regard \rightarrow as having weaker precedence than these modalities, and use parentheses to disambiguate where necessary.

The satisfaction relation for modal logic formulas in ML_{CBI} pre-models is defined exactly as the satisfaction relation for CBI-formulas in CBI-models for the additive connectives, and modalities are given a possibility interpretation :

$$\begin{aligned} r \models_{\rho} e &\Leftrightarrow r \in e \\ r \models_{\rho} \infty &\Leftrightarrow r \in \infty \\ r \models_{\rho} \neg A &\Leftrightarrow \exists r' \in R. r \in -(r') \text{ and } r' \models_{\rho} A \\ r \models_{\rho} A_1 \circ A_2 &\Leftrightarrow \exists r_1, r_2 \in R. r \in r_1 \circ r_2 \text{ and } r_1 \models_{\rho} A_1 \text{ and } r_2 \models_{\rho} A_2 \\ r \models_{\rho} A_1 \multimap A_2 &\Leftrightarrow \exists r_1, r_2 \in R. r \in r_1 \multimap r_2 \text{ and } r_1 \models_{\rho} A_1 \text{ and } r_2 \models_{\rho} A_2 \end{aligned}$$

Then, given any set \mathcal{A} of axioms, we define \mathcal{A} -*models* to be the ML_{CBI} pre-models in which every axiom in \mathcal{A} holds. Moreover, the \mathcal{A} -models in which e is a singleton set are called *unitary* \mathcal{A} -models.

Definition 5.1.3 (Modal logic axioms for CBI). The axiom set AX_{CBI} consists of the following modal logic formulas, where P, Q, R are propositional variables:

- | | |
|--|--|
| (1) $e \circ P \rightarrow P$ | (7) $R \wedge (P \dashv\bullet Q) \rightarrow (\top \dashv\bullet (Q \wedge (R \circ P)))$ |
| (2) $P \rightarrow e \circ P$ | (8) $--P \rightarrow P$ |
| (3) $P \circ Q \rightarrow Q \circ P$ | (9) $P \rightarrow --P$ |
| (4) $(P \circ Q) \circ R \rightarrow P \circ (Q \circ R)$ | (10) $-P \rightarrow (P \dashv\bullet \infty)$ |
| (5) $P \circ (Q \circ R) \rightarrow (P \circ Q) \circ R$ | (11) $(P \dashv\bullet \infty) \rightarrow -P$ |
| (6) $Q \wedge (R \circ P) \rightarrow (R \wedge (P \dashv\bullet Q)) \circ \top$ | |

Lemma 5.1.4. Let $\langle R, \circ, e, -, \infty \rangle$ be a tuple with the same types as in Definition 2.2, and extend $-$ and \circ pointwise to $\mathcal{P}(R) \rightarrow \mathcal{P}(R)$ and $\mathcal{P}(R) \times \mathcal{P}(R) \rightarrow \mathcal{P}(R)$ 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) $-X = X \dashv\bullet \infty$
- (3) $--X = X$

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

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 $x, y \in R$. \square

Lemma 5.1.5. Let $\langle R, \circ, \dashv\bullet, e, -, \infty \rangle$ be an unitary AX_{CBI} -model (so that e is a singleton set). Then ∞ is a singleton set, and $-x$ is a singleton set for any $x \in R$. Moreover, $\langle R, \circ, e, -, \infty \rangle$ is a CBI-model with the modalities $e, -, \infty$ regarded as having the appropriate types.

Proof. We first show that $-x$ is a singleton 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 $--x = \{x\}$.

We prove that ∞ is a singleton by deriving $\infty = -e$:

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

\square

Definition 5.1.6 (Embedding of CBI-models in AX_{CBI} -models). Let $M = \langle R, \circ, e, -, \infty \rangle$ be a CBI-model. The tuple $\lceil M \rceil = \langle R, \circ, \dashv\bullet, e, -, \infty \rangle$ is obtained by regarding the modalities $e, -, \infty$ as having the same types as in Definition 5.1.1 in the obvious way, and by defining $\dashv\bullet : R \times R \rightarrow \mathcal{P}(R)$ as $X \dashv\bullet Y =_{\text{def}} \{z \in R \mid \exists x \in X, y \in Y. y \in x \circ z\}$.

Lemma 5.1.7. If M is a CBI-model then $\lceil M \rceil$ is a unitary AX_{CBI} -model. Moreover, the function $\lceil - \rceil$ is a bijection between CBI-models and unitary AX_{CBI} -models.

Proof. First observe that in any ML_{CBI} pre-model $\langle R, \circ, \dashv, e, -, \infty \rangle$, the AX_{CBI} axioms 6 and 7 hold iff:

$$X \dashv Y = \{z \in R \mid \exists x \in X, y \in Y. y \in x \circ z\}$$

for all X, Y in $\mathcal{P}(R)$.

Let M be a CBI-model. Then axioms 6 and 7 hold in $\ulcorner M \urcorner$ by the above observation. The remaining AX_{CBI} axioms hold as a direct consequence of Lemma 5.1.4. Therefore $\ulcorner M \urcorner$ is a unitary AX_{CBI} -model.

It remains to show that $\ulcorner - \urcorner$ is a bijection. Injectivity is immediate by definition. For surjectivity, let $M' = \langle R, \circ, \dashv, e, -, \infty \rangle$ be a unitary AX_{CBI} model. By Lemma 5.1.5 we have that $\langle R, \circ, e, -, \infty \rangle$ is a CBI-model. Since the interpretation of \dashv is determined by \circ because of the above observation about axioms 6 and 7, it follows that $\ulcorner \langle R, \circ, e, -, \infty \rangle \urcorner = M'$, hence $\ulcorner - \urcorner$ is surjective. \square

Definition 5.1.8 (Translation of CBI-formulas to modal logic formulas). We define a function $\ulcorner - \urcorner$ from CBI-formulas to modal logic formulas by induction on the structure of CBI-formulas, as follows:

$$\begin{aligned} \ulcorner F \urcorner &= F && \text{where } F \in \{P, \top, \perp\} \\ \ulcorner \top^* \urcorner &= e \\ \ulcorner F_1 ? F_2 \urcorner &= \ulcorner F_1 \urcorner ? \ulcorner F_2 \urcorner && \text{where } ? \in \{\wedge, \vee, \rightarrow\} \\ \ulcorner F_1 * F_2 \urcorner &= \ulcorner F_1 \urcorner \circ \ulcorner F_2 \urcorner \\ \ulcorner F_1 \dashv F_2 \urcorner &= \neg(\ulcorner F_1 \urcorner \dashv \neg \ulcorner F_2 \urcorner) \\ \ulcorner \neg F \urcorner &= \neg \ulcorner F \urcorner \\ \ulcorner \perp^* \urcorner &= \neg \infty \\ \ulcorner \sim F \urcorner &= \neg \ulcorner F \urcorner \\ \ulcorner F_1 \star F_2 \urcorner &= \neg \neg (\neg \ulcorner F_1 \urcorner \circ \neg \ulcorner F_2 \urcorner) \end{aligned}$$

where P in the first clause ranges over \mathcal{V} . We extend the domain of $\ulcorner - \urcorner$ to DL_{CBI} conclusions by:

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

where Ψ_- and Υ_- are the functions given in Definition 4.3.

In the following, we write $F[G/P]$ to denote the result of substituting the formula G for all occurrences of the propositional variable P in the formula F . This notation applies both to CBI-formulas and to modal logic formulas.

Lemma 5.1.9. Let F be a CBI-formula, and $M = \langle R, \circ, e, -, \infty \rangle$ a CBI-model. Then F is true in M if and only if $\ulcorner F \urcorner$ is true in $\ulcorner M \urcorner$.

Proof. Let F be a CBI-formula and A a modal logic formula. We define $F \simeq A$ to hold iff for all environments ρ , and all $r \in R$, the following holds:

$$r \models_{\rho} F \text{ wrt. } M \Leftrightarrow r \models_{\rho} A \text{ wrt. } \ulcorner M \urcorner$$

The proof is divided into two parts. The first part establishes the following properties:

- (1) $F \simeq A$ and $G \simeq B$ implies $F[G/P] \simeq A[B/P]$
- (2) $\top^* \simeq e$
- (3) $P_1 * P_2 \simeq P_1 \circ P_2$
- (4) $P_1 \dashv P_2 \simeq \neg(P_1 \dashv \neg P_2)$
- (5) $\perp^* \simeq \neg \infty$
- (6) $\sim P \simeq \neg \neg P$

$$(7) P_1 \star P_2 \simeq \neg\neg(\neg\neg P_1 \circ \neg\neg P_2)$$

We show one interesting case (7). By Lemma 2.9 we have that $P_1 \star P_2$ is equivalent to $\sim(\sim P_1 * \sim P_2)$, therefore it is sufficient to prove $\sim(\sim P_1 * \sim P_2) \simeq \neg\neg(\neg\neg P_1 \circ \neg\neg P_2)$. By (6) we have $\sim P_i \simeq \neg\neg P_i$ for $i \in \{1, 2\}$, hence by (1) and (3) we obtain $(\sim P_1 * \sim P_2) \simeq (\neg\neg P_1 \circ \neg\neg P_2)$. Thus by (1) and (6) we conclude $\sim(\sim P_1 * \sim P_2) \simeq \neg\neg(\neg\neg P_1 \circ \neg\neg P_2)$, as required.

The second part establishes $F \simeq \ulcorner F \urcorner$ by induction on the structure of F , using the results from the first part. \square

Lemma 5.1.10. A consecution $X \vdash Y$ is valid wrt. CBI-models iff $\ulcorner \Psi_X \rightarrow \Upsilon_Y \urcorner$ is valid wrt. unitary AX_{CBI} -models.

Proof. By definition, $X \vdash Y$ is valid wrt. CBI-models iff $\Psi_X \rightarrow \Upsilon_Y$ is true in every CBI-model M . By Lemma 5.1.9, this is equivalent to:

$$\ulcorner \Psi_X \rightarrow \Upsilon_Y \urcorner \text{ is true in every CBI-model } M$$

Since $\ulcorner - \urcorner$ is a bijection on unitary AX_{CBI} -models by Lemma 5.1.7, this is equivalent to:

$$\ulcorner \Psi_X \rightarrow \Upsilon_Y \urcorner \text{ is true in every unitary } \text{AX}_{\text{CBI}}\text{-model } M'$$

i.e. $\ulcorner \Psi_X \rightarrow \Upsilon_Y \urcorner$ is valid wrt. unitary AX_{CBI} -models. \square

5.2. A complete modal logic proof theory for CBI.

Definition 5.2.1 (Modal Logic Proof Theory). The modal logic proof theory generated by a set \mathcal{A} of modal logic axioms, denoted by $\text{L}\mathcal{A}$, consists of a standard Hilbert proof system for propositional classical logic, extended with the following axioms and proof rules:

$$\begin{aligned} (\mathcal{A}) : & \quad \vdash A && \text{where } A \in \mathcal{A} \\ (-\perp) : & \quad \vdash \neg\perp \rightarrow \perp \\ (\circ\perp) : & \quad \vdash P \circ \perp \rightarrow \perp \\ (-\bullet\perp) : & \quad \vdash (\perp \rightarrow\bullet P) \vee (P \rightarrow\bullet \perp) \rightarrow \perp \\ (-\vee) : & \quad \vdash \neg(P \vee Q) \leftrightarrow \neg P \vee \neg Q \\ (\circ\vee) : & \quad \vdash (P \vee Q) \circ R \leftrightarrow (P \circ R) \vee (Q \circ R) \\ (-\bullet\vee\text{L}) : & \quad \vdash (P \vee Q) \rightarrow\bullet R \leftrightarrow (P \rightarrow\bullet R) \vee (Q \rightarrow\bullet R) \\ (-\bullet\vee\text{R}) : & \quad \vdash P \rightarrow\bullet (Q \vee R) \leftrightarrow (P \rightarrow\bullet Q) \vee (P \rightarrow\bullet R) \end{aligned}$$

$$\frac{\vdash A \rightarrow B \quad \vdash A}{\vdash B} \text{ (MP)} \quad \frac{\vdash A}{\vdash A[B/P]} \text{ (Subst)}$$

where A, B range over modal logic formulas, P, Q, R are propositional variables, and $A \leftrightarrow B$ is as usual an abbreviation for $(A \rightarrow B) \wedge (B \rightarrow A)$.

Definition 5.2.2 (Very Simple Sahlqvist Formulas). A *very simple Sahlqvist antecedent* S is a formula given by the grammar:

$$S ::= \top \mid \perp \mid P \mid S \wedge S \mid e \mid \infty \mid \neg S \mid S \circ S \mid S \rightarrow\bullet S$$

where P ranges over \mathcal{V} . A *very simple Sahlqvist formula* is a modal logic formula of the form $S \rightarrow A^+$, where S is a very simple Sahlqvist antecedent and A^+ is a modal logic formula

which is *positive* in that no propositional variable P in A^+ may occur inside the scope of an odd number of occurrences of \neg .

Theorem 5.2.3 (Sahlqvist [4]). For every set \mathcal{A} of modal logic axioms consisting only of very simple Sahlqvist formulas, the modal logic proof theory $L\mathcal{A}$ is complete with respect to the class of \mathcal{A} -models.

By inspection we can observe that the AX_{CBI} axioms (cf. Definition 5.1.3) are all very simple Sahlqvist formulas, whence we obtain from Theorem 5.2.3:

Corollary 5.2.4. $L\text{AX}_{\text{CBI}}$ is complete with respect to the class of AX_{CBI} -models.

We show that the completeness result transfers to unitary AX_{CBI} -models.

Lemma 5.2.5. Let $M = \langle R, \circ, \dashv, e, -, \infty \rangle$ be an AX_{CBI} model. Then there exist unitary AX_{CBI} -models M_x for each $x \in e$ such that the following hold:

- (1) M is the disjoint union of the models M_x for $x \in e$.
- (2) A formula A is valid in M iff it is valid in M_x for all $x \in e$.

Proof. For each $x \in e$, the model M_x is defined by restricting M to $R_x =_{\text{def}} \{r \in R \mid \{r\} \circ \{x\} \neq \emptyset\}$. Disjointness of models follows directly from the fact that $\langle R, \circ, e \rangle$ obeys the first five axioms of AX_{CBI} , which characterize relational commutative monoids. Finally, (1) \Rightarrow (2) is a general result which holds in modal logic [4]. \square

Corollary 5.2.6. $L\text{AX}_{\text{CBI}}$ is complete with respect to the class of unitary AX_{CBI} -models.

5.3. From modal logic proofs to DL_{CBI} proofs.

Definition 5.3.1 (Translation from modal logic formulas to CBI-formulas). We define a function $\llcorner _ \lrcorner$ from modal logic formulas to CBI-formulas by induction on the structure of CBI-formulas, as follows:

$$\begin{aligned}
\llcorner A \lrcorner &= A && \text{where } A \in \{P, \top, \perp\} \\
\llcorner \neg A \lrcorner &= \neg \llcorner A \lrcorner \\
\llcorner A_1 ? A_2 \lrcorner &= \llcorner A_1 \lrcorner ? \llcorner A_2 \lrcorner && \text{where } ? \in \{\wedge, \vee, \rightarrow\} \\
\llcorner A_1 \circ A_2 \lrcorner &= \llcorner A_1 \lrcorner * \llcorner A_2 \lrcorner \\
\llcorner A_1 \dashv A_2 \lrcorner &= \neg(\llcorner A_1 \lrcorner \dashv \llcorner A_2 \lrcorner) \\
\llcorner e \lrcorner &= \top^* \\
\llcorner \neg A \lrcorner &= \neg \sim \llcorner A \lrcorner \\
\llcorner \infty \lrcorner &= \neg \perp^*
\end{aligned}$$

Proposition 5.3.2. The axioms and proof rules of $L\text{AX}_{\text{CBI}}$ (cf. Defn. 5.2.1) are admissible in DL_{CBI} under the embedding $- \mapsto (\emptyset \vdash \llcorner _ \lrcorner)$. That is, for any axiom $\vdash A$ of $L\text{AX}_{\text{CBI}}$ the consecution $\emptyset \vdash \llcorner A \lrcorner$ is DL_{CBI} -provable, and the following two proof rules are admissible in DL_{CBI} :

$$\frac{\emptyset \vdash F \rightarrow G \quad \emptyset \vdash F}{\emptyset \vdash G} \text{ (MP)} \qquad \frac{\emptyset \vdash F}{\emptyset \vdash F[G/P]} \text{ (Subst)}$$

Proof. First, we note that the proof rule (MP) is easily derivable in DL_{CBI} using (Cut), and the rule (Subst) is admissible in DL_{CBI} because each of its proof rules is closed under the substitution of arbitrary formulas for propositional variables (in the case of the axiom rule (Id) this requires an appeal to Proposition 4.7).

It remains to show that $\emptyset \vdash \lfloor A \rfloor$ is DL_{CBI} -derivable for every axiom $\vdash A$ of LAX_{CBI} . The AX_{CBI} axioms are mainly straightforward, with the chief exceptions being axioms (6) and (7). (We remark that axioms (8) and (9) are straightforward once one has DL_{CBI} proofs that \neg and \sim commute; see Figure 4 for a proof of $\sim\neg F \vdash \neg\sim F$.) In the case of AX_{CBI} axiom (6), we need to show the consecution $\emptyset \vdash Q \wedge (R * P) \rightarrow (R \wedge \neg(P \multimap \neg Q)) * \top$ is provable in DL_{CBI} . We give a suitable derivation in Figure 5. The treatment of AX_{CBI} axiom (7) is broadly similar. It remains to treat the generic modal logic axioms of LAX_{CBI} , which again are mainly straightforward and involve showing distribution of the modalities over \vee . E.g., in the case of the axiom $(\rightarrow\bullet\vee\text{L})$ we require to show that $\emptyset \vdash \neg((P \vee Q) \multimap \neg R) \leftrightarrow \neg(P \multimap \neg R) \vee \neg(Q \multimap \neg R)$ is DL_{CBI} -derivable. We give a derivation of one direction of this bi-implication in Figure 6. The other direction of the bi-implication, and the other axioms, are derived in a similar fashion. \square

The following corollary of Proposition 5.3.2 is immediate by induction over the structure of LAX_{CBI} proofs.

Corollary 5.3.3. If $\vdash A$ is provable in LAX_{CBI} then $\emptyset \vdash \lfloor A \rfloor$ is provable in DL_{CBI} .

We write $F \dashv\vdash G$, where F and G are CBI-formulas, to mean that both $F \vdash G$ and $G \vdash F$ are provable (in DL_{CBI}), and call $F \dashv\vdash G$ a *derivable equivalence* (of DL_{CBI}). We observe that derivable equivalence in DL_{CBI} is indeed an equivalence relation: it is reflexive by Proposition 4.7, symmetric by definition and transitive by the DL_{CBI} rule (Cut).

Lemma 5.3.4. $F \dashv\vdash \lceil F \rceil$ is a derivable equivalence of DL_{CBI} for any CBI-formula F .

Proof. By combining the definitions of $\lceil - \rceil$ and $\lfloor - \rfloor$ (cf. Defns. 5.1.8 and 5.3.1) we obtain the following definition of $\lceil - \rceil$, given by structural induction on CBI-formulas:

$$\begin{aligned} \lceil F \rceil &= F && \text{where } F \in \{P, \top, \perp, \top^*\} \\ \lceil \neg F \rceil &= \neg \lceil F \rceil \\ \lceil F_1 ? F_2 \rceil &= \lceil F_1 \rceil ? \lceil F_2 \rceil && \text{where } ? \in \{\wedge, \vee, \rightarrow, *\} \\ \lceil \perp^* \rceil &= \neg\neg\perp^* \\ \lceil \sim F \rceil &= \neg\neg\sim \lceil F \rceil \\ \lceil F_1 \multimap F_2 \rceil &= \neg\neg(\lceil F_1 \rceil \multimap \neg\neg \lceil F_2 \rceil) \\ \lceil F_1 \check{\vee} F_2 \rceil &= \neg\neg\sim(\neg\neg\sim \lceil F_1 \rceil * \neg\neg\sim \lceil F_2 \rceil) \end{aligned}$$

With this in mind, we now proceed by structural induction on F . The base cases, in which $\lceil F \rceil = F$, are immediate since $F \dashv\vdash F$ is a derivable equivalence of DL_{CBI} by Proposition 4.7. Most of the other cases are straightforward using the induction hypothesis and the fact that $\neg\neg F \dashv\vdash F$ is easily seen to be a derivable equivalence of DL_{CBI} . We show one direction of the only non-trivial case, $F = F_1 \check{\vee} F_2$, in Figure 7. The reverse direction is similar. \square

We remark that the following two lemmas, which show how to construct proofs of arbitrary valid consecutions given proofs of arbitrary valid formulas, use techniques first employed by Goré [22].

Lemma 5.3.5. For any structure X the consecutions $X \vdash \Psi_X$ and $\Upsilon_X \vdash X$ are both DL_{CBI} -provable.

Proof. By structural induction on X . The case where X is a formula F follows directly from Proposition 4.7. The other cases all follow straightforwardly from the induction hypothesis

$$\begin{array}{c}
\text{(Prop. 4.7)} \\
\vdots \\
\frac{Q \vdash Q}{\#Q \vdash \#Q} (\equiv_D) \\
\frac{\#Q \vdash \#Q}{\neg Q \vdash \#Q} (\neg L) \\
\text{(Prop. 4.7)} \\
\vdots \\
\frac{P \vdash P \quad \neg Q \vdash \#Q; (R \wedge \neg(P \multimap \neg Q)) * \top}{\neg Q \vdash \#Q; (R \wedge \neg(P \multimap \neg Q)) * \top} (\text{WkR}) \\
\frac{\neg Q \vdash \#Q; (R \wedge \neg(P \multimap \neg Q)) * \top}{P \multimap \neg Q \vdash \#P} (*L) \\
\text{(Prop. 4.7)} \\
\vdots \\
\frac{R \vdash R \quad \#(bP, (\#Q; (R \wedge \neg(P \multimap \neg Q)) * \top)) \vdash \#P \multimap \neg Q}{\#(bP, (\#Q; (R \wedge \neg(P \multimap \neg Q)) * \top)) \vdash \neg(P \multimap \neg Q)} (\equiv_D) \quad \frac{}{\emptyset \vdash \top} (\top R) \\
\frac{\#(bP, (\#Q; (R \wedge \neg(P \multimap \neg Q)) * \top)) \vdash \neg(P \multimap \neg Q)}{\#(bP, (\#Q; (R \wedge \neg(P \multimap \neg Q)) * \top)) \vdash (R \wedge \neg(P \multimap \neg Q))} (\neg R) \quad \frac{}{\emptyset; P \vdash \top} (\text{WkR}) \\
\frac{\#(bP, (\#Q; (R \wedge \neg(P \multimap \neg Q)) * \top)) \vdash (R \wedge \neg(P \multimap \neg Q))}{R; \#(bP, (\#Q; (R \wedge \neg(P \multimap \neg Q)) * \top)) \vdash (R \wedge \neg(P \multimap \neg Q))} (\wedge R) \quad \frac{}{P \vdash \top} (\emptyset R) \\
\frac{R; \#(bP, (\#Q; (R \wedge \neg(P \multimap \neg Q)) * \top)) \vdash (R \wedge \neg(P \multimap \neg Q))}{(R; \#(bP, (\#Q; (R \wedge \neg(P \multimap \neg Q)) * \top))), P \vdash (R \wedge \neg(P \multimap \neg Q)) * \top} (*R) \\
\frac{(R; \#(bP, (\#Q; (R \wedge \neg(P \multimap \neg Q)) * \top))), P \vdash (R \wedge \neg(P \multimap \neg Q)) * \top}{(R; \#(bP, (\#Q; (R \wedge \neg(P \multimap \neg Q)) * \top))), P \vdash \#Q; (R \wedge \neg(P \multimap \neg Q)) * \top} (\text{WkR}) \\
\frac{(R; \#(bP, (\#Q; (R \wedge \neg(P \multimap \neg Q)) * \top))), P \vdash \#Q; (R \wedge \neg(P \multimap \neg Q)) * \top}{R \vdash (bP, (\#Q; (R \wedge \neg(P \multimap \neg Q)) * \top)); (bP, (\#Q; (R \wedge \neg(P \multimap \neg Q)) * \top))} (\equiv_D) \\
\frac{R \vdash (bP, (\#Q; (R \wedge \neg(P \multimap \neg Q)) * \top)); (bP, (\#Q; (R \wedge \neg(P \multimap \neg Q)) * \top))}{\emptyset \vdash Q \wedge (R * P) \rightarrow (R \wedge \neg(P \multimap \neg Q)) * \top} (\text{CtrR}) \\
\frac{R \vdash bP, (\#Q; (R \wedge \neg(P \multimap \neg Q)) * \top)}{R, P \vdash \#Q; (R \wedge \neg(P \multimap \neg Q)) * \top} (\equiv_D) \\
\frac{R, P \vdash \#Q; (R \wedge \neg(P \multimap \neg Q)) * \top}{R * P \vdash \#Q; (R \wedge \neg(P \multimap \neg Q)) * \top} (*L) \\
\frac{R * P \vdash \#Q; (R \wedge \neg(P \multimap \neg Q)) * \top}{Q; R * P \vdash (R \wedge \neg(P \multimap \neg Q)) * \top} (\equiv_D) \\
\frac{Q; R * P \vdash (R \wedge \neg(P \multimap \neg Q)) * \top}{Q \wedge (R * P) \vdash (R \wedge \neg(P \multimap \neg Q)) * \top} (\wedge L) \\
\frac{Q \wedge (R * P) \vdash (R \wedge \neg(P \multimap \neg Q)) * \top}{\emptyset; Q \wedge (R * P) \vdash (R \wedge \neg(P \multimap \neg Q)) * \top} (\emptyset L) \\
\frac{\emptyset; Q \wedge (R * P) \vdash (R \wedge \neg(P \multimap \neg Q)) * \top}{\emptyset \vdash Q \wedge (R * P) \rightarrow (R \wedge \neg(P \multimap \neg Q)) * \top} (\rightarrow R)
\end{array}$$

Figure 5: A DL_{CBI} derivation of the LAX_{CBI} axiom (6) under the embedding $- \mapsto (\emptyset \vdash \underline{\quad})$, needed for the proof of Proposition 5.3.2.

and the logical rules of DL_{CBI} . E.g., when $X = bY$ we have $\Psi_X = \sim\Upsilon_Y$ and $\Upsilon_X = \sim\Psi_Y$, and proceed as follows:

$$\begin{array}{cc}
\text{(I.H.)} & \text{(I.H.)} \\
\vdots & \vdots \\
\frac{\Upsilon_Y \vdash Y}{bY \vdash b\Upsilon_Y} (\equiv_D) & \frac{Y \vdash \Psi_Y}{b\Psi_Y \vdash bY} (\equiv_D) \\
\frac{bY \vdash b\Upsilon_Y}{bY \vdash \sim\Upsilon_Y} (\sim R) & \frac{b\Psi_Y \vdash bY}{\sim\Psi_Y \vdash bY} (\sim L)
\end{array}$$

The remaining cases are similar. □

Lemma 5.3.6. If $\emptyset \vdash \lceil \Psi_X \rightarrow \Upsilon_Y \rceil$ is DL_{CBI} -provable then so is $X \vdash Y$.

$$\begin{array}{c}
\text{(I.H.)} \\
\vdots \\
\frac{F_1 \vdash \ulcorner F_1 \urcorner}{\text{b}\ulcorner F_1 \urcorner \vdash \text{b}F_1} (\equiv_D) \\
\frac{\text{b}\ulcorner F_1 \urcorner \vdash \text{b}F_1}{\sim\ulcorner F_1 \urcorner \vdash \text{b}F_1} (\sim\text{L}) \\
\frac{\sim\ulcorner F_1 \urcorner \vdash \text{b}F_1}{\#\text{b}F_1 \vdash \#\sim\ulcorner F_1 \urcorner} (\equiv_D) \\
\frac{\#\text{b}F_1 \vdash \#\sim\ulcorner F_1 \urcorner}{\#\text{b}F_1 \vdash \neg\sim\ulcorner F_1 \urcorner} (\neg\text{R}) \\
\frac{\#\text{b}F_1 \vdash \neg\sim\ulcorner F_1 \urcorner}{\#\neg\sim\ulcorner F_1 \urcorner \vdash \text{b}F_1} (\equiv_D) \\
\frac{\#\neg\sim\ulcorner F_1 \urcorner \vdash \text{b}F_1}{\neg\neg\sim\ulcorner F_1 \urcorner \vdash \text{b}F_1} (\neg\text{L}) \\
\frac{\neg\neg\sim\ulcorner F_1 \urcorner \vdash \text{b}F_1}{F_1 \vdash \text{b}\neg\neg\sim\ulcorner F_1 \urcorner} (\equiv_D) \\
\hline
\frac{F_1 \checkmark F_2 \vdash \text{b}\neg\neg\sim\ulcorner F_1 \urcorner, \text{b}\neg\neg\sim\ulcorner F_2 \urcorner}{\neg\neg\sim\ulcorner F_1 \urcorner, \neg\neg\sim\ulcorner F_2 \urcorner \vdash \text{b}F_1 \checkmark F_2} (\equiv_D) \\
\frac{\neg\neg\sim\ulcorner F_1 \urcorner, \neg\neg\sim\ulcorner F_2 \urcorner \vdash \text{b}F_1 \checkmark F_2}{\neg\neg\sim\ulcorner F_1 \urcorner * \neg\neg\sim\ulcorner F_2 \urcorner \vdash \text{b}F_1 \checkmark F_2} (*\text{L}) \\
\frac{\neg\neg\sim\ulcorner F_1 \urcorner * \neg\neg\sim\ulcorner F_2 \urcorner \vdash \text{b}F_1 \checkmark F_2}{F_1 \checkmark F_2 \vdash \text{b}\neg\neg\sim\ulcorner F_1 \urcorner * \neg\neg\sim\ulcorner F_2 \urcorner} (\equiv_D) \\
\frac{F_1 \checkmark F_2 \vdash \text{b}\neg\neg\sim\ulcorner F_1 \urcorner * \neg\neg\sim\ulcorner F_2 \urcorner}{F_1 \checkmark F_2 \vdash \sim(\neg\neg\sim\ulcorner F_1 \urcorner * \neg\neg\sim\ulcorner F_2 \urcorner)} (\sim\text{R}) \\
\frac{F_1 \checkmark F_2 \vdash \sim(\neg\neg\sim\ulcorner F_1 \urcorner * \neg\neg\sim\ulcorner F_2 \urcorner)}{\#\sim(\neg\neg\sim\ulcorner F_1 \urcorner * \neg\neg\sim\ulcorner F_2 \urcorner) \vdash \#\text{b}F_1 \checkmark F_2} (\equiv_D) \\
\frac{\#\sim(\neg\neg\sim\ulcorner F_1 \urcorner * \neg\neg\sim\ulcorner F_2 \urcorner) \vdash \#\text{b}F_1 \checkmark F_2}{\neg\sim(\neg\neg\sim\ulcorner F_1 \urcorner * \neg\neg\sim\ulcorner F_2 \urcorner) \vdash \#\text{b}F_1 \checkmark F_2} (\neg\text{L}) \\
\frac{\neg\sim(\neg\neg\sim\ulcorner F_1 \urcorner * \neg\neg\sim\ulcorner F_2 \urcorner) \vdash \#\text{b}F_1 \checkmark F_2}{F_1 \checkmark F_2 \vdash \#\neg\sim(\neg\neg\sim\ulcorner F_1 \urcorner * \neg\neg\sim\ulcorner F_2 \urcorner)} (\equiv_D) \\
\frac{F_1 \checkmark F_2 \vdash \#\neg\sim(\neg\neg\sim\ulcorner F_1 \urcorner * \neg\neg\sim\ulcorner F_2 \urcorner)}{F_1 \checkmark F_2 \vdash \neg\neg\sim(\neg\neg\sim\ulcorner F_1 \urcorner * \neg\neg\sim\ulcorner F_2 \urcorner)} (\neg\text{R})
\end{array}$$

Figure 7: A DL_{CBI} proof for the non-trivial case of Lemma 5.3.4.

□

We can now prove the completeness of DL_{CBI} with respect to CBI-validity.

Proof of Theorem 4.12. Suppose that $X \vdash Y$ is a valid consecution, i.e., that $\Psi_X \rightarrow \Upsilon_Y$ is a valid CBI-formula. Then $\ulcorner \Psi_X \rightarrow \Upsilon_Y \urcorner$ is valid with respect to unitary AX_{CBI} -models by Lemma 5.1.10, and so is LAX_{CBI} -provable by Corollary 5.2.6. By Corollary 5.3.3, $\emptyset \vdash \ulcorner \Psi_X \rightarrow \Upsilon_Y \urcorner$ is then provable in DL_{CBI} and thus, by Lemma 5.3.6, $X \vdash Y$ is then DL_{CBI} -provable as required.

6. RELATED AND FUTURE WORK

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

Bunched logics: In his monograph on BI [31], Pym observes that it makes sense to think not of one bunched logic but rather a family of bunched logics, characterised by the strengths of their additive and multiplicative components. We reprise his diagram of the bunched logic family, suitably updated, in Figure 8. CBI is the strongest version of bunched logic, boasting two classical negations and being characterised by an underlying Boolean algebra in its additive component and a de Morgan algebra in the multiplicative component. Indeed, Pym anticipated the formulation of CBI as presented here in at least two important respects: firstly, he observed that a relevantist approach to multiplicative negation (which we take by using the involution operation ‘ $-$ ’ in our models in place of the Routley star) is classically compatible with the other multiplicative connectives; and, secondly, he noted the problems with cut-elimination seemingly inherent in a two-sided sequent calculus for a classical bunched logic. In this paper, we provide the missing links in the shape of a well-behaved proof theory and, perhaps more importantly, the connection to algebraic resource models with precisely the structure necessary to interpret CBI. Our soundness and completeness results establishing the correspondence between the two, plus cut-elimination for the display calculus DL_{CBI} , can be taken as strong evidence that the formulation of CBI we present here is in some sense canonical.

We remark that there seemingly ought to exist a bunched logic, which we call DMBI (for “de Morgan BI”) in the diagram, which combines intuitionistic additives with classical multiplicatives. To our knowledge this logic has not yet been investigated at all, but it appears likely that it is very closely related to the relevant logic RW (also known as C), as Restall’s display calculus for the latter in [33] is seemingly also the display calculus that most naturally corresponds to DMBI. (RW does not normally include the intuitionistic additive implication and falsity, but Restall showed that these can be added conservatively.) Semantically, DMBI presumably could employ a similar involutive monoid structure to that of CBI-models in order to give a resource reading to the multiplicatives, with the additives being interpreted using standard techniques such as Kripke models. A potentially interesting issue is whether the additive and multiplicative negations can be suitably decoupled in such models, since, in CBI, the multiplicative negation \sim implicitly relies upon a classical notion of additive negation in order for \sim itself to behave classically. (Of course, it also seems likely that the frame semantics of RW will transfer directly to DMBI.)

Display calculi: The use of display logic to formulate sensible proof systems for substructural logics is not new, and indeed could be said to be the main intention behind Belnap’s original formulation of display logic [2], in which the choice of structural rules for a particular logic are identified as the principal factor affecting cut-elimination. Our formulation of DL_{CBI} , and its cut-elimination theorem, are obtained by following Belnap’s original methodology. However, we note that Goré has shown how to automatically generate display calculi for a general class of substructural logics [23], and it seems more than likely that his techniques could have equally well have been used to obtain DL_{CBI} . Notwithstanding these previous developments, our formulation of DL_{CBI} represents the first explicit application of display logic to bunched logics; the first author has subsequently obtained similarly well-behaved display calculi for all four bunched logics [5]. The inclusion of meta-level negation in consecutions is essential in formulating DL_{CBI} , and we suspect that it is exactly the absence

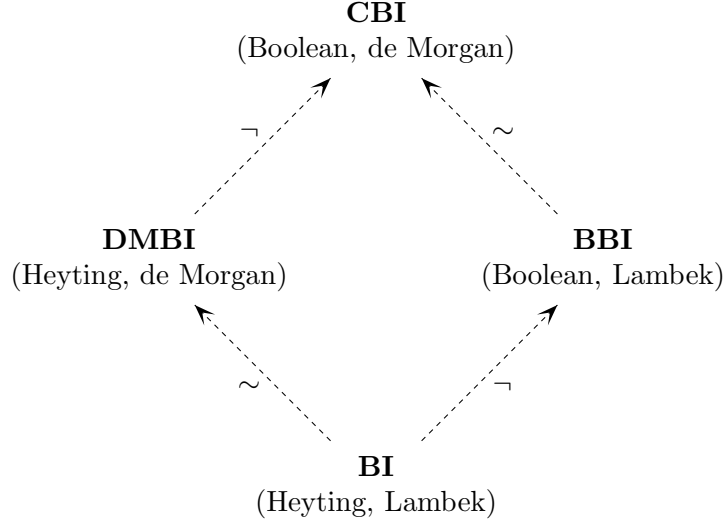


Figure 8: The bunched logic family. The (additive, multiplicative) subtitles denote the strength of the underlying additive and multiplicative algebras. The arrows denote the addition of either additive (\neg) or multiplicative (\sim) classical negation.

of classical negation in BI that enables cut-elimination to go through in its bunched sequent calculus. Indeed, the display system corresponding to BI turns out to be a simple reformulation of this calculus.

It should be borne in mind, however, that even though cut-elimination in DL_{CBI} entails a subformula property, it does not entail a “substructure property”, and the structural and display rules will cause obvious problems for proof search. This should come as no surprise, since many displayable logics are undecidable; indeed, one of Belnap’s original applications of display logic was in giving a display calculus for relevant logic, which was famously proven undecidable by Urquhart [39]. Nonetheless, we argue that there are very good reasons to prefer DL_{CBI} over arbitrary complete proof systems. Display calculi inherit the main virtues of traditional Gentzen systems: they distinguish structural principles from logical ones, and make explicit the considerable proof burden that exists at the meta-level, but nevertheless retain a theoretically very elegant and symmetric presentation. Furthermore, as a result of the subformula property one has in display calculi what might be called a property of “finite choice” for proof search: for any consecution there are only finitely many ways of applying any rule to it in a backwards fashion⁶. The difficulty, as in linear and relevant logics, is that it is unclear whether or not there exists a finite bound on the length of any particular branch in an exhaustive proof search, i.e., whether DL_{CBI} (and thus CBI) is decidable. On the one hand, it seems intuitively plausible that, given any consecution, there is only a finite amount of non-redundant information that can be extracted from it during a proof search, so every branch must eventually reach a point where no more non-redundant information can be added. On the other hand, it is far from clear whether this “saturation” can actually be detected, since in general there are many semantically equivalent but syntactically distinct structures that can arise during proof search. We also note that another potential route

⁶In fact, this is not quite true as it stands because for any consecution there are infinitely many consecutions that are display-equivalent to it, obtained by “stacking” occurrences of \sharp and \flat . However, by identifying structures such as $\sharp\sharp X$ and X , one obtains only finitely many display-equivalent consecutions. See e.g. [34].

to decidability of CBI would be via a finite model property but, unfortunately, we have no idea whether such a property holds.

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) [38]. The differences between the two are intuitively obvious when comparing our money model of CBI (Example 3.1) alongside Girard’s corresponding Marlboro / Camel example [21]. In particular, formulas in our model 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 (see [28] for a discussion), and indeed it seems that the main differences between CBI and CLL are inherited from the wider differences between bunched logic and linear logic in general. These differences are not merely conceptual, but are also manifested at the technical level of logical consequence. For example, $P \multimap Q \vdash P \rightarrow Q$ is a theorem of linear logic for any propositions P and Q , via the encoding of additive implication $P \rightarrow Q$ as $!P \multimap Q$, but $P \multimap Q \vdash P \rightarrow Q$ is not a theorem of bunched logic. Similarly, distributivity of additive conjunction over additive disjunction holds in bunched logics, but fails in linear logics.

Interestingly, however, there is an intersection between CBI-models and the CLL-models obtained from the *phase semantics* of classical linear logic [21]. 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” \perp to be the set $R \setminus \{\infty\}$, whence the linear negation X^\perp 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 $(X^\perp)^\perp = --X = X$. 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 (or indeed relational). 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.

Applications: The main application of BBI so far has been the use of separation logic in program analysis. There are now several program analysis tools [12, 13, 16, 40, 27] which use logical and semantic properties of the heap model of BBI at their core. These tools typically 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 relevant in this area as a foundation for richer resource models. In this paper we have already given several new models and model constructions which, though relatively simple in their present form, are suggestive of the applicability of CBI to more complex domains (cf. Section 3). In particular, we have observed that several models introduced recently for reasoning about concurrent access to resources are CBI models, e.g. fractional permissions as used in deny-guarantee reasoning (cf. Example 3.12).

More speculatively, our display calculus DL_{CBI} might form a basis for the design of new theorem provers, which could easily employ the powerful (and historically difficult to use) implication $-*$ 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 [10] 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.

Finally, CBI could be applied to the study of other logics. For example, Kleene’s 3-valued logic [25] can be modelled using a subset of CBI’s connectives. Consider the two-element CBI model given by $\langle \{e, \infty\}, \circ, e, -, \infty \rangle$, where $\infty \circ \infty = \emptyset$ (note that \circ and $-$ are then determined by the CBI-model axioms). There are CBI-formulas denoting each of the subsets of $\{e, \infty\}$: $\top, \perp, \top^*, \infty$ (where ∞ is used as an abbreviation for $\neg\perp^*$). To model 3-valued logic we focus on \top, \perp, ∞ , with ∞ playing the role of the third logical value, “unknown”. A direct calculation shows that the connectives \wedge, \vee , and \sim indeed generate the truth tables required by 3-valued logic. For example, we have $\infty \vee \sim\infty = \infty \vee \infty = \infty$. We speculate that CBI could be applied to other situations in logic where a non-standard notion of negation is used.

We believe that, aside from its intrinsic technical interest, our development of CBI contributes to the picture of bunched logic and its connections to computer science as a whole, as well as to the broader area of substructural logics in general. Although our suggestions regarding specific applications of CBI are necessarily still somewhat speculative at this early stage in its existence, we hope that the foundations established in this paper will provide a solid platform upon which such applications can, in time, be constructed.

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, Greg Restall, Alex Simpson, and the members of the East London Massive for useful discussions and feedback.

REFERENCES

- [1] Samson Abramsky. Computational interpretations of linear logic. *Theoretical Computer Science*, 111(1-2):3–57, 1993.
- [2] Nuel D. Belnap, Jr. Display logic. *Journal of Philosophical Logic*, 11:375–417, 1982.
- [3] Josh Berdine and Peter O’Hearn. Strong update, disposal and encapsulation in bunched typing. In *Proceedings of MFPS, ENTCS*. Elsevier, 2006.
- [4] Patrick Blackburn, Maarten de Rijke, and Yde Venema. *Modal Logic*. Cambridge University Press, 2001.
- [5] James Brotherston. Bunched logics displayed. Forthcoming, 2009.
- [6] James Brotherston. A cut-free proof theory for Boolean BI (via display logic). Unpublished note; available from <http://www.doc.ic.ac.uk/~jbrother>, 2009.

- [7] 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.
- [8] James Brotherston and Cristiano Calcagno. Classical BI (A logic for reasoning about dualising resource). In *Proceedings of POPL-36*, pages 328–339, 2009.
- [9] Kai Br unnler. Deep inference and its normal form of derivations. In *Proceedings of CiE*, volume 3988 of *LNCS*, pages 65–74, 2006.
- [10] Cristiano Calcagno, Dino Distefano, Peter O’Hearn, and Hongseok Yang. Compositional shape analysis by means of bi-abduction. In *Proceedings of POPL-36*, pages 289–300, 2009.
- [11] Cristiano Calcagno, Philippa Gardner, and Uri Zarfaty. Context logic as modal logic: Completeness and parametric inexpressivity. In *Proceedings of POPL-34*, 2007.
- [12] Cristiano Calcagno, Matthew Parkinson, and Viktor Vafeiadis. Modular safety checking for fine-grained concurrency. In *Proceedings of SAS-14*, LNCS. Springer, 2007.
- [13] Bor-Yuh Evan Chang and Xavier Rival. Relational inductive shape analysis. In *Proceedings of POPL-35*, 2008.
- [14] Wei-Ngan Chin, Cristina David, Huu Hai Nguyen, and Shengchao Qin. Enhancing modular OO verification with separation logic. In *Proceedings of POPL-35*, 2008.
- [15] Matthew Collinson, David Pym, and Edmund Robinson. Bunched polymorphism. *Mathematical Structures in Computer Science*, 18(6):1091–1132, 2008.
- [16] Dino Distefano and Matthew Parkinson. jStar: Towards practical verification for Java. In *Proceedings of OOPSLA*, pages 213–226. ACM, 2008.
- [17] Mike Dodds, Xinyu Feng, Matthew Parkinson, and Viktor Vafeiadis. Deny-guarantee reasoning. In *Proceedings of 18th ESOP*, volume 5502 of *LNCS*, pages 363–377. Springer-Verlag, 2009.
- [18] Michael Dunn. Star and perp: Two treatments of negation. *Philosophical Perspectives*, 7:331–357, 1993.
- [19] D. Galmiche, D. Mery, and D. Pym. The semantics of BI and resource tableaux. *Mathematical Structures in Computer Science*, 15:1033–1088, 2005.
- [20] Didier Galmiche and Dominique Larchey-Wendling. Expressivity properties of Boolean BI through relational models. In *Proceedings of FSTTCS*, 2006.
- [21] 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.
- [22] Rajeev Gor . On the completeness of classical modal display logic. In Heinrich Wansing, editor, *Proof Theory of Modal Logic*, pages 137–140. Kluwer Academic Publishers, 1996.
- [23] Rajeev Gor . Gaggles, Gentzen and Galois: How to display your favourite substructural logic. *Logic Journal of the IGPL*, 6(5):669–694, 1998.
- [24] Samin Ishtiaq and Peter W. O’Hearn. BI as an assertion language for mutable data structures. In *Proceedings of POPL-28*, 2001.
- [25] Stephen Cole Kleene. *Introduction to Metamathematics, 2nd edn.* North-Holland, 1987. Amsterdam.
- [26] Marcus Kracht. Power and weakness of the modal display calculus. In Heinrich Wansing, editor, *Proof Theory of Modal Logic*, pages 93–121. Kluwer Academic Publishers, 1996.
- [27] H.H. Nguyen and W.-N. Chin. Enhancing program verification with lemmas. In *Proceedings of CAV*, 2008.
- [28] P.W. O’Hearn and D. J. Pym. The logic of bunched implications. *Bulletin of Symbolic Logic*, 5(2):215–244, June 1999.
- [29] Matthew Parkinson and Gavin Bierman. Separation logic, abstraction and inheritance. In *Proceedings of POPL-35*, 2008.
- [30] Dag Prawitz. *Natural Deduction: A Proof-Theoretical Study.* Almqvist & Wiksell, 1965.
- [31] 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>.
- [32] David Pym, Peter O’Hearn, and Hongseok Yang. Possible worlds and resources: The semantics of BI. *Theoretical Computer Science*, 315(1):257–305, 2004.
- [33] Greg Restall. Displaying and deciding substructural logics 1: Logics with contraposition. *Journal of Philosophical Logic*, 27:179–216, 1998.
- [34] Greg Restall. *Negation in Relevant Logics (How I stopped worrying and learned to love the Routley Star)*, volume 13 of *Applied Logic Series*, pages 53–67. Kluwer Academic Publishers, 1999.

- [35] Greg Restall. *An Introduction to Substructural Logics*. Routledge, 2000.
- [36] John C. Reynolds. Separation logic: A logic for shared mutable data structures. In *Proceedings of 17th LICS*, 2002.
- [37] Richard Routley and Valerie Routley. Semantics of first-degree entailment. *Noûs*, 3:335–359, 1972.
- [38] Harold Schellinx. Some syntactical observations on linear logic. *Journal of Logic and Computation*, 1(4):537–559, 1991.
- [39] Alasdair Urquhart. The undecidability of entailment and relevant implication. *Journal of Symbolic Logic*, 49(4):1059–1073, 1984.
- [40] H. Yang, O. Lee, J. Berdine, C. Calcagno, B. Cook, D. Distefano, and P. O’Hearn. Scalable shape analysis for systems code. In *Proceedings of CAV*, 2008.

APPENDIX A. CUT-ELIMINATION FOR DL_{CBI} (THEOREM 4.8)

The following definition is taken from Belnap [2]. By a *constituent* of a structure or consecution we mean an occurrence of one of its substructures.

Definition A.1 (Parameters / congruence). Let I be an instance of a rule R of DL_{CBI} . Note that I is obtained by assigning structures to the structure variables occurring in R and formulas to the formula variables occurring in R .

Any constituent of the consecutions in I occurring as part of structures assigned to structure variables in I are defined to be *parameters* of I . All other constituents are defined to be *non-parametric* in I , including those assigned to formula variables.

Constituents occupying similar positions in occurrences of structures assigned to the same structure variable are defined to be *congruent* in I .

We remark that congruence as defined above is an equivalence relation.

Belnap’s analysis guarantees cut-elimination (Theorem 4.8) provided the rules of DL_{CBI} (cf. Figure 3) satisfy the following conditions, which are stated with reference to an instance I of a DL_{CBI} rule R . (Here, following Kracht [26], we state a stronger, combined version of Belnap’s original conditions C6 and C7, since our rules satisfy this stronger condition.) In each case, we indicate how to verify that the condition holds for our rules.

C1: Preservation of formulas. Each formula which is a constituent of some premise of I is a subformula of some formula in the conclusion of I .

Verification. One observes that, in each rule, no formula variable or structure variable is lost when passing from the premises to the conclusions.

C2: Shape-alikeness of parameters. Congruent parameters are occurrences of the same structure.

Verification. Immediate from the definition of congruence.

C3: Non-proliferation of parameters. No two constituents in the conclusion of I are congruent to each other.

Verification. One just observes that, for each rule, each structure variable occurs exactly once in the conclusion.

C4: *Position-alikeness of parameters.* Congruent parameters are either all antecedent or all consequent parts of their respective consecutions.

Verification. One observes that, in each rule, no structure variable occurs both as an antecedent part and a consequent part.

C5: *Display of principal constituents.* If a formula is nonparametric in the conclusion of I , it is either the entire antecedent or the entire consequent of that conclusion. Such a formula is said to be *principal* in I .

Verification. It is easy to verify that the only non-parametric formulas in the conclusions of our rules are the two occurrences of P in (Id) and those occurring in the introduction rules for the logical connectives, which obviously satisfy the condition.

C6/7: *Closure under substitution for parameters.* Each rule is closed under simultaneous substitution of arbitrary structures for congruent formulas which are parameters.

Verification. This condition is satisfied because no restrictions are placed on the structural variables used in our rules.

C8: *Eliminability of matching principal formulas.* If there are inferences I_1 and I_2 with respective conclusions $X \vdash F$ and $F \vdash Y$ and with F principal in both inferences, then either $X \vdash Y$ is equal to one of $X \vdash F$ and $F \vdash Y$, or there is a derivation of $X \vdash Y$ from the premises of I_1 and I_2 in which every instance of cut has a cut-formula which is a proper subformula of F .

Verification. There are only two cases to consider. If F is atomic then $X \vdash F$ and $F \vdash Y$ are both instances of (Id). Thus we must have $X \vdash F = F \vdash Y = X \vdash Y$, and are done. Otherwise F is non-atomic and introduced in I_1 and I_2 respectively by the right and left introduction rule for the main connective of F . In this case, a derivation of the desired form can be obtained using only the display rule (\equiv_D) and cuts on subformulas of F . For example, if the considered cut is of the form:

$$\frac{\frac{\frac{\vdots}{X \vdash F, G} (\forall R)}{X \vdash F \forall G} \quad \frac{\frac{\frac{\vdots}{F \vdash Y} \quad \frac{\vdots}{G \vdash Z}}{F \forall G \vdash Y, Z} (\forall L)}{X \vdash Y, Z} (\text{Cut})$$

then we can reduce this cut to cuts on F and G in the following manner:

$$\begin{array}{c}
\vdots \\
\frac{X \vdash F, G}{X, \flat G \vdash F} (\equiv_D) \quad \vdots \\
\frac{\quad}{F \vdash Y} (\text{Cut}) \\
\hline
\frac{X, \flat G \vdash Y}{X, \flat Y \vdash G} (\equiv_D) \quad \vdots \\
\frac{\quad}{G \vdash Z} (\text{Cut}) \\
\hline
\frac{X, \flat Y \vdash Z}{X \vdash Y, Z} (\equiv_D)
\end{array}$$

The cases for the other connectives are similarly straightforward. This completes the verification of the conditions, and thus the proof. \square