Electronic Notes in Theoretical Computer Science 83 (2005)
URL: http://www.elsevier.nl/locate/entcs/volume83.html 21 pages

Ribbon Proofs

Jules Bean [1,2]

Department of Computer Science
Queen Mary, University of London
London, United Kingdom

Abstract

We present 'Ribbon Proofs', a graphical proof system for the Logic of Bunched Implications (BI). We give the informal, graphical, notation, we formalise the system algebraically and sketch the proof of its soundness and completeness. We discuss the spatial and geometrical nature of the proof system and its relation to BI's spatial model theory.

1 Introduction

The purpose of this paper is to introduce a novel proof system for the Logic of Bunched Implications (BI) [4]. In contrast to the proof theory given in [4] this system will actually tie in with the strong spatial intuitions which are suggested by BI's model theory.

The proof system is an extension of Fitch's box proofs, and it inherits the advantages and disadvantages of that system. Viewed in contrast to natural deduction (of which it should be seen as a variant), the linear box proof system contains two main features. Firstly, it totally internalises the structural rules, allowing a hypothesis to be used multiple times or not at all. Secondly, it isolates discharged hypotheses using non-overlapping boxes, which indicate the scope within which a hypothesis may be used. This is strictly analogous to scope of identifiers in computer programming languages.

The negative consequence of this economy of notation is that formulating a notion of a normal proof is more complex and less natural. One approach to normalization is to consider a translation between the system and either NJ or LJ. Such translations force some equalities between apparently very different proofs; most notably, a box proof can contain a totally unused subproof, these are ignored by the equivalence induced by such a translation.

[1] This work was supported by the author's EPSRC studentship
[2] Email: jules@dcs.qmul.ac.uk

Substitution, on the other hand, sits very nicely in the box proof system: to replace a hypothesis P by a proof of P, you can simply insert all the lines of the proof immediately above the formula P.

We give all the rules of box proofs, showing the notation we will use in this paper, in Fig. 1.

In the next section, we will give an introduction to BI, both its semantics, emphasising how they can be interpreted spatially, and its conventional proof theory. We will state the most important proof-theoretic theorems from [4,2], showing that the logic is in traditional senses a good one. Then we will go onto the main work, of the paper, describing our system of 'Ribbon Proofs', including a formal mathematized definition, a (sketch) proof of relative soundness and completeness, and a term model arising from the proof system. We will conclude by mentioning our ongoing work and possible applications of the system.

2 The Logic of Bunched Implications

2.1 Semantics

Recall that intuitionistic logic has a model using the notion of a universe of 'possible worlds', where at each world a particular set of atomic propositions is said to hold. These worlds are sometimes described as being possible future states of a system, or possible states of knowledge of an ideal observer. The connectives $\wedge$ and $\vee$ are interpreted pointwise at each world in the natural way, and the $\rightarrow$ connective relies on a partial ordering of the worlds. We write $w \models P$ iff a formula P holds at a world w, we decide which atomic formulae hold at each world, build up a complete forcing relation by structural induction, using the following formal rules:

- $w \models \top$ always
- $w \models \bot$ never
- $w \models P \wedge Q$ iff $w \models P$ and $w \models Q$
- $w \models P \vee Q$ iff $w \models P$ or $w \models Q$
- $w \models P \rightarrow Q$ iff, for each $v \sqsubseteq w$, if $v \models P$ then $v \models Q$

We extend these ideas in the following way. We consider universes where we have a notion of combining, or joining together, worlds. As a running example, we will take the logic [3] of O'Hearn, Ishtiaq, Reynolds, Calcagno, and Yang. Worlds are sets ('heaps') of cells in memory, where a cell is thought of as being a value at a location. The notion of combination is the disjoint union of sets, only to be defined when the sets of locations are disjoint. As a sample proposition, we will consider $a \hookrightarrow 3$, which indicates that the cell a exists in the heap and has value 3.

So we add to our possible worlds structure a combining operator, '$\cdot$', which makes them into a partial monoid. Partial, because the notion of combination

1.	$A \wedge B$	premise
2.	A	$\wedge$-*elim*

or

1.	$A \wedge B$	premise
2.	B	$\wedge$-*elim*

$\wedge$-*elim*

1.	A	premise
2.	B	premise
3.	$A \wedge B$	$\wedge$-*intro*

$\wedge$-*intro*

1.	$A \to B$	premise
2.	A	premise
3.	B	$\to$-*elim*

$\to$-*elim*

1.	A	assumption
	$\vdots$	
n.	B	
$n+1$.	$A \to B$	$\to$-*intro*

$\to$-*intro*

1.	A	premise
2.	$A \vee B$	$\vee$-*intro*

or

1.	B	premise
2.	$A \vee B$	$\vee$-*intro*

$\vee$-*intro*

1.	$A \vee B$	premise
2.	A	assumption
	$\vdots$	
n.	C	
$n+1$.	B	assumption
	$\vdots$	
m.	C	
$m+1$.	C	$\vee$-*elim*

$\vee$-*elim*

1.	A	premise
2.	$\neg A$	premise
3.	$\bot$	$\neg$-*elim*

$\neg$-*elim*

1.	A	assumption
	$\vdots$	
n.	$\bot$	
$n+1$.	$\neg A$	$\neg$-*intro*

$\neg$-*intro*

1.	$\bot$	premise
2.	A	$\bot$-*elim*

$\bot$-*elim*

Fig. 1. Box Proofs for Natural Deduction

need not always make sense: $w \cdot v$ will not be defined if w and v are overlapping heaps. For the purposes of this paper, we will assume that the operation is commutative, although there are no theoretical problems with the non-commutative version and it undoubtedly has some interesting applications. The identity of the partial monoid will be denoted e.

Definition 2.1 A *commutative partial monoid* is a set equipped with a partial binary operation '$\cdot$', satisfying the equations $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, $a \cdot b = b \cdot a$, and $a \cdot e = e$ in the sense that whenever the left hand side is defined, the right hand side must be defined, and they are equal, and vice versa.

Corresponding to our new operator on worlds, we can introduce two new logical connectives. Firstly, we add '$*$', which is a spatial 'and'. In our example $P * Q$ would mean that the heap being described can be split into two parts such that one satisfies P and the other Q. $a \hookrightarrow 3 * b \hookrightarrow 4$ means that the heap splits into two parts, one containing cell a with value 3, and one containing cell b with value 4; this is a different statement from $a \hookrightarrow 3 \wedge b \hookrightarrow 4$ because in the former, a and b are guaranteed to be different locations, in the latter they may (or may not) coincide.

Corresponding to that, we add the spatial implication $-\!\!*$. $P -\!\!* Q$ means that, given any heap satisfying P disjoint from the current heap, the combination of that one and the current forms a larger heap satisfying Q. $a \hookrightarrow 3 -\!\!* (a \hookrightarrow 3 * b \hookrightarrow 4)$ means that if we add to the current heap a (disjoint) heap in which the cell a has value 3, then in the new (combined) heap, cell a will have the value 3 and cell b the value 4.

Formally:

- $w \models P * Q$ iff, for some u and v such that $u \cdot v \sqsubseteq w$, $u \models P$ and $v \models Q$
- $w \models P -\!\!* Q$ iff, for every u such that $u \models P$ and $u \cdot w$ is defined, $u \cdot w \models Q$

In practice, many of the intuitive models are simplified by considering the Boolean variant of BI, where the accessibility relation '$\sqsubseteq$' is simply the identity relation.

The power of pointer logic comes in its application to produce a Hoare-style logic of computer programs. In [3] a system is described which considers $\{P\}\mathsf{program}\{Q\}$ assertions about computer programs, where P and Q are the pre- and post-conditions written in Pointer Logic.

2.2 Proof Theory

In [4], Pym presents two calculi for BI. He deals with predicate BI, but we shall restrict our interest to the propositional fragment. The two calculi are equivalent, and both are couched in terms of judgements about sequents, but one (LBI) is an analogue of sequent calculus with rules for introducing each connective on the left and the right, while the other (NBI) has 'natural deduction style' introduction and elimination rules, both acting on connectives on the right. Pym does not give a natural deduction calculus with judgements on

simple formulae. In a sense Ribbon Proofs come as close as currently seems possible to such a calculus.

Both LBI and NBI have sequents of a more general form than LJ. In LJ, (and NJ, and other similar calculi) the sequent is of the form $\Gamma \vdash P$ where Γ is typically a sequence, in some formulations a set, of formulae. This notion, however, is not sufficient for BI. In BI we work with Γ as a *bunch* of formulae, such as $(P, Q); ((R; P), S)$. Intuitively, the commas used to separate the sequence of formulae in an LJ-sequent are $\wedge$-like in their semantics; since BI has two conjunctions on an equal footing, we use a generalisation of a sequence with two punctuation marks, ';' corresponding to $\wedge$ and ',' to $*$.

Definition 2.2 A *bunch* is defined recursively as

$$formula|\emptyset_m|\emptyset_a|(bunch, bunch)|(bunch; bunch)$$

where *formula* is any BI proposition. We define an equivalence relation $\equiv$ on bunches to the effect that ',' and ';' are both associative and commutative (note that they do not distribute over each other), $\emptyset_a$ is the unit of ';', and $\emptyset_m$ of ','.

We will concentrate here on LBI, makes some of our proofs shorter. The system is shown in Fig. 2. Note how the rules for $*$ and $\wedge$ (also $-\!\!*$ and $\rightarrow$) are identical in form. The only difference between $*$ and $\wedge$ is the presence of the weakening and contraction rules for ;. Using the structurals you can reclaim the more familiar form of the $\wedge$ rules. Note that the structural rule of exchange is incorporated into the more general notion of $\equiv$ between bunches.

There are several semantics for BI presented in [4] for which LBI is sound. The simplest semantics for which LBI is complete is the partial monoid semantics we describe above, as proved in [2]:

Theorem 2.3 (Soundness and Completeness) *Any theorem $\Gamma \vdash P$ of LBI holds if and only if the corresponding semantic entailment $\Gamma \models P$ holds in the partial monoid semantics.*

We note a few other important proof theoretic facts from [4] and [2]:

Theorem 2.4 (Cut-Elimination) *To any proof in LBI using Cut, there corresponds a proof of the same sequent without Cut.*

Theorem 2.5 (Decidability) *There is a finite decision process for (propositional) LBI sequents, yielding either a proof or a counterexample.*

Theorem 2.6 (Finite model property) *For any LBI non-theorem, there exists not only a countermodel in the partial monoid semantics, but a finite one.*

$$\frac{}{P \vdash P}\, Axiom \qquad \frac{\Gamma \vdash P \quad \Delta(P)}{\Delta(\Gamma) \vdash P}\, Cut$$

$$\frac{\Gamma(\Delta) \vdash P}{\Gamma(\Delta;\Xi) \vdash P}\, W \qquad \frac{\Gamma(\Delta;\Delta) \vdash P}{\Gamma(\Delta) \vdash P}\, C$$

$$\frac{\Gamma \vdash P}{\Delta \vdash P}\, \Delta \equiv \Gamma$$

$$\frac{\Gamma(\emptyset_m) \vdash P}{\Gamma(I) \vdash P}\, IL \qquad \frac{}{\emptyset_m \vdash I}\, IR$$

$$\frac{\Gamma(\emptyset_a) \vdash P}{\Gamma(\top) \vdash P}\, \top L \qquad \frac{}{\emptyset_a \vdash \top}\, \top R$$

$$\frac{}{\bot \vdash P}\, \bot L$$

$$\frac{\Gamma \vdash P \quad \Delta(\Xi, Q) \vdash R}{\Delta(\Xi, \Gamma, P \mathrel{-\!\!*} Q) \vdash R}\, \mathrel{-\!\!*} L \qquad \frac{\Gamma, P \vdash Q}{\Gamma \vdash P \mathrel{-\!\!*} Q}\, \mathrel{-\!\!*} R$$

$$\frac{\Gamma(P, Q) \vdash R}{\Gamma(P * Q) \vdash R}\, *L \qquad \frac{\Gamma \vdash P \quad \Delta \vdash Q}{\Gamma, \Delta \vdash P * Q}\, *R$$

$$\frac{\Gamma \vdash P \quad \Delta(\Xi; Q) \vdash R}{\Delta(\Xi; \Gamma; P \to Q) \vdash R}\, \to L \qquad \frac{\Gamma; P \vdash Q}{\Gamma \vdash P \to Q}\, \to R$$

$$\frac{\Gamma(P; Q) \vdash R}{\Gamma(P \wedge Q) \vdash R}\, \wedge L \qquad \frac{\Gamma \vdash P \quad \Delta \vdash Q}{\Gamma; \Delta \vdash P \wedge Q}\, \wedge R$$

$$\frac{\Gamma(P) \vdash R \quad \Delta(Q) \vdash R}{\Gamma(P \vee Q); \Delta(P \vee Q) \vdash R}\, \vee L \qquad \frac{\Gamma \vdash P_i}{\Gamma \vdash P_1 \vee P_2}\, \vee R \quad (i = 1 \text{ or } 2)$$

Fig. 2. LBI

3 Ribbon Proofs

3.1 Introduction

$$(A \wedge B) * C \vdash (A * C) \wedge (B * C)$$

The theorem above can take the credit for motivating the system of Ribbon Proofs. It is a natural theorem to think about when exploring the logic; although $\wedge$ and $*$ do not distribute over each other, they do distribute 'one-way'.

It is easy to see the *semantic* proof of the theorem, in terms of the model theory given above. If a world w forces the formula $(A \wedge B) * C$, then there are

worlds u, v s.t. $u \cdot v \sqsubseteq w$, $u \models A \wedge B$ and $v \models C$. But then of course $u \models A$, and so $w \models A * C$; similarly $w \models B * C$. The LBI and NBI proofs of this theorem, whilst straightforward, do not reflect this simple semantic reasoning. The idea of the ribbon proof is to make the formal proof which reflects the spatial intuition of the semantic proof. The ribbon proof is shown in Fig. 3.

1.	$(A \wedge B) * C$		hypothesis
2.	$A \wedge B$	C	$*$-*elim* 1
3.	A		$\wedge$-*elim*2
4.	B		$\wedge$-*elim*2
5.	$A * C$		$*$-*intro* 3,2
6.	$B * C$		$*$-*intro* 4,2
7.	$(A * C) \wedge (B * C)$		$\wedge$-*intro* 4,2

Fig. 3. A ribbon proof

The heavily lined boxes, which we call ribbons, correspond to worlds of the semantics. The first line is a formula in a single ribbon, and the second line contains two ribbons – we will say that the ribbon has divided into two. Then in the fifth line, the two ribbons combine again, which takes the proof back to the original ribbon; we will say that $A * C$ holds in the same ribbon as $(A \wedge B) * C$.

This is the key to the intuitive reading of ribbon proofs. In a box proof, the informal reading of a formula is 'this formula holds, given the hypotheses', and for formulae inside boxes 'hypotheses' must be considered to include the temporary assumptions of the box. This loosely corresponds to a truth-value reading of classical or intuitionistic logic. Any similar truth-theoretical reading of BI needs to consider not only whether a formula holds, but *where* it holds, and this is provided by the ribbons.

Ribbon proofs form an extension of box proofs, so all the box proof rules are used in the familiar way. Premises and conclusion for the box proof rules must all be selected from the same ribbon. When boxes are used, they stretch the entire width of the proof[3], and are drawn as a lighter line to distinguish them from ribbons.

The $*$-*elim* rule, as illustrated in Fig. 3, allows the splitting of the current ribbon into two: if $P * Q$ holds, then somewhere P holds, and somewhere Q holds. The $*$-*intro* rule, conversely, joins two ribbons together to make a conclusion of the form $P * Q$.

The $-\!\!*$-*elim* rule has the same shape as $*$-*intro*. The $-\!\!*$-*intro*, just like $\rightarrow$-*intro*, is a subproof under an assumption. The $-\!\!*$ asssumption, however,

[3] This is not an essential feature of the system, but a design decision which we will stick to in this paper, as the formalism we present incorporates it

is in a separate ribbon – a ribbon which is in itself only hypothetical. To illustrate these rules, in Fig. 4 is a proof of one direction of the currying law for $*$ and $-\!\!*$. This proof also illustrates the pseudo-rule *twist* which allows the ribbons to behave commutatively.

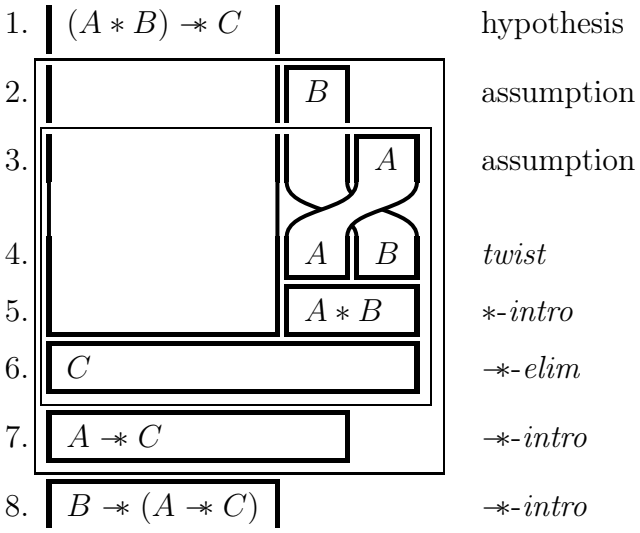


Fig. 4. A proof using $-\!\!*$ and *twist*

Finally, we have rules for the unit I. I-*elim* is the same shape as $*$-*intro*, and deals with the case that one ribbon turns out to be 'empty'. I-*intro* allows a split like $*$-*elim*, but one of the ribbons it creates is 'empty'. These rules are illustrated in Fig. 5.

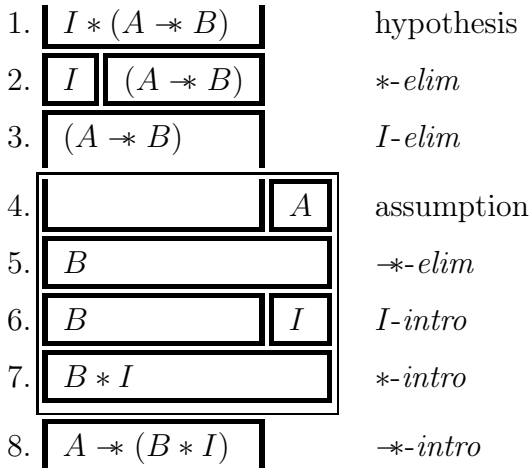


Fig. 5. A proof using I

3.2 Formal Definitons

We are aiming at a formal definition of a ribbon proof. At the heart of a ribbon proof is a particular kind of partial commutative monoid, and we firstly define that.

Definition 3.1 A *ribbon monoid* is a partial commutative monoid M, written additively, equipped with a 'greatest element' 1 satisfying the following:

- $(\forall r \neq e) r + r \uparrow$
- $(\forall r \exists s) r + s = 1$

We define on M a relation $\leq$ by

$$r \leq s \iff (\exists t) r + t = s$$

In fact, a great deal more than this can be shown about the particular ribbon monoids we are interested in, and we could make a stronger definition; for example, $\leq$ will turn out to be a partial order. However, that has no theoretical consequences in this paper, so we omit the proof and work with the above weaker notion of ribbon monoid.

Example 3.2 Take X an arbitrary set, M some subset of $P(X)$ containing $\{\}$, $A + B$ to be $A \cup B$ if $A \cap B = \{\}$, undefined otherwise, and close M under $+$ and complement relative to X. This is a ribbon monoid, e is $\{\}$, 1 is X, $\leq$ is $\subseteq$.

We define ribbon proofs formally in terms of a slightly more general notion, that of a proper ribbon structure — informally, an unfinished proof.

Definition 3.3 We define the following:

- A *ribbon structure* is a distinguished *box*;
- A *box* is a ribbon monoid, and a sequence of *lines* and *boxes*;
- A *line* is a set of triples $\langle r, f, j \rangle$ where
  - r is a *ribbon*,
  - f is a either a formula of (propositional) BI or the special non-formula *nothing*,
  - j is a *justification*;
- A *ribbon* is an element of the monoid;
- A *justification* is the name of a ribbon proof rule, or one of the special justifications *hypothesis*, *assumption*, or *nothing*;

This notion corresponds with our informal depiction of ribbon proofs. A line is just a line on a page containing some formulae. The triples are separated from each other by the thick lines which represent ribbons. We draw the f component of the triples in the ribbons, and we display the j component to the right of the proof; which works because the particular ribbon structures we need contain at most one non-*nothing* justification per line.

The most significant contribution of the notation is the way it indicates how one line relates to the next: the thick lines connect triples with the same ribbon component r; the r-component of the triples, and the structure of the ribbon monoid as a whole, is implicit in the way we join ribbons from one line to the next. The pseudo-rule *twist* makes this possible in more generality.

When we draw two (or more) ribbons s and t, say, in one line spanning exactly the same horizontal space as one ribbon r in the next, we are denoting the monoid identity $r = s + t$.

As an example, take the ribbon proof in Fig. 4. The outermost box (the proof itself) has the two-element monoid $\{e, a\}$ (i.e. $P(\{0\})$). The first line contains the triple $\langle a, (A * B) \mathrel{-\!\!*} C, \mathit{hypothesis}\rangle$. Then there is a box, which has the four element monoid $\{e, a, b, a+b\}$, and first line $\langle a, \mathit{nothing}, \mathit{nothing}\rangle$; $\langle b, B, \mathit{assumption}\rangle$. Next there is a further box, with larger monoid $\{e, a, b, a+b, c, a+c, b+c, a+b+c\}$ and first line $\langle a, \mathit{nothing}, \mathit{nothing}\rangle$; $\langle b, \mathit{nothing}, \mathit{nothing}\rangle$; $\langle c, A, \mathit{assumption}\rangle$. The *twist* gives rise to the same line again (as our formalism works with sets of triples, not sequences). The next line of this innermost box is $\langle a, \mathit{nothing}, \mathit{nothing}\rangle$; $\langle b + c, A * B, *\text{-}\mathit{intro}\rangle$, and the final line $\langle a + b + c, C, \mathrel{-\!\!*}\text{-}\mathit{elim}\rangle$. Returning to the intermediate box we have the line $\langle a + b, A \mathrel{-\!\!*} C, \mathrel{-\!\!*}\text{-}\mathit{intro}\rangle$, and then finallly in the outermost box again the line $\langle a, B \mathrel{-\!\!*} (A \mathrel{-\!\!*} C), \mathrel{-\!\!*}\text{-}\mathit{intro}\rangle$.

We are not interested in all ribbon structures, but rather ones obeying certain well-formedness conditions. We start with the notion of a ribbon structure *corresponding to a bunch*:

Definition 3.4 The ribbon structure *corresponding to a bunch* Γ, written RS_Γ is defined as follows by induction over the structure of bunches. We will write the monoid of RS_Γ as M_Γ, and the identity and greatest elements in that monoid as e_Γ and 1_Γ.

- The ribbon structure RS_P corresponding to a formula P has a single line, with a single triple $\langle 1, P, \mathit{hypothesis}\rangle$, and M_P is the two-element monoid $\{e, 1\}$ with $1 + 1 \uparrow$.
- $\mathsf{RS}_{\emptyset_a}$, corresponding to the 'additive empty bunch' contains a no lines, and $M_{\emptyset_a}$ is the same two-element monoid $\{e, 1\}$.
- $\mathsf{RS}_{\emptyset_m}$, corresponding to the 'multiplicative empty bunch' contains no lines and $M_{\emptyset_m}$ is the one-element monoid $\{e\}$.
- $\mathsf{RS}_{\Gamma;\Delta}$ has all the lines of RS_Γ followed by all the lines of RS_Δ. $M_{\Gamma;\Delta}$ is formed as the set $(M_\Gamma \cup M_\Delta)/\{e_\Gamma = e_\Delta, 1_\Gamma = 1_\Delta\}$. Any sum $r + s$ with $r \in M_\Gamma$ and $s \in M_\Delta$ is undefined, unless one or the other is e.
- $\mathsf{RS}_{\Gamma,\Delta}$ has all the lines of RS_Γ '*alongside*' the lines of RS_Δ. Where there are enough lines, this means taking the (automatically disjoint) union of the sets of triples in each line. Where one structure has fewer lines (w.l.o.g., RS_Γ), it can be padded with lines of the form $\{\langle 1_\Gamma, \mathit{nothing}, \mathit{nothing}\rangle\}$. $M_{\Gamma,\Delta}$ contains the elements $(M_\Gamma \cup M_\Delta)/\{e_\Gamma = e_\Delta\}$ and also, for every $r \neq e_\Gamma \in M_\Gamma$ and $s \neq e_\Delta \in M_\Delta$, a new, distinct, element $r+s$. $1_{\Gamma,\Delta}$ is the element $1_\Gamma + 1_\Delta$.

Definition 3.5 A *proper ribbon structure* is a member of the smallest class that contains all ribbon structures which correspond to bunches, and is closed under a certain set of ribbon structure transformations.

The tranformations are closely related to the ribbon proof rules. There are

in all seventeen transformations, which we will call $\wedge$-*intro*, $\wedge$-*elim*, $\vee$-*intro*, $\rightarrow$-*elim*, $\bot$-*elim*, $*$-*intro*, $-\!\!*$-*elim*, $*$-*elim*, I-*intro*, I-*elim*, Box $\rightarrow$-*intro*, Use $\rightarrow$-*intro*, Box $-\!\!*$-*intro*, Use $-\!\!*$-*intro*, Box$\vee$-*elim*, Use$\vee$-*elim* and *repeat*.

The first five such transformations, and the *repeat* rule, involve adding a single line to a structure. This line must be based on an existing line in the structure; that means it must have exactly the same set of ribbons in its triples. The line will have only one non-*nothing* formula in it, called the *conclusion*, in ribbon r say. There will be either one or two premise lines, which will also contain formulae (called *premises*) in ribbon r. The premise lines, and the line the conclusion is based on, must both be either in the same box as the conclusion or in some enclosing box. The triples in these lines are related as shown in the following table:

Rule	**Conclusion**	**Premises**
$\wedge$-*intro*	$\langle r, P \wedge Q, \wedge\text{-}intro\rangle$	$\langle r, P, j\rangle$ and $\langle r, Q, j'\rangle$
$\wedge$-*elim*	$\langle r, P, \wedge\text{-}elim\rangle$	$\langle r, P \wedge Q, j\rangle$ or $\langle r, Q \wedge P, j\rangle$
$\vee$-*intro*	$\langle r, P \vee Q, \vee\text{-}intro\rangle$	$\langle r, P, j\rangle$ or $\langle r, Q, j'\rangle$
$\rightarrow$-*elim*	$\langle r, Q, \rightarrow\text{-}intro\rangle$	$\langle r, P \rightarrow Q, j\rangle$ and $\langle r, P, j'\rangle$
repeat	$\langle r, P, repeat\rangle$	$\langle r, P, j\rangle$

The transformations relating to the rules $*$-*elim*, $*$-*intro* and $-\!\!*$-*elim* are slightly more involved. $*$-*intro* produces a new line with one fewer ribbons than the line it is based on, containing a ribbon $r + s$ for some pair r, s of ribbons in the line it is based on. It has two premise lines (they may be the same line), one which contains a formula P in the ribbon r and the other contains a formula Q in the ribbon s; its conclusion is the formula $P * Q$ in the newly created ribbon $r + s$.

$-\!\!*$-*elim* has exactly the same structure as $*$-*intro*, except that it expects a formula P in r and $P -\!\!* Q$ in s and produces Q in the new ribbon $r + s$.

The $*$-*elim* actually modifies the monoid of the ribbon structure. It operates on a premise of the form $P * Q$ in a ribbon r, say. The monoid is modified by adjoining two fresh elements s and t such that $s + t = r$.

There is a natural 'simplest' way to adjoin these elements to the monoid. The details are as follows: For every u in the monoid, $s + u$ and $t + u$ are both defined iff $r + u$ is defined. If they are defined, they are (distinct) fresh elements. Considering these elements, $(s + u) + v$ (resp. $(t + u) + v$) is defined to satisfy associativity; defined only if $u + v$ is defined. v itself is either an element of the original monoid (in which case $u + v$ was already defined, and we have already constructed the element $s + (u + v)$), or v is of the form $s + w$, so $s + u + v = s + u + s + w \uparrow$ (as $s + s \uparrow$), or v is of the form $t + w$ so $s + u + v = s + u + t + w = r + u + w$ in the original monoid.

Having modified the monoid, the new line can be inserted into the proof.

It will differ from the line it is based on by having the ribbon r replaced by the two new ribbons s and t. It will contain the two triples $\langle s, P, *\text{-}elim\rangle$ and $\langle t, Q, *\text{-}elim\rangle$.

I-*elim* has the structure of $-\!\!*$-*elim* and $*$-*intro*, but takes premises of the form P and I, and produces a conclusion of the form P.

I-*intro* has the structure of $*$-*elim*, and creates two new ribbons in exactly the same way, it differs in that from a premise of the form P it produces conclusions P and I. I-*intro* can also take a slightly different form, where instead of one ribbon being split into two, a new ribbon with formula I in it is created. This form is necessary for proving certain very simple theorems such as $\emptyset_m \vdash I$. In this case, the monoid is altered by adjoining a new element — but this is a special case of the previous alteration, with e being split into $e + r$ for some new r.

The remaining rules are the rules which use boxes, $\rightarrow$-*intro*, $-\!\!*$-*intro* and $\vee$-*elim*. In each case, the rule gives rise to two transformations: once which introduces a box, and one which uses it.

Using Box $\rightarrow$-*intro* we can introduce a new box into a ribbon structure. This box goes into an existing box, and inherits the monoid of that box. The box contains a single line, containing a single non-*nothing* formula, being an *assumption* formula P in a ribbon r, say. The box should be based on some previous line, so the set of ribbons used in it should be the same as some previous line in the enclosing box. The box is said to be focussed on ribbon r with assumption P.

Using Use $\rightarrow$-*intro*, we use an existing box created by Box $\rightarrow$-*intro* to add a line to the structure. The new line, which is to be placed immediately after the box, should be based on the last line of the box, which should contain a formula Q in the ribbon r that the box is focussed on. The new line contains its only non-*nothing* formula in that same ribbon r, and the formula is $P \rightarrow Q$ where P is the assumption of the box. Once this has been done, the box is said to have been *used*, and boxes may only be used once.

Similary, Box $-\!\!*$-*intro* adds a new box to a ribbon structure. However, in this case the monoid is different. It is the monoid of the enclosing box, with a new element r freely adjoined — by which we mean that $s+r$ is defined for all s in the original monoid, and the new greatest element 1 is formed by adding r to the original greatest element; $1 = 1_{old} + r$. The only line in the box is based on some previous line, and contains all the ribbons in that line (with *nothing* in them) plus additionally the new ribbon r, with an *assumption* P in it.

Now Use $-\!\!*$-*intro* uses a Box $-\!\!*$-*intro* box. A new line is created after the last line of the box, based on it. The last line of the box must contain a formula Q in some ribbon of the form $s + r$, where r was the new ribbon added in the box. The new line has the same ribbons except $s + r$ is replaced by s, and the formula is $P -\!\!* Q$ where P was the assumption. Again, a box may only be used once.

The $\vee$-*elim* rule is very similar to $\rightarrow$-*intro*, except with two boxes. Box$\vee$-*elim* has a premise of the form $A \vee B$ in some ribbon r, and it creates two single-line boxes, both of which must be based on the same line containing r, one with assumption A and one with assumption B. Use$\vee$-*elim* can be used when both boxes have arrived at the same conclusion C in some ribbon s in their last lines, which must both have the same set of ribbons in. The line added is placed after the boxes, and is identical to the two conclusion lines. Again, the boxes are said to be used when this has happened, and can only be used once.

These proper ribbon structures then formalise the notion of a ribbon proof under construction. Note that by the nature of the inductive definition, every such structure is based on some bunch Γ. A complete ribbon proof is simply such a structure which is 'finished':

Definition 3.6 A *ribbon proof* is a proper ribbon structure in which every box except the outermost has been *used* by the appropriate rule, and whose last line contains only a single ribbon, containing a formula P. It is said to be a proof *of* $\Gamma \vdash P$, where Γ is the bunch that the structure is based on.

3.3 Substitution and Normalization

One of the properties we expect from a formal proof system is some kind of substitution property; if we can prove something using a hypothesis P, and we have another proof of P from hypothesis Q, we expect to able to combine these two proofs to form a proof of the original conclusion using Q instead of P as hypothesis.

We use a notation $\Gamma(P)$ to denote a bunch which contains zero or more occurences of a formula P, and then $\Gamma(\Delta)$ to denote a similar bunch with those occurences replaced by a bunch Δ.

Theorem 3.7 (Substitution) *Given a ribbon proof* RP_1 *of* $\Gamma(P) \vdash Q$*, and a ribbon proof* RP_2 *of* $\Delta \vdash P$*, we can produce a ribbon proof* RP_3 *of* $\Gamma(\Delta) \vdash Q$

Proof. (Sketch) Firstly we combine the monoids M_1 and M_2 of the two proofs. For each hypothesis P in RP_1, which occurs in a ribbon r, say, we incorporate a copy of the entire monoid M_2. We do this as follows:

M_3 is defined to be M_1, with, for every hypothesis P in a ribbon r, a 'copy' of M_2. We make each such copy by adding to M_3 an element s_r for every element $1 \neq s \neq e \in M_2$. Within each such copy of M_2, the same monoid structure as M_2 is preserved. We equate 1_{M_2} with r. Then we define addition $t + s_r$ to be defined iff $t + r$ is defined, and to be a fresh element. Other additive cases follow as they must to preserve associativity. (Note that this is a generalisation of the procedure used in the $*$-*elim* construction to add elements to the monoid.)

Now we actually insert copies of the proof RP_2 at each hypothesis P. We delete each P, and below the line it occurred in, we insert a copy of RP_2 line

by line: Each line is based on the line of RP_1 that P occurred in, with the r-triple replaced by the set of all the triples in this line of RP_2, with the ribbons translated into those from this particular copy of M_2 within M_3.

It remains to show that this is indeed a ribbon proof, by showing that it can be constructed starting with the structure corresponding to $\Gamma(\Delta)$ and applying the rules of RP_1 and a number of copies of the rules for RP_2, a straightforward but rather longwinded verification we omit here. □

We mentioned briefly in the introduction that the notion of normalization for box proofs is somewhat messy; unfortunately, this problem is inevitably inherited by ribbon proofs. We will not deal with the details of that process here, but we observe that the difficulties in that process revolve mainly around the structural rules and hence the the intuitionistic box proof system; the multiplicative $*$ and $-\!\!*$ and their associated ribbon rules have simple equational properties.

3.4 Soundness and Completeness

We show that ribbon proofs are a sound and complete system by proving their equivalence to LBI, which is known to be sound and complete. We will outline in some detail the proofs of relative soundness, that every theorem provable with ribbon proofs is LBI provable, and relative completeness, that every theorem provable in LBI has a ribbon proof. Since both proofs proceed by cases for each ribbon proof rule, we give only the base cases and a representative selection of the rule cases.

We need some auxiliary concepts.

Definition 3.8 A *ribbon bunch* is a bunch based on ribbons (elements of the ribbon monoid of a box of a proof) instead of propositions. Given a particular ribbon monoid M, let the set of ribbon bunches over M be denoted $\mathsf{RB}(M)$. We define a partial interpretation function $[-] : \mathsf{RB}(M) \rightharpoonup M$ into ribbons as follows:

- $[r] = r$ for a ribbon r,
- $[\mathcal{R}; \mathcal{S}] = [\mathcal{R}] = [\mathcal{S}]$ if they are indeed equal, undefined if they are not equal,
- $[\mathcal{R}, \mathcal{S}] = [\mathcal{R}] + [\mathcal{S}]$ if that addition is defined in the monoid, undefined if not.

Definition 3.9 The *visible hypotheses* from a particular ribbon r at a particular line of a proof are

- hypotheses,
- assumptions,
- conclusions of $*$-*elim* and I-*intro* rules,

which satisfy the following:

- They occur in previous lines of this box, or previous lines of boxes enclosing this box;

- They occur in ribbons $\leq r$;
- In the case of $*$-*elim* conclusions or the 2-conclusion form of I-*intro*, occuring in the current box, only one of the pair is visible;
- In the case of the 1-conclusion form of I-*intro*, it must actually be in r itself.

What we are trying to do is, for each formula P in the proof, work out which hypotheses it could have been proved from. The delicate part is the inclusion of the $*$-*elim* conclusions: these formulae are neither assumptions nor hypotheses in the normal sense, but nonetheless they are the only way of formulating a local hypothesis notion like this.

Lemma 3.10 *For every formula P in a ribbon r in a ribbon proof, there is a (unique up to $\equiv$) ribbon bunch $\mathcal{R}$ such that*

- $[\mathcal{R}] = r$,
- $\mathcal{R}$ *contains all ribbons which contain hypotheses visible from P,*
- $\mathcal{R}$ *contains only such ribbons,*
- $\mathcal{R}$ *contains each ribbon at most once.*

We omit the proof of this lemma, which is a lengthy induction over the construction of ribbon structures.

Definition 3.11 The *corresponding sequent* to a formula P in ribbon r of a ribbon proof is a sequent $\Gamma \vdash P$, where Γ is a bunch (of BI formulae) constructed from the ribbon bunch $\mathcal{R}$ of Lemma 3.10 by replacing each ribbon s with a bunch Γ_s. Γ_s is an additive bunch (i.e. semicolon-separated) containing each hypothesis in s visible from P in r.

The notion of corresponding sequent, althought slightly delicately defined, is just a formalisation of the question 'What have we proved at this point?'.

Proposition 3.12 *In a ribbon proof of $\Gamma \vdash P$ the corresponding sequent to the conclusion P as it occurs in the final line of the proof is $\Gamma \vdash P$.*

Proof. Note that only hypotheses from the inital bunch can still be visible at P (all boxes must have closed, and both conclusions of any $*$-*elim* will be visible). □

We will prove relative soundness by showing, for every proof rule, that the corresponding sequent at the conclusion can be deduced from the corresponding sequents at the premises of the rule, and the structure of the proof. To do this, we need certain lemmas about these sequents:

Lemma 3.13 *The following hold of corresponding sequents in a ribbon proof:*

(i) *If P, Q and R all occur in that order in the same ribbon r in a proof, with Q in the same box as R or an enclosing one and P in the same box as Q or an enclosing one, then the corresponding sequents will have the form $\Gamma \vdash P$, $\Gamma; \Delta \vdash Q$ and $\Gamma; \Delta; \Xi \vdash R$.*

(ii) *If $\Gamma \vdash P$ is the corresponding sequent to a formula P in a ribbon r, and Γ in fact includes some $*$-elim or I-intro conclusion formula Q, then Γ will be of the form Γ', Q.*

(iii) *If P is a formula in ribbon r, Q in s and R in $r + s$, and there are no $*$-elim or I-intro conclusions visible from P and in the current box which match $*$-elim or I-intro conclusions visible from Q and in the current box, then the corresponding sequents will have the form $\Gamma \vdash P$, $\Delta \vdash Q$ and $((\Gamma; \Gamma'), (\Delta, \Delta')); \Xi \vdash R$.*

(iv) *Alternatively, if $*$-elim or I-intro conclusions $S_0, S_1, \ldots$ visible from P match $T_0, T_1, \ldots$ visible from Q, then the corresponding sequents are of the form $\Gamma, S_0, S_1, \ldots \vdash P$, $\Delta, T_0, T_1, \ldots \vdash Q$ and $(\Gamma, \Delta, \Sigma_0, \Sigma_1, \ldots); \Xi \vdash R$, where $\Sigma_n \vdash S_n * T_n$ is the corresponding sequent at the formula $S_n * T_n$ from which S_0 and T_0 were deduced by $*$-elim, or, alternatively, $\Sigma_n \vdash S_n$ corresponded to S_n from which S_n and I were deduced by I-intro.*

Now we are in a position to move on to our main results.

Theorem 3.14 (Relative Soundness) *If there is a ribbon proof of a sequent $\Gamma \vdash P$, then it is a theorem of LBI.*

Proof. [Sketch] We prove the stronger statement that in a ribbon proof, every corresponding sequent is a theorem of LBI.

We fix a particular ribbon proof $\Gamma \vdash P$, and we work through the proof line by line, proving for each line that every corresponding sequent is an LBI-theorem. By induction, we assume that all corresponding sequents in previous lines are LBI-theorems.

The base step concerns hypotheses. The corresponding sequent to a hypothesis is a (generalised) axiom sequent $\Gamma; P \vdash P$.

There is an inductive step for each of the ribbon proof rules. We will prove here a representative selection. For each case, we show in Fig. 6 a general ribbon proof using the rule, annotated with the corresponding sequents at the important points, and show the LBI proof that the sequent corresponding to the conclusion follows from the other sequents.

- $\wedge$-*intro*: By the first part of Lemma 3.13, the corresponding sequents involved will be $\Gamma_0 \vdash P$, $\Gamma_0; \Gamma_1 \vdash Q$, and $\Gamma_0; \Gamma_1; \Gamma_2 \vdash P \wedge Q$. The last sequent can be deduced as shown from the first two in LBI, using the $\wedge R$ rule and the structurals.
- $-\!\!*$-*elim*: There are two cases for this rule, corresponding to parts (iii) and (iv) of Lemma 3.13.

  In the first case, where no pair of $*$-*elim* formulae is 'reunited' by this rules use, the sequents at P and $P -\!\!* Q$ will be $\Gamma_0 \vdash P$ and $\Gamma_1 \vdash P -\!\!* Q$, and the sequent at Q will be $((\Gamma_0; \Gamma_2), (\Gamma_1; \Gamma_3)); \Gamma_4 \vdash Q$. This follows from the first two using $-\!\!* L$ and structural rules.

  In the second case, some $*$-*elim* formulae are brought back together, and we know more details about the structure of the corresponding sequents.

Now the corresponding sequents will have the forms $\Gamma_0, S_0, S_1, \ldots \vdash P$ and $\Gamma_1, T_0, T_1, \ldots \vdash P \mathrel{-\!\!*} Q$, but the proof must earlier include all the formulae $S_n * T_n$, with corresponding sequents $\Sigma_n \vdash S_n * T_n$, say. The corresponding sequent to Q will be $\Gamma_0, \Gamma_1, \Sigma_0, \Sigma_1, \ldots \vdash Q$, which we can deduce using $*L$, *Cut*, and $\mathrel{-\!\!*} L$.

The similar case with *I-intro* involves use of IR and Cut.

We illustrate both a case with no $*$-*elim* formulae reunited, and a case with two pairs.

- $*$-*intro* is handled exactly like $\mathrel{-\!\!*}$-*elim*, although it is slightly simpler as the $*R$ rule corresponds more closely to $*$-*intro* than $\mathrel{-\!\!*} L$ does to $\mathrel{-\!\!*}$-*elim*. It has the same cases, depending if any unpaired $*$-*elim* or *I-intro* formulae are involved. We illustrate only the simpler case here.
- $*$-*elim* is a special case. As actually used in a proof on a formula $P * Q$, it creates two fresh ribbons s and t and two formulae P and Q whose corresponding sequents will be the axiom sequents $P \vdash P$ and $Q \vdash Q$, so no proof is needed. The actual 'use' of $*$-*elim* comes when the P and Q are 'reunited' and is covered under the rules above. The real work is all in the definition of corresponding sequent.

□

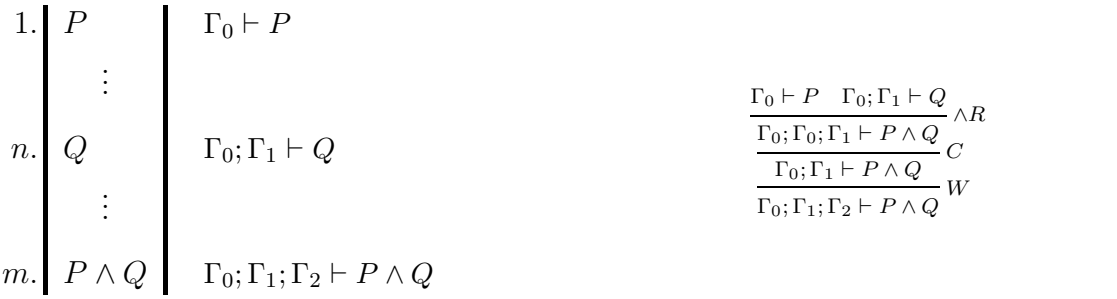
Theorem 3.15 (Relative Completeness) *For every theorem $\Gamma \vdash P$ of LBI, there is a ribbon proof with a single ribbon containing the formula P as its last line, such that the sequent at P is $\Gamma \vdash P$.*

Proof. [Sketch] We prove this by induction over the rules used in the LBI proof of $\Gamma \vdash P$, showing that there is a ribbon proof of every sequent occuring in the proof.

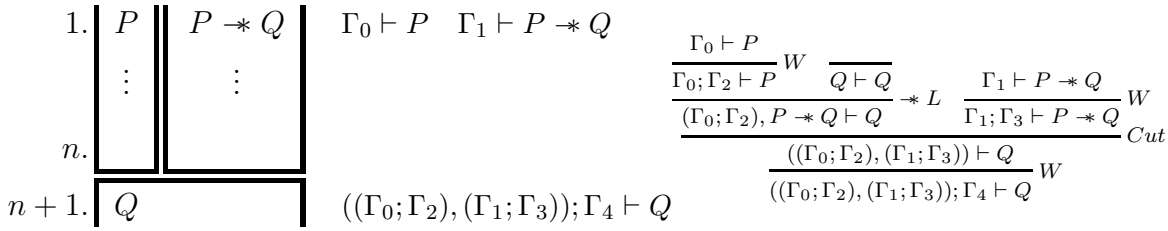
The base case is again the axiom sequent $P \vdash P$. The ribbon proof is that is the two lines, containing the formula P once as a hypothesis, and once as the conclusion of the *repeat* rule.

There is an induction step for each of the LBI rules. Again, we prove here only a few cases. Every case is a straightforward transformation on proofs. Each case discussed is illustrated in Fig. 7.

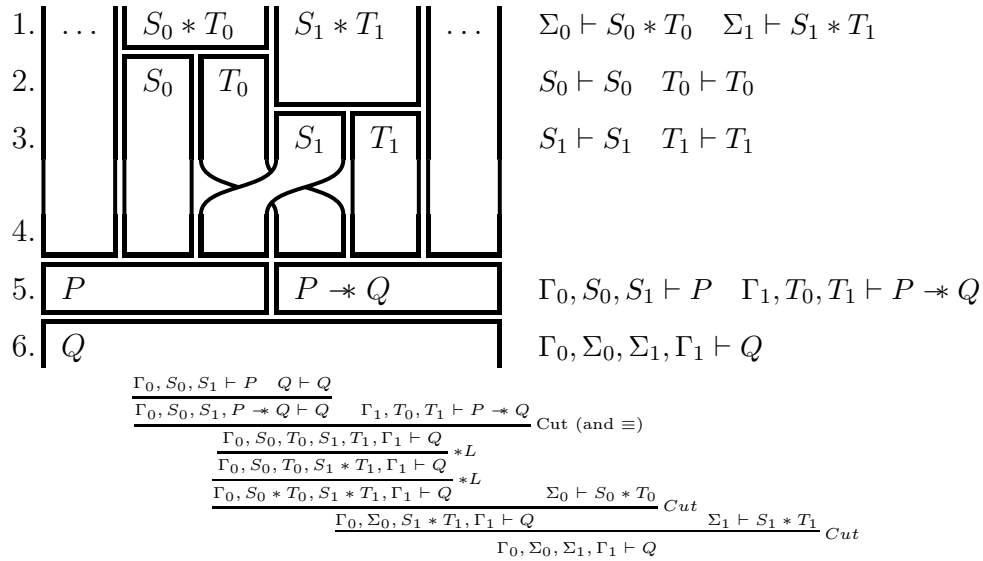
- $\wedge L$: By induction, we have a ribbon proof $\Gamma; A; B \vdash P$. We transform it by adding a hypothesis $A \wedge B$ above the hypotheses A and B. Then we change A and B from being hypotheses to being derived from $A \wedge B$ by use of $\wedge$-*elim*, and leave the rest of the proof the same.
- $*R$: By induction we have ribbon proofs of $\Gamma_0 \vdash P$ and $\Gamma_1 \vdash Q$, and we place them side-by-side and add a final $*$-*intro* step. The formal definition of placing side-by-side is analagous to the notion used to construct the ribbon structure corresponding to a bunch (Δ, Γ).
- $*L$: We have by induction a ribbon proof of $\Gamma, A, B \vdash P$. We write this proof such that A and B occur as horizontally adjacent hypotheses (may



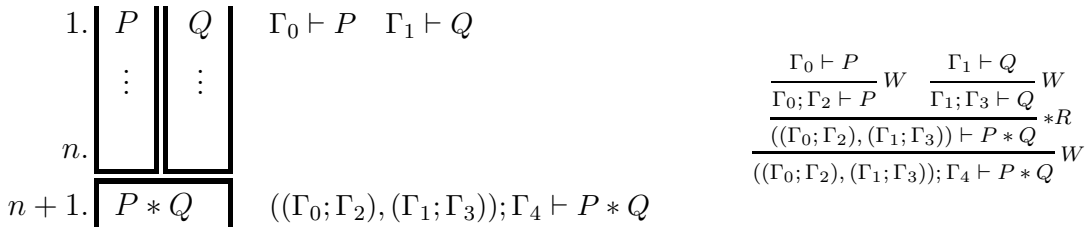
∧-*intro*



−∗-*elim* - simplest case



−∗-*elim* - with 2 pairs of ∗-*elim* formulae involved



∗-*intro*

Fig. 6. Some cases of relative soundness

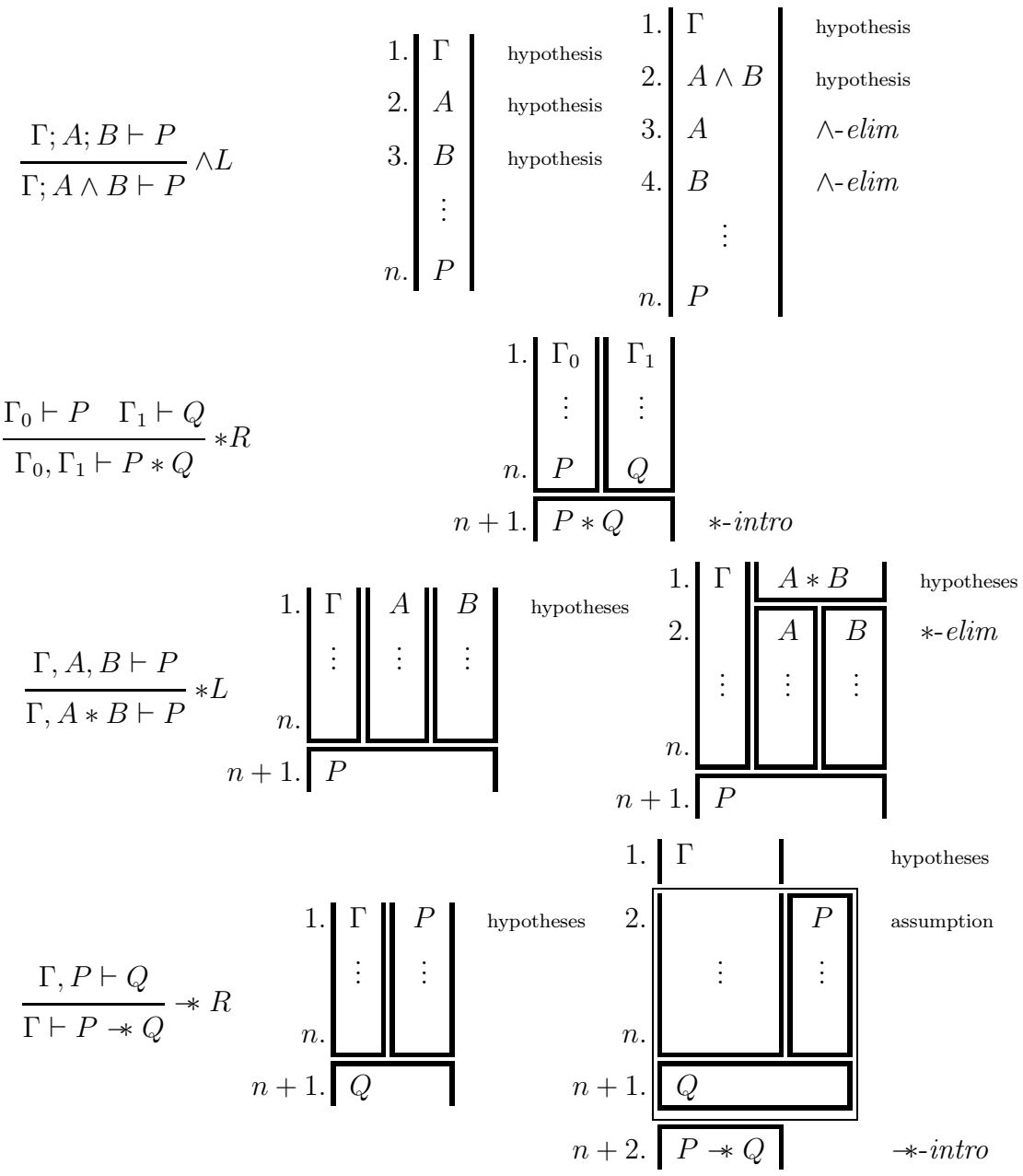


Fig. 7. Some cases of relative completeness

require use of *twist*), and we transform it by placing immediately above A and B the new hypothesis $A * B$. We then alter A and B to no longer be hypotheses, but instead derived from $A * B$ by $*$-*elim*, and leave the rest of the proof intact.

- $\mathrel{-\!\!*}\ R$: By induction we have a ribbon proof of $\Gamma, P \vdash Q$. We construct a proof of $\Gamma \vdash P \mathrel{-\!\!*} Q$ using $\mathrel{-\!\!*}$-*intro* as the final step, and inserting the given proof inside the box produced by the $\mathrel{-\!\!*}$-*intro* rule.

□

3.5 A Spatial 'Term Model'

Ribbon proofs give rise to a model of sorts. Consider a ribbon proof within the $\wedge$, $*$, $-\!\!*$ fragment of BI. Now we *close* the proof in the appropriate sense: we apply the rules $\wedge$-*elim*, $*$-*elim* and $-\!\!*$-*elim* to each applicable formula (twice to each in the case of $\wedge$-*elim*) until this is no longer possible. We also need a reduction from formulae of the form $T -\!\!* P$ to P where T is a multiplicative theorem (i.e. $\emptyset_m \vdash M$).

The resulting proof remains a proof of the original theorem, albeit with various apparently unnecessary rule uses. However, it can also yield a model of the theorem: by a model of a theorem $\Gamma \vdash P$, we mean a witnessing model m such that $m \models \Gamma$ and $m \models P$.

There are two ways of extracting this model. Most abstractly, we extract the model as the ribbon monoid of the proof. We set the forcing relation for atoms to be $r \models A$ iff A occurs as a bare atom in ribbon r in the proof. It is then easy to prove by induction that the forcing rules for $*$, $\wedge$ and $-\!\!*$ will ensure that $m \models \Gamma$ and $m \models P$.

More concretely, we can produce a geometrical model based on the actual representation of the proof on paper, by 'squashing' the proof vertically and taking the model to be, for each ribbon r, a closed interval of the real line. Then define $\cdot$ to be union of 'almost-disjoint' sets: that is, the intersection may be at most a finite set of points. To make the model work, we need to be careful that no $r \neq s$ map to exactly the same set; we also need to understand that although for clarity we allow a small horizontal gap between adjacent ribbons, in a geometrical semantics they should overlap in a line.

The geometrical model is, of course, the same monoid as the first, so the same model in an algebraic sense; it provides a concrete representation of it.

This strategy is too naive to account for I, $\bot$, $\rightarrow$ and $\vee$. Similar models should be possible for these cases.

- I: To account for I, we would have to take a quotient of the monoid so that wherever $r \models I$ we simply set $r = e$.
- $\bot$: The partial monoid semantics uses undefined sums to internalise $\bot$. Accordingly, to modify the the above model to account for $\bot$, we would have to alter the monoid so that if in some ribbon r, $\bot$ is provable, r should be 'undefined'. So we set $r\uparrow$, i.e. for all $s+t=r$, we set $s+t\uparrow$, and further for all u, $r+u\uparrow$ in the same sense.
- $\rightarrow$: The semantics for $\rightarrow$ involves constructing the accessibility relation $\sqsubseteq$. This will inevitably make the model much more complex. As well as adding the $\rightarrow$-*elim* rule to the set of reductions, we have to add many additional worlds to the model. A possible strategy is, for each ribbon r, and each atomic proposition A not already in r, we add a new ribbon $r_A \sqsubseteq r$, and in r_A we add the formula A, and repeat the reduction process. (If we are also in the setting where we account for $\bot$, we only add r_A if it is not inconsistent.)

For every other ribbon s such that $r + s$ was defined, we now have to define a new ribbon $r_A + s = s_{r_A} \sqsubseteq r + s$, say, and continue with the reduction process. This will yield a very large model indeed. Adding $\rightarrow$ also requires reductions for formulae $T \rightarrow P$ where T is an additive theorem.

- $\vee$: To add $\vee$ to our model, we would need to pass in some way from ribbon monoids to sets of ribbon monoids, parallel to the treatment of $\vee$ in the notion of prime bunches in [4]. (In fact, all this term model work is closely related to that notion)

4 Discussion

This research was originally motivated by practical concerns; the proofs which were arising during the ongoing research of O'Hearn et al. To actually develop this proof system into a proof system for Pointer Logic itself would involve two principal enhancements. Firstly, to investigate a minimal set of axioms for the domain-specific concerns of that logic, and secondly to deal with the limited quantification in that logic. This fulls far short of the full complex system of quantifiers in Predicate BI.

Work is currently ongoing into an implementation of the system in ML. Currently this takes the form of an abstraction of the notion of ribbon proof, with some functions representing various proof-transformations. It would be nice to enhance it in the direction of being a visual proof calculator in the style of Jape[1].

Another interesting direction is to consider the graphical nature of the proofs. Having presented what is a visibily graphical system, we have then given it formal meaning in a very algebraic way. We are also investigating whether the proofs can be given a genuinely geometrical semantics mirroring their informal presentation on paper, and whether this can be related to the spatial nature of BI's model theory.

References

[1] R Bornat and BA Sufrin. Animating formal proof at the surface: the Jape proof calculator. *The Computer Journal*, 43(3):177–192, 1999.

[2] Didier Galmiche, Daniel Mery, and David Pym. Resource tableux (extended abstract). In *Proceedings of CSL'02*, LNCS. Springer-Verlag, to appear 2002.

[3] Peter O'Hearn, John Reynolds, and Hongseok Yang. Local reasoning about programs that alter data structures. In *Proceedings of CSL'01*, LNCS, pages 1–19. Springer-Verlag, 2001.

[4] DJ Pym. *The Semantics and Proof Theory of the Logic of Bunched Implications*. Applied Logic Series. Kluwer Academic Publishers Boston/Dordrecht/London, 2002.