Direct elimination of additive-cuts in GL4ip: verified and extracted.

Rajeev Goré

Technical University of Vienna, Austria, and Polish Academy of Science, Poland

Ian Shillito

Australian National University, Australia

Abstract

Recently, van der Giessen and Iemhoff proved cut-admissibility for the sequent calculus GL4ip for propositional intuitionistic provability logic. To do so, they were forced to use an indirection via the GL3ip calculus as GL4ip resists all standard direct cut-admissibility techniques. This indirection leaves little hope for the extraction of a comprehensible cut-elimination procedure for GL4ip from their work.
We eliminate this indirection: we prove the admissibility of additive cut for GL4ip in a direct way by using a recently discovered proof technique which requires the existence of a terminating backward proof-search procedure in this calculus. By formalising our results in Coq we: (1) exhibit a successful direct proof technique for cut-admissibility for GL4ip ; (2) extract a syntactic cut-elimination procedure for GL4ip in Haskell ; and (3) use a local measure on sequents based on the shortlex order to show that the proof-search terminates. Once again, we see an unusual phenomenon in that terminating backward proof-search forms the basis for syntactic cut-elimination rather than for semantic cut-free completeness.

Keywords: Intuitionistic provability logic, Cut elimination, Backward proof-search, Interactive theorem proving, Proof theory.

Acknowledgement

Rajeev Goré supported by the FWF project P 33548. We acknowledge the support of the National Centre for Research and Development, Poland (NCBR), and the Luxembourg National Research Fund (FNR), under the PolLux/FNR-CORE project STV (POLLUX-VII/1/2019).

1 Introduction

Classical modal provability logics have gained a lot of attention because of the ability to interpret the formula $\Box A$ as "A is provable in Peano Arithmetic" [12]. As usual, the completeness of the traditional sequent calculus for provability logic with respect to the traditional Hilbert axiomatisation requires showing cut-admissibility. But cut-admissibility is usually not trivial because the standard double-induction on the size of the cut-formula and the height of the derivation do not suffice. To solve this problem, Valentini [18] introduced a third complex parameter called "width" in addition to these two traditional induction measures. The complications in his cut-admissibility argument in a set-based setting led to many claims and counter-claims, finally resolved thirty years later by Goré and Ramanayake [8] in a multiset setting.

Recently, van der Giessen and Iemhoff [19] showed that the proof-theory of intuitionistic provability logics is also complicated. They gave a cut-free sequent calculus GL3ip for intuitionistic provability logic extending the standard G3ip [17] calculus for intuitionistic logic with the following well known rule:

$$\frac{X, \Box X, \Box A \Rightarrow A}{W, \Box Y, \Box X \Rightarrow \Box A} \text{ (GLR)}$$

Similarly to G3ip, the admissibility of the rules of weakening and contraction can easily be shown for GL3ip. However, the admissibility of cut encounters the same problems as for GL, leading van der Giessen and Iemhoff to successfully adapt the technique developed by Valentini, thus obtaining a direct proof of cut-admissibility for intuitionistic provability logic.

However, GL3ip cannot support a simple terminating backward proof-search strategy because its left-implication rule, inherited from G3ip and shown below, allows trivial cycles up the left premise as is well known:

$$\frac{X, A \to B \Rightarrow A \quad X, B \Rightarrow C}{X, A \to B \Rightarrow C} \text{ (}{\to}\text{L)}$$

To solve this problem and characterize a terminating proof-search procedure, they follow Dyckhoff [6] and Hudelmaier [10] and define the calculus GL4ip by both slightly modifying the rule (GLR) and mimicking G4ip by replacing (→L) with a collection of rules sensitive to the form of the formula A in $A \to B$. To prove cut-admissibility they show that GL3ip and GL4ip are equivalent, in that they prove the same sequents.

They point out that although the calculus GL4ip enjoys terminating backward proof-search, the existence of a direct proof of cut-admissibility is doubtful: all standard methods fail, including Valentini's. While a direct and syntactic proof of cut-admissibility usually leads to a straightforward algorithm for cut-elimination, here the only potential cut-elimination algorithm for GL4ip is quite convoluted: (1) take a GL4ip proof containing cuts; (2) transform it to a GL3ip proof containing cuts ; (3) apply the cut-elimination procedure for GL3ip to obtain a cut-free GL3ip proof ; (4) transform the cut-free GL3ip proof into a cut-free GL4ip proof. In particular, the steps from (2) to (3), which rely on Valentini's complicated argument, and from (3) to (4), which involve intricate transformations, are anything but trivial. This indirection, coupled with the intricacies mentioned, can only lead to a painful and obscure algorithm for cut-elimination for GL4ip.

Naturally, the following question comes to mind: can we eliminate the indirection from GL4ip+(cut) to GL3ip+(cut) to GL3ip to GL4ip, and obtain a direct cut-elimination procedure for GL4ip? Moreover, can we guarantee that this cut-elimination proof is correct?

Here, we answer both questions positively by giving a direct syntactic proof of cut-admissibility for GL4ip. First, we show the admissibility of the structural rules by adapting the arguments from Dyckhoff and Negri [7]. Second, we define a proof-search procedure PSGL4ip on GL4ip. Furthermore, we develop a thorough termination argument by defining a local measure on sequents and a well-founded relation along which this measure decreases upwards in the proof-search. Finally, we directly prove cut-admissibility for GL4ip using the *mhd proof technique*, which makes use of the termination of PSGL4ip to attribute a *m*aximum *h*eight of *d*erivations to each sequent [3]. We use this number as an induction measure in an argument involving local and syntactic transformations, allowing us to exhibit and hence extract a cut-elimination procedure. All of our claims have been formally verified in the interactive theorem prover Coq (https://github.com/ianshil/CE_GL4ip.git). Using the automatic program extraction facilities of Coq, we extracted the formally verified computer program for cut-elimination associated to our formalisation.

2 Preliminaries

Let $\mathbb{V} = \{p, q, r \ldots\}$ be an infinite set of propositional variables. Modal formulae are defined by the following grammar.

$$A ::= p \in \mathbb{V} \mid \bot \mid A \wedge A \mid A \vee A \mid A \to A \mid \Box A$$

We encode formulae as a type `(MPropF V)` over some parametric type `(V)` of propositional variables. A list of such formulae then has the type `list ( MPropF V)`. The usual operations on lists "append" and "cons" are respectively represented by `++` and `::` but Coq also allows us to write lists in infix notation using `;`. Thus the terms `A1 :: A2 :: A3` and `[A1] ++ [A2] ++ [A3]` and `[A1 ; A2 ; A3]` all encode the list A_1, A_2, A_3.

Definition 2.1 The *weight* $w(A)$ of a formula A is defined as follows:

$$\begin{array}{rcl} w(\bot) = w(p) & = & 1 \\ w(C \vee D) = w(C \to D) & = & w(C) + w(D) + 1 \\ w(C \wedge D) & = & w(C) + w(D) + 2 \\ w(\Box C) & = & w(C) + 1 \end{array}$$

We say that a formula A is a *boxed formula* if it has $\Box$ as its main connective. A boxed multiset contains only boxed formulae. For a set $X = \{A_1, \ldots, A_n\}$, define $\boxtimes X = \{A_1, \Box A_1, \ldots, A_n, \Box A_n\}$. We denote the set of subformulae of a formula A, including itself, by $\mathrm{Sub}(A)$. We abuse the notation to designate the set of subformulae of all formulae in the set X by $\mathrm{Sub}(X)$. We use the letters $A, B, C, \ldots$ for formulae and $X, Y, Z, \ldots$ for multisets of formulae.

The Hilbert calculus for the intuitionistic normal modal logic iK extends a Hilbert-calculus for intuitionistic propositional logic with the axiom $\Box(p \to q) \to (\Box p \to \Box q)$ and the inference rule of necessitation: from A infer $\Box A$. Intuitionistic Gödel-Löb logic iGL is obtained by the addition of the axiom $\Box(\Box p \to p) \to \Box p$ to iK. We write $A \in \mathsf{iK}$ when A is a theorem of iK.

A *sequent* is a pair of a multiset of formulae and a formula, denoted $X \Rightarrow C$. For multisets X and Y, the multiset sum $X \uplus Y$ is the multiset whose multiplicity (at each formula) is a sum of the multiplicities of X and Y. We write X, Y to mean $X \uplus Y$. For a formula A, we write A, X and X, A to mean $\{A\} \uplus X$. From the formalisation perspective, a pair of a list of formulae and a formula has type `list (MPropF V) * (MPropF V)`, using the Coq notation `*` for forming pairs. The latter is the type we give to sequents in our formalisation, for which we use the macro `Seq`. Thus the sequent $A_1, A_2, A_3 \Rightarrow B$ is encoded by the term `[A_1 ; A_2 ; A_3] * B`, which itself can also be written as the pair `([A_1 ; A_2 ; A_3], B)`. Note that `[A_1 ; A_2 ; A_3] * B` is different from `[A_2 ; A_1 ; A_3] * B` since the order of the elements is crucial, so our lists do not capture multisets (yet).

A *sequent calculus* consists of a finite set of *sequent rule schemas*. Each rule schema consists of a conclusion sequent and some number of premise sequents. If a rule schema has no premise sequents, then it is called an initial sequent. The conclusion and premises are built in the usual way from propositional-variables, formula-variables and multiset-variables. A *rule instance* is obtained by uniformly instantiating every variable in the rule schema with a concrete object of that type. This is the standard definition from structural proof theory.

Definition 2.2 [Derivation/Proof] A *derivation* of a sequent s in the sequent calculus C is a finite tree of sequents such that (i) the root node is s; and (ii) each interior node and its direct children are the conclusion and premise(s) of a rule instance in C. A *proof* is a derivation where every leaf is an instance of an initial sequent.

In what follows, it should be clear from context whether the word "proof" refers to the object defined in Definition 2.2, or to the meta-level notion. We say that a sequent is *provable* in C if it has a proof in C. We elide the details of the encodings of sequent rules, collections of sequent rules and derivations as these can be found elsewhere [4]. For a sequent calculus C we define two predicates on sequents: `C_drv` for *derivability* in C, and `C_prv` for *provability* in C. Instances of these predicates are `GL4ip_prv`, `GL4ip_cut_prv` or `PSGL4ip_drv`. We note that our encodings primarily rely on the type `Type`, which bears computational content and is crucially compatible with the extraction function of Coq while `Prop` is not.

Definition 2.3 [Height] For any derivation δ, its *height* $h(\delta)$, is the maximum number of nodes on a path from root to leaf.

In this article we assume some familiarity with the notions of admissibility, invertibility, and height-preservation.

The sequent calculus $\mathsf{GL4ip}$ is given in Figure 1. When defining rules we put the label naming the rule on the left of the horizontal line, while the label appears on the right of the line in *instances* of rules.

$$(\bot\mathrm{L})\ \frac{}{\bot, X \Rightarrow C} \qquad (\mathrm{IdP})\ \frac{}{X, p \Rightarrow p}$$

$$(\wedge\mathrm{L})\ \frac{X, A, B \Rightarrow C}{X, A \wedge B \Rightarrow C} \qquad (\wedge\mathrm{R})\ \frac{X \Rightarrow A \qquad X \Rightarrow B}{X \Rightarrow A \wedge B}$$

$$(\vee\mathrm{L})\ \frac{X, A \Rightarrow C \qquad X, B \Rightarrow C}{X, A \vee B \Rightarrow C} \qquad (\vee_i\mathrm{R})\ \frac{X \Rightarrow A_i}{X \Rightarrow A_1 \vee A_2}\ (i \in \{1, 2\})$$

$$(p{\to}\mathrm{L})\ \frac{X, p, A \Rightarrow C}{X, p, p \to A \Rightarrow C} \qquad ({\to}\mathrm{R})\ \frac{X, A \Rightarrow B}{X \Rightarrow A \to B}$$

$$(\Box{\to}\mathrm{L})\ \frac{\boxtimes X, \Box A \Rightarrow A \qquad W, \Box X, B \Rightarrow C}{W, \Box X, \Box A \to B \Rightarrow C} \qquad (\mathrm{GLR})\ \frac{\boxtimes X, \Box A \Rightarrow A}{W, \Box X \Rightarrow \Box A}$$

$$(\wedge{\to}\mathrm{L})\ \frac{X, A \to (B \to C) \Rightarrow D}{X, (A \wedge B) \to C \Rightarrow D} \qquad (\vee{\to}\mathrm{L})\ \frac{X, A \to C, B \to C \Rightarrow D}{X, (A \vee B) \to C \Rightarrow D}$$

$$({\to}{\to}\mathrm{L})\ \frac{X, B \to C \Rightarrow A \to B \qquad X, C \Rightarrow D}{X, (A \to B) \to C \Rightarrow D}$$

Fig. 1. The sequent calculus GL4ip. Here, W does not contain any boxed formula.

In (IdP), a propositional variable instantiating the featured occurrences of p is principal. In a rule instance of ($\wedge$R), ($\wedge$L), ($\vee_i$R), ($\vee$L) or ($\to$R), the *principal formula* of that instance is defined as usual. In a rule instance of ($p{\to}$L), both a propositional variable instantiating p and the formula instantiating the featured $p \to A$ are principal formulae of that instance. In a rule instance of ($\wedge{\to}$L), ($\vee{\to}$L), (${\to}{\to}$L) or ($\Box{\to}$L), the formula instantiating respectively $(A \wedge B) \to C$, $(A \vee B) \to C$, $(A \to B) \to C$ or $\Box A \to B$ is the principal formula of that instance. In a rule instance of (GLR), the formula $\Box A$ is called the *diagonal formula* [14].

Example 2.4 The following are examples of derivations in GL4ip. Note that while the first and second examples are derivations, the third is a proof.

$$p \Rightarrow q \to r \qquad \frac{\Rightarrow p}{\Rightarrow p \vee (p \to \bot)}\ (\vee_1\mathrm{R}) \qquad \cfrac{\cfrac{}{\Box p, p, \Box p \Rightarrow p}\ (\mathrm{IdP})}{\Box p \Rightarrow \Box p}\ (\mathrm{GLR})$$

Example 2.5 A special example of a derivation in GL4ip is the following:

$$\frac{\Box A \to A, \Box(\Box A \to A), A, A, \Box A, \Box A, \Box A \Rightarrow A \qquad \Box(\Box A \to A), A, \Box A, \Box A \Rightarrow A}{\Box A \to A, \Box(\Box A \to A), A, \Box A, \Box A \Rightarrow A}\ (\Box{\to}\mathrm{L})$$

The conclusion and left premise are identical modulo formula multiplicities, so the rule ($\Box{\to}$L) can be infinitely applied upwards on the left branch.

Finally, we consider the additive cut rule.

$$\frac{X \Rightarrow A \qquad A, X \Rightarrow C}{X \Rightarrow C}\ (\mathrm{cut})$$

In the above, we call A the *cut-formula*. It is known that GL4ip+(cut) is sound and complete w.r.t. the Hilbert calculus iGL [19] as stated next.

Theorem 2.6 *For all A we have: $A \in$ iGL iff $\Rightarrow A$ is provable in* GL4ip+(cut).

3 A path to contraction for GL4ip

As mentioned above, our formalisation encodes sequents using lists and not multisets. Despite this distance between our formalisation and the pen-and-paper definition, list-sequents from the former mimic multiset-sequents from the latter. Below, `exch s se` encodes the fact that `se` is obtained from the sequent `s` by permuting two sub-lists in the list representing its antecedent.

Lemma 3.1 (Admissibility of exchange) *For all X_0, X_1, A, B and C, if $X_0, A, B, X_1 \Rightarrow C$ is provable in* GL4ip*, then so is $X_0, B, A, X_1 \Rightarrow C$.*

```
Lemma GL4ip_adm_exch : forall s, (GL4ip_prv s) ->
         (forall se, (exch s se) -> (GL4ip_prv se)).
```

Note that the admissibility of exchange is not an accident, nor is it hard-wired as an explicit rule in Coq. That is, our encoding of the multiset-based rules shown in Figure 1 is designed to entail exchange. For example, the conclusion $X, A \wedge B \Rightarrow C$ of the rule ($\wedge$L) rule is encoded as the list-sequent `(X0++(And A B)::X1, C)` which allows us to "slide" `(And A B)` to any point in the antecedent by appropriate choices of the lists `X0` and `X1`. The list-encoding requires a very pedantic analysis of the position of the occurrence of `(And A B)` in the antecedent of a rule instance. This is a major disadvantage of our approach: for example, the admissibility of exchange itself requires some 5000 lines of Coq code!

Given the above lemma, we allow ourselves to consider that the left-hand side of sequents is indeed a multiset. The remaining of this section extends the work of Dyckhoff and Negri [7] on G4ip to the sequent calculus GL4ip. Thus, the proofs they developed are embedded in our proofs and hence formalised. Most lemmata are proven by straightforward inductions on the structure of formulae or derivations, and the order in which we present them gives an account of the dependencies between them. We omit the Coq encodings for brevity.

Lemma 3.2 (Height-preserving admissibility of weakening) *For all X, A and C, if $X \Rightarrow C$ has a proof π in* GL4ip*, then $X, A \Rightarrow C$ has a proof π_0 in* GL4ip *such that $h(\pi_0) \leq h(\pi)$.*

Lemma 3.3 (Height-preserving invertibility of rules) *The rules $(\wedge R)$, $(\wedge L)$, $(\vee L)$, $(\to R)$, $(p \to L)$, $(\wedge \to L)$, $(\vee \to L)$ are height-preserving invertible.*

Lemma 3.4 *For all X and A, the sequent $A, X \Rightarrow A$ has a proof.*

We can show that the height-preserving invertibility of the rules ($\to\to$L) and ($\Box\to$L) holds for the right premise:

Lemma 3.5 (Height-preserving right-invertibility of rules) *For all X, A, B, D and C:*

(i) *If* $X, (A \to B) \to D \Rightarrow C$ *has a proof* π *in* GL4ip*, then* $X, D \Rightarrow C$ *has a proof* π_0 *in* GL4ip *such that* $h(\pi_0) \leq h(\pi)$*.*

(ii) *If* $X, \Box A \to B \Rightarrow C$ *has a proof* π *in* GL4ip*, then* $X, B \Rightarrow C$ *has a proof* π_0 *in* GL4ip *such that* $h(\pi_0) \leq h(\pi)$*.*

To obtain the key Lemma 3.7 for admissibility of contraction, pertaining to the rule (→→L), we need to show that the usual left-implication rule is admissible:

Lemma 3.6 *The rule (→L) is admissible in* GL4ip*:*

$$\frac{X \Rightarrow A \qquad X, B \Rightarrow C}{X, A \to B \Rightarrow C}\ (\to L)$$

Lemma 3.7 *For all* X*,* A, B, D *and* C*, if* $X, (A \to B) \to D \Rightarrow C$ *is provable in* GL4ip*, then* $X, A, B \to D, B \to D \Rightarrow C$ *is provable in* GL4ip*.*

We finally obtain the admissibility of contraction for GL4ip:

Lemma 3.8 (Admissibility of contraction) *For all* X, A *and* C*: If* $A, A, X \Rightarrow C$ *is provable in* GL4ip*, then* $A, X \Rightarrow C$ *is provable in* GL4ip*.*

In the following section we introduce a second calculus PSGL4ip which embodies a terminating non-deterministic backward proof-search procedure for GL4ip. This will allow us to define the maximum height of derivations for a sequent with respect to this procedure. Later on this will constitute the secondary induction measure in the proof of admissibility of cut.

4 PSGL4ip: terminating backward proof-search

Given a sequent calculus C, one can define a backward proof-search procedure on C by imposing further constraints on the backward applicability of the rules of C. This procedure captures a subset of the set of all derivations of C, i.e. those which are built using the restricted version of the rules of C. Consequently, a backward proof-search procedure can be identified with the calculus PSC consisting of these restricted rules of C, under the condition that PSC allows to decide the provability of sequents in C.

We present such a sequent calculus for GL4ip. PSGL4ip restricts the rules of GL4ip in the following way.

(Ident) The rule (IdP) is replaced by the identity rule (Id) on formulae of any weight shown. Note that it is derivable in GL4ip as shown in Lemma 3.4.

$$\frac{}{A, X \Rightarrow A}\ (\mathrm{Id})$$

(NoInit) The conclusion of no rule is permitted to be an instance of either (Id) or (⊥L).

Before commenting on the above, we note that it is straightforward to prove that GL4ip and PSGL4ip are equivalent in the following sense: a sequent is provable in one if it is provable in the other. So, according to the above general description, it suffices to prove that PSGL4ip can be used to decide the provability of sequents in GL4ip to show that the former deserves its prefix.

Conjointly, these restrictions aim at avoiding repetitions along a branch of a sequent which is either an identity or an instance of (⊥L), as in Example 2.5. Restriction (NoInit) disallows the destruction of a formula upwards in presence of a sequent which is obviously provable, while (Ident) allows to designate the latter as provable. In fact, by showing that no loop can appear in a branch of a PSGL4ip derivation, we concretely show that the only type of loop present in GL4ip are loops on provable sequents.

In the remainder of this section we proceed to show that no loop can exist in PSGL4ip. We do so by proving that each sequent has a derivation of maximum height in PSGL4ip. The existence of such derivations is ensured by the strict decreasing of a local measure on sequents upwards in the rules of PSGL4ip.

4.1 A well-founded order on $(\mathbb{N} \times \mathbb{N} \times \mathit{list}\,\mathbb{N})$

We define a well-founded order on triples $(n, m, l) \in (\mathbb{N} \times \mathbb{N} \times \mathit{list}\,\mathbb{N})$ where $\mathit{list}\,\mathbb{N}$ is the set of all lists of natural numbers.

In the following, we use $<$ to mean the usual ordering on natural numbers. Let us recall the general definition of a lexicographic order.

Definition 4.1 [Lexicographic order] Let $(A_1, <_1), \cdots, (A_n, <_n)$ be a collection of sets A_i with respective (strict total) orders $<_i$ on these sets. We define the lexicographic order $<_{lex}^{(A_1,<_1),\cdots,(A_n,<_n)}$ as follows. For two n-tuples $(a_1, \cdots, a_n)$ and $(a'_1, \cdots, a'_n)$ of the Cartesian product $A_1 \times \cdots \times A_n$, we write $(a_1, \cdots, a_n) <_{lex}^{(A_1,<_1),\cdots,(A_n,<_n)} (a'_1, \cdots, a'_n)$ if there is a $1 \leq j \leq n$ such that:

(i) $a_p = a'_p$, for all $1 \leq p < j$

(ii) $a_j <_j a'_j$

Note that if $<_i$ is a well-founded relation for all $1 \leq i \leq n$, then $<_{lex}^{(A_1,<_1),\ldots,(A_n,<_n)}$ is also well-founded [13]. If $(A_i, <_i) = (A_j, <_j)$ for all $1 \leq i, j \leq n$, then we note $(A_i, <_i)^n$ the sequence $(A_1, <_1), \ldots, (A_n, <_n)$. We define the shortlex order, also called *breadth-first* [11] or *length-lexicographic* order, over lists of natural numbers $\ll$:

Definition 4.2 [Shortlex order] The shortlex order over lists of natural numbers, noted $\ll$, is defined as follows. For two lists l_0 and l_1 of natural numbers, we say that $l_0 \ll l_1$ whenever one of the following conditions is satisfied:

(i) $\mathit{length}(l_0) < \mathit{length}(l_1)$;

(ii) $\mathit{length}(l_0) = \mathit{length}(l_1) = n$ and $l_0 <_{lex}^{(\mathbb{N},<)^n} l_1$;

Intuitively, the shortlex order is ordering lists according to their length and follows the lexicographic order whenever length does not discriminate.

Finally, we define the order $<^3$ on $(\mathbb{N} \times \mathbb{N} \times \mathit{list}\,\mathbb{N})$ as $<_{lex}^{(\mathbb{N},<),(\mathbb{N},<),(\mathit{list}(\mathbb{N}),\ll)}$. Given that $<$ and $\ll$ are well-founded orders, we get that $<^3$ also is.

4.2 A $(\mathbb{N} \times \mathbb{N} \times \mathit{list}\,\mathbb{N})$-measure on sequents

In what follows we use the term "measure" in an informal way. We proceed to attach to each sequent $X \Rightarrow C$ a measure $\Theta(X \Rightarrow C)$ which is a triple

$(\alpha(X \Rightarrow C), \beta(X \Rightarrow C), \gamma(X \Rightarrow C)) \in (\mathbb{N} \times \mathbb{N} \times \mathit{list}\,\mathbb{N})$. For simplicity, in the following paragraphs we consider a fixed sequent $X \Rightarrow C$ for which we define the triple, and thus erase the mention of the sequent in the measures.

First, we focus on γ. As $X \Rightarrow C$ is built from a finite multiset of formulae, it contains a *topmost* formula of maximal weight. Let n be that maximal weight. We can create a list of length n such that at each position m in the list (counting from right to left) for $1 \leq m \leq n$, we find the number of occurrences in $X \Rightarrow C$ of *topmost* formulae of weight m. Such a list gives the count of occurrences in $X \Rightarrow C$ of formulae of weight n in its leftmost (i.e. n-th) component, then of occurrences of formulae of weight $n-1$ in the next (i.e. $(n-1)$-th) component, and so on until we reach 1. We define γ to be this unique list. For example, $\gamma(p \wedge q, p \vee q \Rightarrow q \rightarrow p)$ is the list $[1, 2, 0, 0]$ because $p \wedge q$ is the formula of maximum weight 4, and it is the only formula with this weight occurring in the list, while both $p \vee q$ and $q \rightarrow p$ are of weight 3. Two things needs to be noted about such lists. First, if no topmost occurrence of a formula is of weight $1 \leq k \leq n$, then a 0 appears in position k in the list. This is the case for the weight 2 in the example. Second, as in general no formula is of weight 0 we do not need to dedicate a position for this particular weight in our list.

Why do we need such a list? With this list, the shortlex order becomes an adequate substitute to the Dershowitz-Manna order [5] considered in Dyckhoff's work on G4ip. We recall this order, given two multisets Γ_0 and Γ_1, by quoting van der Giessen and Iemhoff [19]: "$\Gamma_0 \ll \Gamma_1$ if and only if Γ_0 is the result of replacing one or more formulas in Γ_1 by zero or more formulas of lower degree". As our use of the symbol $\ll$ for the shortlex order suggests, the shortlex order can replace the order given above to order finite multisets of formulae.

A similar list was independently formalised in Coq by Daniel Schepler in the study of the calculus G4ip which he calls LJT [15], following Dyckhoff. However, he does not involve this list in a termination argument: instead, he uses it to show the equivalence of G4ip and the usual natural deduction system for intuitionistic logic.

Second, we turn to β. On the contrary to the measure defined by Bílková [1] and used by van der Giessen and Iemhoff, which attributes a natural number to a sequent *appearing in a proof-search tree which depends on the root*, we use a *local* notion of "number of usable boxes" as done by Goré et al. [9].

Definition 4.3 We define:

(i) the *usable boxes* $ub(X \Rightarrow C)$ of $X \Rightarrow C$ as:

$$ub(X \Rightarrow C) := \{\Box A \mid \Box A \in \mathrm{Sub}(X \cup C)\} \setminus \{\Box A \mid \Box A \in X\}$$

(ii) the number $\beta(X \Rightarrow C)$ of usable boxes of $X \Rightarrow C$ as $\beta(X \Rightarrow C) = \mathrm{Card}(ub(X \Rightarrow C))$, where $\mathrm{Card}(U)$ is the cardinality of the set U.

Thus, the notion of usable boxes of $X \Rightarrow C$ is the set of boxed subformulae of $X \Rightarrow C$ minus the topmost boxed formulae in X. Intuitively, this notion captures the set of boxed formulae of a sequent s which might be the diagonal formula of an instance of (GLR) in a derivation of s in PSGL4ip.

Third, we finally consider α. As X is a finite multiset of formulae, the checking of whether or not $X \Rightarrow C$ is an instance of the rule (Id) or ($\bot$L) is decidable. So, we can constructively define the following test function:

$$\alpha(X \Rightarrow C) = \begin{cases} 0 & \text{if } X \Rightarrow C \text{ is an instance of (Id) or } (\bot\text{L}) \\ 1 & \text{otherwise} \end{cases}$$

4.3 Every rule of PSGL4ip reduces Θ upwards

We proceed to prove that the measure Θ decreases upwards through the rules of PSGL4ip on the $<^3$ ordering.

Lemma 4.4 *For all sequents $s_0, s_1, ..., s_n$ and for all $1 \leq i \leq n$, if there is an instance of a rule r of* PSGL4ip *of the form below, then $\Theta(s_i) <^3 \Theta(s_0)$:*

$$\frac{s_1 \quad \ldots \quad s_n}{s_0}\ r$$

Note that contraction and weakening as rules allow Θ to *increase* upwards. While it is rather obvious for contraction, this statement for weakening is surprising. The key point here is to note that weakening allows the deletion of boxed formulae in the antecedent of sequents, leading to a potential increase in the number of usable boxes β: that is, weakening may remove some of the boxes that "block" some applications of (GLR) upwards and so the number of usable boxes increases.

4.4 The existence of a derivation of maximum height

For convenience, we define the order $\lhd\!3$ on sequents as follows:

$$s_0 \lhd\!3\, s_1 \text{ if and only if } \Theta(s_0) <^3 \Theta(s_1)$$

As $<^3$ is a well-founded order, it is obvious that $\lhd\!3$ is so as well. As a consequence we obtain a strong induction principle following the $\lhd\!3$ order.

Theorem 4.5 *For any property P on sequents, to prove the statement $\forall s P(s)$ it is sufficient to show that every sequent s_0 satisfies P under the assumption that all its $\lhd\!3$-predecessors satisfy P.*

```
Theorem less_than3_strong_inductionT:
forall (P : Seq -> Type),
(forall s0, (forall s1, ((s1 <3 s0) -> P s1)) -> P s0)
-> forall s, P s.
```

If we use this principle with the previous Lemma 4.4, we can easily prove the existence of a derivation in PSGL4ip of maximum height for all sequents.

Theorem 4.6 *Every sequent s has a* PSGL4ip *derivation of maximum height.*

```
Theorem PSGL4ip_termin :
 forall s, existsT2 (D: PSGL4ip_drv s), (is_mhd D).
```

Here, `D` is a *derivation*, the existence of which is guaranteed by the constructive existential quantifier `existsT2`. This quantifier not only requires us to construct a witnessing term but also to provide a proof that the witness is of the correct type. The function `is_mhd` returns the constructive Coq proposition `True` if and only if its argument, `D`, is a derivation of maximum height.

As the previous lemma implies the *constructive* existence of a derivation δ of maximum height in PSGL4ip for any sequent s, we are entitled to let $\mathrm{mhd}(s)$ denote the height of δ. As in the work of Goré et al. [9], we later use $\mathrm{mhd}(s)$ as the secondary induction measure used in the proof of admissibility of cut.

Before proving the only property we need from $\mathrm{mhd}(s)$, let us interpret the previous lemma from the point of view of the proof-search procedure underlying PSGL4ip. The existence of a derivation of maximum height for each sequent in PSGL4ip shows that in the backward application of rules of PSGL4ip on a sequent, i.e. the expansion of branches rooted in this sequent, a halting point has to be encountered. As a consequence, the expansion of every branch must meet a halting point: the proof-search procedure *terminates*.

While this is the essence of the content of the previous lemma, we effectively only use the fact that $\mathrm{mhd}(s)$ decreases upwards in the rules of PSGL4ip.

Lemma 4.7 *If r is a rule instance from* PSGL4ip *with conclusion s_0 and s_1 as one of the premises, then $mhd(s_1) < mhd(s_0)$.*

5 Cut-elimination for GL4ip

To reach cut-elimination, our main theorem, we first state and prove cut-admissibility in a purely syntactic way. More precisely, we proceed to prove that the *additive*-cut rule is admissible. The latter statement, stating that the provability of the sequents $X \Rightarrow A$ and $X, A \Rightarrow C$ entails the provability of $X \Rightarrow C$, is formalised in Coq in the following way:

```
Theorem GL4ip_cut_adm : forall A X0 X1 C,
 (GL4ip_prv (X0++X1,A)  *  GL4ip_prv (X0++A::X1,C)) ->
                GL4ip_prv (X0++X1,C).
```

Here, the term `(X0++X1,A)` encodes the sequent $X_0, X_1 \Rightarrow A$ as a pair, thus hiding a lower level occurrence of `*`. Then, given that `GL4ip_prv s` is in `Type` and not in `Prop`, we are required to use the constructor `*` for pairs at the higher level shown instead of `/\` which is the usual conjunction in `Prop`. So, the existence of *proofs* in GL4ip for the sequent `(X0++X1,A)` as well as for the sequent `(X0++A::X1,C)` asserted in the second line entail the existence of a *proof* in GL4ip for the sequent `(X0++X1,C)`. It is now clear that this statement formalises the following theorem:

Theorem 5.1 *The additive cut rule is admissible in* GL4ip*.*

Proof. Let d_1 (with last rule r_1) and d_2 (with last rule r_2) be proofs in GL4ip of $X \Rightarrow A$ and $A, X \Rightarrow C$ respectively, as shown below.

$$\frac{d_1}{X \Rightarrow A}\, r_1 \qquad \frac{d_2}{A, X \Rightarrow C}\, r_2$$

It suffices to show that there is a proof in GL4ip of $X \Rightarrow C$. We reason by strong primary induction (PI) on the weight of the cut-formula A, giving the primary inductive hypothesis (PIH). We also use a strong secondary induction (SI) on mhd of the conclusion of a cut, giving the secondary inductive hypothesis (SIH).

We make a first case distinction: does $X \Rightarrow C$ violate (NoInit)? If it is the case, then this sequent is an instance of (Id) or ($\bot$L). So, we use Lemma 3.4 or apply ($\bot$L) to obtain a proof of $X \Rightarrow C$. If $X \Rightarrow C$ satisfies (NoInit), then it is not an instance of (Id) or ($\bot$L). In this case we consider r_1. In total, there are thirteen cases to consider for r_1: one for each rule in GL4ip. However, we can gather some of the cases together and reduce the number of cases to eight. We separate them by using Roman numerals and showcase the most interesting ones.

(I) $\mathbf{r_1}$ =($\to$R) : Then r_1 has the following form where $A = B \to D$:

$$\dfrac{B, X \Rightarrow D}{X \Rightarrow B \to D}\ (\to\text{R})$$

We consider one sub-case.

(I-a) If r_2 is ($\to\to$L) where the cut formula is not principal in r_2, then it must have the following form where $(E \to F) \to G, X_0 = X$:

$$\dfrac{B \to D, F \to G, X_0 \Rightarrow E \to F \qquad B \to D, G, X_0 \Rightarrow C}{B \to D, (E \to F) \to G, X_0 \Rightarrow C}\ (\to\to\text{L})$$

Thus, we have that the sequents $X \Rightarrow C$ and $X \Rightarrow B \to D$ are respectively of the form $(E \to F) \to G, X_0 \Rightarrow C$ and $(E \to F) \to G, X_0 \Rightarrow B \to D$. Using the right-invertibility of ($\to\to$L), proven in Lemma 3.5, on $(E \to F) \to G, X_0 \Rightarrow B \to D$ we obtain a proof of the sequent $G, X_0 \Rightarrow B \to D$. Then, we make a case distinction on whether the sequent $F \to G, X_0 \Rightarrow E \to F$ is an instance of (Id) or ($\bot$L). If it is the case, then we proceed as follows:

$$\dfrac{F \to G, X_0 \Rightarrow E \to F \qquad \dfrac{G, X_0 \Rightarrow B \to D \qquad B \to D, G, X_0 \Rightarrow C}{G, X_0 \Rightarrow C}\ \text{SIH}}{(E \to F) \to G, X_0 \Rightarrow C}\ (\to\to\text{L})$$

Here the left branch is obviously provable either by invoking Lemma 3.4 or by applying ($\bot$L). If $F \to G, X_0 \Rightarrow E \to F$ is not an instance of these rules, then consider the following proof of this sequent, where Lemma 3.7 deconstructs the implication $(E \to F) \to G$, Lemma 3.8 contracts $F \to G$ and Lemma 3.3 is the invertibility of the rule ($\to$R).

$$\dfrac{\dfrac{\dfrac{\dfrac{(E \to F) \to G, X_0 \Rightarrow B \to D}{E, F \to G, F \to G, X_0 \Rightarrow B \to D}\ \text{Lem.3.7}}{E, F \to G, X_0 \Rightarrow B \to D}\ \text{Lem.3.8} \qquad \dfrac{B \to D, F \to G, X_0 \Rightarrow E \to F}{B \to D, E, F \to G, X_0 \Rightarrow F}\ \text{Lem.3.3}}{E, F \to G, X_0 \Rightarrow F}\ \text{SIH}}{F \to G, X_0 \Rightarrow E \to F}\ (\to\text{R})$$

The crucial point here is to see that the use of SIH is justified, i.e. that $\text{mhd}(E, F \to G, X_0 \Rightarrow F) < \text{mhd}((E \to F) \to G, X_0 \Rightarrow C)$. This is the case as we made sure that the rule applications ($\to\to$L) and ($\to$R) are both instances of rules of PSGL4ip because their respective conclusions $(E \to F) \to G, X_0 \Rightarrow C$ and $F \to G, X_0 \Rightarrow E \to F$ are not instances of (Id) or ($\bot$L). So, we get that $\text{mhd}(E, F \to G, X_0 \Rightarrow F) < \text{mhd}(F \to G, X_0 \Rightarrow E \to F) < \text{mhd}((E \to F) \to$

$G, X_0 \Rightarrow C)$ by Lemma 4.7 hence $\mathrm{mhd}(E, F \to G, X_0 \Rightarrow F) < \mathrm{mhd}((E \to F) \to G, X_0 \Rightarrow C)$ by transitivity of $<$. So, we are done. Note that the created cut could not be justified by usual induction on height, as Lemma 3.7 is not height-preserving.

(II) $\mathbf{r_1}$ =(GLR): Then A is the diagonal formula in r_1:

$$\dfrac{\boxtimes X_0, \Box B \Rightarrow B}{W, \Box X_0 \Rightarrow \Box B}\ (\mathrm{GLR})$$

where $A = \Box B$ and $W, \Box X_0 = X$. Thus, we have that the sequents $X \Rightarrow C$ and $A, X \Rightarrow C$ are respectively of the form $W, \Box X_0 \Rightarrow C$ and $\Box B, W, \Box X_0 \Rightarrow C$. We now consider one case for r_2.

(II-a) If r_2 is $(\Box\!\to\!\mathrm{L})$. Then r_2 is of the following form and where $\Box D \to E, W_0 = W$:

$$\dfrac{B, \Box B, \boxtimes X_0, \Box D \Rightarrow D \qquad E, W_0, \Box B, \Box X_0 \Rightarrow C}{\Box D \to E, W_0, \Box B, \Box X_0 \Rightarrow C}\ (\Box\!\to\!\mathrm{L})$$

We proceed as follows.

$$\dfrac{\begin{array}{c}\pi \\ \boxtimes X_0, \Box D \Rightarrow D\end{array} \qquad \dfrac{\dfrac{\dfrac{\boxtimes X_0, \Box B \Rightarrow B}{\Box X_0 \Rightarrow \Box B}\ (\mathrm{GLR})}{E, W_0, \Box X_0 \Rightarrow \Box B}\ \mathrm{Lem.3.2} \qquad E, W_0, \Box B, \Box X_0 \Rightarrow C}{E, W_0, \Box X_0 \Rightarrow C}\ \mathrm{SIH}}{\Box D \to E, W_0, \Box X_0 \Rightarrow C}\ (\Box\!\to\!\mathrm{L})$$

where π is:

$$\dfrac{\dfrac{\dfrac{\boxtimes X_0, \Box B \Rightarrow B}{\Box X_0 \Rightarrow \Box B}\ (\mathrm{GLR})}{\boxtimes X_0, \Box D \Rightarrow \Box B}\ \mathrm{Lem.3.2} \qquad \dfrac{\dfrac{\boxtimes X_0, \Box B \Rightarrow B}{\boxtimes X_0, \Box B, \Box D \Rightarrow B}\ \mathrm{Lem.3.2} \qquad B, \Box B, \boxtimes X_0, \Box D \Rightarrow D}{\boxtimes X_0, \Box B, \Box D \Rightarrow D}\ \mathrm{PIH}}{\boxtimes X_0, \Box D \Rightarrow D}\ \mathrm{SIH}$$

Note that both uses of SIH are justified here as the assumption (NoInit) ensures that the last rule in this proof is effectively an instance of $(\Box\!\to\!\mathrm{L})$ in PSGL4ip, hence $\mathrm{mhd}(\boxtimes X_0, \Box D \Rightarrow D) < \mathrm{mhd}(\Box D \to E, W_0, \Box X_0 \Rightarrow C)$ and $\mathrm{mhd}(E, W_0, \Box X_0 \Rightarrow C) < \mathrm{mhd}(\Box D \to E, W_0, \Box X_0 \Rightarrow C)$ by Lemma 4.7. Q.E.D.

Before turning to cut-elimination let us comment on the need to use additive cuts in the previous proof. To justify a cut through SIH, we need to link the sequent-conclusion of the initial cut to the sequent-conclusion of the newly created cut by a chain of rule applications which make mhd decrease upwards. Now, contraction and weakening can increase mhd upwards. So, in the mhd technique we cannot use contraction or weakening in the chain linking the two sequent-conclusion, forbidding us from considering multiplicative cuts. The use of additive cuts allows us to circumvent this difficulty. This sensitivity of the proof technique is surprising as both calculi admit weakening and contraction, making additive and multiplicative cuts equivalent.

It is commonly accepted that a purely syntactic proof of cut-admissibility provides a cut-elimination procedure: eliminate topmost cuts first. So, the above proof theoretically establishes that cuts are eliminable in the calculus

GL4ip extended with (cut). To effectively prove this statement in Coq we explicitly encode the additive cut rule as follows:

```
(X0++X1, A)     (X0++A::X1, C)
------------------------------
        (X0++X1, C)
```

With this rule in hand, we can encode the set of rules GL4ip_cut_rules as GL4ip_rules enhanced with (cut), i.e. the calculus GL4ip + (cut). We can finally turn to the elimination of additive cuts:

Theorem 5.2 *The additive cut rule is eliminable from* GL4ip + (*cut*)*.*

```
Theorem GL4ip_cut_elimination : forall s,
 (GL4ip_cut_prv s) -> (GL4ip_prv s).
```

The above theorem shows that given a proof in GL4ip + (cut) of a sequent, i.e. GL4ip_cut_prv s, we can transform this proof directly to obtain a proof in GL4ip of the same sequent. Given that this theorem is in fact a constructive function based on elements defined on Type, we can use the extraction feature of Coq and obtain a cut-eliminating Haskell program.

6 Discussion

The *mhd proof technique* for cut-admissibility, based on terminating backward proof-search, was recently discovered by Brighton [3] and successfully applied to the provability logic GL [2,16] by Goré et al. [9]. The novelty of this technique consists in the binary induction measure it relies on: while the first component is the traditional "size of the cut formula", the second is the intriguing "maximum height of derivations". The latter is defined using a terminating backward proof-search procedure which allows to exhibit for a given sequent a derivation of maximum height, hence bounding the height of all the possible derivations of this sequent. The mhd technique is interesting for four reasons.

First, as shown by Goré et al. [9], the mhd technique gives simpler proofs in difficult cases such as GL and we do not need Valentini's extra measure of width but can utilise only two measures. This advantage carries over to iGL.

Second, it reverses the usual order of cut-admissibility and termination of backward proof-search. Indeed, we usually prove that cut is admissible, then design a proof-search procedure on the cut-free system and show its termination. This oddity is promising for a general treatment of cut admissibility via local transformations for calculi with a terminating backward proof-search.

Third, it is sensitive to the type of cut admitted. More precisely, this technique seems applicable only to *additive* cuts, in cases where weakening and contraction are admissible in the calculus. Intuitively, the mhd technique involves the backward application of rules on the conclusion of the initial cut. For termination, it must exclude (backward applications of) contraction and weakening as both can increase the termination measure upwards. But banishing these also banishes the use of multiplicative cuts of the form below:

$$\frac{X_0 \Rightarrow A \quad X_1 \Rightarrow C}{X_0, X_1 \Rightarrow C}$$

Fourth, many sequent calculi for non-classical logics enjoy terminating backward proof-search, and often, they are based upon G4ip. Is there a general theory of cut-admissibility hidden inside the mhd method for these calculi?

7 Conclusion

In the conclusion of a previous work [9], we hinted at the interest of using mhd as an induction measure to prove the admissibility of cut for a sequent calculus for intuitionistic GL based on Dyckhoff's terminating calculus G4ip. Here, we ventured down this alley and obtained a cut-admissibility result for GL4ip relying on the termination of backward proof-search. More than an alternative proof technique, the use of mhd in the case of GL4ip is to date the only known pathway to a direct proof of admissibility of cut: as admitted by van der Giessen and Iemhoff [19], all other available proof techniques fail.

So, in addition to using a local measure for proving termination of proof-search instead of Bíková's non-local measure [1], and formalising on the way most of Dyckhoff and Negri's results on G4ip, we consequently addressed van der Giessen and Iemhoff's issue by providing a formalised direct proof of cut-admissibility for GL4ip. Crucially, this direct syntactic proof allows to obtain an extractable simple cut-elimination procedure for GL4ip hardly obtainable from the indirection in van der Giessen and Iemhoff's work.

8 Further work

While the use of the termination of a backward proof-search procedure as a basis for cut-elimination is an intriguing and unconventional argument, it seems to have limitations. The calculi GLS, G4ip and GL4ip either contain no cycles or only contain *provable* cycles, i.e. cycles going through a provable sequent. Thus, the proof-search on these calculi only need to get rid of provable cycles. This is done by imposing restrictions on the application of rules which, when violated, entail the provability of the sequent under consideration. For example, if a sequent violates the restrictions of the PSGL4ip calculus, then we know that either it is an instance of ($\bot$L) or (Id), which entails its provability. So, for every rule application of GL4ip we have the crucial case distinction, which we make use of in the admissibility of cut: either it is an instance of PSGL4ip, which makes mhd decrease, or its conclusion is obviously provable. Now, if we face a calculus containing unprovable cycles, such as the standard ones for modal logic K4 or S4, then a terminating proof-search on this calculus need to involve restrictions which, when violated, do not entail the provability of the sequent violating them. Then, the case distinction mentioned above does not give us much when the sequent violates the restrictions of the proof-search: its provability is not obvious. We are currently investigating further adaptations of the technique to sequent calculi with unprovable cycles.

The Haskell program extractable from our formalisation should effectively eliminate cuts from GL4ip + (cut) proofs, as ensured from the extraction feature of Coq. However, we have neither tested it nor tried to optimize it. We intend to follow D'Abrera et al. [4] by exploring both of these alleys in future works.

References

[1] Bílková, M., "Interpolation in modal logics," Ph.D. thesis, Univerzita Karlova, Prague (2006).

[2] Boolos, G., "The Unprovability of Consistency: An Essay in Modal Logic," Cambridge University Press, 1979.

[3] Brighton, J., *Cut Elimination for GLS Using the Terminability of its Regress Process*, Journal of Philosophical Logic **45** (2016), pp. 147–153.

[4] D'Abrera, C., J. E. Dawson and R. Goré, *A formally verified cut-elimination procedure for linear nested sequents for tense logic*, in: A. Das and S. Negri, editors, *Automated Reasoning with Analytic Tableaux and Related Methods - 30th International Conference, TABLEAUX 2021, Birmingham, UK, September 6-9, 2021, Proceedings*, Lecture Notes in Computer Science **12842** (2021), pp. 281–298.
URL https://doi.org/10.1007/978-⊠3-⊠030-⊠86059-⊠2_17

[5] Dershowitz, N. and Z. Manna, *Proving termination with multiset orderings*, Commun. ACM **22** (1979), p. 465–476.
URL https://doi.org/10.1145/359138.359142

[6] Dyckhoff, R., *Contraction-free sequent calculi for intuitionistic logic*, The Journal of Symbolic Logic **57** (1992), pp. 795–807.
URL http://www.jstor.org/stable/2275431

[7] Dyckhoff, R. and S. Negri, *Admissibility of structural rules for contraction-free systems of intuitionistic logic*, The Journal of Symbolic Logic **65** (2000), pp. 1499–1518.
URL http://www.jstor.org/stable/2695061

[8] Goré, R. and R. Ramanayake, *Valentini's cut-elimination for provability logic resolved*, Rev. Symb. Log. **5** (2012), pp. 212–238.
URL https://doi.org/10.1017/S1755020311000323

[9] Goré, R., R. Ramanayake and I. Shillito, *Cut-Elimination for Provability Logic by Terminating Proof-Search: Formalised and Deconstructed Using Coq*, in: A. Das and S. Negri, editors, *Automated Reasoning with Analytic Tableaux and Related Methods - 30th International Conference, TABLEAUX 2021, Birmingham, UK, September 6-9, 2021, Proceedings*, Lecture Notes in Computer Science **12842** (2021), pp. 299–313.
URL https://doi.org/10.1007/978-⊠3-⊠030-⊠86059-⊠2_18

[10] Hudelmaier, J., *An O(n log n)-Space Decision Procedure for Intuitionistic Propositional Logic*, Journal of Logic and Computation **3** (1993), pp. 63–75.
URL https://doi.org/10.1093/logcom/3.1.63

[11] Larchey-Wendling, D. and R. Matthes, *Certification of breadth-first algorithms by extraction*, in: G. Hutton, editor, *Mathematics of Program Construction - 13th International Conference, MPC 2019, Porto, Portugal, October 7-9, 2019, Proceedings*, Lecture Notes in Computer Science **11825** (2019), pp. 45–75.
URL https://doi.org/10.1007/978-⊠3-⊠030-⊠33636-⊠3_3

[12] Leivant, D. M., "Absoluteness of intuitionistic logic," Ph.D. thesis, University of Amsterdam, Amsterdam (1975).

[13] Paulson, L. C., *Constructing recursion operators in intuitionistic type theory*, Journal of Symbolic Computation **2** (1986), pp. 325–355.
URL https://www.sciencedirect.com/science/article/pii/S0747717186800025

[14] Sambin, G. and S. Valentini, *The modal logic of provability: the sequential approach*, Journal of Philosophical Logic **11** (1982), p. 311–342.

[15] Schepler, D., *coq-sequent-calculus*, https://github.com/dschepler/coq-⊠sequent-⊠calculus/blob/master/LJTStar.v (2016).

[16] Solovay, R., *Provability interpretations of modal logic*, Israel Journal of Mathematics **25** (1976), pp. 287–304.

[17] Troelstra, A. S. and H. Schwichtenberg, "Basic Proof Theory," Cambridge Tracts in Theoretical Computer Science, Cambridge University Press, 2000, 2 edition.

[18] Valentini, S., *The modal logic of provability: Cut-elimination*, Journal of Philosophical Logic **12** (1983), p. 471–476.

[19] van der Giessen, I. and R. Iemhoff, *Sequent Calculi for Intuitionistic Gödel-Löb Logic*, Notre Dame Journal of Formal Logic **62** (2021), pp. 221 – 246.
URL https://doi.org/10.1215/00294527-2021-0011

Appendix

Proof. [of Lemma 4.4] We reason by case analysis on r:

(i) If r is (Id) or ($\bot$L), then we are done as there is no premise.

(ii) If r is ($\wedge$R), ($\wedge$L), ($\vee_1$R), ($\vee_2$R), ($\vee$L), ($\to$R), ($p\to$L), ($\wedge\to$L), ($\vee\to$L) or ($\to\to$L), then we have that $\gamma(s_0) \ll \gamma(s_1)$ and $\gamma(s_0) \ll \gamma(s_2)$ (if it exists), as shown by Dyckhoff and Negri [7]. It has to be noted that the use of the different weight for the conjunction is crucial for the case where r is the rule ($\wedge\to$L). Obviously, α can only decrease upwards in these rules, as no rule of PSGL4ip with premises can be applied to an initial sequent. Also, it is not hard to convince oneself that the number of usable boxes can only decrease in these rules as the boxed formulae on the left of the sequent are preserved upwards and the set of boxed subformulae is either stable or loses elements. So we can easily deduce that Θ decreases on $<^3$ from the conclusion to the premises of these rules.

(iii) If r is (GLR) then it must have the following form.

$$\frac{\boxtimes X, \Box B \Rightarrow B}{W, \Box X \Rightarrow \Box B}\ (\text{GLR})$$

Clearly, we have that $\{\Box A \mid \Box A \in \text{Sub}(\boxtimes X \cup \{\Box B\} \cup \{B\})\} \subseteq \{\Box A \mid \Box A \in \text{Sub}(W \cup \Box X \cup \{\Box B\})\}$. Also, given that we consider a derivation in PSGL4ip, we can note that (Id) is not applicable on $W, \Box X \Rightarrow \Box B$ by assumption, hence $\Box B \notin \Box X$. Consequently, we get $\{\Box A \mid \Box A \in W \cup \Box X\} \subset \{\Box A \mid \Box A \in \boxtimes X \cup \{\Box B\}\}$. An easy set-theoretic argument leads to $ub(\boxtimes X, \Box B \Rightarrow B) \subset ub(W, \Box X \Rightarrow \Box B)$. As a consequence we obtain $\beta(\boxtimes X, \Box B \Rightarrow B) < \beta(W, \Box X \Rightarrow \Box B)$, hence $\Theta(\boxtimes X, \Box B \Rightarrow B) <^3 \Theta(W, \Box X \Rightarrow \Box B)$.

(iv) If r is ($\Box\to$L) then it must have the following form.

$$\frac{\boxtimes X, \Box A \Rightarrow A \qquad W, \Box X, B \Rightarrow C}{W, \Box X, \Box A \to B \Rightarrow C}\ (\Box\to\text{L})$$

For the right premise we can straightforwardly see that $\gamma(W, \Box X, B \Rightarrow C) \ll \gamma(W, \Box X, \Box A \to B \Rightarrow C)$, and that both α and β either are stable or decrease upwards. So, we obtain $\Theta(W, \Box X, B \Rightarrow C) <^3 \Theta(W, \Box X, \Box A \to B \Rightarrow C)$. The case of the left premise is more complex but can be treated similarly to the (GLR) as follows. Note that $\{\Box D \mid \Box D \in \text{Sub}(\boxtimes X \cup \{\Box A\} \cup \{A\})\} \subseteq \{\Box D \mid \Box D \in \text{Sub}(W \cup \Box X \cup \{\Box A \to B\} \cup \{C\})\}$. We consider two cases.

In the first case, we have that $\Box A \notin \Box X$. Then as in (GLR) we obtain $\{\Box D \mid \Box D \in W \cup \Box X \cup \{\Box A \to B\}\} \subset \{\Box D \mid \Box D \in \boxtimes X \cup \{\Box A\}\}$ and consequently $\beta(\boxtimes X, \Box A \Rightarrow A) < \beta(W, \Box X, \Box A \to B \Rightarrow C)$. So, regardless of the value of $\alpha(\boxtimes X, \Box A \Rightarrow A)$, we obtain $\Theta(\boxtimes X, \Box A \Rightarrow A) <^3$

$\Theta(W, \Box A, \Box X, \Box A \to B \Rightarrow C)$.

In the second case, we have that $\Box A \in \Box X$. Then the rule application is of the following form:

$$\frac{\boxtimes X, \Box A, A, \Box A \Rightarrow A \qquad W, \Box A, \Box X, B \Rightarrow C}{W, \Box A, \Box X, \Box A \to B \Rightarrow C}\ (\Box{\to}\mathrm{L})$$

Clearly, we get $\alpha(\boxtimes X, \Box A, A, \Box A \Rightarrow A) = 0$ as it is an instance of an initial sequent, hence $\alpha(\boxtimes X, \Box A, A, \Box A \Rightarrow A) < \alpha(W, \Box A, \Box X, \Box A \to B \Rightarrow C)$. Consequently, we get $\Theta(\boxtimes X, \Box A, A, \Box A \Rightarrow A) <^3 \Theta(W, \Box A, \Box X, \Box A \to B \Rightarrow C)$.

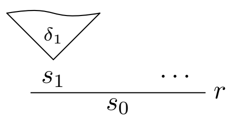
Q.E.D.

Proof. [of Theorem 4.6] We use `less_than3_strong_inductionT`, the strong induction principle on $\lhd 3$ from Theorem 4.5. As the applicability of the rules of PSGL4ip is decidable, we distinguish two cases:

(I) No PSGL4ip rule is applicable to s. Then the derivation of maximum height sought after is simply the derivation constituted of s solely, which is the only derivation for s.

(II) Some PSGL4ip rule is applicable to s. Either only initial rules are applicable, in which case the derivation of maximum height sought after is simply the derivation of height 1 constituted of the application of the applicable initial rule to s. Or, some other rules than the initial rules are applicable. Then consider the finite list $Prems(s)$ of all sequents s_{prem} such that there is an application of a PSGL4ip rule r with s as conclusion of r and s_{prem} as premise of r. Note that this list is effectively computable, as shown by the lemma `finite_premises_of_S` in our formalisation. By Lemma 4.4 we know that every element s_0 in the list $Prem(s)$ is such that $s_{prem} \lhd 3\, s$. Consequently, the strong induction hypothesis allows us to consider the derivation of maximum height of all the sequents in $Prem(s)$. As $Prem(s)$ is finite, there must be an element s_{max} of $Prem(s)$ such that its derivation of maximum height is higher or of same height than the derivation of maximum height of all sequents in $Prem(s)$. It thus suffices to pick that s_{max}, use its derivation of maximum height, and apply the appropriate rule to obtain s as a conclusion: this is by choice the derivation of maximum height of s. Q.E.D.

Proof. [of Lemma 4.7] As $<$ and $=$ are decidable relations over natural numbers, we can reason by contradiction. So, suppose that $\mathrm{mhd}(s_1) \geq \mathrm{mhd}(s_0)$. Let δ_0 be the derivation of s_0 of maximal height and let δ_1 be the derivation of s_1 of maximal height as guaranteed by Theorem 4.6. If r is a rule instance from PSGL4ip with s_1 as one of the premises and with conclusion s_0, then δ_2 as shown below is a derivation of s_0 of height greater than $\mathrm{mhd}(s_1) + 1$:



The maximality of δ_0 implies that the height of δ_0 is greater than the height of δ_2: thus $\text{mhd}(s_1) + 1 \leq \text{mhd}(s_0)$. As our initial assumption implies that $\text{mhd}(s_1) + 1 > \text{mhd}(s_0)$, we reached a contradiction. Q.E.D.

Proof. [of Theorem 5.1] As in the partial proof given in the main body of the article, we need to show the existence of a proof in GL4ip of $X \Rightarrow C$ while being given GL4ip proofs d_1 (with last rule r_1) and d_2 (with last rule r_2) of $X \Rightarrow A$ and $A, X \Rightarrow C$. Here again, we use the primary and secondary inductive hypothesis PIH and SIH.

We make a first case distinction: does $X \Rightarrow C$ violate (NoInit)? If it is the case, then this sequent is an instance of (Id) or ($\bot$L). So, we use Lemma 3.4 or apply ($\bot$L) to obtain a proof of $X \Rightarrow C$. If $X \Rightarrow C$ satisfies (NoInit), then it is not an instance of (Id) or ($\bot$L). In this case we consider r_1. In total, there are thirteen cases to consider for r_1: one for each rule in GL4ip. However, we can gather some of the cases together and reduce the number of cases to eight. We separate them by using Roman numerals.

(I) $\mathbf{r_1}$ =(IdP) : then we have that $A = p$. Consequently, $X \Rightarrow C$ is of the form $X_0, p \Rightarrow C$. Also, the conclusion of r_2 is of the form $X_0, p, p \Rightarrow C$. We can apply the contraction Lemma 3.8 to obtain a proof of $X_0, p \Rightarrow C$.

(II) $\mathbf{r_1}$ =($\bot$L): Then r_1 must have the following form.

$$\frac{}{X_0, \bot \Rightarrow A}\ (\bot\text{L})$$

where $X_0, \bot = X$. Thus, we have that the sequent $X \Rightarrow C$ is of the form $X_0, \bot \Rightarrow C$, and is an instance of $\bot$L. But this is in contradiction with (NoInit). So we are done.

(III) $\mathbf{r_1}$ $\in${($\wedge$L), ($\vee$L), ($p\to$L), ($\wedge\to$L), ($\vee\to$L)}: In all these cases, the cut formula is not principal in r_1 so it is preserved in the premise. Given that the rules considered are invertible, we simply take the conclusion of r_2 and use the corresponding invertibility lemma to destruct the principal formula of r_1. Then, we use SIH to cut on A in the obtained premises, and apply r_1 on the conclusion of the cut.

(IV) $\mathbf{r_1}$ $\in${($\wedge$R), ($\vee_1$R), ($\vee_2$R)}: In all these cases, the cut formula is principal in r_1 so it is deconstructed in the premise. Given that the corresponding left rules are invertible, we simply take the conclusion of r_2 and use the adequate invertibility lemma to destruct the cut formula. Then, we use PIH to cut on the obtained subformulae.

(V) $\mathbf{r_1}$ =($\to$R) : Then r_1 has the following form where $A = B \to D$:

$$\frac{B, X \Rightarrow D}{X \Rightarrow B \to D}\ (\to\text{R})$$

For the cases where $B \to D$ is principal in r_2 and $r_2 \neq (\Box\!\to\!\text{L})$, or where $r_2 \in \{(\text{IdP}), (\bot\text{L})\}$, we refer to Dyckhoff and Negri's proof [7] as the cuts produced in these cases involve the traditional induction hypothesis PIH. We are left with seven sub-cases.

(V-a) If r_2 is ($\to$R) then it must have the following form.

$$\frac{B \to D, E, X \Rightarrow F}{B \to D, X \Rightarrow E \to F}\ (\to\text{R})$$

where $E \to F = C$. We can use Lemma 3.2 on the proof of $X \Rightarrow B \to D$ to get a proof of $E, X \Rightarrow B \to D$. Proceed as follows.

$$\dfrac{\dfrac{E, X \Rightarrow B \to D \qquad B \to D, E, X \Rightarrow F}{E, X \Rightarrow F}\ \text{SIH}}{X \Rightarrow E \to F}\ (\to\text{R})$$

Note that the use of SIH is justified here as the last rule in this proof is effectively an instance of $(\to\text{R})$ in PSGL4ip, hence $\text{mhd}(E, X \Rightarrow F) < \text{mhd}(X \Rightarrow E \to F)$ by Lemma 4.7.

(V-b) If r_2 is $(\wedge\text{R})$ or $(\vee_i\text{R})$, then we simply use cut with the premise(s) of r_2 and the conclusion of r_1 using SIH.

(V-c) If r_2 is $(\wedge\text{L})$, $(\vee\text{L})$, $(p{\to}\text{L})$, $(\vee{\to}\text{R})$ or $(\wedge{\to}\text{R})$ where the cut formula is not principal in r_2, then we use the inversion lemma for r_2 on the conclusion of r_1, and then apply cut using SIH.

(V-d) If r_2 is $({\to}{\to}\text{L})$ where the cut formula is not principal in r_2, then see case (I-a) in the partial proof given in the main body of the article.

(V-e) If r_2 is $(\Box{\to}\text{L})$ with the cut formula as principal formula, then it must have the following form, where $W, \Box X_0 = X$ and $\Box E = B$.

$$\dfrac{\boxtimes X_0, \Box E \Rightarrow E \qquad D, W, \Box X_0 \Rightarrow C}{\Box E \to D, W, \Box X_0 \Rightarrow C}\ (\Box{\to}\text{L})$$

Thus, we have that the sequents $X \Rightarrow C$ and $B, X \Rightarrow D$ are respectively of the form $W, \Box X_0 \Rightarrow C$ and $\Box E, W, \Box X_0 \Rightarrow D$. Then, we proceed as follows.

$$\dfrac{\dfrac{\dfrac{\boxtimes X_0, \Box E \Rightarrow E}{\Box X_0 \Rightarrow \Box E}\ \text{GLR}}{W, \Box X_0 \Rightarrow \Box E}\ \text{Lem.3.2} \qquad \dfrac{\Box E, W, \Box X_0 \Rightarrow D \qquad \dfrac{D, W, \Box X_0 \Rightarrow C}{D, \Box E, W, \Box X_0 \Rightarrow C}\ \text{Lem.3.2}}{\Box E, W, \Box X_0 \Rightarrow C}\ \text{PIH}}{W, \Box X_0 \Rightarrow C}\ \text{PIH}$$

(V-f) If r_2 is $(\Box{\to}\text{L})$ with a principal formula different from the cut formula, then it must have the following form where $\Box E \to F, W, \Box X_0 = X$.

$$\dfrac{\boxtimes X_0, \Box E \Rightarrow E \qquad F, B \to D, W, \Box X_0 \Rightarrow C}{B \to D, \Box E \to F, W, \Box X_0 \Rightarrow C}\ (\Box{\to}\text{L})$$

Thus, we have that $X \Rightarrow C$ and $X \Rightarrow B \to D$ are respectively of the form $\Box E \to F, W, \Box X_0 \Rightarrow C$ and $\Box E \to F, W, \Box X_0 \Rightarrow B \to D$. Using the right-invertibility of $(\Box{\to}\text{L})$, proven in Lemma 3.5, on $\Box E \to F, W, \Box X_0 \Rightarrow B \to D$ we obtain a proof of $F, W, \Box X_0 \Rightarrow B \to D$. Then, we proceed as follows.

$$\dfrac{\boxtimes X_0, \Box E \Rightarrow E \qquad \dfrac{F, W, \Box X_0 \Rightarrow B \to D \qquad F, B \to D, W, \Box X_0 \Rightarrow C}{F, W, \Box X_0 \Rightarrow C}\ \text{SIH}}{\Box E \to F, W, \Box X_0 \Rightarrow C}\ (\Box{\to}\text{L})$$

Note that the use of SIH is justified here as the assumption (NoInit) ensures that the last rule in this proof is effectively an instance of $(\Box{\to}\text{L})$ in PSGL4ip, hence $\text{mhd}(F, W, \Box X_0 \Rightarrow C) < \text{mhd}(\Box E \to F, W, \Box X_0 \Rightarrow C)$ by Lemma 4.7.

(V-g) If r_2 is (GLR) then it must have the following form.

$$\dfrac{\boxtimes X_0, \Box E \Rightarrow E}{W, B \to D, \Box X_0 \Rightarrow \Box E}\ (\text{GLR})$$

where $W, \Box X_0 = X$ and $\Box E = C$. In that case, note that the sequent $X \Rightarrow C$ is of the form $W, \Box X_0 \Rightarrow \Box E$. To obtain a proof of the latter, we apply the rule (GLR) on the premise of r_2 without weakening $B \to D$:

$$\dfrac{\boxtimes X_0, \Box E \Rightarrow E}{W, \Box X_0 \Rightarrow \Box E}\ (\text{GLR})$$

(VI) $\mathbf{r_1}$ =(→→L): Then r_1 is as follows, where $(B \to D) \to E, X_0 = X$.

$$\dfrac{D \to E, X_0 \Rightarrow B \to D \qquad E, X_0 \Rightarrow A}{(B \to D) \to E, X_0 \Rightarrow A}\ (\to\to\text{L})$$

Thus, we have that the sequents $X \Rightarrow C$ and $A, X \Rightarrow C$ are respectively of the form $(B \to D) \to E, X_0 \Rightarrow C$ and $A, (B \to D) \to E, X_0 \Rightarrow C$. Using the right-invertibility of (→→L), proven in Lemma 3.5, on $A, (B \to D) \to E, X_0 \Rightarrow C$ we obtain a proof of the sequent $A, E, X_0 \Rightarrow C$. Then, we proceed as follows.

$$\dfrac{D \to E, X_0 \Rightarrow B \to D \qquad \dfrac{E, X_0 \Rightarrow A \qquad A, E, X_0 \Rightarrow C}{E, X_0 \Rightarrow C}\ \text{SIH}}{(B \to D) \to E, X_0 \Rightarrow C}\ (\to\to\text{L})$$

Note that the use of SIH is justified here as the assumption (NoInit) ensures that the last rule in this proof is effectively an instance of (→→L) in PSGL4ip, hence $\text{mhd}(E, X_0 \Rightarrow C) < \text{mhd}((B \to D) \to E, X_0 \Rightarrow C)$ by Lemma 4.7.

(VII) $\mathbf{r_1}$ =(□→L): We proceed as in (V-f).

(VIII) $\mathbf{r_1}$ =(GLR): Then A is the diagonal formula in r_1:

$$\dfrac{\boxtimes X_0, \Box B \Rightarrow B}{W, \Box X_0 \Rightarrow \Box B}\ (\text{GLR})$$

where $A = \Box B$ and $W, \Box X_0 = X$. Thus, we have that the sequents $X \Rightarrow C$ and $A, X \Rightarrow C$ are respectively of the form $W, \Box X_0 \Rightarrow C$ and $\Box B, W, \Box X_0 \Rightarrow C$. We now consider r_2.

(VIII-a) If r_2 is one of (IdP), (⊥L), (∧R), (∧L), ($\vee_1$R), ($\vee_2$R), (∨L), (→R), (p→L), (∧→L), (∨→L) and (→→L) then proceed similarly to the cases (I), (II), (III), (IV) and (VI), where the cut-formula is not principal in the rules considered by using SIH.

(VIII-b) If r_2 is (□→L), then see case (II-a) in the main body of the article.

(VIII-c) If r_2 is (GLR). Then r_2 is of the following form where $\Box D = C$:

$$\dfrac{B, \Box B, \boxtimes X_0, \Box D \Rightarrow D}{W, \Box B, \Box X_0 \Rightarrow \Box D}\ (\text{GLR})$$

We proceed as follows where π is taken from the case (VIII-b):

$$\dfrac{\begin{array}{c}\pi\\ \boxtimes X_0, \Box D \Rightarrow D\end{array}}{W, \Box X_0 \Rightarrow \Box D}\ (\text{GLR})$$

Note that the use of SIH is justified here as the assumption (NoInit) ensures that the last rule in this proof is effectively an instance of (GLR) in PSGL4ip, hence $\text{mhd}(\boxtimes X_0, \Box D \Rightarrow D) < \text{mhd}(W, \Box X_0 \Rightarrow \Box D)$ by Lemma 4.7. Q.E.D.