Semantic cut elimination for the logic of Bunched Implications, formalized in Coq

Dan Frumin
Bernoulli Institute, University of Groningen
The Netherlands
d.frumin@rug.nl

Abstract

The logic of bunched implications (BI) is a substructural logic that forms the backbone of separation logic, the much studied logic for reasoning about heap-manipulating programs. Although the proof theory and metatheory of BI are mathematically involved, the formalization of important metatheoretical results is still incipient. In this paper we present a self-contained formalized, in the Coq proof assistant, proof of a central metatheoretical property of BI: cut elimination for its sequent calculus.

The presented proof is *semantic*, in the sense that is obtained by interpreting sequents in a particular "universal" model. This results in a more modular and elegant proof than a standard Gentzen-style cut elimination argument, which can be subtle and error-prone in manual proofs for BI. In particular, our semantic approach avoids unnecessary inversions on proof derivations, or the uses of cut reductions and the multi-cut rule.

Besides modular, our approach is also robust: we demonstrate how our method scales, with minor modifications, to (i) an extension of BI with an arbitrary set of *simple structural rules*, and (ii) an extension with an S4-like $\Box$ modality.

1 Introduction

The logic of bunched implications (BI) [OP99] is an extension of intuitionistic logic with substructural connectives. BI (and its classical cousin Boolean BI) is known for, among other things, forming a basis for separation logic [Rey02, O'H19] – a popular program logic for verification of heap-manipulating programs. The BI itself, and many of its important models, are based on the idea that propositions denote ownership of resources and BI includes a *separating conjunction* connective $*$, which signifies ownership of *disjoint* resources [POY04]. As an adjoint to $*$, BI also includes a *magic wand* connective $-\!*$, which is determined by the property

$$A \vdash B -\!* C \qquad \Longleftrightarrow \qquad A * B \vdash C.$$

Additionally, BI includes a unit element Emp for the separating conjunction $*$.

Proof theoretically, BI can be formalized in a Gentzen-style sequent calculus, which operates on the judgments of the form $\Delta \vdash A$, where Δ is not merely a multiset of formulas, but a *bunch* – a tree in which leaves are formulae and nodes are connected with either $\boldsymbol{;}$ or $\boldsymbol{,}$ (signifying connecting the resources using $\wedge$ and $*$, respectively). For example, a bunch might be $((a \wedge b) \boldsymbol{;} c) \boldsymbol{,} (d \boldsymbol{;} e)$. Due to this nested structure of bunches, the left rules in the BI sequent calculus can apply deep inside bunches. For example, an instance of the left rule for $\wedge$, specialized to the bunch above, is

$$\frac{((a \boldsymbol{;} b) \boldsymbol{;} c) \boldsymbol{,} (d \boldsymbol{;} e) \vdash \varphi}{((a \wedge b) \boldsymbol{;} c) \boldsymbol{,} (d \boldsymbol{;} e) \vdash \varphi}$$

That is, $a \wedge b$ got "destructed" into $a \boldsymbol{;} b$ in the context $([\cdot] \boldsymbol{;} c) \boldsymbol{,} (d \boldsymbol{;} e)$, where $[\cdot]$ signifies a "hole" that can be filled.

BI treats $*$ (and hence, $\boldsymbol{,}$) as a substructural connective, that does not admit contraction and weakening (i.e. neither $a \vdash a * a$ nor $a * b \vdash a$ hold), but it retains the structural rules for intuitionistic connective $\wedge$ (and hence, $\boldsymbol{;}$). In the sequent calculus, the corresponding structural rules can as well be applied deeply inside bunches. For example, an instance of a contraction rule might look like this:

$$\frac{\big((a \boldsymbol{,} b) \boldsymbol{;} (a \boldsymbol{,} b)\big) \boldsymbol{,} c \vdash \varphi}{(a \boldsymbol{,} b) \boldsymbol{,} c \vdash \varphi}$$

Here we contract $(a \boldsymbol{,} b)$ inside the context $[\cdot] \boldsymbol{,} c$. In BI we have to permit contraction on arbitrary bunches, whereas in intuitionistic logic contraction on individual formulas is sufficient.

As usual, BI includes a *cut rule*, which formalizes the informal process of applying a lemma in reasoning. Similar to the other rules, the cut rule can be applied on a formula deeply nested inside a bunch:

$$\frac{\Delta' \vdash \psi \qquad \Delta(\psi) \vdash \varphi}{\Delta(\Delta') \vdash \varphi}$$

where $\Delta(-)$ is an arbitrary bunch with a hole.

In this paper we study cut elimination property for BI: every proof in BI that involves the cut rule can be rewritten into a proof that does not require the cut rule. From a theoretical point of view, cut elimination can be used to show important meta-theoretical properties (subformula property, consistency, conservativity). From a more practical standpoint, cut elimination is an important ingredient in proof search.

Why formalize cut elimination? Since cut elimination is a staple in metatheory of logics, and almost always when a new logic is proposed in terms of sequent calculus, the question of cut elimination is raised. Usually it is then proposed that cut elimination is proved directly by a recursive procedure on derivation tree, potentially using additional measure(s) to prove that this procedure terminates.

Proofs organized along those lines are repetitive, consisting of many sub-cases and, and including many implicit details (e.g. about the structure of the contexts). As a result, it is not uncommon to see proofs that are "analogous" to known correct proofs of cut elimination for related systems, or proofs that only discuss a couple of cases that are considered illustrative, with the bulk of the proof being left as a (rarely completed) exercise for the reader.

Unfortunately, due to the interplay and complexity of all the details, such informal proofs can be quite risky. In the case of BI, the deep nested structure of bunches and explicit structural rules contribute to the complexity and the level of details. For example, a proof of cut elimination for BI given in [Pym02, Chapter 6] had a gap, that was later fixed in [AQ12]. The issue seems to arise from the treatment of the contraction rule. In presence of explicit contraction a naive approach of pushing each instance of the cut rule up along the derivation tree does not necessarily work. In order to resolve this, the cut rule should be generalized to the *multicut* rule, combining contraction and cut together. Then cut elimination is generalized to multicut elimination, offering a stronger induction hypothesis that can be applied to subproofs. Unfortunately, this generalization was originally done in a way that only works for some of the cases. See [AQ12] for more details.[1]

This is not the only instance of erroneous proofs of cut elimination slipping in. Several sequent calculus formulations for bi-intuitionistic logic were wrongly believed to enjoy cut elimination. These mistakes were later fixed in [PU09]. Other instances include an incorrect proof of cut elimination for full intuitionistic linear logic, fixed in [dB96, Bie96]; an incorrect proof of cut elimination for nested sequent systems for modal logic [BS09], fixed in [MS14]. While not incorrect in itself, cut elimination for a formulation of the provability logic GL by Sambin and Valentini [SV82] with explicit structural rules was subject of some controversy until it was resolved in [GR12].

Semantic cut elimination. To counterbalance informal pen-and-paper proofs of cut elimination for BI, we provide a fully formalized proof in the Coq proof assistant. However, instead of trying to formalize an intricate Gentzen-style process, as in [AQ12], we approach cut elimination using the ideas of algebraic proof theory: a research area aimed at making tight connections between structural proof theory and algebraic semantics of logics. In our proof we adapt the methods of algebraic semantic cut elimination for linear logic [Oka99, Oka02], in which cut elimination is obtained by constructing a special model for linear logic that is universal w.r.t. cut-free provability. We believe that this approach to cut elimination is more amendable to formalization and extension, than a direct Gentzen-style proof.

Semantic cut elimination for BI was first developed by Galatos and Jipsen [GJ17], building on their work on residuated frames [GJ13]. Their approach is quite general, and the proof makes heavy use of intermediate structures (the aforementioned residuated frames), which lie in between sequent calculus and algebraic semantics. By contrast, the proof presented here only involves the "syntax" (sequent calculus), and the "semantics" (algebraic models) parts. This leaves us with fewer structures to consider in the formalization.

To demonstrate the modularity of our proof, we extend it to cover two different types of extensions of BI. Firstly, we consider BI extended with a particular class of structural rules (*simple structural rules*), which cover weakening and contraction (both for **,** and **;**), as well as many other kinds of structural rules. Secondly, we consider BI extended with an S4-like $\Box$ modality. In both cases we show that we do not have to make a lot of modifications to the proof, and the modifications that we do have to make are, in a way, systematic.

1.1 Contributions and outline

The main contributions of this paper are as follows. We present an algebraic proof of cut elimination for BI. Our proof can be seen as a simplification of the Galatos and Jipsen's method [GJ17], without the framework of residuated frames. We demonstrate the modularity of our approach by extending it to cut elimination of BI with an S4-like modality (modalities were not previously considered in the framework of residuated frames). We formalize the results in the Coq proof assistant, which is to our knowledge the first published formalization of cut elimination for BI.

The remained of the paper is structured as follows. In Section 2 we present the main idea behind semantic proofs of cut elimination. In Section 3 and Section 4 we recall the sequence calculus for BI and its (standard) algebraic semantics via BI algebras. In Section 5 we consider when a closure operator on a BI algebra induces a subalgebra itself. We then apply this construction in Section 6 to obtain a "universal" model for cut-free provability, and use it to prove cut elimination. In Section 7 we extend the proof of cut elimination to all possible extensions of BI with a particular class of structural rules. In Section 8 we extend the proof to account for an S4-like modality. We discuss our formalization efforts in Section 9. We discuss related work in Section 10 and conclude in Section 11.

[1] It is possible to avoid the multicut generalization by using more fine-grained measure functions, see [BDP00] for the case of intuitionistic logic. As another alternative, Brotherston [Bro12] gave a proof of cut elimination for BI by going through a displayed calculus.

2 Semantic cut elimination

In this section we explain some of the ideas and intuitions behind a semantic proof of cut elimination in a semi-formal way, before diving straight into the complexities of BI. The starting point is that there is a class of algebras in which we can interpret logic. The main idea is to find a particular algebra C, in which we can interpret the sequent calculus, and which has a property that if $[\![\psi]\!] \leq [\![\varphi]\!]$ in C, then $\psi \vdash \varphi$ is derivable without applications of the CUT rule. In this case, we say that C is "universal" algebra for cut-free provability. Then, cut elimination can be obtained by the (sound) interpretation of sequent calculus into C.

Finding such a "universal" algebra is reminiscent of proving *completeness* of a logic w.r.t. a class of algebras. In the case completeness, we construct a "universal" algebra $\mathcal{L}$ such that $[\![\psi]\!] \leq [\![\varphi]\!]$ implies derivability of $\psi \vdash \varphi$. This Lindenbaum-Tarski algebra $\mathcal{L}$ is usually defined to be the collection of equivalence classes of formulas modulo interprovability:

$$[\varphi] \triangleq \{\psi \mid (\psi \vdash \varphi) \ \wedge \ (\varphi \vdash \psi)\}$$

And the ordering $\leq$ on $\mathcal{L}$ is induced by provability:

$$[\varphi] \leq [\psi] \iff \varphi \vdash \psi.$$

Provability does not depend on the representative of the equivalence class, and so we get a poset $\mathcal{L}$. The logical operators are interpreted in $\mathcal{L}$ in such a way that $[\![\varphi]\!] = [\varphi]$. The argument for completeness then goes as follows: suppose that $[\![\varphi]\!] \leq [\![\psi]\!]$ in all the possible algebras; then, in particular that inequality holds in $\mathcal{L}$, which amounts to $\varphi \vdash \psi$. Thus, any valid sequent is derivable.

It is precisely the connection between provability and the order on the algebra that makes this model useful. We can imagine a reformulation of the above model in terms of cut-free provability in sequent calculus:

$$[\varphi] \leq [\psi] \iff \varphi \vdash_{\mathrm{cf}} \psi.$$

This adaptation, however, does not work. In order to prove that the ordering $\leq$ is transitive, we need to show

$$\frac{\varphi \vdash_{\mathrm{cf}} \psi \qquad \psi \vdash_{\mathrm{cf}} \chi}{\varphi \vdash_{\mathrm{cf}} \chi}$$

which amounts to showing that CUT is admissible. We seem to be back at square one.

To fix this, instead of interpreting formulas as a sets of equivalent formulas (which is what equivalence classes can be seen as), we would like to interpret formulas as sets of *contexts* which prove the formula:

$$\langle\varphi\rangle \triangleq \{\Delta \mid \Delta \vdash_{\mathrm{cf}} \varphi\}.$$

Then, inclusion of sets is a good candidate for the ordering, since $\langle\psi\rangle \subseteq \langle\varphi\rangle$ implies that $\psi \vdash_{\mathrm{cf}} \varphi$.

But how do we interpret logical connectives? We can interpret $\top$ as the set of all contexts; then, clearly $\top = \langle\mathsf{True}\rangle$. However, we cannot pick the empty set as an interpretation of $\bot$: the set $\langle\mathsf{False}\rangle$ is non-empty, as it contains at least False itself. This already suggests that $\langle-\rangle$ is not going to be a homomorphism w.r.t. the powerset operations.

Instead of considering arbitrary sets of contexts, we need to refine the powerset algebra somehow. It turns out that the structure that we are looking for is a subalgebra of the powerset algebra generated by a particular *closure operator*, that ensures that the sets of contexts that we are working with are sufficiently "closed": for example, they should at least contain False, and should be closed under the cut-free provability. We expand on those ideas in Sections 5 and 6.

But first, to make the matters concrete, we recall the BI sequent calculus and properties of its cut-free fragment (Section 3), and the algebraic semantics for BI (Section 4).

3 Sequent calculus for BI

In this section we briefly recall the sequent calculus formulation of BI [OP99], and some of the properties of its cut-free fragment. The formulas of BI are obtained from the following grammar:

$$\begin{aligned}\varphi, \psi ::= {} & \mathsf{True} \mid \mathsf{False} \mid \varphi \wedge \psi \mid \varphi \vee \psi \mid \varphi \to \psi \\ & \mid \mathsf{Emp} \mid \varphi * \psi \mid \varphi \mathrel{-\!\!*} \psi \mid a \qquad (a \in Atom)\end{aligned}$$

BI extends intuitionistic propositional logic with separating conjunction ($*$), magic wand ($-\!\!*$, adjoint to separating conjunction), and the empty proposition (Emp, unit for separating conjunction). We also include atomic propositions drawn from a fixed set *Atom*.

The sequent calculus for BI is given in Figure 1. It operates on the sequents of the form $\Delta \vdash \varphi$, where φ is a formula and Δ is a *bunch* – a tree composed of binaries nodes labeled with **,** and **;**, and leaves being either formulas or empty bunches $\varnothing_m$ and $\varnothing_a$. Morally, we view bunches as equivalence classes of such trees modulo commutative monoid laws for $(\textbf{,}, \varnothing_m)$, and $(\textbf{;}, \varnothing_a)$. These are given using structural congruence $\equiv$, the rules for which are also given in Figure 1. We could have defined provability on such equivalence classes, but we opt for using explicit context conversions using EQUIV.

Most of the structural rules and the left rules can be applied to formulas that occur nested inside some bunch with a hole $\Delta(-)$. We refer to such bunches with holes *bunched contexts*.

3.1 Cut-free provability

Let us write $\Delta \vdash_{\mathrm{cf}} \varphi$ if $\Delta \vdash \varphi$ is derivable *without* the CUT rule. In the rest of this section we prove invertibility of several rules in the cut-free fragment of BI. Those derived rules will be useful to us when constructing the algebraic model in Section 6.

The first observation about the sequent calculus, is that we have formulated the "axiom" rule $\varphi \vdash \varphi$ only for atomic formulas $a \in Atom$. This will significantly simplify some of the proofs (for example, Lemma 3.3), but does not limit

Equivalence of bunches

$$\Delta_1 \,,\, \Delta_2 \equiv \Delta_2 \,,\, \Delta_1 \qquad \Delta_1 \,;\, \Delta_2 \equiv \Delta_2 \,;\, \Delta_1 \qquad \Delta_1 \,,\, (\Delta_2 \,,\, \Delta_3) \equiv (\Delta_1 \,,\, \Delta_2) \,,\, \Delta_3 \qquad \Delta_1 \,;\, (\Delta_2 \,;\, \Delta_3) \equiv (\Delta_1 \,;\, \Delta_2) \,;\, \Delta_3$$

$$\Delta \,,\, \varnothing_m \equiv \Delta \qquad \Delta \,;\, \varnothing_a \equiv \Delta \qquad \frac{\Delta \equiv \Delta'}{\Gamma(\Delta) \equiv \Gamma(\Delta')}$$

Structural rules

$$\overset{\textsc{ax}}{\dfrac{a \in Atom}{a \vdash a}} \qquad \overset{\textsc{equiv}}{\dfrac{\Delta' \vdash \varphi \qquad \Delta \equiv \Delta'}{\Delta \vdash \varphi}} \qquad \overset{\text{W};}{\dfrac{\Delta(\Delta_1) \vdash \varphi}{\Delta(\Delta_1 \,;\, \Delta_2) \vdash \varphi}} \qquad \overset{\text{C};}{\dfrac{\Delta(\Delta_1 \,;\, \Delta_1) \vdash \varphi}{\Delta(\Delta_1) \vdash \varphi}} \qquad \overset{\textsc{cut}}{\dfrac{\Delta' \vdash A \qquad \Delta(A) \vdash B}{\Delta(\Delta') \vdash B}}$$

Multiplicatives

$$\overset{\text{EmpR}}{\varnothing_m \vdash \mathsf{Emp}} \qquad \overset{\text{EmpL}}{\dfrac{\Delta(\varnothing_m) \vdash \varphi}{\Delta(\mathsf{Emp}) \vdash \varphi}} \qquad \overset{*\text{R}}{\dfrac{\Delta_1 \vdash \varphi \qquad \Delta_2 \vdash \psi}{\Delta_1 \,,\, \Delta_2 \vdash \varphi * \psi}} \qquad \overset{*\text{L}}{\dfrac{\Delta(\varphi \,,\, \psi) \vdash \chi}{\Delta(\varphi * \psi) \vdash \chi}} \qquad \overset{-\!*\text{R}}{\dfrac{\Delta \,,\, \varphi \vdash \psi}{\Delta \vdash \varphi \mathrel{-\!*} \psi}} \qquad \overset{-\!*\text{L}}{\dfrac{\Delta_1 \vdash \varphi \qquad \Delta(\Delta_2 \,,\, \psi) \vdash \chi}{\Delta(\Delta_1 \,,\, \Delta_2 \,,\, \varphi \mathrel{-\!*} \psi) \vdash \chi}}$$

Additives

$$\overset{\text{TrueR}}{\varnothing_a \vdash \mathsf{True}} \qquad \overset{\text{TrueL}}{\dfrac{\Delta(\varnothing_a) \vdash \varphi}{\Delta(\mathsf{True}) \vdash \varphi}} \qquad \overset{\wedge\text{R}}{\dfrac{\Delta_1 \vdash \varphi \qquad \Delta_2 \vdash \psi}{\Delta_1 \,;\, \Delta_2 \vdash \varphi \wedge \psi}} \qquad \overset{\wedge\text{L}}{\dfrac{\Delta(\varphi \,;\, \psi) \vdash \chi}{\Delta(\varphi \wedge \psi) \vdash \chi}} \qquad \overset{\rightarrow\text{R}}{\dfrac{\Delta \,;\, \varphi \vdash \psi}{\Delta \vdash \varphi \rightarrow \psi}} \qquad \overset{\rightarrow\text{L}}{\dfrac{\Delta_1 \vdash \varphi \qquad \Delta(\Delta_2 \,;\, \psi) \vdash \chi}{\Delta(\Delta_1 \,;\, \Delta_2 \,;\, \varphi \rightarrow \psi) \vdash \chi}}$$

$$\overset{\text{FalseL}}{\Delta(\mathsf{False}) \vdash \varphi} \qquad \overset{\vee\text{R1}}{\dfrac{\Delta \vdash \varphi}{\Delta \vdash \varphi \vee \psi}} \qquad \overset{\vee\text{R2}}{\dfrac{\Delta \vdash \psi}{\Delta \vdash \varphi \vee \psi}} \qquad \overset{\vee\text{L}}{\dfrac{\Delta(\varphi) \vdash \chi \qquad \Delta(\psi) \vdash \chi}{\Delta(\varphi \vee \psi) \vdash \chi}}$$

Figure 1. BI sequent calculus.

the expressivity of the system, as witness by the following lemma.

Proposition 3.1 (Identity expansion)**.** *For every formula φ we can derive a sequent $\varphi \vdash_{\mathrm{cf}} \varphi$.*

Proof. By induction on the structure of φ. □

For the construction presented in this paper we need to show that a number of rules are invertible in the cut-free sequent calculus. Specifically, we need to show that $-\!*$R, $\rightarrow$R, $*$L, $\wedge$L, EmpL, and TrueL are invertible.

Lemma 3.2. *The following rules are admissible:*

$$\overset{-\!*R\text{-}\textsc{inv}}{\dfrac{\Delta \vdash_{\mathrm{cf}} \varphi \mathrel{-\!*} \psi}{\Delta \,,\, \varphi \vdash_{\mathrm{cf}} \psi}} \qquad \overset{\rightarrow R\text{-}\textsc{inv}}{\dfrac{\Delta \vdash_{\mathrm{cf}} \varphi \rightarrow \psi}{\Delta \,;\, \varphi \vdash_{\mathrm{cf}} \psi}}$$

Proof. By induction on the derivations $\Delta \vdash_{\mathrm{cf}} \varphi \mathrel{-\!*} \psi$ and $\Delta \vdash_{\mathrm{cf}} \varphi \rightarrow \psi$. □

At the end of the day, the proof of Lemma 3.2 by induction on derivations is not very complicated, because the form of the context on the left-hand side of the sequent is relatively simple. It is easy to show that the left rules can commute with $-\!*$R and $\rightarrow$R. By contrast, showing that the rules $*$L and $\wedge$L are invertible is more involved for several reasons.

First of all, just like for other sequent calculi with explicit contraction, structural induction on the proof is not strong enough. Consider the following derivation of $\varphi * \psi \vdash_{\mathrm{cf}} \chi$:

$$\frac{\varphi * \psi \,;\, \varphi * \psi \vdash_{\mathrm{cf}} \chi}{\varphi * \psi \vdash_{\mathrm{cf}} \chi}$$

By induction hypothesis we can obtain a proof of

$$\varphi * \psi \,;\, (\varphi \,,\, \psi) \vdash_{\mathrm{cf}} \chi,$$

but this proof is not a strict subderivation of the original derivation. So we cannot apply the induction hypothesis to it. In order to circumvent this, we do induction on the *height* of the derivation, strengthening the statement to:

Lemma 3.3. *If there is a derivation of $\Delta(\varphi * \psi) \vdash_{\mathrm{cf}} \chi$ with height n, then there is a derivation of $\Delta(\varphi \,,\, \psi) \vdash_{\mathrm{cf}} \chi$ with height strictly less than n.*

Note that this lemma would be false if we would have included an axiom rule for arbitrary formulas: there would be a proof $\varphi * \psi \vdash_{\mathrm{cf}} \varphi * \psi$ of height 0, but the smallest proof of $\varphi \,,\, \psi \vdash_{\mathrm{cf}} \varphi * \psi$ is of height 1. That is why we have restricted the axiom rule to atomic formulas, and got the general form of the axiom rule as a derived statement (Proposition 3.1).

Similarly, by induction on the derivation height, we show that EmpL and TrueL are invertible. We only care about the derivation height for the purposes of induction, so we summarize the results on invertible rules in the following lemma.

Lemma 3.4. *The following rules are admissible:*

$$\frac{\Delta(\varphi \wedge \psi) \vdash_{\mathrm{cf}} \chi}{\Delta(\varphi \,;\, \psi) \vdash_{\mathrm{cf}} \chi}\ \wedge L\text{-INV} \qquad \frac{\Delta(\varphi * \psi) \vdash_{\mathrm{cf}} \chi}{\Delta(\varphi \,,\, \psi) \vdash_{\mathrm{cf}} \chi}\ *L\text{-INV}$$

$$\frac{\Delta(\mathsf{True}) \vdash_{\mathrm{cf}} \chi}{\Delta(\varnothing_a) \vdash_{\mathrm{cf}} \chi}\ \top L\text{-INV} \qquad \frac{\Delta(\mathsf{Emp}) \vdash_{\mathrm{cf}} \chi}{\Delta(\varnothing_m) \vdash_{\mathrm{cf}} \chi}\ \mathrm{Emp}L\text{-INV}$$

Let us write $(\Delta)^*$ for interpretation of Δ as a formula: we substitute every occurrence of **,** in Δ with $*$, every occurrence of $\varnothing_m$ with Emp, and similarly for the additive connectives. Clearly, there is a derivation from $\Delta \vdash_{\mathrm{cf}} \chi$ to $(\Delta)^* \vdash_{\mathrm{cf}} \chi$, by repeated application of $*$L and $\wedge$L. For the other direction we have the following.

Corollary 3.5. *The following rule is admissible:*

$$\frac{\Delta'((\Delta)^*) \vdash_{\mathrm{cf}} \chi}{\Delta'(\Delta) \vdash_{\mathrm{cf}} \chi}\ \text{COMP-INV}$$

Proof. By induction on Δ, using the Lemma 3.4. □

4 Algebraic semantics for BI

We interpret the BI sequent calculus in the algebraic structures known as BI algebras, which are bounded Heyting algebras with a compatible residuated monoidal structure.

Definition 4.1. A BI algebra $\mathcal{B}$ is a tuple $(B, \bot, \top, \wedge, \vee, \to, \mathsf{Emp}, *, -\!\!*)$ where

- $(B, \bot, \top, \wedge, \vee, \to)$ is a bounded Heyting algebra, i.e. a bounded distributive lattice with the Heyting implication satisfying
$$a \wedge b \le c \iff a \le b \to c$$
- $* : \mathcal{B} \times \mathcal{B} \to \mathcal{B}$ is a monotone commutative and associative function;
- $\mathsf{Emp} : \mathcal{B}$ is a unit element for $*$;
- $-\!\!*: \mathcal{B} \times \mathcal{B} \to \mathcal{B}$ is a binary operation satisfying
$$a * b \le c \iff a \le b -\!\!* c$$

Definition 4.2. Let $\mathcal{B}$ be an arbitrary BI algebra. Given an interpretation $i : Atom \to \mathcal{B}$ of atomic propositions, we interpret formulas of BI in $\mathcal{B}$ in the usual tautological way:

$$\begin{aligned} [\![\mathsf{Emp}]\!] &= \mathsf{Emp} & [\![\mathsf{True}]\!] &= \top \\ [\![\varphi * \psi]\!] &= [\![\varphi]\!] * [\![\psi]\!] & [\![\varphi \wedge \psi]\!] &= [\![\varphi]\!] \wedge [\![\psi]\!] \\ [\![\varphi -\!\!* \psi]\!] &= [\![\varphi]\!] -\!\!* [\![\psi]\!] & [\![\varphi \to \psi]\!] &= [\![\varphi]\!] \to [\![\psi]\!] \\ [\![\varphi \vee \psi]\!] &= [\![\varphi]\!] \vee [\![\psi]\!] & [\![\mathsf{False}]\!] &= \bot \\ [\![a]\!] &= i(a) \end{aligned}$$

Theorem 4.3 (Soundness)**.** *If $\Delta \vdash \varphi$ is derivable, then $[\![(\Delta)^*]\!] \le [\![\varphi]\!]$ holds in any BI algebra.*

Proof. By induction on the derivation. □

4.1 BI algebras from monoids

In practice, a lot of BI algebras arise as predicates over a partial commutative monoid. Let $(M, \cdot, e)$ be a partially commutative monoid; we write $x \cdot y = \bot$ if composition of x and y is undefined. Then the powerset $\wp(M)$ is a (complete) Heyting algebra, and it forms a BI algebra $(\wp(M), \emptyset, M, \cap, \cup, \to, \mathbf{0}, \bullet, -\!\!\bullet)$ with the following operators:

$$\begin{aligned} \mathbf{0} &\triangleq \{e\} \\ X \bullet Y &\triangleq \{x \cdot y \mid x \in X, y \in Y, x \cdot y \neq \bot\} \\ X -\!\!\bullet Y &\triangleq \{z \mid \forall x \in X.\, z \cdot x \neq \bot \implies z \cdot x \in Y\}. \end{aligned}$$

BI algebra from the monoid of contexts. Let us write *Bunch* for the set of bunches, modulo the equivalence $\equiv$ (from Figure 1). We can endow the set *Bunch* of bunches with the structure of a monoid. Composition of two contexts Δ and Δ' is just putting them next to each other using **,**:

$$\Delta \cdot \Delta' \triangleq (\Delta \,,\, \Delta')$$

then, up to equivalence of bunches, $\varnothing_m$ is the unit element. Using the powerset construction we get a BI algebra $\wp(Bunch)$.

This model is very much "freely generated" from syntax, but it is not very useful, as it does not involve any notion of provability (only equivalence of contexts). In this next sections we are going to refine this model, in order to obtain a submodel which can be used to prove completeness and cut-elimination.

5 Moore closures on BI algebras

For cut elimination, we will be interested in subalgebras of the powerset algebra $\wp(M)$ for some partial commutative monoid M; specifically subalgebras arising from a particular closure operator. For the rest of this section we fix a partial commutative monoid M.

Definition 5.1. A Moore collection is a family of sets $C \subseteq \wp(M)$ that is closed under arbitrary intersections:

$$(\forall i \in I.\, A_i \in C) \implies \bigcap_{i \in I} A_i \in C.$$

If $X \in C$ we say that X is *closed.*

Alternatively, a Moore collection can be given in terms of a closure operator $\mathsf{cl}(-)$ satisfying the following conditions:

- $X \subseteq \mathsf{cl}(X)$;
- monotonicity: $X \subseteq Y \implies \mathsf{cl}(X) \subseteq \mathsf{cl}(Y)$;
- idempotence: $\mathsf{cl}(\mathsf{cl}(X)) = \mathsf{cl}(X)$.

Given a Moore collection C we define the associated closure operator as $\mathsf{cl}(X) = \bigcap\{Y \in C \mid X \subseteq Y\}$. In the other direction, given a closure operator we define $\mathsf{cl}(-)$-closed sets as $C = \{X \mid \mathsf{cl}(X) = X\}$.

Some basic theory behind posets with such a closure operator is given in [Eve44]. Here, we recall only the results that we will be needing. First of all, we are going to use the following rule often.

Lemma 5.2. *The closure operator satisfies the following adjunction rule:*

$$\frac{X \subseteq Y \quad \text{in } \wp(M)}{\mathsf{cl}(X) \subseteq Y \quad \text{in } C}$$

for a closed set Y.

Since C is closed under intersections, $X \cap Y$ is a meet of two closed sets X and Y. However, given two closed sets, their union $X \cup Y$ is not always closed. Instead, we interpret join as $\mathsf{cl}(X \cup Y)$.

Proposition 5.3. *The Moore collection C is a complete bounded lattice: the least upper bound is given by $\bigvee_{i\in I} X_i = \mathsf{cl}(\bigcup_{i\in I} X_i)$. In particular, the bottom element of C is $\mathsf{cl}(\emptyset)$. Furthermore, if $X \to Y$ is closed whenever X and Y are closed, then C is a Heyting algebra.*

In light of the previous proposition, we can see that some Heyting algebra structure on C arises from the same operations on $\wp(M)$. Can we similarly lift the BI operations? Let us denote the residuated monoidal structure (defined as in Section 4.1) on $\wp(M)$ as $(\mathbf{0}, \bullet, -\!\bullet)$. In the rest of this section we describe how to lift this structure to C.

5.1 BI algebra structure on closed sets

A sufficient condition for C to be a BI algebra is the following.

Definition 5.4. We say that the closure operator is *strong* if for any X and Y

$$\mathsf{cl}(X) \bullet Y \subseteq \mathsf{cl}(X \bullet Y)$$

If $\mathsf{cl}(-)$ is strong, then we define the BI operators on C as follows:

$$\begin{aligned} \mathsf{Emp} &= \mathsf{cl}(\mathbf{0}) \\ X * Y &= \mathsf{cl}(X \bullet Y) \\ X \mathrel{-\!\!*} Y &= \mathsf{cl}(X \mathrel{-\!\bullet} Y) \end{aligned}$$

We shall verify that with these connectives C is a BI algebra.

Proposition 5.5. *There is an adjunction/Galois connection between $*$ and $-\!\!*$.*

Proof. We reason as follows.

$$\begin{aligned} & X * Y \subseteq Z && \text{(def. of } *) \\ \iff & \mathsf{cl}(X \bullet Y) \subseteq Z && (Z \text{ is closed}) \\ \iff & X \bullet Y \subseteq Z && \text{(adjunction)} \\ \iff & X \subseteq Y \mathrel{-\!\bullet} Z \\ \implies & X \subseteq \mathsf{cl}(Y \mathrel{-\!\bullet} Z). \end{aligned}$$

On the other hand,

$$\begin{aligned} & X \subseteq \mathsf{cl}(Y \mathrel{-\!\bullet} Z) && \text{(monotonicity of } \bullet) \\ \implies & X \bullet Y \subseteq \mathsf{cl}(Y \mathrel{-\!\bullet} Z) \bullet Y && \text{(strength of } \mathsf{cl}(-)) \\ \implies & X \bullet Y \subseteq \mathsf{cl}((Y \mathrel{-\!\bullet} Z) \bullet Y) \\ \implies & X \bullet Y \subseteq \mathsf{cl}(Z) = Z \\ \iff & \mathsf{cl}(X \bullet Y) \subseteq Z. \end{aligned}$$

□

Proposition 5.6. *$(C, *, \mathsf{Emp})$ is a commutative monoid.*

Proof. The commutativity of $*$ is evident from its definition. Let us verify the unit laws:

$$\begin{aligned} \mathsf{Emp} * X &= \mathsf{cl}(\mathsf{cl}(\mathbf{0}) \bullet X) \subseteq \mathsf{cl}(\mathsf{cl}(\mathbf{0} \bullet X)) = X \\ X &= \mathbf{0} \bullet X \subseteq \mathsf{cl}(\mathbf{0}) \bullet X \subseteq \mathsf{cl}(\mathsf{cl}(\mathbf{0}) \bullet X) = \mathsf{Emp} * X. \end{aligned}$$

We reason similarly for associativity of $*$. □

We can summaries these results in the following theorem.

Theorem 5.7. *Given a PCM M, and a closure operator $\mathsf{cl}(-)$ on $\wp(M)$ that is strong, the set C of closed elements is a BI algebra.*

Finally, some times it is more convenient to use an alternative condition in place of closure strength:

Proposition 5.8. *The closure operator is strong iff $X \mathrel{-\!\bullet} Y$ is closed whenever Y is closed, i.e. C forms an exponential ideal.*

Proof. Suppose that C is an exponential ideal w.r.t $-\!\bullet$. Then we reason as follows:

$$\frac{\dfrac{\dfrac{\mathsf{cl}(X) \bullet Y \subseteq \mathsf{cl}(X \bullet Y)}{\mathsf{cl}(X) \subseteq Y \mathrel{-\!\bullet} \mathsf{cl}(X \bullet Y)}}{X \subseteq Y \mathrel{-\!\bullet} \mathsf{cl}(X \bullet Y) \qquad \text{(the r.h.s. is closed)}}}{X \bullet Y \subseteq \mathsf{cl}(X \bullet Y)}$$

Hence, $\mathsf{cl}(-)$ is strong.

For the other direction, if Y is closed, then

$$\begin{aligned} \mathsf{cl}(X \mathrel{-\!\bullet} Y) \subseteq X \mathrel{-\!\bullet} Y &\iff \mathsf{cl}(X \mathrel{-\!\bullet} Y) \bullet X \subseteq Y \\ &\Longleftarrow \mathsf{cl}((X \mathrel{-\!\bullet} Y) \bullet X) \subseteq Y \\ &\iff (X \mathrel{-\!\bullet} Y) \bullet X \subseteq Y \end{aligned}$$

□

A remark on (im)predicativity. In practice, we want to start with some collection $\mathcal{B} \subseteq \wp(M)$ of sets, and generate C freely from arbitrary intersections of elements of $\mathcal{B}$ (think of generating a topology from a closed basis). Then C is a Moore collection and the associated closure operator can be given as $\mathsf{cl}(X) = \bigcap\{Y \in C \mid X \subseteq Y\}$. Unfortunately, this definition is impredicative (we define an element of C by quantifying over elements of C), which, when formalized in type theory, increases the universe level.

That means that we cannot use the closure operator to *define* the set C, i.e. the set $\{X \mid X = \mathsf{cl}(X)\}$ will have a higher universe level than C. To circumvent this, we can instead define the closure operator equivalently by quantifying not over all the closed sets, but only over the basic closed sets: $\mathsf{cl}(X) = \{Y \in \mathcal{B} \mid X \subseteq Y\}$. Then we can define C to be the set of elements satisfying $X = \mathsf{cl}(X)$.

6 Cut-elimination via a syntactic model

In this section we construct a special BI algebra $C \subseteq \wp(\mathit{Bunch})$ that has the following property: if $[\![\varphi]\!] \leq [\![\psi]\!]$ holds in C, then $\varphi \vdash_{\mathsf{cf}} \psi$. By composing this with the soundness theorem, we will obtain the cut-elimination result.

6.1 Principal closed sets

We are going to construct C as a particular Moore collection on $\wp(\mathit{Bunch})$. To define when a predicate X is closed (e.g. when $X \in C$), we start with *principal closed elements*, and generate C as families of intersections of principal closed sets.

Definition 6.1. A *principal* closed set is a set of the form:

$$\langle\varphi\rangle = \{\Delta \mid \Delta \vdash_{\mathsf{cf}} \varphi\}$$

for a formula φ.

We can then generate closed sets by closing the collection of principal closed sets under arbitrary intersections

$$\mathsf{cl}(X) \triangleq \bigcap\{\langle\varphi\rangle \mid X \subseteq \langle\varphi\rangle\} = \bigcap\{\langle\varphi\rangle \mid \forall\Delta \in X.\, \Delta \vdash_{\mathsf{cf}} \varphi\}$$

and define the collection C of closed sets as

$$C \triangleq \{X \mid X = \mathsf{cl}(X)\}.$$

Let us briefly describe some useful properties of closed sets:

Proposition 6.2. *Let X be a closed set. Then the following holds.*

1. $\mathsf{False} \in X$;
2. $\Delta \in X \implies (\Delta\,;\Delta') \in X$;
3. $(\Delta\,;\Delta) \in X \implies \Delta \in X$;
4. $\Delta \in X \iff (\Delta)^* \in X$.

Proof. For the first point, observe that $\mathsf{False} \vdash_{\mathsf{cf}} \varphi$, so $\mathsf{False} \in \langle\varphi\rangle$ for any formula φ.

For the second point, let X be $\bigcap_{i\in I}\langle\varphi_i\rangle$. Then, $\Delta \in X \iff \forall i \in I.\, \Delta \vdash_{\mathsf{cf}} \varphi_i$. If $\Delta \in X$, then, using weakening:

$$\frac{\Delta \vdash_{\mathsf{cf}} \varphi_i}{\Delta\,;\Delta' \vdash_{\mathsf{cf}} \varphi_i}$$

for any $i \in I$. Hence, $\Delta; \Delta' \in X$.

Similarly for the other two cases, using contraction, and the left rules, and Corollary 3.5. ◻

As an example of a calculation in C, we show the following characterization of meets.

Proposition 6.3. *The following holds in C:*

$$X \cap Y = \mathsf{cl}(\{\Delta\,;\Delta' \mid \Delta \in X, \Delta' \in Y\})$$

Proof. For the inclusion from left to right: suppose that $\Delta \in X \cap Y$. Then, by Proposition 6.2, $\Delta; \Delta \in X \cap Y$. That implies that

$$(\Delta;\Delta) \in \{\Delta;\Delta' \mid \Delta \in X, \Delta' \in Y\} \subseteq \mathsf{cl}(\{\Delta;\Delta' \mid \Delta \in X, \Delta' \in Y\})$$

which, again, by Proposition 6.2, implies that

$$\Delta \in \mathsf{cl}(\{\Delta\,;\Delta' \mid \Delta \in X, \Delta' \in Y\}).$$

For the inclusion from right to left: it suffices to show:

$$\{\Delta\,;\Delta' \mid \Delta \in X, \Delta' \in Y\} \subseteq X \cap Y.$$

If $\Delta \in X$ and $\Delta' \in Y$, then $\Delta\,;\Delta' \in X \cap Y$ by Proposition 6.2. ◻

6.2 BI structure.

In order to apply Theorem 5.7 and obtain a BI algebra structure on C, we have to ensure that the Heyting implication of closed sets is closed, and that $X \multimap\!\!\bullet\, Y \in C$ whenever $Y \in C$.

For the following lemma we will use the fact that the $-\!\!*$R is invertible and Corollary 3.5.

Lemma 6.4. *If Y is closed, then so is $X \multimap\!\!\bullet\, Y$; furthermore, it can be described as:*

$$X \multimap\!\!\bullet\, Y = \{\Delta \mid \forall\Delta' \in X.\, (\Delta\,,\Delta') \in Y\}.$$

Proof. It is straightforward to check that $X \multimap\!\!\bullet\, Y$ defined as above is indeed a right adjoint to the $\bullet$ operation. Thus, it remains to show that $X \multimap\!\!\bullet\, Y$ is closed.

Let $Y = \bigcap_{j\in J}\langle\varphi_j\rangle$. Then, we claim,

$$X \multimap\!\!\bullet\, Y = \bigcap_{(\Delta',j)\in X\times J}\langle(\Delta')^* \mathrel{-\!\!*} \varphi_j\rangle.$$

Direction from left to right: let $\Delta \in X \multimap\!\!\bullet\, Y$, and let $\Delta' \in X$, $j \in J$. To show: $\Delta \vdash_{\mathsf{cf}} (\Delta')^* \mathrel{-\!\!*} \varphi_j$. We argue as follows:

$$\dfrac{\dfrac{\Delta\,,\Delta' \vdash_{\mathsf{cf}} \varphi_j}{\Delta\,,(\Delta')^* \vdash_{\mathsf{cf}} \varphi_j}}{\Delta \vdash_{\mathsf{cf}} (\Delta')^* \mathrel{-\!\!*} \varphi_j}$$

Direction from right to left: suppose $\Delta \in \bigcap_{(\Delta',j)\in X\times J}\langle(\Delta')^* \mathrel{-\!\!*} \varphi_j\rangle$; let $\Delta' \in X$. We are to show $\Delta\,,\Delta' \vdash_{\mathsf{cf}} \varphi_j$ for any $j \in J$. By the assumption we have

$$\Delta \vdash_{\mathsf{cf}} (\Delta')^* \mathrel{-\!\!*} \varphi_j.$$

We the reason similarly as in the previous direction, but using the inversion Lemma 3.2 and corollary 3.5:

$$\dfrac{\dfrac{\Delta \vdash_{\mathsf{cf}} (\Delta')^* \mathrel{-\!\!*} \varphi_j}{\Delta\,,(\Delta')^* \vdash_{\mathsf{cf}} \varphi_j}}{\Delta\,,\Delta' \vdash_{\mathsf{cf}} \varphi_j}$$

◻

We can give a similar characterization of the Heyting implication in C:

Proposition 6.5. *For every closed X, Y, the Heyting implication is closed and can be described as:*

$$X \to Y = \{\Delta \mid \forall \Delta' \in X,\ (\Delta\,;\,\Delta') \in Y\}.$$

Proof. Using Proposition 6.3, it is straightforward to check that $X \to Y$ as defined above is a right adjoint to the meet operation $\cap$. The proof of closedness follows the proof of Lemma 6.4. □

To sum up, by Theorem 5.7 we have a BI algebra C in which operations are defined as follows:

$$\mathsf{Emp} = \mathsf{cl}(\{\varnothing_m\}) \qquad \top = \mathit{Bunch}$$

$$\bot = \mathsf{cl}(\emptyset) \qquad X \vee Y = \mathsf{cl}(X \cup Y)$$

$$X * Y = \mathsf{cl}(\{\Delta\,,\,\Delta' \mid \Delta \in X, \Delta' \in Y\})$$

$$X \wedge Y = \mathsf{cl}(\{\Delta\,;\,\Delta' \mid \Delta \in X, \Delta' \in Y\})$$

$$X \mathrel{-\!\!*} Y = \{\Delta \mid \forall \Delta' \in X.\ (\Delta\,,\,\Delta') \in Y\}$$

$$X \to Y = \{\Delta \mid \forall \Delta' \in X.\ (\Delta\,;\,\Delta') \in Y\}$$

6.3 Fundamental property of C

We can interpret formulas in the model C by picking the interpretation of atomic propositions to be $[\![a]\!] = \langle a \rangle$. Now we are ready to prove the main theorem: if $[\![\varphi]\!] \subseteq [\![\psi]\!]$, then $\varphi \vdash_{\mathrm{cf}} \psi$. For this, we need to show $[\![\varphi]\!] \subseteq \langle \varphi \rangle$ for any formula φ. We prove it by induction on the formula φ; but we need to show a stronger statement in order to strengthen the induction hypothesis. This idea is due to Okada [Oka99].

Lemma 6.6 (Okada's property)**.** *For any formula φ,*

$$\varphi \in [\![\varphi]\!] \subseteq \langle \varphi \rangle$$

(where the leftmost instance of φ is a bunch consisting of a single leaf with the formula φ).

Proof. By induction on φ.

Case $\varphi = \mathsf{False}$. We have $[\![\mathsf{False}]\!] = \mathsf{cl}(\emptyset)$. Clearly, $\mathsf{cl}(\emptyset) \subseteq \langle \varphi \rangle$, because $\langle \varphi \rangle$ is closed and $\emptyset \subseteq \langle \varphi \rangle$. By Proposition 6.2 we have $\mathsf{False} \in [\![\mathsf{False}]\!]$.

Case $\varphi = \mathsf{True}$. We have $[\![\mathsf{True}]\!] = \mathit{Bunch} = \langle \mathsf{True} \rangle$.

Case $\varphi = \mathsf{Emp}$. In order to show $[\![\mathsf{Emp}]\!] = \mathsf{cl}(\{\varnothing_m\}) \subseteq \langle \mathsf{Emp} \rangle$, it suffices to show $\{\varnothing_m\} \subseteq \langle \mathsf{Emp} \rangle$, by the characterization of the closure operator. That inclusion holds because $\varnothing_m \vdash_{\mathrm{cf}} \mathsf{Emp}$. In order to show $\mathsf{Emp} \in \mathsf{cl}(\{\varnothing_m\})$, it suffices to show $\varnothing_m \in \mathsf{cl}(\{\varnothing_m\})$ by Proposition 6.2, which holds trivially.

Case $\varphi = \psi_1 * \psi_2$. In order to show the set inclusion $[\![\psi_1 * \psi_2]\!] = \mathsf{cl}([\![\psi_1]\!] \bullet [\![\psi_2]\!]) \subseteq \langle \psi_1 * \psi_2 \rangle$, it suffices to show $[\![\psi_1]\!] \bullet [\![\psi_2]\!] \subseteq \langle \psi_1 * \psi_2 \rangle$, by the characterization of the closure operator. If $(\Delta_1, \Delta_2) \in [\![\psi_1]\!] \bullet [\![\psi_2]\!]$, then, by the induction hypothesis $\Delta_i \vdash_{\mathrm{cf}} \psi_i$, and we can reason as follows:

$$\frac{\Delta_1 \vdash_{\mathrm{cf}} \psi_1 \qquad \Delta_2 \vdash_{\mathrm{cf}} \psi_2}{\Delta_1, \Delta_2 \vdash_{\mathrm{cf}} \psi_1 * \psi_2}$$

Hence, $(\Delta_1, \Delta_2) \in \langle \psi_1 * \psi_2 \rangle$.

As for the element inclusion $\psi_1 * \psi_2 \in \mathsf{cl}([\![\psi_1]\!] \bullet [\![\psi_2]\!])$, note that by Proposition 6.2 it suffices to show $(\psi_1, \psi_2) \in \mathsf{cl}([\![\psi_1]\!] \bullet [\![\psi_2]\!])$, which is evident from the induction hypotheses.

Case $\varphi = \psi_1 \wedge \psi_2$. In order to show the set inclusion, suppose that $\Delta \in [\![\psi_1 \wedge \psi_2]\!] = [\![\psi_1]\!] \cap [\![\psi_2]\!]$. Then, by the induction hypothesis, $\Delta \in \langle \psi_1 \rangle \cap \langle \psi_2 \rangle$, and we can reason as follows:

$$\cfrac{\cfrac{\Delta \vdash_{\mathrm{cf}} \psi_1 \qquad \Delta \vdash_{\mathrm{cf}} \psi_2}{\Delta\,;\,\Delta \vdash_{\mathrm{cf}} \psi_1 \wedge \psi_2}}{\Delta \vdash_{\mathrm{cf}} \psi_1 \wedge \psi_2}$$

As for th element inclusion $\psi_1 \wedge \psi_2 \in [\![\psi_1]\!] \cap [\![\psi_2]\!]$, we argue as follows. By the induction hypothesis, $\psi_1 \in [\![\psi_1]\!]$. By Proposition 6.2 (item 1), $(\psi_1; \psi_2) \in [\![\psi_1]\!]$, and by Proposition 6.2 (item 3), $\psi_1 \wedge \psi_2 \in [\![\psi_1]\!]$. Similarly we can show $\psi_1 \wedge \psi_2 \in [\![\psi_2]\!]$.

Case $\varphi = \psi_1 \mathrel{-\!\!*} \psi_2$. In order to show $[\![\psi_1 \mathrel{-\!\!*} \psi_2]\!] = [\![\psi_1]\!] \mathrel{-\!\!*} [\![\psi_2]\!] \subseteq \langle \psi_1 \mathrel{-\!\!*} \psi_2 \rangle$, suppose that $\Delta \in [\![\psi_1]\!] \mathrel{-\!\!*} [\![\psi_2]\!]$. We are to show $\Delta \vdash_{\mathrm{cf}} \psi_1 \mathrel{-\!\!*} \psi_2$. By the induction hypothesis, $\psi_1 \in [\![\psi_1]\!]$; hence

$$(\Delta\,,\,\psi_1) \in [\![\psi_2]\!] \subseteq \langle \psi_2 \rangle.$$

We can then reason using the right rule for $\mathrel{-\!\!*}$:

$$\frac{\Delta\,,\,\psi_1 \vdash_{\mathrm{cf}} \psi_2}{\Delta \vdash_{\mathrm{cf}} \psi_1 \mathrel{-\!\!*} \psi_2}$$

In order to show $\psi_1 \mathrel{-\!\!*} \psi_2 \in [\![\psi_1]\!] \mathrel{-\!\!*} [\![\psi_2]\!]$, suppose that $\Delta \in [\![\psi_1]\!]$. We are to show $(\Delta\,,\,\psi_1 \mathrel{-\!\!*} \psi_2) \in [\![\psi_2]\!]$. Let us write $[\![\psi_2]\!]$ as $\bigcap_{i \in I} \langle \varphi_i \rangle$. Then our goal can be reduced to showing

$$\Delta\,,\,\psi_1 \mathrel{-\!\!*} \psi_2 \vdash_{\mathrm{cf}} \varphi_i$$

for any $i \in I$. We argue as follows, using the left rule for $\mathrel{-\!\!*}$:

$$\frac{\Delta \vdash_{\mathrm{cf}} \psi_1 \qquad \psi_2 \vdash_{\mathrm{cf}} \varphi_i}{\Delta\,,\,\psi_1 \mathrel{-\!\!*} \psi_2 \vdash_{\mathrm{cf}} \varphi_i}$$

where the first assumption holds because $\Delta \in [\![\psi_1]\!] \subseteq \langle \psi_1 \rangle$ and the second assumption holds because $\psi_2 \in \langle \psi_2 \rangle$.

Case $\varphi = \psi_1 \to \psi_2$. Similarly to the case $\varphi = \psi_1 \mathrel{-\!\!*} \psi_2$, using the characterization of the Heyting implication in C.

Case $\varphi = \psi_1 \vee \psi_2$. In order to show $[\![\psi_1 \vee \psi_2]\!] = [\![\psi_1]\!] \vee [\![\psi_2]\!] \subseteq \langle \psi_1 \vee \psi_2 \rangle$, it suffices to show $[\![\psi_1]\!] \subseteq \langle \psi_1 \vee \psi_2 \rangle$ and $[\![\psi_2]\!] \subseteq \langle \psi_1 \vee \psi_2 \rangle$. To show that $[\![\psi_i]\!] \subseteq \langle \psi_1 \vee \psi_2 \rangle$, for $i = 1, 2$, it suffices to show $\langle \psi_i \rangle \subseteq \langle \psi_1 \vee \psi_2 \rangle$. We show that using the right rules for disjunction.

To show $\psi_1 \vee \psi_2 \in [\![\psi_1 \vee \psi_2]\!] = \mathsf{cl}([\![\psi_1]\!] \cup [\![\psi_2]\!])$, we appeal to the definition of $\mathsf{cl}(-)$: Let φ be a formula such that $[\![\psi_1]\!] \cup [\![\psi_2]\!] \subseteq \langle \varphi \rangle$. We are to show $\psi_1 \vee \psi_2 \in \langle \varphi \rangle$, i.e. $\psi_1 \vee \psi_2 \vdash_{\mathrm{cf}} \varphi$. By assumption we have $\psi_i \in [\![\psi_i]\!]$, for $i = 1, 2$, and, hence

$\psi_i \in \langle \varphi \rangle$, or, equivalently, $\psi_i \vdash_{\mathrm{cf}} \varphi$. We obtain the desired result using $\vee$L. ◻

Theorem 6.7. *The* CUT *rule is admissible in BI.*

Proof. Suppose that $\Delta \vdash \varphi$ is derivable. Then, $[\![(\Delta)^*]\!] \subseteq [\![\varphi]\!]$ in C. By Lemma 6.6, we have $(\Delta)^* \in [\![(\Delta)^*]\!] \subseteq [\![\varphi]\!] \subseteq \langle \varphi \rangle$. Thus, $(\Delta)^* \in \langle \varphi \rangle$. By Proposition 6.2, we have $\Delta \in \langle \varphi \rangle$, and, hence, $\Delta \vdash_{\mathrm{cf}} \varphi$. ◻

Overview. In the next sections we will be looking at adjusting the construction of C to extensions of BI. At this point we would like to give an overview of the argument, and see what kind of conditions we need.

- To show that the closure operator $\mathsf{cl}(-)$ is strong, we had to use invertibility of certain rules. Firstly, we used the fact that BI satisfies a strong form of the deduction theorem for both implications (the rules $\to$R and $-\!\!*$R are invertible). Secondly, we used the fact that the left rules are invertible for connectives that form bunches (EmpL, TrueL, $\wedge$L, $*$L).
- Additionally, we need to verify that all the rules of sequent calculus are validated in C.
- Finally, we need to show that the Okada's property (Lemma 6.6) holds in C.

This list gives us a sort of roadmap for extending the cut elimination argument. For every rule that we want to add to BI, we need to re-verify the invertibility of certain rules, and that the rule is validated in C. If we want to add a new connective to the system, we need to additionally come up with the interpretation of this connective on C, and re-verify the Okada's property.

7 Extending the logic: simple structural rules

An important extension of BI is *affine BI*, which extends the sequent calculus of Figure 1 with the weakening rule for **,**:

$$\frac{\Delta(\Delta_1) \vdash \varphi}{\Delta(\Delta_1 \,\mathbf{,}\, \Delta_2) \vdash \varphi}\ \mathrm{W}\mathbf{,}$$

An algebraic structure for interpreting affine BI is a BI algebra in which the following inequality holds: $p * q \leq p$. Can we extend the argument presented so far to cover affine BI? As we discussed at the end of the previous section, because we are adding a new rule, we have to make sure that the analogues of Lemma 3.2 and Lemma 3.4 still hold (the appropriate rule are invertible), and that C validates the inequality $X * Y \subseteq X$.

To verify that $X * Y \subseteq X$ it suffices to verify that $X \bullet Y \subseteq X$, since X is closed. Let us write $X = \bigcap_{i \in I} \langle \varphi_i \rangle$. Suppose that $\Delta_1 \in X, \Delta_2 \in Y$. We are to show that $\Delta_1 \,\mathbf{,}\, \Delta_2 \vdash_{\mathrm{cf}} \varphi_i$ for any i; however we know that $\Delta_1 \vdash_{\mathrm{cf}} \varphi_i$ by the assumption, and the desired result follows by W**,**.

This kind of argument for W**,** can be generalized to infinitely many structural rules of a particular shape, which we call, following [GJ13], *simple structural rules.* In the remainder of this section we show how to define such simple structural rules, and we prove cut elimination for BI extended with any combination of such rules.

7.1 Simple structural rules and bunched terms

Simple structural rules are rules of the shape

$$\frac{T_1[\Delta_1, \ldots, \Delta_n] \vdash \varphi \qquad \ldots \qquad T_m[\Delta_1, \ldots, \Delta_n] \vdash \varphi}{T[\Delta_1, \ldots, \Delta_n] \vdash \varphi}$$

where $T_1, \ldots, T_m, T$ are *bunched terms* – bunches built out of connectives **,** **;** and variables $x_1, \ldots, x_n$. The notation $T_i[\vec{\Delta}]$ stands for the bunch obtained from T_i by replacing all the variables x_j with Δ_j. Furthermore, we require that T is a *linear* bunched term – a term in which every variable x_j occurs at most once.

We identify a structural rule with a tuple $(\{T_1, \ldots, T_m\}, T)$. The rule W**,** above is represented with a tuple $(\{x_1\}, x_1 \,\mathbf{,}\, x_2)$. If L is a set of such tuples, we write BI+L for a sequent calculus of BI extended with the structural rules from L.

For the rest of this section, we fix a finite collection L of simple structural rules and the extended system BI+L. We write $\vdash_{\mathrm{cf}}$ for cut-free provability in BI+L, and we denote by C the BI algebra constructed in Section 6, but for BI+L-provability.

Firstly, we need to check that the construction of C works out. We need to verify that the rules $\to$L, $-\!\!*$L, $\wedge$L, $*$L, TrueL, EmpL are still invertible, in presence of the additional rules from L. For that, we just follow the proof of Lemma 3.4.

7.2 Interpretation of simple structural rules in C

Additionally, we need to verify that C validates all the rules from L.

Each bunched term $T[x_1, \ldots, x_n]$ can be interpreted as a function $[\![T]\!] : A^n \to A$ on any BI algebra A. For example, a (non-linear) bunched term $(x_1 \,\mathbf{,}\, x_2) \,\mathbf{;}\, x_1$ gives rise to a mapping $(X_1, X_2) \mapsto (X_1 * X_2) \wedge X_1$.

We say that an algebra A validates a simple structural rule $(\{T_1, \ldots, T_m\}, T)$ if the following inequality holds in A:

$$[\![T]\!](a_1, \ldots, a_n) \leq [\![T_1]\!](a_1, \ldots, a_n) \vee \cdots \vee [\![T_m]\!](a_1, \ldots, a_n)$$

for any $a_1, \ldots, a_n \in A$. For example, recall that the weakening rule W**,** for **,** is represented as $(\{x_1\}, (x_1 \,\mathbf{,}\, x_2))$. Then the associated inequality is

$$[\![x_1 \,\mathbf{,}\, x_2]\!](p, q) \leq [\![x_1]\!](p, q) \qquad \Longleftrightarrow \qquad p * q \leq p.$$

Lemma 7.1. *If a BI algebra A validates the rules in L, then $\Delta \vdash \varphi$ implies $[\![\Delta]\!] \leq [\![\varphi]\!]$ in A.*

In order to show that C validates all the rules from L, we need the following lemmas about $[\![T]\!]$. For the algebra C we have the following description:

Lemma 7.2. *Let $X_1, \dots, X_n \in \mathcal{C}$, and $\Delta_i \in X_i$ for $1 \le i \le n$. Then for any bunched term T,*

$$T[\vec{\Delta}] \in [\![T]\!](\vec{X})$$

Proof. By induction on T. □

Lemma 7.3. *For any $X_1, \dots, X_n \in \mathcal{C}$ and any linear bunched term T we have*

$$[\![T]\!](X_1, \dots, X_n) = \mathsf{cl}(\{T[\Delta_1, \dots, \Delta_n] \mid \Delta_i \in X_i, 1 \le i \le n\})$$

Proof. In view of Lemma 7.2 it suffices to show that the left-hand side is included in the right-hand side. This is done by induction on T. We show only the case for $\mathbf{,}$ as the other case is similar. If $T(\vec{x}) = F(\vec{x}) \mathbf{,} U(\vec{x})$, then, since T is linear, we can write it down as

$$T(\vec{y}\vec{z}) = F(\vec{y}) \mathbf{,} U(\vec{z})$$

for some factorization $\vec{y}\vec{z} = \vec{x}$, and for some linear terms F and U. By the induction hypothesis we have

$$[\![T]\!](\vec{Y}\vec{Z}) = \mathsf{cl}(\mathsf{cl}(\{F[\vec{\Gamma}] \mid \vec{\Gamma} \in \vec{Y}\}) \bullet \mathsf{cl}(\{U[\vec{\Gamma}] \mid \vec{\Gamma} \in \vec{Z}\})).$$

In order to show the inclusion into $\mathsf{cl}(\{T[\vec{\Delta}] \mid \vec{\Delta} \in \vec{Y}\vec{Z}\})$ it suffices to show

$$\{F[\vec{\Gamma}] \mid \vec{\Gamma} \in \vec{Y}\} \bullet \{U[\vec{\Gamma}] \mid \vec{\Gamma} \in \vec{Z}\} \subseteq \{T[\vec{\Delta}] \mid \vec{\Delta} \in \vec{Y}\vec{Z}\}.$$

Let $\vec{\Gamma} \in \vec{Y}$ and $\vec{\Theta} \in \vec{Z}$. Then, $\vec{\Gamma}\vec{\Theta} \in \vec{X}$, and, hence $F[\vec{\Gamma}] \mathbf{,} U[\vec{\Theta}] = T[\vec{\Gamma}\vec{\Theta}]$, which concludes the proof the inclusion. □

With the two lemmas at hand we can prove that $\mathcal{C}$ is a model of BI+L.

Lemma 7.4. *Every rule from the set L is validated in $\mathcal{C}$.*

Proof. Suppose that $(\{T_1, \dots, T_m\}, T)$ is a simple structural rule from L. We have to show $[\![T]\!](\vec{X}) \subseteq \mathsf{cl}(\bigcup_{1 \le i \le m} [\![T_i]\!](\vec{X}))$. By Lemma 7.3, it suffices to show

$$\{T[\Delta_1, \dots, \Delta_n] \mid \vec{\Delta} \in \vec{X}\} \subseteq \mathsf{cl}(\bigcup_{1 \le i \le m} [\![T_i]\!](\vec{X}))$$

where $\vec{\Delta} \in \vec{X}$ is a shorthand for $\Delta_i \in X_i$ for all $1 \le i \le n$.

Suppose that φ is such that $\bigcup_{1 \le i \le n} [\![T_i]\!](\vec{X}) \subseteq \langle\varphi\rangle$. We are to show that $T[\vec{\Delta}] \vdash_{\mathsf{cf}} \varphi$, for any $\vec{\Delta} \in \vec{X}$. By Lemma 7.2, we have $T_i[\vec{\Delta}] \in [\![T_i]\!](\vec{X}) \subseteq \langle\varphi\rangle$. So we get $T_i[\vec{\Delta}] \vdash_{\mathsf{cf}} \varphi$, from which we can conclude that $T[\vec{\Delta}] \vdash_{\mathsf{cf}} \varphi$ □

Theorem 7.5. *The* CUT *rule is admissible for BI+L.*

8 Extending the logic: an S4 modality

In this section we describe a different kind of extension to BI by "freely" adding an (intuitionistic) S4-like modality to BI. This would amount to adding the following rules (usual for intuitionistic formulation of S4 sequent calculus [Bd00]):

$$\square\mathrm{R}\ \frac{\square\Delta \vdash A}{\square\Delta \vdash \square A} \qquad \square\mathrm{L}\ \frac{\Delta(A) \vdash B}{\Delta(\square A) \vdash B}$$

where $\square\Delta$ is the same as Δ, but with boxes $\square$ put in front of all the formulas, e.g.

$$\square(\varnothing_m \mathbf{;} (\varphi \mathbf{,} \psi) \mathbf{;} \chi) \triangleq \varnothing_m \mathbf{;} (\square\varphi \mathbf{,} \square\psi) \mathbf{;} \square\chi.$$

We denote the extended system (the sequent calculus from Figure 1 with the rules □R, □L above) as BIS4. We can verify that the relevant rules are still invertible (a version of Lemma 3.4 and Lemma 3.2 for BIS4).

Interpreting the modality. As per the roadmap at the end of Section 6 we need to interpret the modality □ on $\mathcal{C}$ somehow. The usual way of interpreting a □ modality in intuitionistic setting is with an interior operator (c.f. the notion of a CS4 algebra [AMdR01, Definition 3]).

Definition 8.1. A *BIS4 algebra* is a tuple $(\mathcal{B}, \square)$ where $\mathcal{B}$ is a BI algebra and $\square : \mathcal{B} \to \mathcal{B}$ is a monotone function satisfying:

1. $\square p \le p$;
2. $\square p \le \square\square p$;
3. $\top = \square\top$
4. $\mathsf{Emp} = \square\mathsf{Emp}$;
5. $\square p \wedge \square q \le \square(p \wedge q)$;
6. $\square p * \square q \le \square(p * q)$.

We define the interior operator □ on $\mathcal{C}$ as:

$$\square X \triangleq \mathsf{cl}(\{\square\Delta \mid \Delta \in X\}).$$

In order to show that $\mathcal{C}$ satisfies the conditions from Definition 8.1, we will use the following lemmas.

Lemma 8.2. *The following rule is admissible:*

$$\square\text{-}\mathit{IDEMP}\ \frac{\Gamma(\square\square\Delta) \vdash \varphi}{\Gamma(\square\Delta) \vdash \varphi}$$

Proof. By induction on the height of the derivation, similar to the proof of Lemma 3.4. □

Lemma 8.3. *Let X be a closed set.*

- *If $\Delta \in X$, then $\square\Delta \in X$.*
- *If $\square\square\Delta \in X$, then $\square\Delta \in X$.*

Proof. By examining the definitions of □ and $\mathsf{cl}(-)$, using Lemma 8.2 for the second item. □

Lemma 8.4. *$(\mathcal{C}, \square)$ is a BIS4 algebra.*

Proof. The conditions (1) and (2) follow from Lemma 8.3. The conditions (3) and (4) can be shown by examining the definitions of all the connectives involved.

The condition (6) can be shown as follows. To show $\square X * \square Y \subseteq \square(X * Y)$, we reason as follows:

$$\square X * \square Y = \mathsf{cl}(\mathsf{cl}(\{\square\Delta \mid \Delta \in X\}) \bullet \mathsf{cl}(\{\square\Delta \mid \Delta \in Y\})) \subseteq$$
$$\mathsf{cl}(\mathsf{cl}(\{\square\Delta \mid \Delta \in X\} \bullet \mathsf{cl}(\{\square\Delta \mid \Delta \in Y\}))) =$$
$$\mathsf{cl}(\{\square\Delta \mid \Delta \in X\} \bullet \mathsf{cl}(\{\square\Delta \mid \Delta \in Y\})).$$

To show that

$$\mathsf{cl}(\{\Box\Delta \mid \Delta \in X\} \bullet \mathsf{cl}(\{\Box\Delta \mid \Delta \in Y\})) \subseteq \Box(X * Y)$$

it suffices to show that

$$\{\Box\Delta \mid \Delta \in X\} \bullet \mathsf{cl}(\{\Box\Delta \mid \Delta \in Y\}) \subseteq \Box(X * Y).$$

And, since

$$\{\Box\Delta \mid \Delta \in X\} \bullet \mathsf{cl}(\{\Box\Delta \mid \Delta \in Y\}) \subseteq \mathsf{cl}(\{\Box\Delta \mid \Delta \in X\} \bullet \{\Box\Delta \mid \Delta \in Y\}),$$

it suffices to show

$$\{\Box\Delta \mid \Delta \in X\} \bullet \{\Box\Delta \mid \Delta \in Y\} \subseteq \Box(X * Y).$$

Let Δ be such that $\Delta = \Box\Delta_1 \mathbin{,} \Box\Delta_2$, for $\Delta_1 \in X$, $\Delta_2 \in Y$. Then $\Delta = \Box(\Delta_1 \mathbin{,} \Delta_2)$, with $\Delta_1 \mathbin{,} \Delta_2 \in X * Y$.

Finally, the condition (5) is shown similarly. □

All it remains to verify is that the Okada's property (Lemma 6.6) still holds. Since we have added only the □ modality we need to check one extra case:

Lemma 8.5. *Assume that φ is such that $\varphi \in [\![\varphi]\!] \subseteq \langle\varphi\rangle$. Then*

$$\Box\varphi \in [\![\Box\varphi]\!] \subseteq \langle\Box\varphi\rangle.$$

Proof. In order to show the first inclusion, note that by the hypothesis, we have $\varphi \in [\![\varphi]\!]$. Hence, $\Box\varphi \in \{\Box\Delta \mid \Delta \in [\![\varphi]\!]\} \subseteq \Box[\![\varphi]\!]$.

To show the second inclusion, note that it suffices to show

$$\{\Box\Delta \mid \Delta \in [\![\varphi]\!]\} \subseteq \langle\Box\varphi\rangle.$$

So, let us assume $\Delta \in [\![\varphi]\!]$. By the induction hypothesis we have $\Delta \vdash_{\mathsf{cf}} \varphi$, and, hence $\Box\Delta \vdash_{\mathsf{cf}} \Box\varphi$. Which gives us the desired result $\Box\Delta \in \langle\Box\varphi\rangle$. □

Theorem 8.6. *The* CUT *rule is admissible for BIS4.*

9 The Coq formalization

As we mentioned, the results of this paper has been formalized in the Coq proof assistant. In this section we describe some of the design choices and trade-offs that we made.

For the algebraic semantics, we used a slightly modified formalization of BI algebras from the Iris Coq library [Iri, KJJ+18]. The Iris formalization makes heavy use of setoids, which allows us to easily formulate the model $\wp(\mathit{Bunch})$ of predicates on bunches quotiented by bunch equivalence.

The trickiest proofs to formalize were were the admissibility of the inverted rules (Lemma 3.4) in the cut-free sequent calculus. Firstly, as was mentioned in Section 3, those admissibility proofs proceed by induction on the height of the derivation. To handle this in the Coq formalization, we use an auxiliary relation `provesN : nat → bunch → formula → Prop` which includes the (upper bound on the) height of the derivation.

Our reasoning behind this definition is that if we were to define a proof height function and do induction on its value, we would have to formulate our goal (and the proof) in a rather unwieldy way: then we would have to package together the context, the formula, and the derivation into a Σ-type: `(`$\Sigma(\Delta : \mathit{Bunch})(\varphi : \mathit{Frml})$`, proves Δ φ)`.

Secondly, even with induction on proof height, in the proof of Lemma 3.4 we often end with a situation where we have a bunch Δ that can be decomposed multiple ways that we need to related to each other.

For example, in the proof of invertibility of $*$L, we want to obtain a proof of $\Delta_0(\varphi \mathbin{,} \psi) \vdash \chi$ from a proof of $\Delta_0(\varphi * \psi) \vdash \chi$. Suppose that the last applied rule in the proof was weakening

$$\frac{\Delta_1(\Gamma_1) \vdash_{\mathsf{cf}} \chi}{\Delta_1(\Gamma_1 \mathbin{;} \Gamma_2) \vdash_{\mathsf{cf}} \chi}$$

with $\Delta_1(\Gamma_1 \mathbin{;} \Gamma_2) = \Delta_0(\varphi * \psi)$. In order to apply the induction hypothesis we have to locate the formula $\varphi * \psi$ somewhere in the bunch $\Delta_1(\Gamma_1)$. The formula may appear either in Γ_1, Γ_2, or be part of the bunched context $\Delta_1(\cdot)$, depending on the relation between Δ_0 and Δ_1. This is an example of informal observation that comes up often in the BI sequent calculus because all the left rules (and structural rules) can be applied deep inside an arbitrary bunch. As such, reasoning about what appears where in bunched contexts is of importance.

In order to reason about situations like this in Coq, we define an auxiliary inductive system $\Delta \rightsquigarrow \langle\Pi(-) \mid \Delta'\rangle$ (intended pronunciation: *"Δ decomposes into $\Pi(-)$ and Δ'"*) that captures exactly when $\Delta = \Pi(\Delta')$. The rules for the decomposition of bunches is given in Figure 2.

$$\Delta \rightsquigarrow \langle(-) \mid \Delta\rangle \qquad \frac{\Delta_1 \rightsquigarrow \langle\Pi(-) \mid \Delta\rangle}{\Delta_1 \mathbin{,} \Delta_2 \rightsquigarrow \langle\Pi(-) \mathbin{,} \Delta_2 \mid \Delta\rangle}$$

$$\frac{\Delta_2 \rightsquigarrow \langle\Pi(-) \mid \Delta\rangle}{\Delta_1 \mathbin{,} \Delta_2 \rightsquigarrow \langle\Delta_1 \mathbin{,} \Pi(-) \mid \Delta\rangle}$$

$$\frac{\Delta_1 \rightsquigarrow \langle\Pi(-) \mid \Delta\rangle}{\Delta_1 \mathbin{;} \Delta_2 \rightsquigarrow \langle\Pi(-) \mathbin{;} \Delta_2 \mid \Delta\rangle} \qquad \frac{\Delta_2 \rightsquigarrow \langle\Pi(-) \mid \Delta\rangle}{\Delta_1 \mathbin{;} \Delta_2 \rightsquigarrow \langle\Delta_1 \mathbin{;} \Pi(-) \mid \Delta\rangle}$$

Figure 2. Inductive rules for decomposition of bunches.

Lemma 9.1. $\Delta = \Pi(\Delta')$ *if and only if* $\Delta \rightsquigarrow \langle\Pi \mid \Delta'\rangle$.

Using this inductive system we can prove the following lemmas about decomposition of contexts, that we use for formalizing proofs from Section 3:

Lemma 9.2. *If* $\Pi(\Delta) = \varphi$ *then* Π *is an empty context and* $\Delta = \varphi$.

Lemma 9.3. *If* $\Pi(\Delta) \rightsquigarrow \langle\Pi'(-) \mid \varphi\rangle$ *then one of the two conditions hold:*

- *The formula φ appears in Δ itself. That is, there is $\Pi_0(-)$ such that $\Delta \rightsquigarrow \langle\Pi_0(-) \mid \varphi\rangle$ and $\Pi'(-) = \Pi(\Pi_0(-))$.*
- *Or the formula φ appears in the context $\Pi(-)$. Then we can think of $\Pi'(-)$ as a context with two holes, one of*

which is already filled with Δ. Formally we represent this situation as follows. There are functions Π_0, Π_1 from bunches to bunched contexts, such that:

- *For any bunch Λ, we have $\Pi(\Lambda) \rightsquigarrow \langle \Pi_0(\Lambda)(-) \mid \varphi \rangle$.*
- *For any bunch Λ, we have $\Pi'(\Lambda) \rightsquigarrow \langle \Pi_1(\Lambda)(-) \mid \Delta \rangle$.*
- *For any bunches Λ, Λ', we have $\Pi_0(\Lambda)(\Lambda') = \Pi_1(\Lambda')(\Lambda)$.*

Similarly, in order to prove the invertibility of relevant rules for the extension of BI with a set of simple structural rules (as in Section 7), we additionally make use of the following auxiliary lemma:

Lemma 9.4. *If T is a linear bunched term with variables $x_1, \ldots, x_n$, and $T[\vec{\Delta}] = \Pi(\varphi)$ for some bunched context Π, then there is a variable x_j occurring in T, and a context Π' such that*

- *$\Delta_j = \Pi'(\varphi)$;*
- *for any bunch Γ,*

$$T[\Delta_1, \ldots, \Delta_{j-1}, \Pi'(\Gamma), \Delta_{j+1}, \ldots, \Delta_n] = \Pi(\Gamma).$$

In order to prove the invertibility of relevant rules for BIS4 (Section 8), including Lemma 8.2 we make use of the following auxiliary lemma:

Lemma 9.5. *If $\Box\Delta = \Pi(\Box\varphi)$, then there is a bunched context Π' such that*

- *$\Delta = \Pi'(\varphi)$;*
- *for any Γ, $\Box\Pi'(\Gamma) = \Pi(\Box\Gamma)$.*

10 Related work

There has been a long line of work on formalizing cut elimination and other meta-theoretical properties of logics in proof assistants. Here, we mention a few recent ones. Chaudhuri, Lima, and Reis [CLR17] have formalized cut elimination for various fragments of linear logic in Abella. Xavier, Olarte, Reis, and Nigam [XORN18] have formalized cut elimination and completeness of focusing for first-order linear logic in Coq, along with some other meta-theoretical properties. In [DG10], Dawson and Goré describe their framework for formalizing sequent calculus with explicit structural rules in Isabelle/HOL. They apply their framework for the provability logic GL and formalize the cut elimination argument for it. Their framework was later ported Coq [DDG21] and used to formalize cut elimination for a modal logic Kt. Another proof of cut elimination for GL was formalized in Coq [GRS21]; the authors noticed during the formalization process that the proof can be simplified in several parts.

Tews [Tew13] used Coq to formalize Pattinson's and Schröder's proof [PS10] of cut elimination for coalgebraic modal logics. During his formalization effort, Tews has uncovered a number of fixable gaps in the proof. As Tews puts it:

> A formalization of this extent does always uncover a number of typos and errors in the formalized work. It is a clear sign for the quality and accurateness of the pen-and-paper proofs of Pattinson and Schröder that I found only 4 errors beyond the level of nitpicking.

The formalized proofs mentioned above are syntactic. A formalized semantic proof of cut elimination for the $(\forall, \to, \bot)$ fragment of intuitionistic FOL was given by Herbelin and Lee [HL09], using Kripke models. The only similar formalization that we are aware is the formalization by Larchey-Wendling [Lar] of the Okada's semantic proof of cut elimination for linear logic [Oka99, Oka02]. A similar formalization of cut elimination for implicational relevance logic was used by the author used part of a larger formalization [Lar20]. In personal communication Larchey-Wendling mentioned that he has adapted his phase semantics proof to the logic of Bunched Implications, but was not completely satisfied with the formalization and did not publicize it.

After Okada's proof, related methods for proving cut elimination were discussed for various logics. For example, Belardinelli, Jipsen, and Ono [BJO04] use intermediate structures (Gentzen structures) to interpret sequent calculi and prove cut elimination for various substructural variants of the Lambek calculus. This method was generalized to handle non-associative logics (i.e. without the exchange rule) [GO10]. Ciabattoni, Galatos, and Terui [CGT08] prove semantic cut elimination for a wide ride of hypersequent calculi for non-classical logics.

Galatos and Jipsen [GJ13] introduced the framework of residuated frames which they use to prove cut elimination (and other related properties) for many extensions of Lambek calculus with arbitrary structural rules. The authors later extended their framework [GJ17] to cover extensions of distributive Lambek calculus and BI.

Our proof can be seen as a simplification of the Galatos and Jipsen's method. Instead of making heavy use of the residuated frames, our proof goes directly through algebraic semantics. While this is a less general framework, it still allows us to extend the proof to cover, e.g. modal extensions of BI, which were not covered by the residuated frames framework. We conjecture that the algebra we construct in Section 6 is isomorphic to the Galois algebra constructed in [GJ17, Section 4].

11 Conclusion and future work

In this paper we have presented a fully formalized semantic-based proof of cut elimination for the logic of bunched implications. We show that this proof can be extended to cover various extensions of BI, and demonstrated which parts of the proof have to be modified, and which remain unchanged.

As for future work, we see several ways of going forward. Firstly, we can look at extensions of BI. For example, we can probably extend the construction presented here to cover first-order/predicate BI. The algebra C is already complete (has all the meets and joins), so it is suitable for interpreting quantifiers. Unfortunately, formalizing this would require dealing with variable binders. It would also be natural to look at extensions such as GBI [GJ17], or extensions of BI with various modalities that are used in separation logic [BB18, DAH08].

Secondly, it would be interesting to go from logic to type theory. The algebra C is a subalgebra of predicates $\mathit{Bunch} \to \mathit{Prop}$, where Prop is the set of propositions. One can imagine it is possible to consider instead presheaves $\mathit{Bunch} \to \mathit{Set}$, and look for a categorification of C – a reflexive subcategory of the category of presheaves, which is universal for cut-free provability. That might give us some insight into the connections to the normalization-by-evaluation method for type theories [AHS95], which is usually based on the category of presheaves.

Acknowledgments

The author would like to thank Jorge Pérez, Revantha Ramanayake, and Niels van der Weide for giving comments on the draft version of this article, and Dominique Larchey-Wendling for informing the author about relevant related work.

References

[AHS95] Thorsten Altenkirch, Martin Hofmann, and Thomas Streicher. Categorical reconstruction of a reduction free normalization proof. In David Pitt, David E. Rydeheard, and Peter Johnstone, editors, *Category Theory and Computer Science*, Lecture Notes in Computer Science, pages 182–199, Berlin, Heidelberg, 1995. Springer.

[AMdR01] Natasha Alechina, Michael Mendler, Valeria de Paiva, and Eike Ritter. Categorical and Kripke Semantics for Constructive S4 Modal Logic. In Laurent Fribourg, editor, *Computer Science Logic*, Lecture Notes in Computer Science, pages 292–307, Berlin, Heidelberg, 2001. Springer.

[AQ12] Ryuta Arisaka and Shengchao Qin. LBI Cut Elimination Proof with BI-MultiCut. In *2012 Sixth International Symposium on Theoretical Aspects of Software Engineering*, pages 235–238, July 2012.

[BB18] Aleš Bizjak and Lars Birkedal. On Models of Higher-Order Separation Logic. *Electronic Notes in Theoretical Computer Science*, 336:57–78, April 2018.

[Bd00] G. M. Bierman and V. C. V. de Paiva. On an Intuitionistic Modal Logic. *Studia Logica*, 65(3):383–416, August 2000.

[BDP00] Mirjana Borisavljević, Kosta Došen, and Zoran Petrić. On permuting cut with contraction. *Mathematical Structures in Computer Science*, 10(2):99–136, April 2000.

[Bie96] G. M. Bierman. A note on full intuitionistic linear logic. *Annals of Pure and Applied Logic*, 79(3):281–287, June 1996.

[BJO04] Francesco Belardinelli, Peter Jipsen, and Hiroakira Ono. Algebraic Aspects of Cut Elimination. *Studia Logica*, 77(2):209–240, July 2004.

[Bro12] James Brotherston. Bunched Logics Displayed. *Studia Logica*, 100(6):1223–1254, 2012.

[BS09] Kai Brünnler and Lutz Straßburger. Modular Sequent Systems for Modal Logic. In Martin Giese and Arild Waaler, editors, *Automated Reasoning with Analytic Tableaux and Related Methods*, Lecture Notes in Computer Science, pages 152–166, Berlin, Heidelberg, 2009. Springer.

[CGT08] Agata Ciabattoni, Nikolaos Galatos, and Kazushige Terui. From Axioms to Analytic Rules in Nonclassical Logics. In *2008 23rd Annual IEEE Symposium on Logic in Computer Science*, pages 229–240, June 2008.

[CLR17] Kaustuv Chaudhuri, Leonardo Lima, and Giselle Reis. Formalized Meta-Theory of Sequent Calculi for Substructural Logics. *Electronic Notes in Theoretical Computer Science*, 332:57–73, June 2017.

[DAH08] Robert Dockins, Andrew W. Appel, and Aquinas Hobor. Multimodal Separation Logic for Reasoning About Operational Semantics. *Electronic Notes in Theoretical Computer Science*, 218:5–20, October 2008.

[dB96] Valeria de Paiva and Torben Braüner. Cut-Elimination for Full Intuitionistic Linear Logic, April 1996.

[DDG21] Caitlin D'Abrera, Jeremy Dawson, and Rajeev Goré. A Formally Verified Cut-Elimination Procedure for Linear Nested Sequents for Tense Logic. In Anupam Das and Sara Negri, editors, *Automated Reasoning with Analytic Tableaux and Related Methods*, Lecture Notes in Computer Science, pages 281–298, Cham, 2021. Springer International Publishing.

[DG10] Jeremy E. Dawson and Rajeev Goré. Generic Methods for Formalising Sequent Calculi Applied to Provability Logic. In Christian G. Fermüller and Andrei Voronkov, editors, *Logic for Programming, Artificial Intelligence, and Reasoning*, Lecture Notes in Computer Science, pages 263–277, Berlin, Heidelberg, 2010. Springer.

[Eve44] C. J. Everett. Closure Operators and Galois Theory in Lattices. *Transactions of the American Mathematical Society*, 55(3):514–525, 1944.

[GJ13] Nikolaos Galatos and Peter Jipsen. Residuated Frames with Applications to Decidability. *Transactions of the American Mathematical Society*, 365(3):1219–1249, 2013.

[GJ17] Nikolaos Galatos and Peter Jipsen. Distributive residuated frames and generalized bunched implication algebras. *Algebra universalis*, 78(3):303–336, November 2017.

[GO10] Nikolaos Galatos and Hiroakira Ono. Cut elimination and strong separation for substructural logics: An algebraic approach. *Annals of Pure and Applied Logic*, 161(9):1097–1133, June 2010.

[GR12] Rajeev Goré and Revantha Ramanayake. Valentini's cut-elimination for provability logic resolved. *The Review of Symbolic Logic*, 5(2):212–238, June 2012.

[GRS21] Rajeev Goré, Revantha Ramanayake, and Ian Shillito. Cut-Elimination for Provability Logic by Terminating Proof-Search: Formalised and Deconstructed Using Coq. In Anupam Das and Sara Negri, editors, *Automated Reasoning with Analytic Tableaux and Related Methods*, Lecture Notes in Computer Science, pages 299–313, Cham, 2021. Springer International Publishing.

[HL09] Hugo Herbelin and Gyesik Lee. Forcing-Based Cut-Elimination for Gentzen-Style Intuitionistic Sequent Calculus. In Hiroakira Ono, Makoto Kanazawa, and Ruy de Queiroz, editors, *Logic, Language, Information and Computation*, Lecture Notes in Computer Science, pages 209–217, Berlin, Heidelberg, 2009. Springer.

[Iri] Iris team. The Iris Project website and Coq development. https://iris-project.org/. Accessed: 2021-09-08.

[KJJ+18] Robbert Krebbers, Jacques-Henri Jourdan, Ralf Jung, Joseph Tassarotti, Jan-Oliver Kaiser, Amin Timany, Arthur Charguéraud, and Derek Dreyer. MoSeL: A general, extensible modal framework for interactive proofs in separation logic. *PACMPL*, 2(ICFP):77:1–77:30, 2018.

[Lar] Dominique Larchey-Wendling. Semantic cut-elimination for ILL via relational phase semantics. https://github.com/DmxLarchey/Coq-Phase-Semantics. Accessed: 2021-09-08.

[Lar20] Dominique Larchey-Wendling. Constructive Decision via Redundancy-Free Proof-Search. *Journal of Automated Reasoning*, 64(7):1197–1219, October 2020.

[MS14] Sonia Marin and Lutz Straßburger. Label-free modular systems for classical and intuitionistic modal logics. In *Advances in Modal Logic 10*, Groningen, Netherlands, August 2014.

[O'H19] Peter O'Hearn. Separation logic. *CACM*, 62(2):86–95, 2019.

[Oka99] Mitsuhiro Okada. Phase semantic cut-elimination and normalization proofs of first- and higher-order linear logic. *Theoretical Computer Science*, 227(1-2):333–396, 1999.

[Oka02] Mitsuhiro Okada. A uniform semantic proof for cut-elimination and completeness of various first and higher order logics. *Theoretical Compututer Science*, 281(1):471–498, June 2002.

[OP99] Peter O'Hearn and David Pym. The Logic of Bunched Implications. *The Bulletin of Symbolic Logic*, 5(2):215–244, 1999.

[POY04] David Pym, Peter O'Hearn, and Hongseok Yang. Possible worlds and resources: The semantics of BI. *Theoretical Computer Science*, 315(1):257–305, May 2004.

[PS10] Dirk Pattinson and Lutz Schröder. Cut elimination in coalgebraic logics. *Information and Computation*, 208(12):1447–1468, December 2010.

[PU09] Luís Pinto and Tarmo Uustalu. Proof Search and Counter-Model Construction for Bi-intuitionistic Propositional Logic with Labelled Sequents. In Martin Giese and Arild Waaler, editors, *Automated Reasoning with Analytic Tableaux and Related Methods*, Lecture Notes in Computer Science, pages 295–309, Berlin, Heidelberg, 2009. Springer.

[Pym02] David Pym. *The Semantics and Proof Theory of the Logic of Bunched Implications*. Applied Logic Series. Springer Netherlands, 2002.

[Rey02] John C. Reynolds. Separation logic: A logic for shared mutable data structures. In *LICS*, pages 55–74. IEEE Computer Society, 2002.

[SV82] Giovanni Sambin and Silvio Valentini. The modal logic of provability. The sequential approach. *Journal of Philosophical Logic*, 11(3):311–342, August 1982.

[Tew13] Hendrik Tews. Formalizing Cut Elimination of Coalgebraic Logics in Coq. In Didier Galmiche and Dominique Larchey-Wendling, editors, *Automated Reasoning with Analytic Tableaux and Related Methods*, Lecture Notes in Computer Science, pages 257–272, Berlin, Heidelberg, 2013. Springer.

[XORN18] Bruno Xavier, Carlos Olarte, Giselle Reis, and Vivek Nigam. Mechanizing Focused Linear Logic in Coq. *Electronic Notes in Theoretical Computer Science*, 338:219–236, October 2018.