# The depth of intuitionistic cut free proofs

Samuel R. Buss*
Department of Mathematics
University of California, San Diego
La Jolla, CA 92093-0112, USA
sbuss@math.ucsd.edu

Rosalie Iemhoff†
Institut für Algebra und Computermathematik
Technische Universität Wien
Wiedner Hauptstrasse 8-10
A-1040 Wien, Austria
iemhoff@logic.at

April 3, 2003

**Abstract**

We prove a quadratic upper bound for the depth of cut free proofs in propositional intuitionistic logic formalized with Gentzen's sequent calculus. We discuss bounds on the necessary number of reuses of left implication rules. We exhibit an example showing that this quadratic bound is optimal. As a corollary, this gives a new proof that propositional validity for intuitionistic logic is in PSPACE.

## 1 Introduction

This paper studies the depth of propositional intuitionistic cut free proofs; our main results establish a quadratic upper bound on the optimal depth of these proofs, along with an example showing that this bound is optimal.

The *depth* of a proof is defined to equal the maximum number of inferences along any path in the proof. For the purpose of measuring depth, proofs may be considered to be tree-like without loss of generality, and the

*Supported in part by NSF grant DMS-0100589.
†Supported by NWO grant S61-499, and EU Marie Curie fellowship HPMC-2001-01383.

depth of a proof is the height of the corresponding tree of sequents. We formalize intuitionistic propositional logic (IPC) with a sequent calculus PJ which has the usual Gentzen rules and in which sequents are treated as multi-sets of formulas (PJ is defined formally below). Our main result, Theorem 2, states that any intuitionistically valid formula containing $n$ connectives has a PJ-proof of depth at most $n^2$.

For classical propositional logic, it is well-known that the depth of cut free proofs can be linearly bounded: any classical tautology with $n$ connectives has a cut free proof of depth $n$. This can be proved from the fact that the rules of inference for classical logic are invertible, and that, traversing a proof upward, each inference in a cut free proof reduces the number of connectives in the sequent(s). For this, see for instance [1].

The situation for intuitionistic logic is more complicated. The intuitionistic left implication rule has the form

$$\mathrm{L}{\rightarrow}\text{:}\quad \frac{\Gamma, A \rightarrow B \Rightarrow A \qquad \Gamma, B \Rightarrow C}{\Gamma, A \rightarrow B \Rightarrow C}$$

Note that its principal formula appears in one of the upper sequents in addition to in the lower sequent. Thus, the L$\rightarrow$ inference can need to have its upper sequent be no less complex than its lower sequent; also, it may be necessary to have paths in the proof tree where the same formula is used more than once as the principal formula of a L$\rightarrow$ inference. (Section 4 will give examples of sequents where this must happen repeatedly in any cut free proof.) This makes it more difficult to prove the cut elimination theorem for intuitionistic logic, and also makes it harder to bound the depth of cut free PJ-proofs.

There has been some prior work on bounding the depth of cut free proofs for intuitionistic propositional logic, motivated in part by the desire to find good search procedures for generating proofs in IPC. The unpublished work of Franzen [3] and Waaler [10] obtained upper bounds on the necessary reuses of the L$\rightarrow$ rule along a branch of a cut free intuitionistic proof. Heuerding et al. [4] obtained bounds on proof search that use constructions similar to what we use for our Lemma 4. Indeed, quadratic upper bounds on the depth of optimal cut free proofs can be obtained from the methods of any of these three papers. We discuss the results of Franzen and Waaler at the end of Section 3 and prove a slightly strengthened version of their bounds.

Other work has focused on variants of the proof system IPC tailored to aid proof search. Dyckhoff [2] and Hudelmaier [5] independently introduced a small set of inference rules to replace the usual L$\rightarrow$ rules. Their new

inference rules have the property that there are more cases where the rules are invertible and, concomitantly, more cases where the upper sequents of a rule have simpler logical complexity than the lower sequents. Those systems have linear depth cut free proofs, but unfortunately, sequents in cut free proofs can be exponentially big compared to the size of the endsequent. Subsequently, Hudelmaier [6] was able to show that a variation of these rules gave a formalization of the intuitionistic propositional sequent calculus in which valid formulas have cut free proofs that (a) have only linear depth, and (b) have all sequents polynomially bounded in size.

Our result, Theorem 2 below, gives only a quadratic upper bound on the depth of cut free proofs, but it has the advantage of applying to a standard formulation $\mathsf{PJ}$ of the sequent calculus. The system $\mathsf{PJ}$ is a more traditional proof system, and, unlike the proof systems of Dyckhoff and Hudelmaier, satisfies useful properties such as the subformula property. The subformula property immediately implies a quadratic bound on the size of all sequents in the cut free proof, since the sequents can contain only subformulas of formulas in the endsequent.

### Connections with computational complexity

The complexity of cut free proofs is closely related to the computational complexity of recognizing valid formulas, c.f. Hudelmaier [6]. A crucial difference between the complexities of classical and intuitionistic propositional logics is that, for the former system, cut free proofs can always be generated with rules which are "invertible", whereas this is conjectured to not be possible for intuitionistic propositional logic.

**Definition** *An inference rule $\mathcal{I}$ is* invertible *provided that, for any instance of the rule, the lower sequent of the inference is valid if and only if all the upper sequents are valid.*

Classical propositional logic is known to have a set of invertible inference rules which suffice to generate cut free proofs. In fact, the usual Gentzen rules are invertible for classical logic. In addition, these invertible rules are complete with respect to cut free provability even when the principal formula is not repeated in any of the upper sequents.

These two properties of classical propositional sequent calculus can be used to give a proof that the set of classical tautologies is in coNP. Namely, any propositional formula is a tautology if and only if it has a linear depth cut free proof. We think of this linear depth proof as being created from the

bottom up; and given any sequent in the cut free proof, there is a polynomial time algorithm to decide which inference should be used to prove that sequent. Thus, the following is an coNP method for test for the existence of a cut free proof: universally quantify over all the linear depth branches in the proof and verify the local consistency of each inference along each branch and that the branch ends with a valid axiom.

This is a somewhat roundabout way to prove that the set of tautologies is in coNP, but it illustrates the point that whenever there is a deterministic proof search method which generates proofs of polynomial depth such that all sequents in the proof have polynomial size, then the decision problem of recognizing valid formulas is in coNP.

For intuitionistic logic, the validity problem is known to be PSPACE-hard [7, 8]. Correspondingly, the rules L$\rightarrow$ and R$\vee$ are not invertible, and for this reason, there is (presumably) no polynomial algorithm that can be used to decide which rules should be used in the bottom up generation of cut free proofs. Indeed, if there is such an algorithm, then $NP$ would equal PSPACE.

The polynomial bound for the depth of cut free intuitionistic proofs can be used to give a proof that intuitionistic validity is in PSPACE.

**Theorem 1** [7] *The satisfiability problem for intuitionistic propositional logic is in* PSPACE.

**Proof** By the classic result of Savitch, nondeterministic polynomial space (NPSPACE) is equal to PSPACE; therefore, it suffices to prove that there is a nondeterministic PSPACE algorithm that searches for cut free proofs of $n^2$-depth.

Consider a formula $\varphi$, where the size of $\varphi$ is $n$. The NPSPACE algorithm performs a depth-first search for a proof of depth $n^2$. By the subformula property, every formula appearing in the proof is a subformula $\varphi$; therefore each line in the proof has only $O(n^2)$ symbols. During the depth-first search, the procedure stores the current sequent, the current position in the proof, and a description of the inferences between the root of the proof and the current position. Together, all this information can be encoded by a string of length $O(n^2 \log n)$. Therefore the nondeterministic depth-first search can be carred out using only $O(n^2 \log n)$ space. When the search proceeds higher into the proof, it nondeterministically (existentially) decides what inference is used to derive a sequent. For backtracking, it is necessary only to backtrack down the current branch, and this is straightforward to accomplish from the information about the inferences along the current branch. $\Box$

The above proof method was already used by Hudelmaier [6]: since the depth of cut free proofs in his system is only $O(n)$, he gets better nondeterministic space bounds of $O(n \log n)$. In contrast, the first proof of Theorem 1, by Ladner: [7], used a detour through S4, whose satisfiability problem also belongs to PSPACE and in which IPC is embeddable.

## 2 Preliminaries

We now explain our conventions for the sequent calculus; the reader can consult [1, 9] for background information on the sequent calculus systems. Our language is the language of intuitionistic propositional logic, with variables $p, q, r, p_i, q_i, r_i, \ldots$, and connectives $\bot, \wedge, \vee, \rightarrow$, and $\neg A$ is $(A \rightarrow \bot)$. We omit parentheses when possible, using the convention that negation binds stronger than $\wedge$ and $\vee$, which in turn bind stronger than $\rightarrow$. $A, B, C, \ldots$ will range over formulas, and $\Gamma, \Delta$ over multisets of formulas. For a sequent $\Gamma \Rightarrow C$, we call $\Gamma$ the *antecedent* of the sequent, and $C$ the *succedent*. The size of a formula is defined to equal the number of occurrences of binary connectives in the formula (occurrences of the atomic connective $\bot$ are not counted). The notation $|\varphi|$ denotes the size of $\varphi$, and $|\Gamma \Rightarrow C|$ denotes the size of the sequent $\Gamma \Rightarrow C$ which is by definition the sum of the sizes of the formulas in $\Gamma$ and the formula $C$.

Given a formula $B$, a subformula $A$ of $B$ is said to be *negatively bound* by an occurrence of an implication in $B$, if $A$ is a subformula of the first argument of that implication. We say that $A$ occurs *positively* (*negatively*) in $B$ if it is negatively bound by an even (odd) number of implications in $B$. A subformula occurring in a sequent $\Gamma \Rightarrow D$ is said to be occurring positively if it occurs positively in $D$ or negatively in $\Gamma$, otherwise it occurs negatively.

Proofs, or deductions, in a sequent calculus are finite trees with a single root. Each node in the tree is labeled with a sequent. Leaf nodes are axioms, or *initial sequents*, and the sequent at the root is the *endsequent*. Internal nodes are also labeled with a full description of the inference rule used to derive the sequent labeling the node from the sequents of its children. We use $P$ as well as $\mathcal{D}$ to denote proofs. We often use $\mathcal{D}$ to denote a deduction that is part of another proof that we are considering.

The sequent calculus PJ for the intuitionistic propositional logic is formulated without any structural rules; in particular, there are no weakening inferences, and instead initial sequents are allowed to have arbitrary side formulas. This latter convention does not affect the depth of proofs, since

weakenings can just be pushed up to the initial sequents. The axioms and rules of inference for PJ are as follows. (The cut rule is included in PJ, but in this paper, we are interested exclusively in cut free proofs.)

$$\textit{axiom}: \quad \Gamma, p \Rightarrow p \quad p \text{ a variable} \qquad\qquad \mathrm{L}\bot: \quad \Gamma, \bot \Rightarrow$$

$$\mathrm{L}\wedge: \ \frac{\Gamma, A, B \Rightarrow C}{\Gamma, A \wedge B \Rightarrow C} \qquad\qquad \mathrm{R}\wedge: \ \frac{\Gamma \Rightarrow A \qquad \Gamma \Rightarrow B}{\Gamma \Rightarrow A \wedge B}$$

$$\mathrm{L}\vee: \ \frac{\Gamma, A \Rightarrow C \qquad \Gamma, B \Rightarrow C}{\Gamma, A \vee B \Rightarrow C} \qquad\qquad \mathrm{R}\vee: \ \frac{\Gamma \Rightarrow A_i}{\Gamma \Rightarrow A_0 \vee A_1}\, i = 0, 1$$

$$\mathrm{L}\rightarrow: \ \frac{\Gamma, A \rightarrow B \Rightarrow A \qquad \Gamma, B \Rightarrow C}{\Gamma, A \rightarrow B \Rightarrow C} \qquad\qquad \mathrm{R}\rightarrow: \ \frac{\Gamma, A \Rightarrow B}{\Gamma \Rightarrow A \rightarrow B}$$

$$\mathrm{Cut}: \ \frac{\Gamma \Rightarrow A \qquad \Gamma, A \Rightarrow C}{\Gamma \Rightarrow C}$$

The *principal formula* of an inference is the formula occurring in the lower sequent that is not in $\Gamma$, and not denoted $C$. The formula $C$ and the formulas that appear in $\Gamma$ are called *side formulas*. The *auxiliary formulas* of an inference are the formulas $A$, $A_i$ and $B$ in the upper sequents. We define the notion of *ancestor* as the reflexive, transitive closure of the *immediate ancestor relation* that is defined as follows. A side formula in an upper sequent of an inference is an immediate ancestor of the corresponding occurrence of the same side formula in the lower sequent. An auxiliary formula in an inference that is not a cut inference, is an immediate ancestor of the principal formula of the inference.

A couple comments about the inference rules of PJ are in order. First, it is easy to check that every inference rule is invertible, except for the R$\vee$ and L$\rightarrow$ rules. Second, there is no explicit contraction rule. The lack of a contraction rule does not increase the depth of cut free proofs however. Third, there is implicitly a contraction rule included in the L$\rightarrow$ rule, since the principal formula $A \rightarrow B$ appears also explicitly in the upper sequent, but only appears once in the lower sequent. The 'contraction-free' variant of the L$\rightarrow$ rule,

$$\mathrm{L}\rightarrow': \ \frac{\Gamma \Rightarrow A \qquad \Gamma, B \Rightarrow C}{\Gamma, A \rightarrow B \Rightarrow C}$$

is a admissible rule of inference however, since the formula $A \to B$ may be added to the upper right sequent and to the sequents in the subproof deriving that sequent. However the contraction-free rule, $\mathrm{L}{\to}'$, is not as strong as the $\mathrm{L}{\to}$ rule, in that the system obtained from $\mathsf{PJ}$ by replacing $\mathrm{L}{\to}$ with $\mathrm{L}{\to}'$ is not as strong as $\mathrm{L}{\to}$ with respect to cut free provability.

The fact that there is an implicit contraction in the $\mathrm{L}{\to}$ rule means that, in general, one application of this rule to the same implication may not suffice in cut free proofs. That is, there may be implications $(A \to B)$ for which applications of the rule $\mathrm{L}{\to}$ with $(A \to B)$ as a principal formula occur more than once along one branch in a cut free proof. The following example shows that this is indeed the case. (Other examples may be found in [9].) Consider the following sequent:

$$\Big((p \to \bot) \vee p\Big) \to \bot \Rightarrow \bot. \tag{1}$$

The shortest cut free proof of this sequent is

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{p, ((p \to \bot) \vee p) \to \bot \Rightarrow p}{p, ((p \to \bot) \vee p) \to \bot \Rightarrow (p \to \bot) \vee p}\mathrm{L}{\to} \qquad p, \bot \Rightarrow \bot}{p, ((p \to \bot) \vee p) \to \bot \Rightarrow \bot}\mathrm{L}{\to}}{((p \to \bot) \vee p) \to \bot \Rightarrow p \to \bot}}{((p \to \bot) \vee p) \to \bot \Rightarrow (p \to \bot) \vee p}\mathrm{L}{\to} \qquad \bot \Rightarrow \bot}{((p \to \bot) \vee p) \to \bot \Rightarrow \bot}\mathrm{L}{\to}$$

Note how the $\mathrm{L}{\to}$ inference is used twice along the leftmost branch of the proof with the same principal formula. In fact, it is not difficult to show that any cut free proof of the sequent (1) must contain a branch that has two $\mathrm{L}{\to}$ inferences with the same principal formula. Intuitively, when one reads the above proof bottom up,[1] some information in the succedent of a sequent can disappear. Namely, first one has to extract $(p \to \bot)$ from the antecedent $((p \to \bot) \vee p)$ of the implication, to obtain $p$ in the antecedent of the sequent. However, in doing this, one has to apply $\mathrm{R}{\vee}$, and the other disjunct, $p$, then disappears. One has to apply $\mathrm{L}{\to}$ again, to get a $p$ in the succedent of the sequent and thereby reach an axiom.

Section 4 discusses more sophisticated examples were linearly many reuses of $\mathrm{L}{\to}$ inferences are needed.

Careful examination of the reasoning used in the example suggests that one does not have to apply the rule $\mathrm{L}{\to}$ more than $O(n)$ times to an implication $(A \to B)$, where $n$ is the size of the endsequent. We will see that

[1] By "bottom up," we mean starting at the endsequent.

this is indeed the case. The proof of our main theorem will need to analyze proofs in still more detail, to better bound both the number of reuses of $\mathrm{L}\rightarrow$ and the total depth of the cut free proof.

## 3 Main theorem and proofs

**Theorem 2** *Every provable sequent of size $n$ has a cut free proof in* PJ *of depth at most $n^2$.*

In addition to a bound on the depth of cut free proofs, we obtain a bound on the number of applications of the rule $\mathrm{L}\rightarrow$ along a branch in a cut free proof.

**Theorem 3** *Every provable sequent of size $n$ has a cut free proof in* PJ *of depth at most $n^2$, in which there are at most $(n+1)$ applications of the rule $\mathrm{L}\rightarrow$ along a branch.*

We will actually prove something stronger than the bounds in the above theorems. A binary connective occurring in a sequent is said to occur *positively* (resp., *negatively*) if is the principal connective of an positive (resp., negative) occurrence of a subformula in the endsequent. We let $n^+$ (respectively, $n^-$) be the number of positive (respectively, negative) occurrences of binary connectives in the sequent. The proof of Theorem 3 will show that the sequent has a cut free proof of depth $< (1+n^-)(2+n^+)$ with at most $(1+n^-)$ many application of $\mathrm{L}\rightarrow$ along any branch. Theorems 6 and 8 will further improve the bound $n^-+1$ on the number of applications of the $\mathrm{L}\rightarrow$ rule.

**Proof** (of Theorem 3.) To make the proof more transparent, we reformulate PJ in such a way that both the antecedents of the upper sequents of a rule contain all the formulas in the antecedent of the lower sequent. Thus the rules for the succedents (the R-rules) remain the same, and we replace the

rules L$\wedge$, L$\vee$ and L$\rightarrow$ by respectively

$$\mathrm{L}\wedge\text{:}\ \frac{\Gamma, A\wedge B, A, B \Rightarrow C}{\Gamma, A\wedge B \Rightarrow C}$$

$$\mathrm{L}\vee\text{:}\ \frac{\Gamma, A\vee B, A \Rightarrow C \qquad \Gamma, A\vee B, B \Rightarrow C}{\Gamma, A\vee B \Rightarrow C}$$

$$\mathrm{L}\rightarrow\text{:}\ \frac{\Gamma, A\rightarrow B \Rightarrow A \qquad \Gamma, A\rightarrow B, B \Rightarrow C}{\Gamma, A\rightarrow B \Rightarrow C}$$

We will use the name $\mathsf{PJ}^*$ for the system obtained from $\mathsf{PJ}$ by reformulating the rules in the way as explained above and by adding the following rule:

$$\mathrm{R}^{\mathrm{s}}\rightarrow\text{:}\ \frac{\Gamma \Rightarrow B}{\Gamma \Rightarrow A\rightarrow B}$$

*Claim 0.* A cut free proof in $\mathsf{PJ}^*$ can be transformed into a cut free proof in $\mathsf{PJ}$ without increasing the depth of the proof, and vice versa.
*Proof of Claim 0.* It is not difficult to see that a cut free proof in $\mathsf{PJ}$ can be transformed into a cut free proof in $\mathsf{PJ}^*$ without increasing the depth of the proof. To see that the converse is also true, observe that the following holds, where $\mathsf{PJ} \vdash^d \mathcal{S}$ means that the sequent $\mathcal{S}$ has a cut free derivation of depth $\leq d$.

$$\begin{array}{lllll}
(a) & \mathsf{PJ} \vdash^d \Gamma, A\wedge B, A, B, \Rightarrow C & \text{implies} & \mathsf{PJ} \vdash^d \Gamma, A, B, \Rightarrow C \\
(b) & \mathsf{PJ} \vdash^d \Gamma, A_0\vee A_1, A_i \Rightarrow C & \text{implies} & \mathsf{PJ} \vdash^d \Gamma, A_i \Rightarrow C \quad (i=0,1) \\
(c) & \mathsf{PJ} \vdash^d \Gamma, A\rightarrow B, B \Rightarrow C & \text{implies} & \mathsf{PJ} \vdash^d \Gamma, B \Rightarrow C
\end{array}$$

Proofs of (a)-(c) can be found in [9]. We use induction to the depth $d$ to show that a cut free proof of depth $\leq d$ in $\mathsf{PJ}^*$ can be transformed into a cut free proof in $\mathsf{PJ}$ of depth $\leq d$. We treat the case that $d>0$ and the last inference of the proof is L$\rightarrow$. Suppose the endsequent is $\Gamma, A\rightarrow B \Rightarrow C$, then the upper sequents are $\Gamma, A\rightarrow B \Rightarrow A$ and $\Gamma, A\rightarrow B, B \Rightarrow C$. By assumption they have $\mathsf{PJ}^*$-derivations of depth $\leq d-1$. By the induction hypothesis both sequents have a proof of depth $\leq d-1$ in $\mathsf{PJ}$. By (c), $\Gamma, B \Rightarrow C$ has a proof of depth $\leq d-1$ in $\mathsf{PJ}$. An application of L$\rightarrow$ gives a proof of depth $\leq d$ in $\mathsf{PJ}$ of $\Gamma, A\rightarrow B \Rightarrow C$. We leave the rest of the proof of the claim to the reader.

Examination of the proof of Claim 0 shows that the transformations between cut free $\mathsf{PJ}^*$- and $\mathsf{PJ}$ proofs do not increase the number of L$\rightarrow$

inferences. Therefore, it suffices to prove Theorem 3 for $\mathsf{PJ}^*$. The idea of the proof is the following. Consider a branch in a proof and two sequents $\Gamma \Rightarrow C$, $\Gamma' \Rightarrow C'$ in the branch, where $\Gamma' \Rightarrow C'$ is immediately below $\Gamma \Rightarrow C$. Thus $\Gamma' \Rightarrow C'$ is the result of an application of a rule to $\Gamma \Rightarrow C$ and (possibly) some other sequent. Since we are working in $\mathsf{PJ}^*$, $\Gamma$ contains $\Gamma'$ (as a multiset).

If the rule is one of the rules L$\wedge$, L$\vee$ and R$\rightarrow$, or it is L$\rightarrow$ and $\Gamma \Rightarrow C$ is the right upper sequent, then $\Gamma$ contains more formulas than $\Gamma'$. We call such a step in the branch a *1-step*. If the rule is one of the rules R$\wedge$, R$\vee$, R$^{\mathrm{S}}\rightarrow$ or it is L$\rightarrow$ and $\Gamma \Rightarrow C$ is the left upper sequent, then $\Gamma$ is equal to $\Gamma'$. We call such a step a *2-step*.

We introduce a method of labeling formulas for the purpose of keeping track of the identities of formulas at different places in a proof. Intuitively, this is similar to keeping track of whether two different occurrences of the same formula are ancestors of the same formula in the endsequent; however, just keeping track of ancestors is not enough. In labeled proofs, each occurrence of a formula in the proof will be given a label. Two occurrences of a formula that get the same label will be viewed as being linked, and being different copies of the same formula.

To distinguish carefully between "formulas" and "occurrences of formulas", we use the convention that the phrase "occurrence of a formula in a sequent" means either a formula in the sequent or a subformula of a formula in the sequent. The phrase "occurrence of a formula in a proof" is defined similarly. We use the phrase "appearance of a formula in a sequent" to mean that the formula is in the sequent, i.e., is a member of either the antecedent or succedent. The verbs "occur" and "appear" are used with the corresponding meanings. Also, a sequent "contains" a formula iff the formula appears in the sequent.

**Definition [Labeling of formulas in a proof]** *Consider a cut free* $\mathsf{PJ}^*$*-proof $P$ of a sequent $\Delta \Rightarrow H$. The labels of occurrences of formulas in $P$ will be sequences of numbers. Let $S(\Delta \Rightarrow H)$ be the set of all occurrences of formulas in $\Delta \Rightarrow H$. A* labeling *of the sequent $\Delta \Rightarrow H$ must satisfy the following properties. First, each member of $S(\Delta \Rightarrow H)$, (i.e., each occurrence of a formula in the sequent) gets a single label. Second, for $\circ \in \{\wedge, \vee, \rightarrow\}$ we have that if $(A \circ B) \in S(\Delta \Rightarrow H)$ has label $\sigma$, then $A$ has label $\sigma 0$ and $B$ has label $\sigma 1$. Third, two occurrences of formula may be assigned the same label only if they are occurrences of the same formula.*

*The labeling of the endsequent $\Delta \Rightarrow H$ is then extended to a labeling of all occurrences of formulas in the proof $P$. This is done by letting the*

*labeling of the endsequent extend in a natural way to all the sequents in the proof. Suppose all formulas in the lower sequent of the application of a rule are already labeled, then the following table shows how we extend this labeling to the upper sequent(s). We only indicate the label for the active formulas in the rule, all the side formulas in the upper sequents receive the same label as the corresponding side formulas in the lower sequent.*

$$\mathrm{L}\wedge\text{:}\ \frac{\Gamma, (A \wedge B)^\sigma, A^{\sigma 0}, B^{\sigma 1} \Rightarrow C}{\Gamma, (A \wedge B)^\sigma \Rightarrow C} \qquad \mathrm{R}\wedge\text{:}\ \frac{\Gamma \Rightarrow A^{\sigma 0} \qquad \Gamma \Rightarrow B^{\sigma 1}}{\Gamma \Rightarrow (A \wedge B)^\sigma}$$

$$\mathrm{L}\vee\text{:}\ \frac{\Gamma, (A \vee B)^\sigma, A^{\sigma 0} \Rightarrow C \qquad \Gamma, (A \vee B)^\sigma, B^{\sigma 1} \Rightarrow C}{\Gamma, (A \vee B)^\sigma \Rightarrow C}$$

$$\mathrm{R}\vee\text{:}\ \frac{\Gamma \Rightarrow A_i^{\sigma i}}{\Gamma \Rightarrow (A_0 \vee A_1)^\sigma}$$

$$\mathrm{L}\rightarrow\text{:}\ \frac{\Gamma, (A \rightarrow B)^\sigma \Rightarrow A^{\sigma 0} \qquad \Gamma, (A \rightarrow B)^\sigma, B^{\sigma 1} \Rightarrow C}{\Gamma, (A \rightarrow B)^\sigma \Rightarrow C}$$

$$\mathrm{R}\rightarrow\text{:}\ \frac{\Gamma, A^{\sigma 0} \Rightarrow B^{\sigma 1}}{\Gamma \Rightarrow (A \rightarrow B)^\sigma} \qquad \mathrm{R}^s\rightarrow\text{:}\ \frac{\Gamma \Rightarrow B^{\sigma 1}}{\Gamma \Rightarrow (A \rightarrow B)^\sigma}$$

*A proof that is labeled according to the rules above, is called a* loosely labeled proof. *When moreover all the occurrences of formulas in the endsequent have different labels, the proof is called a* strictly labeled proof.

The notion of a loosely labeled proof enables us to view a subproof of a labeled proof as a labeled proof itself. A subproof of a strictly or loosely labeled proof is in general not strictly labeled, but it is easy to see that it is loosely labeled.

Note that when a formula is obtained more than once in the same way, it will receive the same label again. Furthermore, if in a strictly labeled proof multiple copies of a formula have the same label, then they are obtained in the same way in the proof.

In the rest of the proof we will call two labeled formulas the same if they are literally the same expression, i.e. if the formulas are syntactically identical, and the formulas have the same label. When we write multiple occurrences of a formula, these copies are meant to be the same formula with the same label. From now on, a proof will always mean a strictly labeled proof. If a proof is only loosely labeled we will explicitly say so. The assumption that all proofs are labeled in no way affects the generality

of our theorems, since any unlabeled cut free proof can be strictly labeled, and since, conversely, any loosely labeled proof can be transformed into an ordinary proof by just erasing the labels. In order to avoid heavy notation we will not indicate the labels in the sequents that occur in a proof.

**Definition [Contracted proofs, h-constant parts, i-normal proofs]** *A labeled sequent is called* contracted *if its antecedent does not contain two occurrences of any (labeled) formula. A proof is called* contracted *if all the sequents in the proof are contracted.*

*A part of a branch of a proof which consist only of 2-steps, and which is maximal as such, is called an* h-constant *part. The "h" refers to the* hypotheses *(antecedents) of the sequents in such a part. An h-constant part is of the form*

$$\begin{array}{c} \Gamma \Rightarrow D \\ \vdots \\ \Gamma \Rightarrow E \end{array}$$

*where all the sequents between* $\Gamma \Rightarrow D$ *and* $\Gamma \Rightarrow E$ *have the same antecedent* $\Gamma$*, i.e. they are all of the form* $\Gamma \Rightarrow F$*, for some formula* $F$*. The maximality requirement means that any sequent immediately above* $\Gamma \Rightarrow D$ *or immediately below* $\Gamma \Rightarrow E$ *has antecedent different from* $\Gamma$*.*

*Given an h-constant part t, we say that a rule is applied along t if both the lower sequent and one of the upper sequents of the rule belong to t. Observe that for an* $\mathrm{L}{\rightarrow}$ *inference, both the lower sequent and the leftmost upper sequent belong to the same h-constant part.*

*An* i-normal form proof *is defined to be a contracted, cut free proof in which the rule* $\mathrm{L}{\rightarrow}$ *is applied at most once along each h-constant part. The "i" refers to* implication*.*

Consider a (labeled) proof $P$ in $\mathsf{PJ}^*$ of a sequent $\Delta \Rightarrow H$, and suppose the size of $\Delta \Rightarrow H$ is $n$. First we show, Lemma 4, that the proof $P$ can be transformed into a contracted proof. Consider any branch in a contracted proof: the number of formulas in the antecedents can only increase as the branch is followed upwards from the endsequent. Since endsequent has size $n$, there are at most $2n$ possible formulas that can occur anywhere in the proof that do not already appear in the endsequent. (To prove this, note that if $m+1$ formulas appear in the endsequent, $m$ of them in the antecedent, then there are total of $2n+m$ many occurrences of formulas in the endsequent.) Thus, there can be at most $2n$ 1-steps along any branch since each 1-step must introduce at least one new formula into the endsequent. Consequently, there

are at most $2n+1$ many h-constant parts along any branch in a contracted proof.

To see that every h-constant part has length at most $2n+1$ is not difficult. We can assume that all sequents along an h-constant part are different. For if they are not, we could collapse equal sequents and still have a contracted proof of the same endsequent. Now, there are at most $2n+1$ many formulas that occur positively in the endsequent; thus there are at most $2n+1$ possible distinct antecedents. This shows that every contracted cut free proof can be transformed into a contracted cut free proof in which every h-constant part has length $\leq 2n+1$. Therefore, Lemma 4, together with this last observation, proves a weakened version of Theorem 2 with the bound $n^2$ replaced by $(2n+1)^2$.

Lemma 5 is about the 2-steps in a branch. It states that along every h-constant part of a branch, there is at most one $\mathrm{L}\rightarrow$ inference. It follows then, the number of $\mathrm{L}\rightarrow$ inferences along any branch is less than or equal to the number of h-constant parts in the branch. From this, we get a proof of a weakened version of Theorem 3 with the bounds $n^2$ and $n+1$ replaced by $(2n+1)^2$ and $2n+1$, respectively.

Of course, we want to prove Theorems 2 and 3 as stated, not the weakened versions. However, we will first state and prove Lemmas 4 and 5, and afterward we will sharpen the arguments in the previous three paragraphs to complete the proofs of the two theorems.

**Lemma 4** *Every cut free proof of a contracted sequent can be transformed into a contracted cut free proof of the same sequent without increasing the depth of the proof.*

**Proof** We prove the lemma by induction on the depth $d$ of proofs. We need the following claim, the proof of which we leave to the reader.

*Claim 1.* If $\Gamma, A, A \Rightarrow C$ has a loosely labeled cut free proof, then $\Gamma, A \Rightarrow C$ has a loosely labeled cut free proof of the same depth. (Recall that all formulas are labeled and that multiple copies of a formula, e.g. the $A$'s, denote copies of the same formula with the same label.)

Consider a cut free proof of $\Gamma \Rightarrow D$ of depth $d$. If $d = 0$, the proof consists of a single axiom, the endsequent. Since we have assigned different labels to the formulas in the endsequent, that sequent certainly is contracted. For $d > 0$, we distinguish by cases according to the last rule that is applied in the proof.

If the last rule is $\mathrm{R}\wedge$ then there are $A$ and $B$ such that $D = A \wedge B$ and the proof looks as follows.

$$\dfrac{\begin{array}{cc}\vdots\,\mathcal{D} & \vdots\,\mathcal{D}' \\ \Gamma \Rightarrow A & \Gamma \Rightarrow B\end{array}}{\Gamma \Rightarrow A \wedge B}$$

Since $\Gamma \Rightarrow A \wedge B$ is the endsequent, this sequent is certainly contracted, whence so are the two upper sequents. By the induction hypothesis there are contracted cut free proofs of depth $\leq d-1$ of the sequents $\Gamma \Rightarrow A$ and $\Gamma \Rightarrow B$. An application of R$\wedge$ gives a contracted cut free proof of $\Gamma \Rightarrow A \wedge B$ of depth $\leq d$. The cases that the last rule is R$\vee$ or R$^{\mathrm{S}}\!\rightarrow$ are similar and left to the reader.

Suppose the last rule is L$\wedge$ with principal formula $(A \wedge B)$. Hence the upper sequent of the last rule is $\Gamma, A, B \Rightarrow D$. Since the endsequent $\Gamma \Rightarrow D$ is contracted, the only multiple copies of a labeled formula that can appear in the upper sequent are $A$ or $B$. If $\Gamma$ contains neither $A$ nor $B$, the upper sequent is contracted. By the induction hypothesis it has a contracted cut free proof of depth $\leq d-1$. Applying L$\wedge$ gives the desired result.

Suppose $\Gamma$ contains $A$ or $B$. We treat the case that it contains both, the other cases are similar. Thus $\Gamma = \Gamma', A \wedge B, A, B$ and the proof looks as follows.

$$\dfrac{\vdots\,\mathcal{D}}{\Gamma', A \wedge B, A, B, A, B \Rightarrow D}$$
$$\Gamma', A \wedge B, A, B \Rightarrow D$$

The proof of the upper sequent has depth $\leq d-1$. Thus by Claim 1, there exists a proof of $\Gamma', A \wedge B, A, B \Rightarrow D$ of depth $\leq d-1$. By the induction hypothesis $\Gamma', A \wedge B, A, B \Rightarrow D$ has a contracted cut free proof of depth $\leq d-1$, thus certainly of depth $\leq d$. The case that the last rule is L$\vee$ is similar and left to the reader.

If the last rule is R$\rightarrow$, then $D = A \rightarrow B$ and the upper sequent is $\Gamma, A \Rightarrow B$. If $A$ does not appear in $\Gamma$, then the upper sequent is contracted, and whence by the induction hypothesis it has a contracted cut free proof. By applying R$\rightarrow$ to the sequent we obtain a contracted cut free proof of $\Gamma \Rightarrow A \rightarrow B$ of depth $\leq d$. If $A$ does appear in $\Gamma$, the upper sequent is of the form $\Gamma', A, A \Rightarrow B$, where $\Gamma = \Gamma', A$. Since the endsequent $\Gamma \Rightarrow A \rightarrow B$ is contracted, so is the sequent $\Gamma', A \Rightarrow B$. By Claim 1, there exists a cut free proof of $\Gamma', A \Rightarrow B$ of depth $\leq d-1$. By the induction hypothesis it has a contracted cut free proof of the same depth. Apply rule R$^{\mathrm{S}}\!\rightarrow$ to obtain a contracted cut free proof of $\Gamma', A \Rightarrow A \rightarrow B$ of depth $\leq d$.

Finally, suppose the last rule is L$\rightarrow$ with principal formula $(A \rightarrow B)$. Then the upper sequents of the last rule are $\Gamma \Rightarrow A$ and $\Gamma, B \Rightarrow D$. If $\Gamma$

does not contain $B$, both upper sequents of the rule are contracted. By the induction hypothesis these sequents have contracted cut free proofs of depth $\leq d-1$. An application of L$\rightarrow$ gives a contracted cut free proof of $\Gamma \Rightarrow D$ of depth $\leq d$.

If $\Gamma$ does contain the formula $B$, say $\Gamma = \Gamma', A \rightarrow B, B$, the proof looks as follows.

$$\dfrac{\begin{array}{cc} \vdots\,\mathcal{D} & \vdots\,\mathcal{D}' \\ \Gamma', A \rightarrow B \Rightarrow A & \Gamma', A \rightarrow B, B, B \Rightarrow D \end{array}}{\Gamma', A \rightarrow B, B \Rightarrow D}$$

When we apply Claim 1 to the rightmost upper sequent we obtain a proof of $\Gamma', A \rightarrow B, B \Rightarrow D$ of depth $\leq d-1$. By the induction hypothesis it has a contracted cut free proof of depth $\leq d-1$. □

**Lemma 5** *Every contracted cut free proof of a sequent can be transformed into an i-normal form proof of the same sequent.*

**Proof** Consider a contracted cut free proof $P$ of a sequent $\Gamma \Rightarrow F$. For a smooth induction we have to consider not only the sequents that appear in $P$, but all sequents that may appear in some proof of $\Gamma \Rightarrow F$. Therefore, we define the sets $S_p$ and $S_n$ which contain all the formulas that occur respectively positively and negatively in $\Gamma \Rightarrow F$.

From now on in this proof we consider only sequents $\Gamma \Rightarrow F$ for which $\Gamma \subseteq S_n$ and $F \in S_p$. Since the proofs we consider are contracted, every formula of $S_n$ appears at most once in $\Gamma$. Let $k$ be the cardinality of $S_n$, then $\Gamma$ can contain no more than $k$ formulas. We prove the lemma by induction on $k-m$, where $m$ is the number of formulas in $\Gamma$. We use a subinduction on the depth $d$ of $P$.

If $m = k$, then $\Gamma = S_n$. Since $P$ is contracted this implies that all sequents in the proof are of the form $\Gamma \Rightarrow D$, for some $D$. Therefore, the rule L$\rightarrow$ can never be applied, and thus the proof is in i-normal form.

Suppose $m < k$. If $d = 0$, $\Gamma \Rightarrow F$ is an axiom, whence $P$ is in i-normal form. Suppose $d > 0$. First consider the case when the last rule of $P$ is L$\wedge$, L$\vee$ or R$\rightarrow$. In these cases, the antecedents of the upper sequents contain more formulas than $\Gamma$. Therefore, it follows from the induction hypothesis that the upper sequents have i-normal form proofs. It is easy to see that this implies that the lower sequent $\Gamma \Rightarrow F$ has an i-normal form proof.

Suppose the last rule of $P$ is R$\wedge$, R$\vee$ or R$^{\mathrm{S}}\rightarrow$. In this case the antecedents of the upper sequents are the same as the antecedent of the lower sequent,

but the depth of their proofs is $\leq d-1$. Therefore, it follows from the induction hypothesis that the upper sequents have i-normal form proofs. This implies that the lower sequent $\Gamma \Rightarrow F$ has a proof in i-normal form.

Finally, suppose the last rule of $P$ is $\mathrm{L}{\rightarrow}$. The proof looks as follows, where $\Gamma = \Gamma', A \rightarrow B$.

$$\dfrac{\begin{array}{cc}\vdots & \vdots \\ \Gamma', A \rightarrow B \Rightarrow A & \Gamma', A \rightarrow B, B \Rightarrow E\end{array}}{\Gamma', A \rightarrow B \Rightarrow E}$$

By the induction hypothesis we may assume that both upper sequents have i-normal form proofs. The sequents $\Gamma', A \rightarrow B \Rightarrow A$ and $\Gamma', A \rightarrow B \Rightarrow E$ belong to an h-constant part. Let us call this h-constant part $t$. Let $t'$ denote the result of removing the last sequent, the endsequent, from $t$. Note that $t'$ is an h-constant part in the i-normal form proof of $\Gamma', A \rightarrow B \Rightarrow A$. Therefore, there is at most one $\mathrm{L}{\rightarrow}$ inference along $t'$. If there is no $\mathrm{L}{\rightarrow}$ inference along $t'$, there is at most one $\mathrm{L}{\rightarrow}$ inference along $t$. In this case $P$ is in i-normal form. Suppose there is a $\mathrm{L}{\rightarrow}$ inference along $t'$. Then $P$ looks as follows, where $\Gamma'', A \rightarrow B, C \rightarrow D \Rightarrow E'$ is the highest sequent of $t$.

$$\dfrac{\dfrac{\begin{array}{c}\vdots \\ \Gamma'', A \rightarrow B, C \rightarrow D \Rightarrow E' \\ \vdots \end{array}}{\begin{array}{cc}\vdots & \vdots \\ \Gamma'', A \rightarrow B, C \rightarrow D \Rightarrow C & \Gamma'', A \rightarrow B, C \rightarrow D, D \Rightarrow A'\end{array}}}{\begin{array}{c}\Gamma'', A \rightarrow B, C \rightarrow D \Rightarrow A' \\ \vdots \end{array}}}{\begin{array}{cc}\vdots & \vdots \\ \Gamma'', A \rightarrow B, C \rightarrow D \Rightarrow A & \Gamma'', A \rightarrow B, B, C \rightarrow D \Rightarrow E\end{array}}$$
$$\Gamma'', A \rightarrow B, C \rightarrow D \Rightarrow E$$

The only rules that are applied in the two vertical dotted parts, are $\mathrm{R}{\wedge}$, $\mathrm{R}{\vee}$ and $\mathrm{R}^{\mathrm{S}}{\rightarrow}$. We replace this part of the proof by

$$\dfrac{\dfrac{\begin{array}{c}\vdots \\ \Gamma'', A \rightarrow B, C \rightarrow D \Rightarrow E' \\ \vdots \end{array}}{\begin{array}{cc}\vdots & \vdots \\ \Gamma'', A \rightarrow B, C \rightarrow D \Rightarrow C & \Gamma'', A \rightarrow B, C \rightarrow D, D \Rightarrow E\end{array}}}{\Gamma'', A \rightarrow B, C \rightarrow D \Rightarrow E}$$

where $\mathcal{D}$ is the vertical dotted part.

Clearly, the part of the proof above $\Gamma'', A \to B, C \to D \Rightarrow C$ remains unchanged. This implies that the part of the proof outside $\mathcal{D}$ is in i-normal form. Thus if $\mathcal{D}$ is in i-normal form, so is the whole proof. To see that there is a suitable $\mathcal{D}$ in i-normal form, we reason as follows. Let $\mathcal{S}$ be the sequent $\Gamma'', A \to B, C \to D, D \Rightarrow E$. First note that the sequent $\mathcal{S}$ is weaker than the endsequent of $P$; hence it is valid and has a cut free proof. Further, since $\Gamma'', A \to B, C \to D, D \Rightarrow A'$ appears in a contracted proof, it must be contracted, and thus $\mathcal{S}$ is also contracted. Thus by Lemma 4, $\mathcal{S}$ has a contracted proof. Hence, by the induction hypothesis, $\mathcal{S}$ has an i-normal form proof: this is the proof we take for $\mathcal{D}$. This concludes the induction step. □

We are now ready to finish the proof of Theorems 2 and 3. Let $P$ be a i-normal proof of $\Gamma \Rightarrow C$. Recall that $n$ is the size of the sequent, i.e., the number of binary connectives in the sequent. If $n = 0$, the sequent contains only atomic formulas, thus it must be an axiom and have a proof of depth 0. Also, if $n = 1$, there is a single non-atomic formula in the endsequent; it is easy to check that in this case the sequent has a cut free proof which contains a single inference and is of depth 1. Likewise if $n = 2$, it is straightforward to check that there is a cut free proof of depth $\leq 2$.

So suppose $n \geq 3$. Recall the notations $n^+$ and $n^-$. Note $n = n^+ + n^-$. We further let $n^-_{\to}$ be the number of negative occurrences of $\to$'s in the sequent, and let $n^-_{\wedge\vee}$ be the total number of negative occurrences of $\wedge$'s and $\vee$'s in the sequent. For $A$ a formula, we let $n^+(A)$ be the number of binary connectives that occur positively in $A$.

Consider any branch $\pi$ through $P$. We wish to bound the number of inferences along $\pi$. The left inferences along the path can be counted as follows:

1. There are $p \leq n^-_{\wedge\vee}$ many L$\wedge$ and L$\vee$ inferences.

2. There are $q \leq n^-_{\to}$ many L$\to$ inferences along $\pi$ such that $\pi$ contains the upper right sequent of the inference.

3. There are $\leq n^- + 1 - q$ many L$\to$ inferences along $\pi$ such that $\pi$ contains the upper left sequent of the inference. This bound follows since there are most $n^- + 1$ many h-constant parts along $\pi$ and Lemma 5 states that there is at most one L$\to$ inference in any h-constant part.

Now we need to bound the number of right inferences. First, note that any right inference that lies below all the L$\to$ inferences of $\pi$ must have a

positive subformula of $C$ as its principal formula. However, not all formulas in the antecedents along $\pi$ need to be positive subformulas of $C$. When $\pi$ contains the upper left hypothesis of a $\mathrm{L}\!\rightarrow$ inference with principal formula $A \rightarrow B$, the inference causes the formula $A$ to be transferred to the antecedent. Once $A$ is transferred to the antecedent, right inferences use positive subformulas of $A$ as principal formulas. The number of right inferences that act on positive subformulas of a single transferred copy $A$ can be bounded by $n^+(A) \leq n^+ - n^+(C)$. Thus the total number of right inferences can be bounded by:

1. $\leq n^+(C)$ many inferences that have a positive subformula of $C$ as principal formula.

2. $\leq (n^- + 1 - q)(n^+ - n^+(C))$ many right inferences that have as principal formula a subformula of a formula $A$ transferred to the antecedent by a $\mathrm{L}\!\rightarrow$ inference.

Therefore, the total number of inferences along $\pi$ is at most

$$\begin{aligned} & n^-_{\wedge\vee} + q + (n^- + 1 - q)(1 + n^+ - n^+(C)) + n^+(C) \\ \leq\ & n^-_{\wedge\vee} + (n^- + 1)(1 + n^+ - n^+(C)) + n^+(C) \\ <\ & (n^- + 1)(n^+ + 2). \end{aligned}$$

Now, since $n^- + n^+ = n \geq 3$, we have $(n^- + 1)(n^+ + 2) \leq n^2$, and the proof of (the strengthened forms of) Theorems 2 and 3 is finished. □

The above arguments established bounds on the total number of $\mathrm{L}\!\rightarrow$ inferences along a branch. As mentioned in the introduction, Franzen and Waaler have earlier and independently obtained better bounds on the number of times a $\mathrm{L}\!\rightarrow$ rule needs to be applied along a single branch for a given principal formula. Franzen [3] defined the number $bc(A)$ inductively by

1. $bc(p) = 0$, for $p$ a variable, or $p = \bot$.

2. $bc(A \vee B) = bc(A \wedge B) = bc(A) + bc(B)$, for $A$, $B$ any formulas.

3. $bc(\ A_1 \rightarrow (A_2 \rightarrow \cdots (A_n \rightarrow B) \cdots)\ ) = 1 + bc(B)$, provided $B$ is not an implication.

If $A$ contains a subformula $D = A_1 \rightarrow (A_2 \rightarrow \cdots (A_n \rightarrow B) \cdots)$, where $D$ is not in the scope of an implication and where $B$ is not an implication, then we call $\{A_1, \ldots, A_n\}$ a *block of components* of $A$. Clearly, $bc(A)$ is equal to the number of blocks of components of $A$.

**Theorem 6** [3, 10] *Let $\mathcal{S}$ be an intuitionistically valid sequent. Then $\mathcal{S}$ has a cut free proof such that, along any branch of the proof, each formula $A \to B$ is used as the principal formula of a* L$\to$ *inference at most $bc(A)+1$ times.*

Waaler proved a weaker version of this theorem: he defined a function $e(A)$ just like $bc(A)$ except that the third clause was replaced by $e(A \to B) = 1 + bc(B)$ for all $A$, $B$.

To prove this theorem, we need a definition and lemma. First, the concept of *r-greedy* says in effect that reversible rules are applied whenever possible, with right rules applied first.

**Definition** *A proof $P$ is said to be* r-greedy *if the following conditions hold for every sequent in $P$:*

1. *If the sequent has the form $\Pi \Rightarrow A \wedge B$, then it is the conclusion of an* R$\wedge$ *rule.*
2. *If the sequent has the form $\Pi \Rightarrow A \to B$, then it is the conclusion of an* R$\to$ *rule if $A$ does not appear in $\Pi$, and is the conclusion of an* R$^s\to$ *rule otherwise.*
3. *If the two above cases do not apply and the antecedent contains a formula $A \wedge B$ or $A \vee B$ where neither $A$ nor $B$ appear in the antecedent, then the sequent is inferred with either an* L$\wedge$ *or an* L$\vee$ *inference.*

**Lemma 7** *Any valid contracted sequent has an r-greedy, i-normal proof.*

**Proof** Since the rules R$\wedge$, R$\to$, L$\wedge$ and L$\vee$ are invertible, it is clear that every valid sequent has a r-greedy proof. The proof of Lemma 4 then shows that any sequent with a r-greedy proof also has a r-greedy, contracted proof. Finally, the proof of Lemma 5 shows that any sequent with an r-greedy, contracted proof has a r-greedy, i-normal proof. This proves the lemma. □

**Proof** (of Theorem 6) Let $P$ be an r-greedy, i-normal proof. Let $\pi$ be a branch through $P$. Consider a formula $A \to B$ which is used as the principal formula of some L$\to$ inferences along $\pi$. Let $I$ denote one of these inferences.

If $\pi$ includes the upper right sequent of $I$, then we claim that $I$ is the uppermost inference along $\pi$ that has $A \to B$ as principal formula. To prove this, note that the inference $I$ introduces $A$ into the antecedent of its upper right hypothesis. If there were another inference, $I'$, above $I$ that used $A \to B$ as principal formula, then $I'$ would introduce another instance of $A$

in the antecedent of its upper right hypothesis. But this is not permitted, because the proof $P$ is contracted.

Now suppose $\pi$ contains the upper left sequent of $I$, and consider the inferences along $\pi$ starting with this upper sequent and moving up along $\pi$. Let $\Pi$ be the antecedent of the lower sequent and the upper left sequent of $I$. Let $\pi_I$ be the subpath of $\pi$ which contains the sequents of $\pi$ above $I$ that have antecedent $\Pi$. That is, $\pi_I$ is the h-constant (sub)part of $\pi$ starting at the upper sequent of $I$. We claim that the topmost sequent of $\pi_I$ is either (a) an axiom, or (b) the lower sequent of a $\mathrm{R}\rightarrow$ inference. To prove this, first note that Lemma 5 implies that $\pi_I$ does not contain any $\mathrm{L}\rightarrow$ inferences. Second, $\Pi$ cannot contain any formulas with principal connective $\wedge$ or $\vee$, as otherwise the $\mathrm{L}\rightarrow$ inference $I$ would not have been permitted in the r-greedy proof $P$. Therefore, there are no left inferences in $\pi_I$. Third, the only remaining inference rule that can change the antecedent is the $\mathrm{R}\rightarrow$ rule, so our claim is proved.

Suppose that $\pi_I$ does not have uppermost sequent an axiom, but instead ends at a $\mathrm{R}\rightarrow$ inference. The $\mathrm{R}\rightarrow$ inference moves a formula $A_1$ which is a component of $A$ to the antecedent. In fact, since the proof is r-greedy, there must be a series of $\mathrm{R}\rightarrow$ inferences that moves an entire block of components of $A$ to the antecedent. Since the proof is contracted, a block of components can be transferred at most once to the antecedent.

Thus we can bound the number of $\mathrm{L}\rightarrow$ inferences along $\pi$ which have $A \rightarrow B$ as principal formula as follows: First, there are at most $bc(A)$ many such inferences that lie below $\mathrm{R}\rightarrow$ inferences that transfer a block of components of $A$ to the antecedent. Second, there can be one additional $\mathrm{L}\rightarrow$ inference $I$ such that either (a) the branch contains the upper right sequent of $I$, or (b) $\pi_I$ ends with an axiom and $\pi$ contains only $\mathrm{R}\wedge$, $\mathrm{R}\vee$ and $\mathrm{R}^{\mathrm{S}}\rightarrow$ inferences above $I$. $\square$

The next theorem gives a modest improvement on the Franzen-Waaler bounds. We recursively define $fc(B)$ by:

1. $fc(p) = 1$, $p$ a variable or $p = \bot$.
2. $fc(A \vee B) = 1$.
3. $fc(A \wedge B) = \max\{fc(A), fc(B)\}$.
4. $fc(A \rightarrow B) = 0$.

And then define $bc'(A)$ recursively by

1. $bc'(p) = 0$, for $p$ a variable or $p = \bot$.

2. $bc'(A \vee B) = bc'(A \wedge B) = bc'(A) + bc'(B)$, for $A$, $B$ any formulas.

3. $bc'(\ A_1 \to (A_2 \to \cdots (A_n \to B) \cdots)\ ) = fc(B) + bc'(B)$, provided $B$ is not an implication.

Since $fc(A)$ always equals 0 or 1, we have $bc'(A) \leq bc(A)$.

**Theorem 8** *Let $\mathcal{S}$ be an intuitionistically valid sequent. Then $\mathcal{S}$ has a cut free proof such that, along any branch of the proof, each formula $A \to B$ is used as the principal formula of a* $\mathrm{L}\to$ *inference at most $bc'(A) + 1$ times.*

The proof of this theorem is essentially identical to our proof of Theorem 6. One still considers an r-greedy, i-normal proof $P$. The only further observation needed is that when $fc(D)$ equals zero, and if $\Gamma \Rightarrow D$ appears in $P$, then at least one block of components of $D$ is transferred to the antecedent by the right inferences that lie above the sequent.

# 4 The optimality of the bounds

We first mention an example due to Franzen [3] that shows that our bounds on the depths of proofs are tight to within a constant factor. (Compare to the example in Section 2).

**Theorem 9** *Let $n \geq 1$. Any cut free* PJ*-proof of the sequent*

$$\Big(\bigvee_{i=1}^{n}(p_i \to \bot) \vee \bigwedge_{i=1}^{n} p_i\Big) \to \bot \Rightarrow \bot \tag{2}$$

*has a branch that contains $\Omega(n^2)$ inferences and contains at least $(n+1)$ uses of the* $\mathrm{L}\to$ *rule applied to the formula in the antecedent of $\mathcal{S}_n$. (The disjunctions and conjunctions in the sequent (2) are associated to the right.)*

We leave the proof of Theorem 9 to the reader. The sequents do have proofs of depth less than $n^2$ in which there are exactly $n+1$ uses of the $\mathrm{L}\to$ rule.

For a second example, define sequents $\mathcal{S}_n$ to equal

$$\Big(\bigwedge_{i=1}^{n}((p_i \to \bot) \to p_i) \to p_i\Big) \to \bot \Rightarrow \bot,$$

with the $\wedge$'s associated to the right. The sequents $\mathcal{S}_n$ are in the $\{\to, \wedge\}$-fragment of intuitionistic logic. Since the definition of $fc(A)$ and Theorem 8

suggest that $\wedge$'s may contribute less than $\vee$'s to the necessary reuses of $\mathrm{L}{\rightarrow}$ rules, it is natural to ask whether formulas that involve only the connectives $\rightarrow$ and $\wedge$ have substantially better bounds on the reuses of $\mathrm{L}{\rightarrow}$ rules. The next theorem shows that the answer to this question is "no," and that even sequents that have no $\vee$'s may need $\Omega(n)$ reuses of $\mathrm{L}{\rightarrow}$ inferences.

The sequents $\mathcal{S}_n$ are indeed intuitionistically valid. To prove this, note that $\bigwedge_i(\neg p_i \rightarrow p_i) \rightarrow p_i)$ is classically valid, and use Glivenko's theorem that if $A$ is classically valid, then $\neg\neg A$ is intuitionistically valid.

Let $H_n$ be the formula in the antecedent of $\mathcal{S}_n$.

**Theorem 10** *Any cut free* PJ *proof of the sequents $\mathcal{S}_n$ requires depth $\Omega(n^2)$ and contains a branch with at least $n{+}1$ reuses of the* $\mathrm{L}{\rightarrow}$ *rule with principal formula $H_n$.*

**Proof** Fix $n \geq 1$. We will give a cut free proof $P$ of $\mathcal{S}_n$ that contains a path of length $\Omega(n^2)$ along which there are $(n+1)$ applications of the rule $\mathrm{L}{\rightarrow}$ to $H_n$. It will be easy to see that every proof of $\mathcal{S}_n$ will contain such paths. This will prove the theorem. To shorten our formulas, we introduce some names for subformulas occurring in $\mathcal{S}_n$; we let $A_i$ be $p_i \rightarrow \bot$, $B_i$ be $A_i \rightarrow p_i$, $C_i$ be $B_i \rightarrow p_i$, and $D$ be $\bigwedge_{i=1}^{n} C_i$. Thus, $D \rightarrow \bot$ is $H_n$.

Let $\sigma$ range over sequences of numbers $1, \ldots, n$, in which no number occurs twice. Let $*$ denote concatenation, $\langle\rangle$ denotes the empty sequence. We write $i \in \sigma$ if $i$ occurs in $\sigma$. Let

$$\Gamma_\sigma = \{D \rightarrow \bot\} \cup \{B_i, p_i \mid i \in \sigma\}.$$

Thus $\Gamma_{\langle\rangle} = D \rightarrow \bot$. We inductively define derivations $\mathcal{D}^i_\sigma$ as follows. For $i \in \sigma$, let $\mathcal{D}^i_\sigma$ be

$$R^s \rightarrow \frac{\Gamma_\sigma \Rightarrow p_i}{\Gamma_\sigma \Rightarrow C_i}$$

Observe that this includes all the cases in which $\sigma$ has length $n$. Note that the upper sequent is indeed an axiom. For $\sigma$ of length $< n$, $i \notin \sigma$, let $\mathcal{D}^i_\sigma$ be

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma_\sigma, B_i, p_i \Rightarrow C_1}\quad \dfrac{\dfrac{}{\Gamma_\sigma, B_i, p_i \Rightarrow C_2}\quad \dfrac{}{\Gamma_\sigma, B_i, p_i \Rightarrow C_3 \wedge (\bigwedge_{i=4}^{n} C_i)}}{\Gamma_\sigma, B_i, p_i \Rightarrow C_2 \wedge (\bigwedge_{i=3}^{n} C_i)}}{\Gamma_\sigma, B_i, p_i \Rightarrow D}\quad \dfrac{}{\Gamma_\sigma, B_i, p_i, \bot \Rightarrow \bot}}{\Gamma_\sigma, B_i, p_i \Rightarrow \bot}}{\Gamma_\sigma, B_i \Rightarrow p_i \to \bot}\quad \dfrac{}{\Gamma_\sigma, B_i, p_i \Rightarrow p_i}}{\Gamma_\sigma, B_i \Rightarrow p_i}}{\Gamma_\sigma \Rightarrow C_i}$$

Finally, the proof $P$ is the following proof.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma_{\langle\rangle} \Rightarrow C_1}\quad \dfrac{\dfrac{}{\Gamma_{\langle\rangle} \Rightarrow C_2}\quad \dfrac{}{\Gamma_{\langle\rangle} \Rightarrow C_3 \wedge (\bigwedge_{i=4}^{n} C_i)}}{\Gamma_{\langle\rangle} \Rightarrow C_2 \wedge (\bigwedge_{i=3}^{n} C_i)}}{\Gamma_{\langle\rangle} \Rightarrow D}\quad \dfrac{}{\Gamma_{\langle\rangle}, \bot \Rightarrow \bot}}{\Gamma_{\langle\rangle} \Rightarrow \bot}}$$

Consider $\sigma = \langle 1, \ldots, m\rangle$. Note that if $m = n$, $\mathcal{D}^m_\sigma$ contains no $\mathrm{L}\to$ inferences. Using induction to $(n-m)$, it is easy to show that for $m < n$, $\mathcal{D}^{m+1}_\sigma$ contains a path of length $\geq \Sigma^n_{k=m+2} k$ along which there are $(n-m)$ reuses of $\mathrm{L}\to$ with principal formula $H_n$. By taking $m = 0$, this shows that $\mathcal{D}^1_{\langle\rangle}$ contains a path of length $\Omega(\Sigma^n_{k=2} k) = \Omega(n^2)$ that contains $n$ applications of the rule $\mathrm{L}\to$ to $H_n$. Whence $P$ has depth $\Omega(n^2)$ and contains a path along which there are $(n+1)$ applications of the rule $\mathrm{L}\to$ to $H_n$.

Apart from redundant inferences, the only significant difference between $P$ and other proofs of $\mathcal{S}_n$ may be caused by deferring an application of $\mathrm{L}\to$ to $B_i$. However, note that this will not shorten the proof or decrease the number of applications of $\mathrm{L}\to$ to $H_n$ along a branch. □

**Acknowledgement.** We thank the anonymous referee for helpful comments on an earlier draft.

## References


[1] S. R. Buss, *An introduction to proof theory*, in Handbook of Proof Theory, S. R. Buss, ed., North-Holland, 1998, pp. 1–78.

[2] R. Dyckhoff, *Contraction-free sequent calculi for intuitionistic logic*, Journal of Symbolic Logic, 57 (1992), pp. 795–807.

[3] T. Franzen, *Algorithmic aspects of intuitionistic propositional logic*, Tech. Rep. SICS R87010B, Swedish Institute of Computer Science, 1988.

[4] A. Heuerding, M. Seyfried, and H. Zimmermann, *Efficient loop-check for backward proof search in some non-classical propositional logics*, in Tableaux 96, Lecture Notes in Computer Science #1071, Springer-Verlag, 1996, pp. 210–225.

[5] J. Hudelmaier, *Bounds for cut elimination in intuitionistic propositional logic*, Archive for Mathematical Logic, 31 (1992), pp. 331–354.

[6] ——, *An $O(n \log n)$-space procedure for intuitionistic propositional logic*, Journal of Logic and Computation, 3 (1993), pp. 63–75.

[7] R. E. Ladner, *The computational complexity of provability in systems of modal propositional logic*, SIAM Journal on Computing, 6 (1977), pp. 467–480.

[8] R. Statman, *Intuitionistic propositional logic is polynomial-space complete*, Theoretical Computer Science, 9 (1979), pp. 67–72.

[9] A. S. Troelstra and H. Schwichtenberg, *Basic Proof Theory*, Tracts in Theoretical Computer Science #43, Cambridge University Press, Cambridge, 2nd ed., 2000.

[10] A. Waaler, *Essential contractions in intuitionistic logic*. Position paper, *Tableaux 2000* (unpublished), 2000.