A Connection Based Proof Method for Intuitionistic Logic

Jens Otten Christoph Kreitz

Fachgebiet Intellektik, Fachbereich Informatik
Technische Hochschule Darmstadt
Alexanderstr. 10, 64283 Darmstadt, Germany
{jeotten,kreitz}@intellektik.informatik.th-darmstadt.de

Abstract. We present a proof method for intuitionistic logic based on Wallen's matrix characterization. Our approach combines the connection calculus and the sequent calculus. The search technique is based on notions of paths and connections and thus avoids redundancies in the search space. During the proof search the computed first-order and intuitionistic substitutions are used to simultaneously construct a sequent proof which is more human oriented than the matrix proof. This allows to use our method within interactive proof environments. Furthermore we can consider *local* substitutions instead of global ones and treat substitutions occurring in different branches of the sequent proof independently. This reduces the number of extra copies of formulae to be considered.

1 Introduction

Intuitionistic logic ($\mathcal{J}$), due to its constructive nature, is often viewed as the logic of computation. It has an essential significance for the derivation of verifiably correct programs since theorems proven within $\mathcal{J}$ can be considered as specifications of algorithms which are implicitly contained in the proof. Every formula valid in intuitionistic logic is valid in classical logic as well. The intuitionistic *proof*, however, contains more information than a classical one and many of the well known classical normal forms and equivalences are not valid intuitionistically. As a consequence, it is considerably more difficult to prove a theorem in $\mathcal{J}$ than finding a classical proof. Reasoning in classical logic can be automated sufficiently well (see e.g. [5, 12, 19, 2]) but there is not yet an efficient intuitionistic proof procedure.

Gödel has shown that $\mathcal{J}$ can be embedded into the modal logic $S4$ [10]: there is a mapping $\mathcal{M}$ from $\mathcal{J}$ into $S4$ such that a formula F is valid in $\mathcal{J}$ if $\mathcal{M}(F)$ is valid in $S4$. In his investigations on non-classical logics Wallen has used this embedding to develop a matrix characterization for the validity of intuitionistic formulae [18] which extends Bibel's characterization for classical validity [3, 4].

In propositional classical logic a formula F is valid if there is a spanning set of connections for F. A *connection* is a pair of atomic formulae with different *polarities*. A set of connections *spans* a formula F if every path through a matrix representation of F contains at least one connection. This characterization also applies to predicate logic if all the terms contained in connected formulae can be made identical by some global (*first-order*) (quantifier-) substitution σ.

In *sequent calculi* (like Gentzen's $\mathcal{LK}$ and $\mathcal{LJ}$ [9] or Fitting's calculi [7]) the difference between classical and intuitionistic reasoning is expressed by certain restrictions on the intuitionistic rules. If rules are inverted for the purpose of proof search then these restrictions cause formulae to be deleted from a sequent. Applying a rule (i.e. *reducing* a sub-formula) too early may thus delete a formula which later will be necessary to complete the proof. Therefore the order of rule applications must be arranged appropriately. In Wallen's matrix characterization this requirement is expressed by an *intuitionistic* substitution which makes the *prefixes* of connected sub-formulae identical where a prefix essentially describes the position of a sub-formula in the tree representation of the formula to be proved.

Both the first-order and the intuitionistic substitution have to be computed by unification algorithms. For the latter a specialized *string unification* is required. Together with the ordering of the formula tree these substitutions determine the ordering in which a given formula F has to be reduced by the rules of the sequent calculus. This ordering must be acyclic since otherwise no proof for F can be given. During the proof process it may become necessary to create multiple instances of the same sub-formula. The number of copies generated to complete the proof is called *multiplicity*. Again, a multiplicity may be due to a quantifier or specific to intuitionistic reasoning.

Developing an automated procedure which constructs intuitionistic proofs on the basis of Wallen's matrix characterization means extending Bibel's connection method [4] accordingly. The advantage of such a method is that the emphasis on connections drastically reduces the search space compared to calculi analyzing the outer structure of formulae such as the sequent calculus [9, 7] or tableaux calculi [1, 16]. Furthermore it avoids the notational redundancy contained in these calculi by a very compact representation.

The connection method is efficient for *finding* proofs according to the matrix characterization of validity. Its result, however, is almost impossible to read. Therefore attempts have been made to convert matrix proofs back into sequent proofs which are much closer to 'natural' mathematical reasoning. This is comparably easy for classical propositional logic but becomes rather difficult for predicate logic [11] or intuitionistic logic [15]. In these cases the reduction ordering induced by the substitutions has to be taken into account.

Although originally we were interested only in finding a matrix proof for a given formula the above considerations led to the development of a proof search method which constructs the matrix proof and a sequent proof almost simultaneously. The partial sequent proof, however, is more than a byproduct since it can also be used to support the proof search. It allows, for instance, to consider *local* substitutions instead of global ones, i.e. substitutions which can be applied independently within sub-proofs of a sequent proof. Such a local view reduces the number of copies of sub-formulae which have to be generated to find a (global) substitution and keeps the search space and the size of the proof smaller. Therefore we have developed a hybrid method which combines the connection method and the sequent calculus.

After resuming the sequent calculus, the matrix characterization, and a version of the connection method operating on non-normal forms in section 2 we shall describe the relation between the sequent calculus and the connection method in section 3. Section 4 will present our proof method and in section 5 we shall discuss local substitutions and a modified matrix characterization. We conclude with a few remarks on implementation issues and future investigations.

2 Preliminaries

2.1 Formula Trees, Types and Polarities

We assume the reader to be familiar with the language for first-order logic. A *formula tree* is a representation of a formula as tree whose nodes are marked by *positions* denoted by $a_0, a_1, \ldots$. Each position corresponds to a *label* consisting of the major connective or quantifier of a sub-formula or of the sub-formula itself if it is atomic. *Atomic positions* are nodes labeled with atomic formulae and are leafs of the tree. A formula tree for $\forall x Px \Rightarrow Pa \wedge Pb$ is shown in figure 1. The *tree-ordering* $<$ is the (partial) ordering given by the formula tree: $a_i < a_j$ if the position a_i is below a_j in the formula tree.

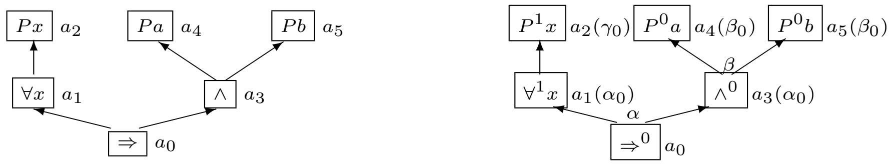


Fig. 1. Formula tree without/with labels for principal/secondary types and polarities

Each sub-formula of a given formula F uniquely corresponds to a position in the formula tree. A position is associated with a polarity, a principal type, and a secondary type. The *polarity* (0 or 1) of a position is determined by the label and polarity of its parent. The root position has polarity 0. The *principal type* of a position is determined by its polarity and its label. Atomic positions have no principal type. The *secondary type* of a position is determined by the principal type of its parents. The root position has no secondary type. Polarity, principal type, and secondary type of a position are defined in table 1 whose first entry, for instance, means that a position labeled with $\wedge$ and polarity 1 has principal type α and its successor nodes have polarity 1 and secondary type α_0.

principal type α	*secondary type* α_0		*principal type* β	*secondary type* β_0	
$(A \wedge B)^1$	A^1	B^1	$(A \wedge B)^0$	A^0	B^0
$(A \vee B)^0$	A^0	B^0	$(A \vee B)^1$	A^1	B^1
$(A \Rightarrow B)^0$	A^1	B^0	$(A \Rightarrow B)^1$	A^0	B^1
$(\neg A)^1$	A^0				
$(\neg A)^0$	A^1				
principal type γ	*secondary type* γ_0		*principal type* δ	*secondary type* δ_0	
$(\forall x A)^1$	A^1		$(\forall x A)^0$	A^0	
$(\exists x A)^0$	A^0		$(\exists x A)^1$	A^1	

Table 1. Polarity, principal type, and secondary type of positions

A formula tree for $\forall x Px \Rightarrow Pa \wedge Pb$ where the nodes additionally are labeled with their types and polarity is also given in figure 1. For a given formula we shall use $\alpha, \alpha_0, \beta, \beta_0$, $\varGamma, \varGamma_0, \varDelta$, and $\varDelta_0$ to denote the sets of positions of type α, α_0, β, β_0, γ, γ_0, δ, and δ_0 respectively.

2.2 The Sequent Calculus

A *sequent* has the form $\Gamma \vdash \Delta$ where Γ (the *antecedent*) and Δ (the *succedent*) are sets of formulae. A *proof* of the sequent $\Gamma \vdash \Delta$ is a tree rooted with $\Gamma \vdash \Delta$ whose nodes are determined by rules and whose leafs are axioms. A formula F is *valid* iff there is a proof of the sequent $\vdash F$. Table 2 shows the axioms and logical rules of the intuitionistic sequent calculus.

$$\Gamma, A \vdash A, \Delta \quad \textit{axiom}$$

$\dfrac{\Gamma, A \vdash \Delta \qquad \Gamma, B \vdash \Delta}{\Gamma, A \lor B \vdash \Delta}\ \lor left$	$\dfrac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \lor B, \Delta}\ \lor right$
$\dfrac{\Gamma, A, B \vdash \Delta}{\Gamma, A \land B \vdash \Delta}\ \land left$	$\dfrac{\Gamma \vdash A, \Delta \qquad \Gamma \vdash B, \Delta}{\Gamma \vdash A \land B, \Delta}\ \land right$
$\dfrac{\Gamma, \neg A \vdash A, \Delta}{\Gamma, \neg A \vdash \Delta}\ \neg left$	$\dfrac{\Gamma, A \vdash}{\Gamma \vdash \neg A, \Delta}\ \neg right$
$\dfrac{\Gamma, A \Rightarrow B \vdash A, \Delta \qquad \Gamma, B \vdash \Delta}{\Gamma, A \Rightarrow B \vdash \Delta}\ \Rightarrow left$	$\dfrac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B, \Delta}\ \Rightarrow right$
$\dfrac{\Gamma, \forall x A, A[x\backslash t] \vdash \Delta}{\Gamma, \forall x A \vdash \Delta}\ \forall left$	$\dfrac{\Gamma \vdash A[x\backslash a]}{\Gamma \vdash \forall x A, \Delta}\ \forall right^*$
$\dfrac{\Gamma, A[x\backslash a] \vdash \Delta}{\Gamma, \exists x A \vdash \Delta}\ \exists left^*$	$\dfrac{\Gamma \vdash A[x\backslash t], \exists x A, \Delta}{\Gamma \vdash \exists x A, \Delta}\ \exists right$

Table 2. A cut-free sequent calculus for intuitionistic logic

The parameter a of the rules $\forall right^*$ and $\exists left^*$ must not occur free in the conclusion of the rule (i.e. not in Γ, A, or Δ). Similarly the term t in $\exists right$ and $\forall left$ must not contain variables which occur free in the conclusion. The calculus is complete and correct for intuitionistic logic [7]. It differs from the Gentzen's calculus $\mathcal{LJ}$ [9] in the sense that *sets* of formulae are used instead of sequences – which allows to omit structural rules like weakening and contraction – and that more than one formula may occur in the succedent of a sequent. It is, however, possible to convert proofs in the above calculus into $\mathcal{LJ}$-proofs (see e.g. [8]).

The sequent calculus for intuitionistic logic differs from the classical one only in the rules $\Rightarrow right$,$\neg right$ and $\forall right$. Whereas in the intuitionistic case the succedent of the conclusion consists of at most one formula, the corresponding classical rules may contain multiple formulae. We call these rules *special rules.* An application of an inverted rule (read from the conclusion to the premise) is called a *reduction.* Figure 2 presents a proof of the formula $\forall x Px \Rightarrow Pa \land Pb$.

$$\dfrac{\dfrac{Pa \vdash Pa}{\forall x Px \vdash Pa}\ \forall left \qquad \dfrac{Pb \vdash Pb}{\forall x Px \vdash Pb}\ \forall left}{\vdash \forall x Px \Rightarrow Pa \land Pb}\ \Rightarrow right$$

Fig. 2. Sequent proof for $\forall x Px \Rightarrow Pa \land Pb$

2.3 A Matrix Characterization for Intuitionistic Logic

The matrix characterization for intuitionistic logic developed by Wallen [17, 18] is based on the notion of paths and connections pioneered by Bibel for classical logic [3, 4]. We first resume the characterization for classical first-order logic.

Theorem 1. *A formula F is classically valid iff there is*

- *a multiplicity μ encoding the number of distinct instances of sub-formulae to be considered during the proof,*
- *an admissible first-order substitution σ_Q assigning a term to every variable in the formula,*
- *a set of connections which are complementary under σ_Q such that every path through the formula F contains a connection from this set.*

For technical reasons we replace the variables in atomic formulae by their quantifier positions. Thus positions of type γ and δ appear in atomic formulae instead of variables. Consequently a *first-order substitution* σ_Q is a mapping from the set $\varGamma$ of positions of type γ to terms where again variables are replaced by positions. The substitution[1] σ_Q induces a *relation* $\sqsubset_Q$ on $\varDelta \times \varGamma$ in the following way: if $\sigma_Q(u) = t$ then $v \sqsubset_Q u$ for all $v \in \varDelta$ that are sub-terms of t. A *connection* is a pair of atomic positions labeled with atomic formulae having the same predicate symbol but different polarities. If they are identical under σ_Q the connection is said to be *complementary* under σ_Q. A *path* through a formula F is a subset of the atomic positions of its formula tree; it is a horizontal path through the matrix representation of F (see example in figure 3 and 4).

Since the quantifier rules $\exists left$ and $\forall right$ are constrained by the eigenvariable condition the relation $v \sqsubset_Q u$ expresses that the sub-formula labeled by v should be reduced before reducing the one labeled by u. The transitive closure of the union of $\sqsubset_Q$ and the tree-ordering $<$ is called the *reduction ordering* $\lhd$, i.e. $\lhd := (< \cup \sqsubset_Q)^+$. A first-order substitution σ_Q is *admissible* if the reduction ordering $\lhd$ is irreflexive. In this case a proof in the sequent calculus is constructible. This technique was first proposed by Bibel [4] as an alternative for skolemization in classical logic.

The intuitionistic sequent calculus contains special rules which, if used analytically, cause formulae to be deleted from a sequent. To ensure that formulae containing two atomic formulae of a connection as sub-formulae are not deleted by special rules the corresponding atomic positions of this connection have to be made complementary under an additional *intuitionistic substitution*.

To explain the necessary modifications of the classical matrix characterization we extend the definitions of types and positions. A *special position* in a formula tree is a position labeled with an atomic formula, negation ($\neg$), implication ($\Rightarrow$), or a universal quantifier ($\forall x$). If a special position has polarity 1 it has *intuitionistic type* ϕ and otherwise type ψ. To denote the set of positions of intuitionistic type ϕ and ψ we use $\varPhi$ and $\varPsi$ respectively. With each atomic position u we associate a sequence pre(u) of positions called the *prefix* of u as follows: if $u_1 < u_2 < \ldots < u_n \leq u$ $(1 \leq n)$ are the elements of $\varPhi \cup \varPsi$ that dominate u in the formula tree then pre(u)= $u_1 u_2 \cdots u_n$. Intuitionistic complementarity of atomic positions requires that their prefixes can be unified[2] by an intuitionistic substitution.

An *intuitionistic substitution* σ_J is a mapping from $\varPhi$ to $(\varPhi \cup \varPsi)^*$. It induces a relation $\sqsubset_J$ on $\mathcal{P}os \times (\varPhi \cup \varPsi)$ [3] in the following way: if $\sigma_J(u) = p$ then $v \sqsubset_J u$

[1] For technical reasons we consider a substitution σ to be *idempotent* (i.e. $\sigma\sigma = \sigma$).

[2] To unify two prefixes we need an algorithm for special string unification [14].

[3] By $\mathcal{P}os = \alpha \cup \beta \cup \varGamma \cup \varDelta$ we denote the set of all the positions in a formula tree.

and pdc$(u) \sqsubset_J v$ for all $v \in \Psi$ occuring in the prefix p, where $u \in \Phi$ and pdc(u) is the predecessor of u in the formula tree. As in the first-order case $v \sqsubset_J u$ means that v should be 'reduced' before u. A *combined substitution* consist of a first-order substitution σ_Q and an intuitionistic substitution σ_J. It is *admissible* if the reduction ordering $\lhd := (< \cup \sqsubset_Q \cup \sqsubset_J)^+$ is irreflexive.

Theorem 2. *A formula F is intuitionistically valid iff there is*

- *a multiplicity μ,*
- *an admissible combined substitution $\sigma := (\sigma_Q, \sigma_J)$,*
- *a set of connections which are complementary under σ and such that every path through the formula F contains a connection from this set.*

Consider the formula $\forall x Px \Rightarrow Pa \wedge Pb$. Its formula tree is shown in figure 3; its *matrix representation* in figure 4 where we place components of α-type sub-formulae horizontally and components of β-type sub-formulae vertically.

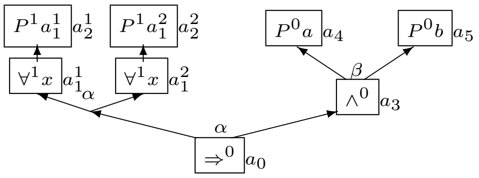


Fig. 3. Formula tree for F

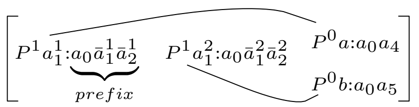

$P^1 a_1^1{:}a_0\bar{a}_1^1\bar{a}_2^1$
prefix
$P^1 a_1^2{:}a_0\bar{a}_1^2\bar{a}_2^2$
$P^0 a{:}a_0 a_4$
$P^0 b{:}a_0 a_5$

Fig. 4. Matrix representation for F

The two instances of the formula $\forall x Px$ are to be considered components of an implicit α-type position (in the matrix they stay side by side). In the prefixes the positions of type ϕ are emphasized with an over-bar. There are two paths through the matrix, namely $\{Pa_1^1, Pa_1^2, Pa\}$ and $\{Pa_1^1, Pa_1^2, Pb\}$. They contain the connections $\{Pa_1^1, Pa\}$ and $\{Pa_1^2, Pb\}$ respectively which are both complementary under the substitutions $\sigma_Q = \{a_1^1 \backslash a, a_1^2 \backslash b\}$ and $\sigma_J = \{\bar{a}_1^1 \backslash \epsilon, \bar{a}_1^2 \backslash \epsilon, \bar{a}_2^1 \backslash a_4, \bar{a}_2^2 \backslash a_5\}$. Therefore the formula is intuitionistically valid.

2.4 The Connection Method

A proof method for classical first-order logic based on theorem 1 is the connection method developed by Bibel [4]. The proof search is driven by connections instead of connectives as in the sequent calculus. Once a connection has been identified all paths containing this connection are eliminated. If every paths is deleted the formula is valid. In the following we present a proof method similar to the original connection method which deals with formulae in non-normal form because of the absence of such a form in the intuitionistic logic.

Definition 3. Two atomic formulae P and Q are *α-/β-related* iff the first common node in the formula tree - going from the nodes labeled with P and Q down to the root - is a position of type α/β. No atomic formula P is α-/β-related to itself.

If two atoms (atomic formulae) are α-related they appear side by side in a matrix representation. They appear on top of each other if they are β-related.

Definition 4. An atom P is *α-/β-related* to a *set* of atomic formulae $\mathcal{S}$ iff P and Q are α-/β-related for all formulae $Q \in \mathcal{S}$. Every atom P is α-/β-related to the empty set $\emptyset$.

Let $\mathcal{A}$ be the set of all atoms[4] in a given first-order formula F. Then the following procedure returns *true* iff F is intuitionistically valid.

```
Main-procedure
    repeat
        $\sigma := (\emptyset, \emptyset)$;   valid := PROOF($\emptyset, \emptyset$);
        if valid = false then increase the multiplicity $\mu$ of the given formula $F$
    until valid = true
Sub-procedure PROOF($\mathcal{P}, \mathcal{C}$)   ($\mathcal{P} \subseteq \mathcal{A}$ is the active path. $\mathcal{C} \subseteq \mathcal{A}$ are proven subgoals.)
    if no atom $A \in \mathcal{A}$ is $\alpha$-related to $\mathcal{P}$ and $\beta$-related to $\mathcal{C}$   then return true
    $\mathcal{E} := \emptyset$;   $\sigma' := \sigma$
    repeat
        select an atom $A \in \mathcal{A}$ which is $\alpha$-related to $\mathcal{P} \cup \mathcal{E}$ and $\beta$-related to $\mathcal{C}$
        if there is no such atom $A$ then return false
        $\mathcal{E} := \mathcal{E} \cup \{A\}$;   $\mathcal{D} := \emptyset$;   valid := false;   noconnect := false
        repeat
            select an atom $\bar{A} \in \mathcal{A}$ where $\bar{A} \notin \mathcal{D}$ and either $\bar{A} \in \mathcal{P}$ or $\bar{A}$ is $\alpha$-related
            to $\mathcal{P} \cup \{A\}$ and $(A, \bar{A})$ is a connection which is complementary under an
            admissible combined substitution $\sigma$ computed using $\sigma'$
            if there is no such atom $\bar{A}$
                then noconnect := true
                else $\mathcal{D} := \mathcal{D} \cup \{\bar{A}\}$;   valid := PROOF($\mathcal{P} \cup \{A\}, \{\bar{A}\}$)
                    if valid = true then valid := PROOF($\mathcal{P}, \mathcal{C} \cup \{A\}$)
        until valid = true or noconnect = true
    until valid = true
    return true
```

Note that in PROOF all variables except for the set $\mathcal{A}$ and the substitution σ are local. An example proof using the connection method is given in the next section.

3 Relating Sequent Calculus and Connection Method

In this section we point out the relationship between a proof with the connection method and the corresponding sequent proof. Firstly we deal with classical propositional logic. After that we consider the intuitionistic propositional case.

3.1 Classical (Propositional) Logic

Consider $F \equiv (S \wedge (\neg(T \Rightarrow R) \Rightarrow P)) \Rightarrow (\neg((P \Rightarrow Q) \wedge (T \Rightarrow R)) \Rightarrow (S \wedge \neg\neg P))$. The formula tree (skeleton) of this formula is shown in figure 5, its matrix representation in figure 6. In the skeleton only the positions of principal type β, i.e. $\beta_1, \beta_2, \beta_3$ and β_4, are marked.[5] Additionally each branch rooted at such a β-position is marked with a letter, namely a,b,...,h. Since we deal with formulae in

[4] Different atoms having the same predicate symbol are considered distinct.

[5] Positions of type β play the essential role during the proof process. In our presentation of a formula tree we focus our attention on positions of this type and omit the others.

non-normal form the matrix in figure 6 is nested which means that an entry in a matrix can itself be a matrix. Components of sub-formulae of type β are placed one upon the other. Atoms are marked with their polarities, whereas polarity 0 indicates that the atom occurs positively within the negational normal form and polarity 1 means that it occurs negatively. A *reduction* of a position means the sub-formula rooted at this position has to be reduced in the sequent calculus.

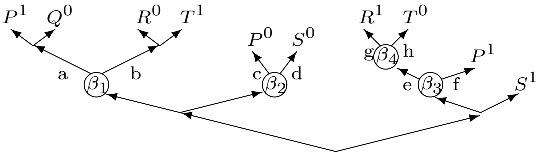


Fig. 5. Skeleton of the formula tree for F

$$\left[\begin{array}{cccc} \left[\begin{array}{c}[\,P^1\ \ Q^0\,]\\ [\,R^0\ \ T^1\,]\end{array}\right] & \begin{bmatrix}P^0\\ S^0\end{bmatrix} & \begin{bmatrix}R^1\\ T^0\\ P^1\end{bmatrix} & S^1\end{array}\right]$$

Fig. 6. Matrix of the formula F

We begin by proving the classical validity of the formula F. After each connection step we show the structure of the corresponding sequent proof. In the first step – shown in figure 7 – we connect atom P^1 which is in branch 'a' of the formula tree with P^0 in branch 'c'. If these atoms shall form an *axiom* in the sequent proof we have to reduce positions β_1 and β_2. Whenever we reduce a position of principal type β the sequent proof will split into two branches. Thus after reducing β_1 there is a split into two branches 'a' and 'b'. Now we reduce β_2 in the 'a'-branch of the sequent proof which results in the branches 'c' and 'd'. The 'c'-branch now contains an *axiom* of the form $\Gamma, P^1 \vdash P^0, \Delta$. This branch is said to be *closed.*[6] Note that we do not perform reductions of positions which do not have type β (i.e. are of type α, γ, or δ) explicitly. Since reducing positions of type α, γ, or δ do not split the sequent proof they can be reduced straightforwardly.

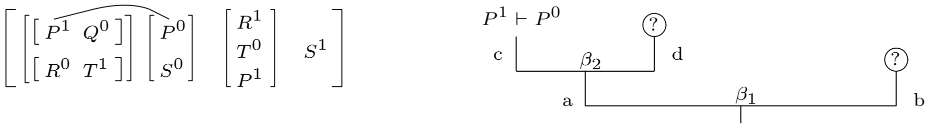


Fig. 7. The first step in the connection/sequent proof of F

In the sequent proof there are two branches 'b' and 'd' which do not contain an *axiom.* They are said to be *open.* We first want to close branch 'd'. In the formula tree this branch only contains the atom S^0. Connecting it with atom S^1 (obtained without reducing any β-position) leads to an *axiom* of the form $\Gamma, S^1 \vdash S^0, \Delta$ which closes this branch as shown in figure 8.

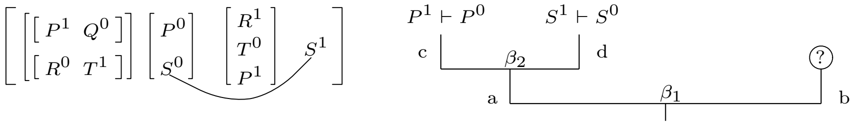


Fig. 8. The second step in the connection/sequent proof of F

[6] Open branches (corresponding to open subgoals) are marked with a '?' whereas '•' (see e.g. figure 13) indicates closed branches.

The only branch not containing an *axiom* is the open branch 'b'. In the third step we connect R^0 with R^1 (see figure 9). Since R^1 occurs in the 'e'/'g'-branch of the formula tree we first have to reduce position β_3 and β_4 successively. Therefore the 'b'-branch in the sequent proof is split twice. Whereas β_3 is responsible for splitting into the branches 'e' and 'f', β_4 splits the 'e'-branch into 'g' and 'h'. As the 'g'-branch is closed by an *axiom* the only open branches are 'h' and 'f'. In the next step we connect from T^0 to T^1 closing the 'h'-branch in the sequent calculus as shown in figure 9. Since the 'b'-branch already contains T^1 we do not have to reduce a β-position.

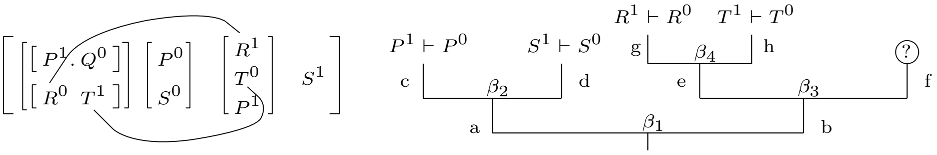


Fig. 9. The third/fourth step in the connection/sequent proof of F

There is only one open branch left, namely the 'f'-branch. Connecting from P^1 to P^0 splits it into the branches 'c' and 'd', as the atom P^0 occurs in the 'c'-branch of the formula tree (see figure 10). Closing this 'c'-branch with an *axiom* in the sequent proof, we finally have to close the 'd'-branch. In this last step we connect from S^0 to S^1, which does not lead to any open branches, since the atom S^1 can be reached without a reduction of β-positions.

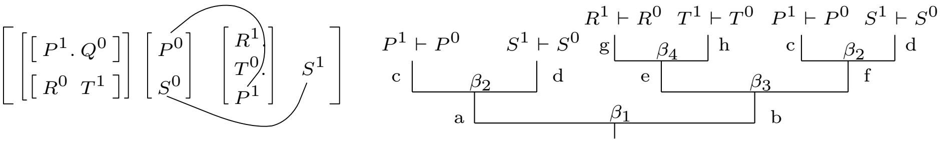


Fig. 10. The fifth/sixth step in the connection/sequent proof of F

We successfully completed the connection proof and every leaf in the sequent proof is an *axiom*. Therefore the formula F is classically valid.

3.2 Intuitionistic (Propositional) Logic

In intuitionistic logic we additionally have to unify the prefixes of the atomic formulae in every connection. This leads to an intuitionistic substitution σ_J which induces a relation $\sqsubset_J$ on the positions of the formula tree as defined in section 2.3. Together with the tree ordering $<$ it determines the reduction ordering $\lhd$ where $v \lhd u$ means that position v should be reduced before position u. Performing all these steps w.r.t. the formula F above eventually leads to the following reduction ordering on the positions of principal type β (i.e. $\beta_1, \beta_2, \beta_3$ and β_4):

$$\beta_2 \lhd \beta_3 \lhd \beta_1 \lhd \beta_4 \ .$$

For the sequent proof this means that we have to split the position β_2 *before* we reduce β_3 and so on. Therefore the intuitionistic sequent proof shown in figure 11 differs from the classical one in order of rule application.[7]

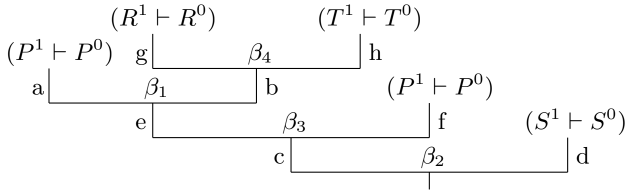


Fig. 11. The structure of an intuitionistic sequent proof of F

The sequent proof in intuitionistic logic cannot be derived as easily as in classical propositional logic. In the latter case each connection in a matrix proof corresponds to exactly one *axiom* in the sequent calculus. For intuitionistic logic (even in the propositional part) this property does not hold anymore. The situation is similar for classical *predicate* logic because the eigenvariable condition restricts the order in which positions can be reduced (encoded in the relation $\sqsubset_Q$ defined in section 2.3). To avoid these problems our approach will take the reduction ordering $\lhd$ into account *during* the construction of the proof.

4 A Connection Based Proof Method

Before we present our proof procedure we shall investigate the intuitionistic validity of the previous section's example a little more detailed.

4.1 An Introductory Example

We have seen that it is more efficient to consider the reduction ordering $\lhd$ (particularly $\sqsubset_J$) during the process of constructing a matrix proof and a sequent proof simultaneously. Due to the importance of β-positions within the reduction ordering we slightly modify the definition of active paths and define *open subgoals*.

Definition 5. The *β-prefix* of an atomic position u, denoted by β-pre(u), is the set of all elements $v_1, \ldots, v_n \in \beta_0$ (positions of type β_0) that dominate u in the formula tree, i.e. $\beta\text{-pre}(u) := \{v \in \beta_0 \mid v < u\}$.

In the previous section as well as in the example below we have marked branches in the sequent proof with letters (e.g. a, b,...) to keep the notation simple. For the following definitions we have to point out that each letter corresponds to exactly one position of type β_0. If, for instance, the reduction of a β-position β_1 leads to the branches 'a' and 'b' in the sequent proof, they will be identified by the two successor positions of β_1 in the formula tree which are both of type β_0.

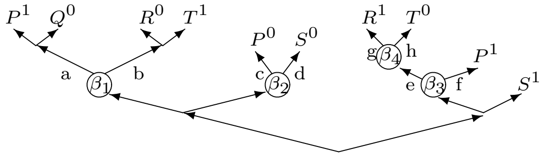
[7] Note that an intuitionistic proof does not necessarily differ from the classical one.

Definition 6. The *active β-path $\mathcal{P}_\beta \subseteq \beta_0$ for a position u* of type β_0 is the set of all the labels (positions of type β_0) obtained by going from the root of the sequent proof to the node marked with u while collecting the label of every branch. An active β-path $\mathcal{P}_\beta$ induces an *active path $\mathcal{P}$ for the position u* where $\mathcal{P} = \{v \mid v$ atomic position and $\beta\text{-pre}(v) \subseteq \mathcal{P}_\beta\}$.

The active path $\mathcal{P}$ for u is thus the set of all the atoms which can be reached from the u-branch in the sequent proof (i.e. the branch leading from the root to the position u) without passing through a β-position. In other words, it is the set of atoms which can be obtained by reducing the corresponding sequent without reducing positions of type β.

Definition 7. The set of *open subgoals $\mathcal{C}_\beta \subseteq \beta_0$* is the set of the positions of type β_0 labeling the open branches in the sequent proof. Each open branch is assigned its active (β-)path.

Consider again $F \equiv (S \wedge (\neg(T \Rightarrow R) \Rightarrow P)) \Rightarrow (\neg((P \Rightarrow Q) \wedge (T \Rightarrow R)) \Rightarrow (S \wedge \neg\neg P))$ and its formula tree given below



To prove F we first select an atom[8] , say P^1, in branch 'a' of the formula tree and connect it with the atom P^0 in the 'c'-branch. For that we have to reduce two β-positions, namely β_1 and β_2. Unifying the prefixes of the two atoms leads to an intuitionistic substitution. Together with the tree ordering it induces the reduction ordering $\beta_2 \lhd \beta_1$. Thus we have to split into the branches 'c' and 'd' (corresponding to β_2) before we split the 'c'-branch into 'a' and 'b' (corresponding to β_1). This closes the 'a'-branch in the sequent proof as shown in figure 12. In the next step we choose the 'd'-branch from the set of open subgoals $\mathcal{C}_\beta$ = {b, d}. The active β-path $\mathcal{P}_\beta$ = {d} for 'd' induces an active path $\mathcal{P} = \{S^1, S^0\}$. The only atom S^0 in the 'd'-branch of the formula tree can therefore be connected to S^1 in the active path which closes this branch.

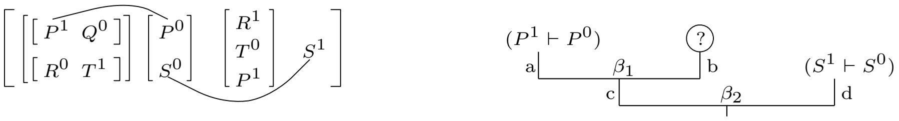


Fig. 12. The first and second proof step

The only open branch is now the 'b'-branch ($\mathcal{C}_\beta$ = {b}). In the formula tree this branch contains two atoms R^0 and T^1 from which we select R^0 and connect it with R^1 which is not included in the active path $\mathcal{P} = \{S^1, P^0, R^0, T^1\}$ for 'b' ($\mathcal{P}_\beta$ = {c,b}). To make R^0 form an *axiom* with R^1 we have to reduce β_3

[8] To keep the notation simple, we speak of atoms meaning the position labeling it.

which splits the proof into 'e' and 'f' and (in branch 'e') β_4 which splits the 'e'-branch into 'g' and 'h'. The unification of the prefixes of these two atoms yields an intuitionistic substitution which – together with the tree ordering – induces the reduction ordering (concerning the β-positions) $\beta_2 \lhd \beta_3 \lhd \beta_1 \lhd \beta_4$. That means we have to insert the split into 'e' and 'f' *between* the reduction of β_2 and β_1 (leaving the rest of the partial sequent proof remains unchanged) and split into the branches 'g' and 'h' after reducing β_1, as shown in figure 13.

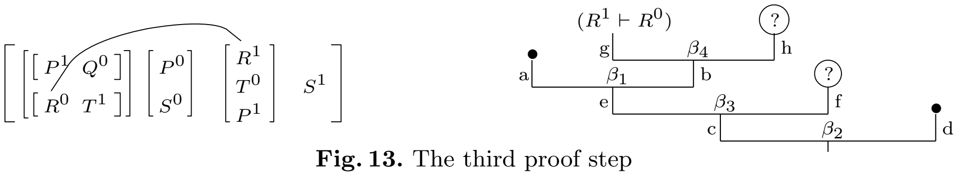


Fig. 13. The third proof step

After closing branch 'g' we get two additional open branches 'f' and 'h' ($\mathcal{C}_\beta =$ {f, h}). The active β-paths for 'f' ($\mathcal{P}_\beta = \{c, f\}$) and for 'h' ($\mathcal{P}_\beta = \{c, e, b, h\}$) induce $\mathcal{P} = \{S^1, P^0, P^1\}$ and $\mathcal{P} = \{S^1, P^0, R^0, T^1, T^0\}$ respectively. To close these branches we connect P^1 in the 'f'-branch of the formula tree to P^1 in the active path for 'f' and T^0 in the 'h'-branch to T^1 in the active path for 'h'. These steps conclude the intuitionistic proof for F, since $\mathcal{C}_\beta = \emptyset$ and therefore each branch in the sequent proof is closed.

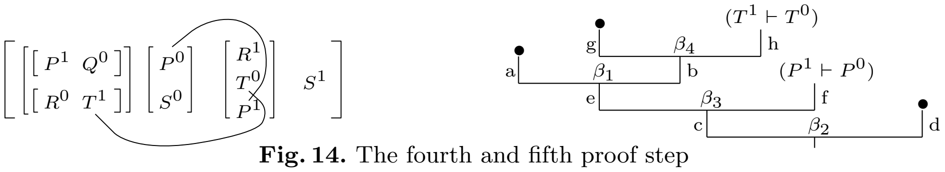


Fig. 14. The fourth and fifth proof step

4.2 The Proof Procedure

The explanations given in the above example should be sufficient to understand the procedure carrying out our proof method. In principle it is similar to the version of the connection method introduced in section 2.4. There is, however, a difference in the handling of subgoals and active paths. The original connection method focuses on connecting new atoms which are selected according to the current active path $\mathcal{P}$ and the set $\mathcal{C}$ of already proven subgoals. $\mathcal{P}$ and $\mathcal{C}$ are parameters of the procedure. The method which we shall describe below aims at closing open subgoals of type β_0 (a set which may grow or decrease in the process) and uses connections related to their active β-paths for this purpose. The active path depends on the selected subgoal and will be computed within the process.

Let $\mathcal{A}$ be the set of all atoms in a given first-order formula F. The following procedure returns *true* iff F is intuitionistically valid.

```
Main-procedure
  repeat
     $\sigma := (\emptyset, \emptyset)$;   initialize $\lhd_\beta$;   valid := PROOF($\{\emptyset\}$)
     if valid = false  then increase the multiplicity $\mu$ of the given formula $F$
  until valid = true
```

```
Sub-procedure PROOF($\mathcal{C}_\beta$)   ($\mathcal{C}_\beta \subseteq \mathcal{B}_0^i$ are subgoals which still have to be proven)
    if $\mathcal{C}_\beta = \emptyset$ then return true
    $\mathcal{E} := \emptyset$;   $\sigma' := \sigma$;   $\lhd'_\beta := \lhd_\beta$;   select an element $a_\beta \in \mathcal{C}_\beta$
    repeat
        select an atom $A \in \mathcal{A}$ where $a_\beta \subseteq \beta$-pre$(A)$ which is $\alpha$-related to $\mathcal{E}$
        if there is no such atom $A$  then return false
        $\mathcal{E} := \mathcal{E} \cup \{A\}$;   $\mathcal{D} := \emptyset$ ;   valid := false ;   noconnect := false
        compute the active $\beta$-path $\mathcal{P}_\beta$ for $a_\beta$ and its active path $\mathcal{P}$
            using the $\beta$-reduction ordering $\lhd'_\beta$
        repeat
            select an atom $\bar{A} \in \mathcal{A}$ where $\bar{A} \notin \mathcal{D}$ and either $\bar{A} \in \mathcal{P}$ or $\bar{A}$ is $\alpha$-related
            to $\mathcal{P} \cup \{A\}$ and $(A, \bar{A})$ is a connection which is complementary under an
            admissible combined substitution $\sigma$ and an admissible $\beta$-reduction ordering
            $\lhd_\beta$ computed using $\sigma'$ and $\lhd'_\beta$
            compute the set $\mathcal{C}_\beta$ expanded by the new open subgoals
            if there is no such atom $\bar{A}$
                then noconnect := true
                else $\mathcal{D} := \mathcal{D} \cup \{\bar{A}\}$;   valid := PROOF($\mathcal{C}_\beta \setminus \{a_\beta\}$)
        until valid = true or noconnect = true
    until valid = true
    return true
```

Note that all variables in PROOF – except for $\mathcal{A}$, σ, and $\lhd_\beta$ – are local.

The above algorithm uses a few new concepts which deserve explanation. Since it is possible to reduce the same formula in different branches of the sequent proof we have to distinguish these branches (identified with positions of type β_0) by an index. $\mathcal{B}_0^i$ is a set of indexed positions of type β_0 included in the sequent proof.

Previously we had required that the reduction ordering defines a definite relation between all β-positions. This is not strictly necessary. If a substitution does not lead to an ordering between two branches in the sequent proof we have to encode the permutability between these branches. This is done by an extended definition of paths together with a so-called *β-reduction ordering* $\lhd_\beta$. $\lhd_\beta$ consists of two relations, namely $\approx \subseteq \beta_0 \times \beta_0$ and $\not\approx \subseteq \beta_0 \times \beta_0$. The relation $u \approx v$ $(u, v \in \beta_0)$ means that there is a sequent proof where the branches u and v are in the same *β-path* (that is a way from the root to a leaf), whereas $u \not\approx v$ $(u, v \in \beta_0)$ means that there is no such a sequent proof. These two relations induce an active path $\mathcal{P}_\beta := (\mathcal{P}_\beta^n, \mathcal{P}_\beta^p)$. The *n-path $\mathcal{P}_\beta^n$ for a β_0-position* u contains all β_0-positions which are necessarily in the active β-path for u in all sequent proofs under consideration. The *p-path $\mathcal{P}_\beta^p$ for* u denotes the set of β_0-positions which are possibly in the active β-path of u. [9]

Our method always attempts to select a reduction ordering which allows to connect to the active path. This shortens proofs substantially since a connection to the active path does not lead to any new open subgoal. If we ignore the reduction ordering during the search for connections we will get a version of the connection method. Therefore our method is a generalization of the original connection method.

[9] In the above procedure we have omitted such details. For a full description see [14].

5 Local Substitutions

The sequent proof makes it possible to use so-called *local substitutions* instead of *global* ones. We present an approach to treat first-order as well as intuitionistic substitutions *locally*.

The connection method and our proof method presented above use *global* substitutions. If we substitute a term t for a variable x then *every* occurence of x in the corresponding sequent proof has to be replaced by t. This is not very reasonable, since in a sequent proof we are allowed to replace different terms for the same variable if it occurs in different branches of the proof.

Let us consider the formula $\forall x Px \Rightarrow Pa \wedge Pb$ from section 2. In the matrix proof in section 2.3 we needed a copy of the subformula $\forall x Px$ (even in the classical case) since we had to assign two terms a and b to the variable x. However in the sequent proof (see figure 15) a duplication does not (explictly) occur. We could avoid this duplication if we treat the substitutions of the two branches of the sequent proof independently. Therefore we take two substitutions into account, namely $\sigma_1 = \{x\backslash a\}$ and $\sigma_2 = \{x\backslash b\}$, which are related to the two different branches in the sequent proof shown in figure 15.

$$\dfrac{\dfrac{Pa \vdash Pa}{\forall x Px \vdash Pa} \quad \dfrac{Pb \vdash Pb}{\forall x Px \vdash Pb}}{\vdash \forall x Px \Rightarrow Pa \wedge Pb}$$

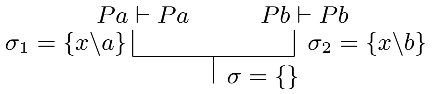

$Pa \vdash Pa$
$Pb \vdash Pb$
$\sigma_1 = \{x\backslash a\}$
$\sigma_2 = \{x\backslash b\}$
$\sigma = \{\}$

Fig. 15. A sequent proof for $\forall x Px \Rightarrow Pa \wedge Pb$ and its structure

To perform such a step it is necessary that the β-position a_β (a_3 in our example) responsible for the split is reduced before the γ-position a_γ (a_1 labeled with $\forall x$ in our example).[10] That is, either the reduction-ordering yields $a_\beta \lhd a_\gamma$ or we have to introduce this ordering and look if it is admissible. This technique is similar to Bibel's *splitting* technique [4]. Our approach, however, is simpler and can be applied more rigorously since we are able to exploit the sequent proof. When computing the substitution which has to make a connection complementary we only have to consider substitutions related to branches of the active β-path. After that we have to divide the computed substitution such that its parts relate to the corresponding branches.

In the following example we deal with the intuitionistic substitution. Consider the formula $F \;\equiv\; \neg\neg P \Rightarrow \neg\neg P \wedge \neg\neg P$. Its matrix representation together with the prefixes of the atoms is given in figure 16.

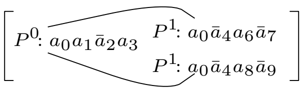

P^0: $a_0a_1\bar{a}_2a_3$
P^1: $a_0\bar{a}_4a_6\bar{a}_7$
P^1: $a_0\bar{a}_4a_8\bar{a}_9$

Fig. 16. Matrix for F

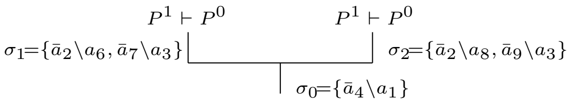

$P^1 \vdash P^0$
$P^1 \vdash P^0$
$\sigma_1 = \{\bar{a}_2\backslash a_6, \bar{a}_7\backslash a_3\}$
$\sigma_2 = \{\bar{a}_2\backslash a_8, \bar{a}_9\backslash a_3\}$
$\sigma_0 = \{\bar{a}_4\backslash a_1\}$

Fig. 17. Structure of the sequent proof for F

There are two paths through the matrix each of them containing a connection. To make the first connection complementary we have to unify the pre-

[10] Otherwise we have to replace the variable in the common branch before the split which makes it necessary to consider an explicit duplication of the formula.

fixes $a_0a_1\bar{a}_2a_3$ and $a_0\bar{a}_4a_6\bar{a}_7$[11] which results in the intuitionistic substitution $\sigma_J = \{\bar{a}_4\backslash a_1\bar{b},\ \bar{a}_2\backslash\bar{b}\,a_6\bar{c},\ \bar{a}_7\backslash\bar{c}\,a_3\}$[12] where $\bar{b}$ and $\bar{c}$ are new variables. Applying this substitution to the prefixes of the second connection leads to the prefixes $a_0a_1\bar{b}\,a_6\bar{c}\,a_3$ and $a_0a_1\bar{b}\,a_8a_9$ respectively which do not unify. It would be necessary to duplicate the subformula $\neg P^0$ although this copy does not appear (explicitly) in the sequent proof. To avoid this duplication we again consider local substitutions. Since the position labeled with $\wedge$ is reduced before $\neg P^0$ (induced by the substitution) the subformula $\neg P^0$ with the prefix $\bar{a}_2a_3$ occurs in both branches of the sequent proof. Therefore also the variable $\bar{a}_2$ can substituted by two different strings which make the second connection complementary. The local substitutions σ_1 and σ_2 and the substitution σ_0 which is common to both branches together with the structure of the sequent proof are shown in figure 17.[13] Both connections are now complementary under the substitution $\sigma_0 \cup \sigma_1$ and $\sigma_0 \cup \sigma_2$ respectively.

Employing local substitutions reduces the number of copies of formulae to be considered in a proof and thus the *multiplicity.* A copy will be required if and only if this copy also appears *explicitly* in the sequent proof. Since duplicated formulae can be very large this reduces the search space for a proof as well as its size.

We conclude this section by presenting a matrix characterisation for intuitionistic logic using *local substitutions.*

Definition 8. A *local connection* $((A,a),\ (\bar{A},\bar{a}))$, where $a,\bar{a}\in\mathcal{B}_0^i$, $a=\beta^\ell$-pre(A)[14] and $\bar{a} = \beta^\ell$-pre$(\bar{A})$, is *locally complementary* under $\lhd_\beta$ and σ^* if the connection $(A,\bar{A})$ is complementary under the admissible combined substitution $\sigma := \bigoplus(\,\sigma^*(u) \mid u \in \mathcal{P}_\beta \text{ for } a \quad \text{or} \quad u \in \mathcal{P}_\beta \text{ for } \bar{a})$ where $\bigoplus$ is the combination of substitutions (for details see [14]).

Theorem 9. *A formula F is intuitionistically valid iff there is*
- *a multiplicity μ,*
- *an admissible β-reduction ordering $\lhd_\beta$ (encoding the sequent proof structure),*
- *a local substitution σ^* which assigns each indexed β_0-position $u \in \mathcal{B}_0^i$ a combined substitution $\sigma := (\sigma_Q, \sigma_J)$,*
- *a set of local connections which are locally complementary under $\lhd_\beta$ and σ^* such that every path through F contains a connection from this set.*

6 Conclusion

In this paper he have presented a proof method for intuitionistic logic which develops a matrix proof and a sequent proof simultaneously. Our method extends Bibel's connection method [4] according Wallen's matrix characterization of intuitionistic validity [18] but it does not require a normal form. Due to an emphasis on connections instead of the outer structure of formulae the search space can be kept comparably small. Developing the sequent proof during the proof process leads to a natural representation of a formal proof which can be used within

[11] We emphasize the positions of type ϕ which play the part of variables by an overbar.

[12] This (and only this !) is in fact the *most general unifier.*

[13] We have omitted the *extra* variables $\bar{b}$ and $\bar{c}$.

[14] β^ℓ-pre(A) is the last position of type β_0 that dominates A in the formula tree.

interactive proof systems. Furthermore, it allows considering *local* substitutions instead of global ones which reduces the search space even more than a purely matrix-oriented proof method would do.

The efficiency of our proof procedure also depends on the unification algorithm computing the so-called intuitionistic substitutions. In [14] we have developed a specialized string unification algorithm which is more efficient than the one presented in [13] since it computes only the *most general* substitutions which make the prefixes equal.

The sequent proof generated by our procedure can easily be transformed into a Gentzen-style sequent proof (see [15] for details). Thus we can realize our procedure as a tactic of the NuPRL system [6] in order to support the development of proofs and verified routine programs within a rich constructive theory.

References

1. E. W. Beth. *The foundations of mathematics.* North–Holland, 1959.
2. W. Bibel, S. Brüning, U. Egly, T. Rath. Komet. In *Proceedings of the 12th CADE*, LNAI 814, p. 783–787. Springer Verlag, 1994.
3. W. Bibel. On matrices with connections. *Jour. of the ACM*, 28, p. 633–645, 1981.
4. W. Bibel. *Automated Theorem Proving.* Vieweg Verlag, 1987.
5. K. Bläsius, N. Eisinger, J. Siekmann, G. Smolka, A. Herold, C. Walther. The Markgraf Karl refutation procedure. In *IJCAI-81*, p. 511–518, 1981.
6. R. L. Constable et. al. *Implementing Mathematics with the NuPRL proof development system.* Prentice Hall, 1986.
7. M. C. Fitting. *Intuitionistic logic, model theory and forcing.* Studies in logic and the foundations of mathematics. North–Holland, 1969.
8. J. Gallier. Constructive logics. Part I: A tutorial on proof systems and typed λ-calculi. Technical Report 8, Digital Equipment Corporation, 1991.
9. G. Gentzen. Untersuchungen über das logische Schließen. *Mathematische Zeitschrift*, 39:176–210, 405–431, 1935.
10. K. Gödel. An interpretation of the intuitionistic sentential logic. In *The Philosophy of Mathematics*, p. 128–129. Oxford University Press, 1969.
11. D. S. Korn. KonSequenz – Ein Konnektionsmethoden-gesteuertes Sequenzenbeweis-Verfahren. Master's thesis, TH Darmstadt, FG Intellektik, 1993.
12. R. Letz, J. Schumann, S. Bayerl, W. Bibel. Setheo: A high-performance theorem prover. *Journal of Automated Reasoning*, 8:183–212, 1992.
13. H. J. Ohlbach. A resolution calculus for modal logics. Ph.D. Thesis (SEKI Report SR-88-08), FB Informatik, Universität Kaiserslautern, 1988.
14. J. Otten. Ein konnektionenorientiertes Beweisverfahren für intuitionistische Logik. Master's thesis, TH Darmstadt, FG Intellektik, 1995.
15. S. Schmitt, C. Kreitz. On transforming intuitionistic matrix proofs into standard-sequent proofs. In *Proceedings Tableaux Workshop 1995*, this volume.
16. R. M. Smullyan. *First-Order Logic*, *Ergebnisse der Mathematik* 43. 1968.
17. L. Wallen. Matrix proof methods for modal logics. *IJCAI-87* , p. 917–923. 1987.
18. L. Wallen. *Automated deduction in nonclassical logic.* MIT Press, 1990.
19. L. Wos et. al. Automated reasoning contributes to mathematics and logic. In *Proceedings of the 10th CADE*, LNCS 449, p. 485–499. Springer Verlag 1990.

This article was processed using the LaTeX macro package with LLNCS style