On Sequent Calculi for Intuitionistic Propositional Logic

Vítězslav Švejdar*†

Jan 29, 2005

The original publication is available at CMUC.

Abstract

The well-known Dyckoff's 1992 calculus/procedure for intuitionistic propositional logic is considered and analyzed. It is shown that the calculus is Kripke complete and the procedure in fact works in polynomial space. Then a multi-conclusion intuitionistic calculus is introduced, obtained by adding one new rule to known calculi. A simple proof of Kripke completeness and polynomial-space decidability of this calculus is given. An upper bound on the depth of a Kripke counter-model is obtained.

Keywords: intuitionistic logic, polynomial-space, sequent calculus, Kripke semantics

Classification: 03B20, 03B35, 03F05.

1 Introduction

A non-classical logic often is or can be defined by means of its *Kripke semantics*: a propositional formula A may or may not be satisfied in a node of a Kripke model K, if it is not satisfied in some node of K then K is a counter-model for A, and a tautology of the given logic is defined as a formula having no counter-model in the class $\mathcal{C}$ of models chosen to represent that logic. R. Ladner in [7] constructs *decision procedures* for the most common modal logics like S4 or T based purely on Kripke semantics. When attempting to decide whether a given formula A has a counter-model in the class $\mathcal{C}$ one often faces the need to construct a Kripke model with a node a such that all formulas from a certain finite set Γ are satisfied and simultaneously all formulas from another finite set Δ are not satisfied in a. *Sequent calculi* are not mentioned in [7], but a model K with a node a such that a satisfies all formulas in Γ and violates all formulas in Δ is the same as a

*Charles University, Prague, vitezslavdotsvejdaratcunidotcz, http://www1.cuni.cz/~svejdar/. Palachovo nám. 2, 116 38 Praha 1, Czech Republic.

†This work is a part of the research plan MSM 0021620839 that is financed by the Ministry of Education of the Czech Republic.

Kripke counter-model for the sequent $\langle \Gamma \Rightarrow \Delta \rangle$. So there exists a natural link from Kripke semantics to sequent (Gentzen) calculi: when constructing a decision procedure one is sometimes able to simultaneously design a sequent calculus for the logic in question.

A decision procedure can also be based on a sequent calculus itself. It works so that it constructs the proof of the given sequent by using the rules of the calculus in reverse, i.e. by starting from a given sequent and using the rules of the calculus in backward direction, with a hope to arrive at axioms (i.e. initial sequents). Then it may be a problem to ensure termination of the procedure. For example the *contraction rule*, if used in reverse, allows one to duplicate any formula of the given sequent. So an unorganized use of the contraction rule may cause the procedure to cycle. It is known that the presence of the contraction rule is essential for many calculi met in the literature. If, as in this paper, sequents consist of sets rather than sequences of formulas then there is no contraction rule, but the option to duplicate a formula is still there because the rules allow a principal formula to simultaneously be a side formula.

R. Dyckoff in [4] found a terminating calculus for intuitionistic propositional logic. However the paper [4] does not mention Kripke semantics and is not specific about the computational complexity of the procedure obtained. We analyze the paper [4] and show that a Kripke completeness theorem is in fact implicit in it. Thus this paper offers a better insight into [4], especially to those who primarily think about Kripke semantics. We also show that if some improvements are implemented then it can be shown that the decision procedure works in polynomial space. Then we consider a second calculus for intuitionistic logic, now a multi-conclusion one, allowing any number of formulas in succedent. We again show, in this case by a much simpler proof, that the calculus in question is complete w.r.t. Kripke semantics and yields a polynomial-space decision procedure. We also obtain an upper bound on the depth of Kripke counter-model. The advantage of our multi-conclusion calculus is that it differs from calculi known e.g. from [11] and [6] in only one simple additional rule.

This paper pays more attention to the question whether decision procedures can be derived from known calculi than to the question how to construct the most efficient decision procedure. I believe that it is of some interest to have a relatively simple proofs that simultaneously show Kripke completeness, cut eliminability and polynomial-space decidability for calculi more or less traditional. Note however that J. Hudelmaier [5] constructed a calculus and a decision procedure with much lower space requirements than ours.

2 Kripke semantics and sequent calculi

We choose $\{\&, \vee, \rightarrow, \bot\}$ as the base set of logical *connectives*. So propositional *formulas* are built up from (propositional) atoms and the symbol $\bot$ for falsity using conjunction, disjunction, and implication. We treat $\neg A$ as a shorthand for $A \to \bot$. In syntax analysis, implication $\to$ has lower priority than conjunction & and disjunction $\vee$. So e.g. $p \vee q \to r$ is a shorthand for $(p \vee q) \to r$. A *sequent* is a pair of finite sets of formulas; we write $\langle\, \Gamma \;\Rightarrow\; \Delta \,\rangle$ for a sequent consisting of sets Γ and Δ. The sets Γ and Δ are called *antecedent* and *succedent* of the sequent $\langle\, \Gamma \;\Rightarrow\; \Delta \,\rangle$. When writing down sequents we use the usual notational conventions and omit curly braces and symbols for set union and the empty set. So e.g. $\langle\, \Gamma, C \;\Rightarrow\; \rangle$ is a shorthand for $\langle\, \Gamma \cup \{C\} \;\Rightarrow\; \emptyset \,\rangle$, etc.

A *Kripke frame* for intuitionistic logic is a pair $\langle W, \leq \rangle$ where $W \neq \emptyset$ and $\leq$ is a reflexive and transitive relation on W. The elements of W are *nodes*; if $x \leq y$ then the node y is said to be *accessible* from x. A *truth relation* (or a *forcing relation*) on a Kripke frame $\langle W, \leq \rangle$ is a relation $\Vdash$ between nodes and propositional formulas satisfying the *persistency condition* (if $x \Vdash p$ for an atom p and $x \leq y$ then $y \Vdash p$), respecting conjunctions, disjunctions, and falsity ($x \Vdash A \,\&\, B$ iff $x \Vdash A$ and $x \Vdash B$, $x \Vdash A \vee B$ iff $x \Vdash A$ or $x \Vdash B$, and $x \nVdash \bot$) and satisfying the well-known "modal" condition for implication: $x \Vdash A \to B$ iff for each y accessible from x it is the case that $y \Vdash B$ whenever $y \Vdash A$. It can easily be verified that any relation between nodes and propositional atoms satisfying the persistency condition extends uniquely to a truth relation. Also, if $\Vdash$ is a truth relation on a frame $\langle W, \leq \rangle$ then the persistency condition holds for all formulas, not just atoms. A *Kripke model* for intuitionistic propositional logic is a triple $\langle W, \leq, \Vdash \rangle$ where $\langle W, \leq \rangle$ is a Kripke frame and $\Vdash$ is a truth relation on $\langle W, \leq \rangle$.

If $K = \langle W, \leq, \Vdash \rangle$ is a Kripke model then $x \Vdash A$ is read "A is satisfied in x" or "x satisfies A". If A is satisfied in all $x \in W$ then A is *valid* in K. The model K is a *counter-model* for a sequent $\langle\, \Gamma \;\Rightarrow\; \Delta \,\rangle$ if some element of its domain W satisfies all formulas in Γ and simultaneously none formula from Δ. A sequent $\langle\, \Gamma \;\Rightarrow\; \Delta \,\rangle$ is *intuitionistically tautological* if it has no counter-model. A formula A is an *intuitionistic tautology* if the sequent $\langle \;\Rightarrow\; A \,\rangle$, with empty antecedent and A as the only formula in succedent, is intuitionistically tautological. It is evident that A is an intuitionistic tautology iff A is valid in each Kripke model.

An example of a Kripke frame is the structure $\langle \{a, b\}, \{[a, a], [a, b], [b, b]\} \rangle$ having two nodes a and b, with b accessible from a but a not accessible from b. Let a truth relation on this frame be defined by stipulating that p is satisfied in b and violated in a, while q is violated in both a and b. One can easily check that the formula $p \to q$ is nowhere satisfied, hence $a \Vdash (p \to q) \to p$. Thus this model is a counter-model for the sequent $\langle\, (p \to q) \to p \;\Rightarrow\; p \,\rangle$. This model also shows that the formula $((p \to q) \to p) \to p$ is not an intuitionistic tautology.

Examples of sequents that are intuitionistically tautological are

$$\langle\, \Gamma, p \;\Rightarrow\; p \,\rangle, \qquad \langle\, \Gamma, \bot \;\Rightarrow\; G \,\rangle. \tag{1}$$

Another example of an intuitionistically tautological sequent is any sequent of the form $\langle\, (A \to B) \vee (B \to A) \to \bot \;\Rightarrow\; \rangle$.

We call the least element (if it exists) of a Kripke model K a *root* of K. If $K = \langle W, \leq, \Vdash \rangle$ and $a_0 \in W$ then *submodel generated by* a_0 is the model

$K_0 = \langle W_0, \leq_0, \Vdash_0 \rangle$ where $W_0 = \{\, x \in W \,;\, a_0 \leq x \,\}$ and $\leq_0$ and $\Vdash_0$ are the restrictions of $\leq$ and $\Vdash$ to W_0. One can easily verify that if A is a propositional formula and $x \in W_0$ then $x \Vdash A \Leftrightarrow x \Vdash_0 A$. So in the sequel we can assume that if K is a counter-model for A then K has a root a and that it is the root a where $a \nVdash A$. More about Kripke models can be found in various sources, e.g. in [2] or [11].

Sequent calculi have unary and binary deduction rules. An example of a binary rule (with two premises) is

$$\langle \Gamma, E \Rightarrow G \rangle, \langle \Gamma, F \Rightarrow G \rangle \;/\; \langle \Gamma, E \vee F \Rightarrow G \rangle. \tag{4}$$

The formula in which the connective is introduced, which is the formula $E \vee F$ in case of the rule (4), is called *principal formula*, while the formulas that may disappear by using the rule, which are the formulas E and F in case of the rule (4), could be called *minor formulas* of the rule in question. The formulas that are not changed by using the rule, which are the formulas in $\Gamma \cup \{G\}$ in case of (4), are called *side formulas*. Both minor and principal formulas may simultaneously be side formulas. This, in case of the rule (4), means that each of the formulas E, F and $E \vee F$ can be an element of the set Γ.

The rule (4) is *sound* in the sense that if both sequents $\langle \Gamma, E \Rightarrow G \rangle$ and $\langle \Gamma, F \Rightarrow G \rangle$ are intuitionistically tautological then also the resulting sequent $\langle \Gamma, E \vee F \Rightarrow G \rangle$ is intuitionistically tautological. The rule (4), moreover, is *invertible* in the sense that $\langle \Gamma, E \vee F \Rightarrow G \rangle$ is intuitionistically tautological if and only if both sequents $\langle \Gamma, E \Rightarrow G \rangle$ and $\langle \Gamma, F \Rightarrow G \rangle$ are intuitionistically tautological.

3 A single-conclusion decision procedure

In this section we consider a single-conclusion calculus for intuitionistic propositional logic, where all sequents have exactly one formula in succedent. We will specify a decision procedure for intuitionistic propositional logic based on this calculus.

Lemma 1 *The following rules:*

$$\langle \Gamma \Rightarrow E \rangle, \langle \Gamma \Rightarrow F \rangle \;/\; \langle \Gamma \Rightarrow E \,\&\, F \rangle \tag{2}$$

$$\langle \Gamma, E, F \Rightarrow G \rangle \;/\; \langle \Gamma, E \,\&\, F \Rightarrow G \rangle \tag{3}$$

$$\langle \Gamma, E \Rightarrow G \rangle, \langle \Gamma, F \Rightarrow G \rangle \;/\; \langle \Gamma, E \vee F \Rightarrow G \rangle \tag{4}$$

$$\langle \Gamma, E \Rightarrow F \rangle \;/\; \langle \Gamma \Rightarrow E \rightarrow F \rangle \tag{5}$$

$$\langle \Gamma, p, D \Rightarrow G \rangle \;/\; \langle \Gamma, p, p \rightarrow D \Rightarrow G \rangle, \tag{6}$$

where D, E, F, G are formulas and p is an atom, are sound and invertible. The rules

$$\langle \Gamma \Rightarrow E \rangle \;/\; \langle \Gamma \Rightarrow E \vee F \rangle, \qquad \langle \Gamma \Rightarrow F \rangle \;/\; \langle \Gamma \Rightarrow E \vee F \rangle \tag{7}$$

$$\langle \Gamma, C \to D \Rightarrow C \rangle, \langle \Gamma, D \Rightarrow G \rangle \;/\; \langle \Gamma, C \to D \Rightarrow G \rangle \tag{8}$$

are sound. The rule

$$\langle \Gamma, D \Rightarrow G \rangle \;/\; \langle \Gamma, D, C_1 \to (C_2 \to (\,.\,. \to (C_k \to D)\,.\,.) \Rightarrow G \rangle \tag{9}$$

is sound and invertible.

Proof Look at (5). Let $K = \langle W, \leq, \Vdash \rangle$ be a counter-model for $\langle \Gamma \Rightarrow E \to F \rangle$. Assume that K has a root a and that a satisfies all formulas in Γ and violates the implication $E \to F$. So there is a node a_0 such that $a_0 \Vdash E$ and $a_0 \nVdash F$. By the persistency condition, a_0 satisfies all formulas in Γ. So the submodel K_0 of K generated by a_0 is a counter-model for the sequent $\langle \Gamma, E \Rightarrow F \rangle$. All the remaining cases are trivial. ∎

We intend to base our decision procedure on the rules in Lemma 1 and on other rules specified below. It starts with a given sequent $\langle \Sigma \Rightarrow H \rangle$ and (essentially) repeatedly applies the rules (2)–(6) to it in the reverse (right to left) direction, thus reducing the question whether a given sequent is intuitionistically tautological to same questions about one or two simpler sequents. If all paths of the computation terminate with an *initial sequent* of the form (1) then the original sequent $\langle \Sigma \Rightarrow H \rangle$ is intuitionistically tautological. If none of the rules (2)–(6), still in the right to left direction, is applicable to a sequent which is not initial then the sequent is *irreducible* in the sense of the following definition. When speaking about application of a rule, we will omit the words "in reverse" or "right to left" when the direction is clear from context.

Definition 2 *A sequent* $\langle \Gamma \Rightarrow G \rangle$ *is* irreducible *if*

- *G is a disjunction, or an atom p such that $p \notin \Gamma$, or the formula $\bot$,*
- *no formula in Γ is a conjunction, disjunction, or the formula $\bot$,*
- *Γ contains no pair p, $p \to D$ where p is an atom.*

This definition, as well as the rule (6) above, is taken from R. Dyckhoff's [4]. Note that if $\langle \Gamma \Rightarrow G \rangle$ is irreducible then Γ contains only implications and atoms.

Theorem 3 *An irreducible sequent $\langle \Gamma \Rightarrow G \rangle$ is intuitionistically tautological if and only if* some *of the following conditions is true:*

- *G has the form $E \vee F$ and some of the sequents $\langle \Gamma \Rightarrow E \rangle$ and $\langle \Gamma \Rightarrow F \rangle$ is intuitionistically tautological, or*
- *there is an implication $C \to D \in \Gamma$ such that C is compound (not an atom or $\bot$) and both sequents $\langle \Gamma \Rightarrow C \rangle$ and $\langle \Gamma - \{C \to D\}, D \Rightarrow G \rangle$ are intuitionistically tautological.*

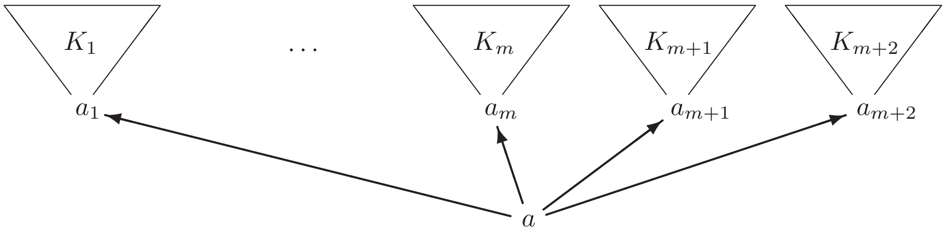

Figure 1: Amalgamation of Kripke models

Proof The non-trivial direction is $\Rightarrow$. Assume that G is $E \vee F$; the other cases, where G is $\bot$ or an atom, are similar but simpler. Let $C_1 \to D_1, .., C_m \to D_m$ be the list of all implications $C \to D$ in Γ such that C is compound. Assume that none of the sequents $\langle \Gamma \Rightarrow E \rangle$ and $\langle \Gamma \Rightarrow F \rangle$ is intuitionistically tautological and assume that for each i some of the two sequents $\langle \Gamma - \{C_i \to D_i\}, D_i \Rightarrow G \rangle$ and $\langle \Gamma \Rightarrow C_i \rangle$ is not intuitionistically tautological. It is evident that any Kripke counter-model for $\langle \Gamma - \{C_i \to D_i\}, D_i \Rightarrow G \rangle$ is automatically the desired counter-model for the sequent $\langle \Gamma \Rightarrow G \rangle$. So we may assume that for each i it is the sequent $\langle \Gamma \Rightarrow C_i \rangle$ which is not intuitionistically tautological. Let $K_1, .., K_m$ be counter-models for $\langle \Gamma \Rightarrow C_1 \rangle$ to $\langle \Gamma \Rightarrow C_m \rangle$ respectively, and let K_{m+1} and K_{m+2} be counter-models for $\langle \Gamma \Rightarrow E \rangle$ and $\langle \Gamma \Rightarrow F \rangle$. We may assume that the models $K_1, .., K_{m+2}$ have roots $a_1, .., a_{m+2}$, all nodes a_i satisfy all formulas in Γ, the node a_i for $i \leq m$ violates C_i, and a_{m+1} and a_{m+2} violate E and F respectively. Let K be the model depicted in Fig. 1, with a new root a. To finish the definition of the model K we have to specify the truth relation $\Vdash$, i.e. to state the truth values of atoms in a. Let all atoms $p \in \Gamma$ be evaluated positively in a and all remaining atoms negatively in a. Note that this choice does not violate the persistency condition, since all atoms in Γ are positive in all nodes of all submodels K_j. Each of the formulas C_i may be satisfied in various nodes of the submodels K_j, but the fact that C_i is violated in a_i is sufficient for a conclusion that $a \nVdash C_i$. Similarly $a \nVdash E$ and $a \nVdash F$. We have to check that all formulas in Γ are satisfied in a. The set Γ contains only atoms and implications, and atoms are satisfied in a by definition. An implication with a compound premise must be one of $C_i \to D_i$. To verify $a \Vdash C_i \to D_i$ we have to check that $x \Vdash D_i$ for each x accessible from a such that $x \Vdash C_i$. If x is a node of some K_j then this is true because all formulas in Γ are valid in K_j. If x is a then this is also true since $x \nVdash C_i$. Note that a similar argument applies also to implications of the form $\bot \to D$ and $p \to D$. If $p \to D \in \Gamma$ then, by the definition of irreducible sequent, p is not in Γ and as such is evaluated negatively in a. ∎

So if $\langle \Gamma \Rightarrow G \rangle$ is an intuitionistically tautological sequent then the rules (7) and (8) may be not applicable (in reverse) to any formula we choose; but if $\langle \Gamma \Rightarrow G \rangle$ is irreducible then Theorem 3 guarantees that *some* of these rules is applicable to *some* formula. Theorem 3 can be viewed as a generalization of Harrop's theorem. A similar theorem appears also in [1] and is implicit in [5]. Unfortunately Theorem 3 is still not sufficient for a decision procedure to be based on: it is not sure that the sequent $\langle \Gamma \Rightarrow C_i \rangle$ is shorter than $\langle \Gamma \Rightarrow G \rangle$, and thus it is not guaranteed that using the left implication rule (8) in reverse yields two simpler sequents. The solution is—when processing an implication in antecedent—to closer look at the form of its premise. This is one of the important ideas in [4].

Lemma 4 *The following rules are sound and invertible:*

$$\langle \Gamma, A \rightarrow (B \rightarrow D) \Rightarrow G \rangle \ / \ \langle \Gamma, A \,\&\, B \rightarrow D \Rightarrow G \rangle, \tag{10}$$

$$\langle \Gamma, A \rightarrow D, B \rightarrow D \Rightarrow G \rangle \ / \ \langle \Gamma, A \vee B \rightarrow D \Rightarrow G \rangle, \tag{11}$$

$$\langle \Gamma, A, B \rightarrow D \Rightarrow B \rangle \ / \ \langle \Gamma, (A \rightarrow B) \rightarrow D \Rightarrow A \rightarrow B \rangle. \tag{12}$$

Proof is obvious. ■

Now we are able to specify the decision procedure for sequents with one formula in succedent, and prove its properties. The heart of the procedure is a Boolean function S which decides about a given sequent whether it is intuitionistically tautological. The function S recursively calls itself in some cases. The decision procedure (main program) reads the input sequent $\langle \Sigma \Rightarrow H \rangle$ and simply calls the function S with a parameter $\langle \Sigma \Rightarrow H \rangle$. The function S denotes its parameter $\langle \Gamma \Rightarrow G \rangle$ and works as follows:

(a) If G is $E \,\&\, F$ then call S on $\langle \Gamma \Rightarrow E \rangle$ and then on $\langle \Gamma \Rightarrow F \rangle$. Return true if both calls return true, return false otherwise.

If G is $E \rightarrow F$ then use the rule (5), i.e. call S on $\langle \Gamma, E \Rightarrow F \rangle$ and return whatever it returns.

If Γ contains a formula of the form $E \,\&\, F$, $E \vee F$, $A \,\&\, B \rightarrow D$, or $A \vee B \rightarrow D$, then proceed analogically, i.e. use the rule (3), (4), (10), or (11), respectively.

(b) If Γ contains a pair p, $p \rightarrow D$ then: replace $p \rightarrow D$ by D (i.e. use the rule (6)), remove all formulas of the form $C_1 \rightarrow (\,.\,. \rightarrow (C_k \rightarrow D)\,.\,.)$ from Γ (i.e. use the rule (9) repeatedly), call S on the resulting sequent and return whatever it returns.

(c) If $\bot \in \Gamma$ or if G is an atom such that $G \in \Gamma$ then return true.

(d) If G is $E \vee F$ then call S on $\langle \Gamma \Rightarrow E \rangle$ and on $\langle \Gamma \Rightarrow F \rangle$. If some of the calls returns true then return true.

(e) Create a list $(A_1 \rightarrow B_1) \rightarrow D_1, .\,.\,, (A_m \rightarrow B_m) \rightarrow D_m$ of all implications in Γ with a compound premise. Denote Γ_i the set $\Gamma - \{(A_i \rightarrow B_i) \rightarrow D_i\}$ and denote Γ_i^- the set resulting from Γ_i by removing all implications of the form $C_1 \rightarrow (\,.\,. \rightarrow (C_k \rightarrow D_i)\,.\,.)$. For $i := 1$ to m call S on $\langle \Gamma_i, A_i, B_i \rightarrow D_i \Rightarrow B_i \rangle$ and on $\langle \Gamma_i^-, D_i \Rightarrow G \rangle$. If for some i both calls return true then return true. Otherwise return false.

If the function S reaches the instruction (e) then the sequent $\langle \Gamma \Rightarrow G \rangle$ is irreducible, and moreover, compound premises of implications in Γ must again be implications. If the number of such implications is zero then the function S returns false. Further explanation about the instruction (e) is in the final part of proof of Theorem 5.

Theorem 5 *The procedure specified above works in polynomial space and correctly decides whether a given sequent is intuitionistically tautological.*

Proof The computation of a function like S, calling recursively itself in some cases, can be viewed as a tree $\mathcal{T}$ with vertices labeled by parameters of the calls. If S has to process a sequent $\langle \Gamma \Rightarrow G \rangle$, and when doing so it recursively calls itself with parameters $\langle \Gamma_1 \Rightarrow G_1 \rangle$ to $\langle \Gamma_m \Rightarrow G_m \rangle$, then the tree $\mathcal{T}$ contains a vertex labeled by $\langle \Gamma \Rightarrow G \rangle$, with m immediate successors labeled by $\langle \Gamma_1 \Rightarrow G_1 \rangle$ to $\langle \Gamma_m \Rightarrow G_m \rangle$. The root of $\mathcal{T}$ is labeled by the input sequent $\langle \Sigma \Rightarrow H \rangle$. We have to show that each path in $\mathcal{T}$ terminates, i.e. ends with a vertex labeled by a sequent processed without recursive calls.

We associate *weights* with connectives and sequents. As in [4], the weight of conjunction & is 2 while the weight of $\vee$ and $\rightarrow$ is 1. The weight of an atom is also 1. A weight of a sequent depends on the way how the sequent appeared in the data of the function S. To define it we think of some occurrences of implications as *highlighted*. It will be clear from what is said below that a highlighted implication never occurs in the scope of a conjunction or a disjunction or in the “left scope” of an implication. It also never occurs in a succedent of a sequent. Highlighted implications and the notion of suffix defined below are meant to trace how a formula occurred in an antecedent of a sequent.

Initially no implication is highlighted. If the function S uses the rule (10), replacing some formula $A \& B \rightarrow D \in \Gamma$ by $A \rightarrow (B \rightarrow D)$, then if the formula $A \rightarrow (B \rightarrow D)$ is *new*, i.e. not an element of Γ, all implications inside or (immediately) before the subformula D are *preserved*, i.e. highlighted or not according to whether they were highlighted in the original formula $A \& B \rightarrow D$. The new implication, which is the main connective in $A \rightarrow (B \rightarrow D)$, is *not* highlighted. If S uses the rule (11) and replaces a formula $A \vee B \rightarrow D$ by two formulas $A \rightarrow D$ and $B \rightarrow D$, then for each of these two formulas, if the formula is new, all implications inside the subformula D are preserved, and the main implication, before the formula D, *becomes* highlighted. When S applies instruction (e) it chooses a formula $(A \rightarrow B) \rightarrow D$ in Γ and replaces it by the pair A, $B \rightarrow D$ in one embedded call and by the formula D in the associated embedded call. In the first case, if $B \rightarrow D$ is new then implications inside and immediately before the subformula D are preserved. In the second case, if D is new then implications inside it are preserved. In the remaining cases nothing happens with highlighted implications: in instructions (b) and (e) some implications, highlighted or not, merely disappear, and if S uses any of the rules (2)–(5) or (7), in instructions (a) or (d), then it processes a formula containing no highlighted implications.

$$\cfrac{\cfrac{\cfrac{\cfrac{\langle \Gamma, \overset{1}{t} \overset{2}{\underset{\cdot}{\to}} (\overset{3}{w} \overset{4}{\to} \overset{5}{r}), \overset{6}{q} \underset{\cdot}{\to} (w \to r), \overset{7}{u} \overset{8}{\underset{\cdot}{\to}} (\overset{9}{w} \overset{10}{\underset{\cdot}{\to}} \overset{11}{r}), \overset{12}{v} \underset{\cdot}{\to} (w \underset{\cdot}{\to} r), \overset{13}{s} \underset{\cdot}{\to} r \Rightarrow G \rangle}{\langle \Gamma, t \vee q \to (w \to r), u \underset{\cdot}{\to} (w \underset{\cdot}{\to} r), v \underset{\cdot}{\to} (w \underset{\cdot}{\to} r), s \underset{\cdot}{\to} r \Rightarrow G \rangle}}{\langle \Gamma, t \vee q \to (w \to r), (u \vee v) \to (w \underset{\cdot}{\to} r), s \underset{\cdot}{\to} r \Rightarrow G \rangle}}{\langle \Gamma, t \vee q \to (w \to r), (u \vee v) \,\&\, w \underset{\cdot}{\to} r, s \underset{\cdot}{\to} r \Rightarrow G \rangle}}{\langle \Gamma, t \vee q \to (w \to r), ((u \vee v) \,\&\, w) \vee s \to r \Rightarrow G \rangle}$$

Figure 2: Weights and highlighted implications

In any stage of the computation, each formula $E \in \Gamma$ can be written in the form $C_1 \to (\,.\,.\, \to (C_k \to D)\,.\,.)$ where none of the formulas C_i and D contain highlighted implications. The number k can be zero and D can still be an implication. The part $\to (C_i \to (\,.\,.\, \to (C_k \to D)\,.\,.)$ of the formula E, together with an information which implications are highlighted in it, is a *suffix* of E provided its leftmost symbol is a highlighted implication. So the number of different suffixes of E equals the number of highlighted implications in E. *Weight of a sequent* $\langle \Gamma \Rightarrow G \rangle$ is defined as the sum of weights of all occurrences of connectives and atoms in $\Gamma \cup \{G\}$, with the following exception. If a formula $E \in \Gamma$ has a suffix $\to D$ then the symbols in this suffix count only once for each formula in Γ that also has $\to D$ as a suffix.

An example of how the weights are determined is given in Fig. 2. The five sequents can be viewed as both a fragment of a proof or local data of the function S, where higher sequents correspond to deeper recursive calls. Highlighted implications are marked with dots. In the formulas shown in the topmost sequent we have a suffix $\underset{\cdot}{\to} (w \to r)$ which occurs twice, then a suffix $\underset{\cdot}{\to} (w \underset{\cdot}{\to} r)$ which also occurs twice, and a suffix $\underset{\cdot}{\to} r$ which occurs three times. Numbers above symbols show how the weight is computed. If Γ contains no highlighted implications then the weight of the topmost sequent is 13 plus the number of symbols in $\Gamma \cup \{G\}$ plus the number of conjunctions in $\Gamma \cup \{G\}$.

Let the input sequent $\langle \Sigma \Rightarrow H \rangle$ have n symbols. Then its weight can be bounded by $2n$. We would like to claim that whenever S calls itself while processing a sequent $\langle \Gamma \Rightarrow G \rangle$, the weight of the parameter(s) of the embedded call is lower than the weight of the current parameter $\langle \Gamma \Rightarrow G \rangle$. In most cases it is true. For example, if S uses the rule (11), replacing a formula $A \vee B \to D$ by two formulas $A \to D$ and $B \to D$, then the connectives inside D and the implication next to D do not count twice, and the profit is the removal of one disjunction. If S uses the rule (6), replacing a formula $p \to D$ by D, then it is quite possible that only the atom p in $p \to D$ counts, while in the embedded call more symbols in D count. This happens if the outermost implication is highlighted, i.e. if the formula $p \to D$ has a suffix $\to D$, and there are more formulas in Γ with the same suffix. Note however that when the function S applies instruction (b) it simultaneously removes all other formulas having the same suffix $\to D$. So the minimal possible profit of replacing the formula $p \to D$

by D and removing all formulas of the form $C_1 \to (\,.\,.\to (C_k \to D)\,.\,.)$ is a decrease in weight by 1, the weight of the atom p. The same phenomenon occurs in instruction (e), when $(A \to B) \to D$ is replaced by D. The only exception when the weight may not decrease is that call in instruction (e) where the function S replaces a sequent $\langle\, \Pi, (A \to B) \to D \;\Rightarrow\; G \,\rangle$ by $\langle\, \Pi, A, B \to D \;\Rightarrow\; B \,\rangle$: the formula B appears twice in the embedded call and it can be of higher weight than the removed formula G. However, this happens at most once for each (occurrence of a) subformula B of the original sequent $\langle\, \Sigma \;\Rightarrow\; H \,\rangle$. Thus we can claim that whenever the function S recursively calls itself, the weight of the parameter of the embedded call is lower, except that at most n times the weight is increased by at most $2n$. This means that each path in the tree $\mathcal{T}$ of embedded calls has length at most quadratic in the length of the input sequent $\langle\, \Sigma \;\Rightarrow\; H \,\rangle$, and our decision procedure terminates on any input $\langle\, \Sigma \;\Rightarrow\; H \,\rangle$. It is known ([3], [8], ...) that the space requirements of a function like S, calling recursively itself, is determined by the sum of sizes of local data of instances of S along any path in the tree of recursive calls. When S is called with parameter $\langle\, \Gamma \;\Rightarrow\; G \,\rangle$ its local data is essentially the sequent $\langle\, \Gamma \;\Rightarrow\; G \,\rangle$ itself, and one can check that its size is also quadratic in n. So our procedure works in polynomial space.

Let's say that a vertex in the tree $\mathcal{T}$ labeled by $\langle\, \Gamma \;\Rightarrow\; G \,\rangle$ is *positive* or *negative* according to whether S returns true or false when processing it. Let the *depth* of a vertex v be the length of the longest path starting at v, where the length of a one-element path is zero. Consider the following claim. *Let the depth of a vertex $v \in \mathcal{T}$ labeled by $\langle\, \Gamma \;\Rightarrow\; G \,\rangle$ be k. Then v is positive if and only if $\langle\, \Gamma \;\Rightarrow\; G \,\rangle$ is intuitionistically tautological.* This claim is proved by induction on k. Let, for example, v be a vertex of depth k labeled by a sequent $\langle\, \Gamma \;\Rightarrow\; G \,\rangle$ which is intuitionistically tautological and such that none of instructions (a)–(c) in S is applicable. Assume that G is not a disjunction. Then G must be $\perp$ or an atom p such that $p \notin \Gamma$, and Γ contains, besides the implications $(A_1 \to B_1) \to D_1, .\,., (A_m \to B_m) \to D_m$ created in instruction (e), only some atoms and some implications $p \to D$ where $p \notin \Gamma$. Theorem 3 says that for some i both sequents $\langle\, \Gamma_i, (A_i \to B_i) \to D_i \;\Rightarrow\; A_i \to B_i \,\rangle$ and $\langle\, \Gamma_i, D_i \;\Rightarrow\; G \,\rangle$ are intuitionistically tautological. It follows from invertibility of rules (12) and (9) that both sequents $\langle\, \Gamma_i, A_i, B_i \to D_i \;\Rightarrow\; B_i \,\rangle$ and $\langle\, \Gamma_i^-, D_i \;\Rightarrow\; G \,\rangle$, which act as parameters of the embedded calls, are intuitionistically tautological. The immediate successors of v labeled by these two sequents have depth lower than k. So, by the induction hypothesis, S returns true when called on them. Hence the result of the computation in instruction (e) is true, i.e. v is positive. We leave the remaining cases to the reader. ∎

A corollary of our considerations is that the single-conclusion calculus with initial sequents (1) and rules (2)–(7) and (9)–(12), or (2)–(9), is sound and complete with respect to Kripke semantics of intuitionistic logic. Note that as to termination of the decision procedure the paper [4] refers the reader to [3] which gives a general and widely applicable method for proving termination but says nothing about polynomial-space. Note also that J. Hudelmaier [5] constructs a calculus and a decision procedure much more efficient than ours: it works in space $O(n \log n)$.

4 A multi-conclusion decision procedure

The left implication rule (8) from the previous section is inherently non-invertible because if it is used in reverse and the formula B replaces the formula G, the formula G disappears without a refund. The multi-conclusion calculus, allowing any number of formulas in succedent, is more convenient in this respect because the usual multi-conclusion left implication rule

$$\langle \Gamma \Rightarrow \Delta, A \rangle, \langle \Gamma, B \Rightarrow \Delta \rangle \ / \ \langle \Gamma, A \to B \Rightarrow \Delta \rangle, \tag{$*$}$$

while still non-invertible, can be replaced by the following "non-extending" variant

$$\langle \Gamma, A \to B \Rightarrow \Delta, A \rangle, \langle \Gamma, A \to B, B \Rightarrow \Delta \rangle \ / \ \langle \Gamma, A \to B \Rightarrow \Delta \rangle \tag{20}$$

which is invertible. Note that (20) can be simulated by $(*)$ by taking $\Gamma \cup \{A \to B\}$ for the set Γ in $(*)$. The rule (20) is a restricted variant of $(*)$: while the rule $(*)$ allows the principal formula $A \to B$ to simultaneously be a side formula, the rule (20) requires it. To simplify (thinking about) the decision procedure specified below, we formulate also the rules for conjunction and disjunction as non-extending. So our multi-conclusion calculus has initial sequents

$$\langle \Gamma, p \Rightarrow \Delta, p \rangle, \qquad \langle \Gamma, \bot \Rightarrow \Delta \rangle, \tag{13}$$

and the following rules:

$$\langle \Gamma \Rightarrow \Delta, A \,\&\, B, A \rangle, \langle \Gamma \Rightarrow \Delta, A \,\&\, B, B \rangle \ / \ \langle \Gamma \Rightarrow \Delta, A \,\&\, B \rangle \tag{14}$$
$$\langle \Gamma \Rightarrow \Delta, A \vee B, A, B \rangle \ / \ \langle \Gamma \Rightarrow \Delta, A \vee B \rangle \tag{15}$$
$$\langle \Gamma, A \Rightarrow B \rangle \ / \ \langle \Gamma \Rightarrow \Delta, A \to B \rangle \tag{16}$$
$$\langle \Gamma \Rightarrow \Delta, A \to B, B \rangle \ / \ \langle \Gamma \Rightarrow \Delta, A \to B \rangle \tag{17}$$
$$\langle \Gamma, A \,\&\, B, A, B \Rightarrow \Delta \rangle \ / \ \langle \Gamma, A \,\&\, B \Rightarrow \Delta \rangle \tag{18}$$
$$\langle \Gamma, A \vee B, A \Rightarrow \Delta \rangle, \langle \Gamma, A \vee B, B \Rightarrow \Delta \rangle \ / \ \langle \Gamma, A \vee B \Rightarrow \Delta \rangle \tag{19}$$
$$\langle \Gamma, A \to B \Rightarrow \Delta, A \rangle, \langle \Gamma, A \to B, B \Rightarrow \Delta \rangle \ / \ \langle \Gamma, A \to B \Rightarrow \Delta \rangle. \tag{20}$$

Note that the calculus is very similar to calculi defined e.g. in [6] and [11]. The main difference is the additional rule (17) which can be called *weak implication rule*. It can easily be checked that all rules (14)–(20) are sound with respect to Kripke semantics, and that all rules except (16) are invertible. The right implication rule (16) is now the only rule which is inherently non-invertible. Note also that the rule (16) is the only rule which can bring new formulas: any formula not introduced as a member of the set Δ in (16) must come from initial sequents.

The rule (16) is applicable only to a sequent with exactly one formula in succedent. Without this restriction, the rule would not be sound.

Let us think about a decision procedure based on our multi-conclusion calculus. As in the previous section, the procedure reads the input sequent $\langle \Sigma \Rightarrow \Omega \rangle$ and calls a Boolean function, now named M, on it. The function M denotes its parameter $\langle \Gamma \Rightarrow \Delta \rangle$, and in some cases recursively calls itself. It works as follows:

(a) If Δ contains a formula $A \,\&\, B$ such that $A \notin \Delta$ and $B \notin \Delta$ then call M on $\langle \Gamma \Rightarrow \Delta, A \rangle$ and on $\langle \Gamma \Rightarrow \Delta, B \rangle$. Return true if both calls return true, return false if some returns false.

Otherwise, use one of the rules (15) and (17)–(20) accordingly, but only if profitable, i.e. if the embedded call or both embedded calls has or have parameter(s) different from $\langle \Gamma \Rightarrow \Delta \rangle$.

(b) If instruction (a) is not applicable then return true if $\bot \in \Gamma$ or if Γ and Δ have an atom in common.

If instruction (a) is not applicable, i.e. if none of the rules (14), (15), (17)–(20) can be profitably used, then the sequent $\langle \Gamma \Rightarrow \Delta \rangle$ is *saturated* in the following sense.

Definition 6 *A sequent $\langle \Gamma \Rightarrow \Delta \rangle$ is* saturated *if the following conditions are satisfied:*

- *if $A \,\&\, B \in \Gamma$ (or $A \vee B \in \Delta$) then both formulas A and B are in Γ (or in Δ, respectively),*
- *if $A \vee B \in \Gamma$ (or $A \,\&\, B \in \Delta$) then at least one of the formulas A and B is in Γ (or in Δ, respectively),*
- *if $A \rightarrow B \in \Gamma$ then $A \in \Delta$ or $B \in \Gamma$,*
- *if $A \rightarrow B \in \Delta$ then $B \in \Delta$.*

Theorem 7 *A saturated sequent $\langle \Gamma \Rightarrow \Delta \rangle$ is intuitionistically tautological if and only if it is initial or if there is a formula $A \rightarrow B \in \Delta$ such that $A \notin \Gamma$ and the sequent $\langle \Gamma, A \Rightarrow B \rangle$ is intuitionistically tautological.*

Proof Again the nontrivial implication is $\Rightarrow$. So let $\langle \Gamma \Rightarrow \Delta \rangle$ be saturated, intuitionistically tautological and not initial. Let $A_1 \rightarrow B_1, .., A_m \rightarrow B_m$ be a list of all implications $A \rightarrow B \in \Delta$ such that $A \notin \Gamma$. Assume that none of the sequents $\langle \Gamma, A_i \Rightarrow B_i \rangle$ is intuitionistically tautological. Let $K_1, .., K_m$ be counter-models for $\langle \Gamma, A_i \Rightarrow B_i \rangle$. Assume that $a_1, .., a_m$ are roots of $K_1, .., K_m$. Let K be the model constructed from $K_1, .., K_m$ as in the proof of Theorem 3, i.e. by stipulating that $a_1, .., a_m$ are the only immediate successors of a new root a. Again, we evaluate all atoms in Γ positively and all the remaining atoms negatively in a. Now the following claim can be proved by induction on complexity of a formula D: *if* $D \in \Gamma$ *then* $a \Vdash D$*, and if* $D \in \Delta$ *then* $a \nVdash D$. If D is an atom in Γ then $a \Vdash D$ by definition. If D is an atom in Δ then, since the sequent $\langle \Gamma \Rightarrow \Delta \rangle$ is not initial, we have $D \notin \Gamma$ and thus $a \nVdash D$. So the claim is true if D is an atom. It is evidently true also if D is $\perp$. If D is $A \,\&\, B$ and $D \in \Delta$ then, by the definition of saturated sequent, $A \in \Delta$ or $B \in \Delta$. The induction hypothesis says $a \nVdash A$ or $a \nVdash B$. So indeed $a \nVdash A \,\&\, B$. The remaining cases when D is a conjunction or a disjunction in Γ or in Δ are similar. So let D be $A \to B$. First assume that $D \in \Gamma$. We have to verify that $x \Vdash B$ whenever $a \leq x$ and $x \Vdash A$. If x is an element of some submodel K_i of K then there is nothing to do since $a_i \Vdash D$. If $x = a$ then, because $\langle \Gamma \Rightarrow \Delta \rangle$ is saturated, we have $A \in \Delta$ or $B \in \Gamma$, so $x \nVdash A$ or $x \Vdash B$. Finally assume that $D \in \Delta$. If D is some of the formulas $A_1 \to B_1, \ldots, A_m \to B_m$, say $A_i \to B_i$, then for $x = a_i$ we have $x \Vdash A$ and $x \nVdash B$. If D is different from all $A_1 \to B_1, \ldots, A_m \to B_m$ then $A \in \Gamma$. The fact that $\langle \Gamma \Rightarrow \Delta \rangle$ is saturated yields $B \in \Delta$. Note that this is the place where the weak implication rule (17) is helpful. By the induction hypothesis, for $x = a$ we have $x \Vdash A$ and $x \nVdash B$. So in all cases when $A \to B \in \Delta$ there is an x accessible from a such that $x \Vdash A$ and $x \nVdash B$. So $a \nVdash A \to B$. ■

Having Theorem 7 we can complete our decision procedure for multi-conclusion calculus:

> (c) If none of (a), (b) is applicable then create a list $A_1 \to B_1, \ldots, A_m \to B_m$ of all implications in Δ whose premise is not in Γ. Call M on $\langle \Gamma, A_1 \Rightarrow B_1 \rangle$ to $\langle \Gamma, A_m \Rightarrow B_m \rangle$. Return true if some of the calls returns true, return false otherwise.

In the formulation of the following Theorem 8 we need the notion of *positive* and *negative* occurrences of formulas in a sequent $\langle \Gamma \Rightarrow \Delta \rangle$. All members of Γ are positive, all members of Δ are negative. If a formula $A \,\&\, B$ or $A \vee B$ is positive (negative) then both subformulas A and B are positive (or negative, respectively). If a formula $A \to B$ is positive then the subformula A is negative and the subformula B is positive. If a formula $A \to B$ is negative then the subformula A is positive and the subformula B is negative. For example, in the sequent $\langle \neg\neg p \to p \Rightarrow p \vee \neg p \rangle$, the formula $\neg p$ (i.e. $p \to \perp$) occurs twice: positively as a part of the implication $\neg\neg p$, and negatively as a part of the disjunction $p \vee \neg p$.

Theorem 8 *The procedure specified above works in polynomial space and correctly decides whether a given sequent* $\langle \Sigma \Rightarrow \Omega \rangle$ *is intuitionistically tautological. If the sequent* $\langle \Sigma \Rightarrow \Omega \rangle$ *contains* n *logical connectives and* r *negative implications then it either has a proof of depth* $O(n^2)$ *in the calculus with initial sequents* (13) *and rules* (14)–(20)*, or it has a Kripke counter-model of depth at most* r*, in which every node has at most* r *immediate successors.*

Proof Let $\mathcal{T}$ be the tree of all calls of the function M, which occur when the procedure processes a sequent $\langle \Sigma \Rightarrow \Omega \rangle$ with n logical connectives and r negative implications $E_1 \to F_1, .., E_r \to F_r$, where obviously $r \le n$. Each vertex v of T is labeled by a sequent $\langle \Gamma \Rightarrow \Delta \rangle$, the parameter of the call of M corresponding to the vertex v. If M uses instruction 1 then v has one or two immediate successors according to whether M uses (in reverse) a unary or a binary rule. If M uses instruction 2 then v has no successors, i.e. is a leaf in T. In both cases M returns true if and only if *all* of the embedded calls return true. If M uses instruction 3 then the sequent $\langle \Gamma \Rightarrow \Delta \rangle$ is saturated and non-initial and has m immediate successors where m is the number of implications $A \to B$ in Δ such that $A \notin \Gamma$. The number m can be zero in which case the vertex v is a leaf.

A step made from a vertex v labeled by a saturated sequent to one of the immediate successors of v corresponds to the situation where M processes an implication $A \to B \in \Delta$ by calling itself on $\langle \Gamma, A \Rightarrow B \rangle$. Note that in this case the implication $A \to B$ must be a member of the set $\{ E_i \to F_i \,;\, 1 \le i \le r \}$ of all negative implications. Also note that the same implication is never processed again on a path in $\mathcal{T}$. From this it follow that each path in $\mathcal{T}$ contains at most $r+1$ saturated sequents. The distance from one saturated sequent to another saturated sequent on a path is bounded by $2n + 1$, the number of all subformulas of a sequent with n logical connectives. This is because each use of an invertible rule adds at least one new formula to $\Gamma \cup \Delta$. Thus each path in $\mathcal{T}$ terminates and has length $O(n^2)$. The size of local data of any instance of M is quadratic in n. So the procedure works in polynomial space.

As in Theorem 5, let's say that a vertex in $\mathcal{T}$ labeled by $\langle \Gamma \Rightarrow \Delta \rangle$ is *positive* or *negative* according to whether M returns true or false when processing it. Consider the following claim. *Let a vertex v of $\mathcal{T}$ labeled by $\langle \Gamma \Rightarrow \Delta \rangle$ be such that the depth of the subtree of $\mathcal{T}$ generated by v is k and such that on any path from v to some leaf there are at most $m + 1$ saturated sequents. Then if v is positive it has a proof of depth at most k, and if v is negative it has a counter-model of depth at most m in which every node has at most r immediate successors.* This claim is proved by an induction on k. Indeed, if $k = 0$ then either M applies instruction (b), in which case v is positive and the sequent $\langle \Gamma \Rightarrow \Delta \rangle$ is initial, i.e. having a proof of depth 0, or M applies instruction (c) with no embedded calls, in which case v is negative and $\langle \Gamma \Rightarrow \Delta \rangle$ has a one-element, i.e. of depth 0, Kripke counter-model. The induction step and the remaining considerations are left to the reader. ∎

To know that intuitionistic propositional logic is decidable in polynomial space is interesting in connection with the fact that it is polynomial-space hard. That is proved in [9]; a relatively easy semantical proof can also be found in my [10]. Let me remark that the precise role of the additional implication rule (17) is not quite clear. It is redundant in the sense that it can be simulated by cuts and the calculus without this rule allows cut-elimination. However, I do not know whether the calculus with rules (14)–(16) and (18)–(20) directly (polynomially) simulates the calculus with all rules (14)–(20). Our treatment of multi-conclusion calculus, where the decision procedure never removes a formula from a sequent, can be viewed as showing that avoiding contraction is not the only way how to ensure termination.

References

[1] S. R. Buss and P. Pudlák. On the computational content of intuitionistic propositional proofs. *Ann. Pure Appl. Logic*, 109:49–64, 2001.

[2] D. van Dalen. Intuitionistic logic. In D. M. Gabbay and F. Guenthner, editors, *Handbook of Philosophical Logic*, number 164–167 in Synthese Library, chapter III.4, pages 225–340. Kluwer, Dordrecht, 1986.

[3] N. Dershowitz and Z. Manna. Proving termination with multiset orderings. *Communications of the ACM*, 22:465–476, 1979.

[4] R. Dyckhoff. Contraction-free sequent calculi for intuitionistic logic. *J. Symb. Logic*, 57:795–807, 1992.

[5] J. Hudelmaier. An $O(n \log n)$-space decision procedure for intuitionistic propositional logic. *J. Logic Computation*, 3(1):63–75, 1993.

[6] S. C. Kleene. *Introduction to Metamathematics*. D. van Nostrand, 1952.

[7] R. Ladner. The computational complexity of provability in systems of modal logic. *SIAM J. Comput.*, 6(3):467–480, 1977.

[8] C. H. Papadimitriou. *Computational Complexity*. Addison-Wesley, 1994.

[9] R. Statman. Intuitionistic propositional logic is polynomial-space complete. *Theoretical Comp. Sci.*, 9:67–72, 1979.

[10] V. Švejdar. On the polynomial-space completeness of intuitionistic propositional logic. *Archive Math. Logic*, 42(7):711–716, 2003.

[11] G. Takeuti. *Proof Theory*. North-Holland, Amsterdam, 1975.

[12] A. S. Troelstra and H. Schwichtenberg. *Basic Proof Theory*. Cambridge University Press, 1996.