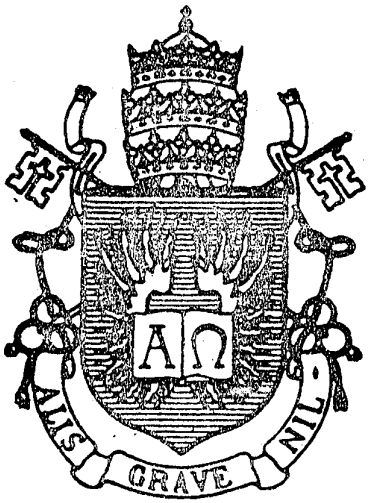


PUC

Series: Monografias em Ciência da Computação, 03/88

TOWARDS A TABLEAU-BASED INTUITIONISTIC THEOREM PROVER

by

Oliver Bittel
Paulo Sergio C. de Alencar

Departamento de Informática

PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO DE JANEIRO

ARQUÊS DE SÃO VICENTE, 225 – CEP 22453

RIO DE JANEIRO – BRASIL

PUC/RJ - DEPARTAMENTO DE INFORMÁTICA

Series: Monografias em Ciência da Computação, 03/88
Editor: Paulo Augusto Silva Veloso April, 1988

TOWARDS A TABLEAU-BASED INTUITIONISTIC THEOREM PROVER *

by

Oliver Bittel**
Paulo Sérgio C. de Alencar***

* This work has been partially sponsored by FINEP.
** GMD - Karlsruhe, Germany
*** On leave of absence from the University of Brasília, Brasil.

In charge of publications:

Rosane Teles Lins Castilho
PUC/RJ-Depto. de Informática
Assessoria de Biblioteca, Documentação e Informação
Rua Marquês de São Vicente, 225 - Gávea
22453 - Rio de Janeiro, RJ BRASIL

ABSTRACT

A proof procedure for the first-order intuitionistic logic which is based on an improved version of the intuitionistic Beth tableau calculus is presented. It also treats treats the problem of proving under an intuitionistic theory.

KEYWORDS: theorem proving, intuitionistic logic, tableau calculus, proof procedure.

RESUMO

Apresenta-se um procedimento de prova para a lógica intuicionista de primeira ordem baseado em uma versão melhorada do cálculo de tableau intuicionista de Beth. Este procedimento também trata o problema da prova a partir de uma teoria intuicionista.

PALAVRAS-CHAVE: provadores de teorema, lógica intuicionista, procedimento de prova, cálculo de tableau.

C O N T E N T S

I. INTRODUCTION 1
II. THE INTUITIONISTIC TABLEAU CALCULUS..... 2
II.1 PRELIMINARIES..... 3
II.2 THE INTUITIONISTIC BETH TABLEAU..... 7
III. A PROOF PROCEDURE FOR THE TABLEAU CALCULUS..... 11
III.1 THE PROPOSITIONAL LOGIC..... 13
III.2 PROVING UNDER A THEORY..... 19
III.3 THE QUANTIFIER RULES..... 24
IV. CONCLUSION..... 30
REFERENCES.....31

I. INTRODUCTION

The tableau method introduced by Beth [Beth 1959] has been mainly used to prove the completeness of various logic calculi such as the modal and intuitionistic logic.Since recently these non-standard logics are becoming more used in various branches of artifficial intelligence and computer science, as a means for expressing program development and program strategies and as logics of knowledge and belief ([Sintzoff 1986],[de Groote 1986],[Halpern 1985]), the need arises for efficient proof systems for these logics.

The available tableau-based intuitionistic proof systems constitute a very readable means of investigating the validity of arbitrary first-order formulas. Beyond that, as one might think of a tableau as an exploration of a hypothetical counter-model to a particular formula, if the tableau does not end successfully we get also a model in which the formula is not valid.

In this work we propose an intuitionistic first-order proof procedure based on an improved tableau system for the intuitionistic logic. We also investigate the problem of proving under a theory. In section II we present an introduction to the intuitionistic Kripke's semantic and a particular tableau system. In section III we improve the tableau system presented in section II for both the propositional and predicate parts of the logic and study the problem of proving under a theory.

II THE INTUITIONISTIC TABLEAU CALCULUS

In order to get an adequate characterization of a decision procedure for validity of first-order intuitionistic formulas we define the so-called Kripke semantics for the intuitionistic logic. We assume familiarity with the aspects of this non-standard logic which motivate the present semantic concept.

In the next two sections a Kripke's model theory for intuitionistic logic is presented from which we get the particular intuitionistic Beth tableau defined according to the uniform $\alpha, \beta, \gamma, \delta$ notation introduced by Smullyan [Smullyan 1968].

In addition some notational conventions and useful definitions that are used in the next sections are also presented.

The intuitionistic Kripke-style semantics and the intuitionistic tableau calculus are taken from [Fitting 1983]. We let A, B range over predicate signed formulas, p,q range over propositional signed formulas and X, Y range over sets of signed formulas.

II.1 PRELIMINARIES

In this section we present Kripke's model theory for the intuitionistic logic. We assume familiarity with the usual definition of the intuitionistic language and formulas.

The pair $\langle G,R \rangle$ is called an intuitionistic frame if G is a non-empty set and R is a reflexive, transitive relation on G. Let D be some non-empty set. A first-order intuitionistic frame over D is a triple $\langle G,R,P \rangle$ where $\langle G,R \rangle$ is an intuitionistic frame and P is a mapping from G to non-empty subsets of D meeting the monotonicity condition: if wRw' then $P(w) \subseteq P(w')$. One might think of w G and P(w) as being a state of knowledge and the "things" that exist in world w, respectively.

We present a Kripke's intuitionistic semantic version using signed formulas. By a signed formula we mean +A or -A where A is a formula and "+", "-" are two new formal symbols.

For ease the exposition we use a uniform notation due to Smullyan and Fitting that classifies signed formulas according to their sign and major connective/operator as shown in the following table. Each formula class is presented together with the definition of it's components. For example, for each α-formula two components, α_1 and α_2 are defined. In the following charts we assume the language is L(C), all sentences are in L(C) and all constant symbols are chosen entirely from the set C.

α	α_1	α_2
$+(A \,\&\, B)$	$+A$	$+B$
$-(A \vee B)$	$-A$	$-B$
$-(A \supset B)$	$+A$	$-B$
$-\sim A$	$+A$	$+A$

β	β_1	β_2
$+(A \vee B)$	$+A$	$+B$
$-(A \,\&\, B)$	$-A$	$-B$
$+(A \supset B)$	$-A$	$+B$
$+\sim A$	$-A$	$-B$

γ	$\gamma(a)$
$+(\forall x)\ A(x)$	$+A(a)$
$-(\exists x)\ A(x)$	$-A(a)$

δ	$\delta(a)$
$+(\exists x)\ A(x)$	$+A(a)$
$-(\forall x)\ A(x)$	$-A(a)$

In addition we use various first-order languages described as follows. We assume C_0 is some designated infinite collection of formal constant symbols and $L(C_0)$ is the formal first-order intuitionistic language (the formal language of discourse) we will be primarily interested in. A disjoint set of the same cardinality, P_0 is also set aside as parameters. Then $L(C_0 \cup P_0)$ will be the language used in formal proofs (the formal language of proofs). Likewise each intuitionistic model has a domain D and we use L(D) as the language of that model.

A <u>first-order intuitionistic model</u> over a domain D is a quadruple $\langle G,R,P,\Vdash\rangle$ where $\langle G,R,P\rangle$ is a first-order intuitionistic frame over D and $\Vdash$ is a relation between members of G and sentences of L(D), the language of that model, such that for all $w \in G$:

For regular connectives $(\&, \vee, \exists)$

R1) $w \Vdash \alpha$ iff $w \Vdash \alpha_1$ and $w \Vdash \alpha_2$

R2) $w \Vdash \beta$ iff $w \Vdash \beta_1$ or $w \Vdash \beta_2$

R3) $w \Vdash \gamma$ iff $w \Vdash \gamma(a)$ for every $a \in P(w)$

R4) $w \Vdash \delta$ iff $w \Vdash \delta(a)$ for some $a \in P(w)$

For special connectives ($\sim, \supset, \forall$)

S1) $w \Vdash \alpha$ iff $(\exists w^*)$ $(w^* \Vdash \alpha_1$ and $w^* \Vdash \alpha_2)$

S2) $w \Vdash \beta$ iff $(\forall w^*)$ $(w^* \Vdash \beta_1$ or $w^* \Vdash \beta_2)$

S3) $w \Vdash \gamma$ iff $(\forall w^*)$ $(w^* \Vdash \gamma(a)$ for every $a \in P(w^*))$

S4) $w \Vdash \delta$ iff $(\exists w^*)$ $(w^* \Vdash \delta(a)$ for some $a \in P(w^*))$

We have also the following conditions:

C1) A atomic, if $w \Vdash +A$ then $w^* \Vdash +A$

C2) if A atomic then exactly one of $w \Vdash +A$, $w \Vdash -A$.

Here w^* denotes an arbitrary world in the relation R to w.

Different versions of the intuitionistic first-order logic can be obtained by restricting the way in which P varies from world to world. If we take the P map as constant, $P(w)=P(w')$ for all w,w' belonging to G, we get the constant domain version of this logic and if we don't impose this restriction on P we get the varying domain intuitionistic first-order logic.

Note that at a world w of an intuitionistic model $\langle G, R, \Vdash \rangle$ we have

$w \Vdash +A$ for $w \Vdash A$

$w \Vdash -A$ for $w \not\Vdash A$.

Note also that -A and ~A play very different roles. One might say that $w \Vdash \sim A$ asserts that, given the state-of-knowledge w, a disproof of A can be achieved. But $w \Vdash -A$ merely asserts that no proof of X is possible with knowledge w.

We now define the <u>interpretation</u> of a formal language into the language of the model. Suppose C and D are two sets of constants and $v: C \to D$ is a mapping of the constants in C to the constants in D. In the obvious way we extend v to a mapping of languages $v: L(C) \to L(D)$. As $L(C_0 \cup P_0)$ is the formal language to be used in proofs an interpretation of this language in a first-

order Kripke model $\langle G,R,P,\Vdash\rangle$ over D is a mapping $v: C_0 \cup P_0 \to D$.

We say that a sentence A of L(D) is valid in the model $\langle G,R,P,\Vdash\rangle$ if $w \Vdash A$ for every w G such that all constants of A are in P(w). We say that a sentence A of $L(C_0 \cup P_0)$ is valid under an interpretation v in a intuitionistic model if v(A) is valid in this model in the sense used above.

Finally a first-order sentence A of $L(C_0 \cup P_0)$ is intuitionistically valid if X is valid under every interpretation in every first-order intuitionistic model.

II.2 THE INTUITIONISTIC BETH TABLEAUS

In the last section we followed the approach based on the observation that the connectives $\sim, \supset$ and $\not\forall$ behave in a "special" way while &, $\forall$ and $\exists$ behave in a more regularregular fashion. By this approach we obtained a direct characterization of intuitionistic models, in terms of signed formulas using the presented uniform notation that will provide us with a tableau system.

In tableau systems proofs (or derivations) are written in tree form, branching downward. At each node of the tree occurs a signed formula. An attempted proof of A begins with a one-branch, one-node tree whose only node is -A. Then the tree is enlarged using certain extension rules. For example, if +(A & B) occurs on a branch, +A and +B may be added to the end of the branch. As another example, if +(A $\forall$ B) occurs on a branch, the end of the branch may be split into a left and a right continuation and +A added to the end of the left fork, and +B to the end of the right. The full set of branch extension rules will be given latter. A branch is called closed if it contains +A and -A for some formula A. A tableau (or tree) is called closed if each branch of it is closed. A closed tableau for -A is, by definition, a proof of A.

One may think of a tableau for -A as an exploration of a hypothetical counter-model to A: if one had -A what else would one have. A closed tableau for -A is the verification that there are no counter-models to A, hence A must be valid. In other words, beginning a tableau proof of A by putting down -A amounts to supposing there is a world in which A is not forced (in this

world $w \in G$, $w \Vdash A$); an ensuing contradiction will tell us A is forced everywhere, i.e. A is intuitionistically valid.

Before we present the full set of tableau rules some previous comments about how these rules are obtained are made. The conditions R1 - R4 of the last section suggest that for regular connectives we can adopt rules similar to the classical ones. The special connectives need a more careful treatment. We see that condition S1 give us information, not about the world w, but about some world w* acessible from w. We jump from one world to another when this condition is applied. Next we investigate what information we may take with us in such a jump. We note that condition C1 can be generalized. If $\langle G,R,P,\Vdash\rangle$ is an intuitionistic model and w G then: if $w \Vdash A$ then $w^* \Vdash A$ for all formulas A. This is proved by induction on the degree of A, using the properties of the R relation for intuitionistic models. Thus, to see what information we may take along if we move from w to w* we define the set of the positively signed formulas of X as

$$X^+ := \{+A \mid +A \in X\} .$$

Then we see that in an intuitionistic model if $w \Vdash X$ then $w^* \Vdash X^+$. This is proved by the generalization of condition C1.We conclude that we may take with us positive but not negative information. A similar argument is applicable to the condition S4. If X is the set of signed formulas on the branch, we replace it by X^+. So we get a rether convenient way of schematizing these critical rules (for special and special) latter. The condition S2 offers much less trouble because the special β formulas are positively signed. Then

$$w \Vdash \beta \quad \text{iff } (\forall w^*)\ (w^* \Vdash \beta) \quad (\beta \text{ is positive})$$
$$\text{iff } (\forall w^*)\ (w^* \Vdash \beta_1 \text{ or } w^* \Vdash \beta_2) \quad (\text{by R2})$$

and only the condition R2 is sufficient for the special β formulas. A similar argument is applicable to the condition S3.

In addition a certain infinite set of formal constants C_0 and a disjoint set P_0 of parameters are introduced to characterize the language $L(C_0 \cup P_0)$ of formal proofs. Note that tableau proofs will be of sentences of $L(C_0)$, tableau derivations will be from sets of sentences of $L(C_0)$, but in tableaus sentences of $L(C_0 \cup P_0)$ may be used.

The full set of intuitionistic brach extension rules is given by:

$$(\&+)\quad \frac{+(A \,\&\, B) \in X}{X \cup \{+A,\ +B\}} \qquad (\vee+)\quad \frac{+(A \mid B)\quad X}{X \cup \{+A\} \mid X \cup \{+B\}}$$

$$(\vee-)\quad \frac{-(A \mid B) \in X}{X \cup \{-A,\ -B\}} \qquad (\&-)\quad \frac{-(A \,\&\, B) \in X}{X \cup \{-A\} \mid X \cup \{-B\}}$$

$$(\supset-)\quad \frac{-(A \supset B) \in X}{X^{+} \cup \{+A,\ -B\}} \qquad (\supset+)\quad \frac{+(A \supset B)\quad X}{X \cup \{-A\} \mid X \cup \{+B\}}$$

$$(\sim-)\quad \frac{-\ \sim A \in X}{X^{+} \cup \{+A\}} \qquad (\sim+)\quad \frac{+\ \sim A \in X}{X^{+} \cup \{-A\}}$$

$$(\forall+)\quad \frac{+(\forall x)\ A(x)\quad X}{X \cup \{+A(a)\}} \qquad (\forall-)\quad \frac{-(\forall x)\ A(x)\quad X}{X \cup \{-A(\underline{a})\}}$$

$$(\exists-)\quad \frac{-(\exists x)\ A(x)\quad X}{X \cup \{-A(a)\}} \qquad (\exists+)\quad \frac{+(\exists x)\ A(x)\quad X}{X \cup \{+A(\underline{a})\}}$$

where $X^{+} := \{+A \mid +A \in X\}$, $a \in C_0 \cup P_0$ is any constant and $\underline{a} \in P_0$ is any new parameter, where new means new to the branch.

It is known that this tableau system is sound and complete [Fitting 1983]: a formula A has an intuitionistic Beth tableau proof iff A is valid in all intuitionistic first-order models.

As an example we apply this intuitionistic tableau system to the formula $\sim\sim(\sim p \vee p)$:

$$
\begin{array}{lll}
- \sim\sim(\sim p \vee p) & (1) & (\sim -) \\
+ \sim (\sim p \vee p) & (2) & (\sim +) \\
+ \sim (\sim p \vee p),\ -\sim p \vee p & (3) & (\mid -) \\
+\sim(\sim p \vee p),\ -\sim p \vee p, -\sim p, -p & (4) & (\sim -) \\
+\sim(\sim p \vee p),\ +p & (5) & (\sim +) \\
+\sim(\sim p \vee p),\ -\sim p \vee p,\ +p & (6) & (\mid -) \\
+\sim(\sim p \vee p),\ -\sim p \vee p, -\sim p, -p, +p & (7) &
\end{array}
$$

We use also the following notation for rule applications:

$$X \xrightarrow{(\mu, +/-)} Y$$

where X and Y are signed formula sets and μ and +/- are a formula main connective/operator and a formula polarity, respectively.

By the number of choice points a particular formula X has we mean the number of rules that can be applied to this set. For example, if $X = \{+(p \,\&\, q),\ -(p \vee q)\}$, then the rules (&+) and ($\vee$-) are applicable to X. Thus, we say that X has two choice points for rule applications.

III A PROOF SYSTEM FOR THE TABLEAU CALCULUS

A direct implementation of the above presented tableau calculus would lead to several problems concerning efficiency:

(1) The non-crucial rules are adding formulas to the formula set X, e.g., the rule (&+) adds +p and +q to X if + (p & q) occurs in X;

(2) In general there are several elements in a set to which the tableau rules are applicable. For example, consider the case when both rules (~+) and (~-) can be applied to the formula set $\{+\sim p, -\sim q\}$. This kind of indeterminism is increased still more by the first point;

(3) As a consequence of the crucial rules which are deleting formulas and the non-crucial rules we note that loop-checking must be considered in a theorem prover implementation. For example, the following sequence of rule applications yields a loop:

$$\{+\sim\sim p,\ +p\} \xrightarrow{(\sim+)} \{+\sim\sim p,\ +p,\ -\sim p\} \xrightarrow{(\sim-)} \{+\sim\sim p,\ +p\}$$

In the next sections these problems are tackled. Our considerations are divided into three parts. For the case of propositional logic we present pure replacement rules in such a way that problems (1) and (3) disappear. A rule strategy is given in order to keep the number of choice points small. In the next step we are concerned with the problem of proving a propositional formula under a theory. For that aim a proof search procedure is presented which chooses axioms from the theory in order to get a proof in a more systematic way. The

formulas of the predicate intuitionistic logic are investigated in the last section. Here the critical point is the problem of moving the quantifier in a systematic way. The method investigated for this case will turn out to be a generalization of the method presented in the last section.

III.1 THE PROPOSITIONAL LOGIC

The essential aim of this section is to change the tableau rules in such a way that they become pure replacement rules.For example, instead of

$$X \cup \{+\ p\ \&\ q\} \xrightarrow{(\&+)} X \cup \{+\ p\ \&\ q,\ +p,\ +q\}$$

we replace $+\ p\ \&\ q$ by $+p,\ +q$:

$$X \cup \{+\ p\ \&\ q\} \xrightarrow{(\&+)'} X \cup \{+p,\ +q\}$$

where now $(\&+)'$ is the improved tableau rule

$$(\&+)' \qquad \frac{+\ p\ \&\ q}{+p,\ +q}$$

But that change towards pure replacement rules does not work in all cases. The rule

$$(\sim+)' \qquad \frac{+\sim p}{-p}$$

is too weak, so that the tableau for example from section II does not close:

$-\ \sim\sim(\ p \vee \sim p)$	(1)
$+\ \sim\ (\ p \vee \sim p)$	(2)
$-\ \ \ (\ p \vee \sim p)$	(3)
$-p,\ -\ \sim p$	(4)
$+p$	(5)

The point is that in line (3) we have lost the information that $+\ \sim(\ p \vee \sim p)$ can be used once more in line (5). To compensate that loss of information we reformulate rule $(\sim+)'$

by:

$$(\sim+)' \qquad \frac{+\sim p}{-p^*}$$

The starred negatively signed formula $-p^*$ means that it can be carried over if a crucial rule is applied. And this is exactly what $+\sim p$ means: $+\sim p$ can be carried over if a crucial rule is applied. And after a crucial rule is applied, $+\sim p$ can be decomposed to $-p$. Consequently, the modified tableau rules can be written in the following way:

$$(\&+)' \quad \frac{+\ p\ \&\ q}{+p,\ +q} \qquad (\&-)' \quad \frac{-\ p\ \&\ q^{\,m}}{-p^m \mid -q^m}$$

$$(\vee+)' \quad \frac{+\ p\ \vee\ q}{+\ p \mid +q} \qquad (\vee-)' \quad \frac{-\ p\ \vee\ q^{\,m}}{-\ p^m, -\ q^m}$$

$$(\sim+)' \quad \frac{+\ \sim p}{-p^*} \qquad (\sim-)' \quad \frac{X \cup \{-\sim p^m\}}{X^+ \cup \{+p\}}$$

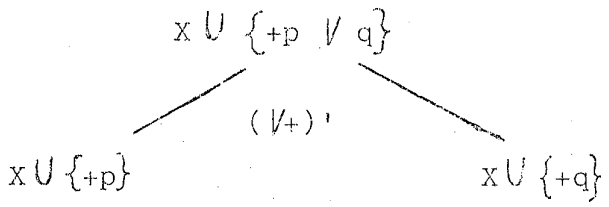
$$(\supset+)' \quad \frac{+\ p \supset q}{-p^* \mid +q} \qquad (\supset-)' \quad \frac{X \cup \{-\ p \supset q^{\,m}\}}{X^+ \cup \{+p,\ -q^m\}}$$

where $m \in \{'*', '\_'\}$ and

$$X^+ := \{+p \mid +p \in X\} \cup \{-p^* \mid -p^* \in X\} \ .$$

The modified rules call for some comments. Since we have two types of negatively signed formulas $-p$ and $-p^*$, we must define two rules for each negatively signed logical connective. This is done in a generic way by m which can be either '*' or '_'. Thus, $-p^m$ stands either for $-p^*$ or $-p^{'\_'}$ that is identified with $-p$. The branching rules effect that the remaining formulas

are carried over to each branch, e.g.



Note the new definition of X^+. For the crucial rules a different kind of notation was used in order to express that the non-starred negatively signed formulas must be deleted. Although the definition of X^+ was restated one might continue to think this set of formulas constitutes the information that we may take along when state transition occurs.

If the signed formula set X associated with a node of the tableau contains $+p^m$ and $-p^m$, then this branch of the tableau is called closed. The tableau for an arbitrary formula q is closed iff all it's branches are closed.

In order to solve the problem of the indeterminism of the application of the tableau rules we make the number of choice points of the formula set X smaller by the adoption of the following rule order:

$$(\&+)' < (\&-)' < (|+)' < (|-)' < (\sim+)' < (\sim-)'$$

In addition all these six rules are less than (~-) and (-).Thus in the tableau construction process the smaller rules are applied first. Moreover, if one of the six former rules is applicable to two (or more) different elements, one may assume that all sets of signed formulas are ordered in any way and take the first element. The two latter rules must be treated in another way. For them the previous solution does not hold and we have to retain all the choice points for their applications and consider the order in which these rules are applied essential because

when applied to a set X all negatively signed formulas in X are deleted.

We exemplify the use of backtracking in order to solve the indeterminism of the application of the crucial rules by applying the present procedure to the formula $(p \supset q) \vee (q \supset p)$:

$- (p \supset q) \vee (q \supset p)$	(1)	$(\vee-)'$
$- (p \supset q), -(q \supset p)$	(2)	$(\supset-)'$
$+ p, - q$	(3)	.

Note that the rule $(\supset-)'$ when applied to the first element of the set $\{- (p \supset q), - (q \supset p)\}$ gave a non-closed branch as can be seen by line (3). As the two choice points for the application of the rule $(\supset-)'$ are retained one can backtrack and find the other solution which is the same as the previous one with the exception that line (3) is substituted by:

$+ q, - p$	(3)'	.

As we got a non-closed tableau this formula is not valid in the intuitionistic propositional logic.

As another example we apply the proposed procedure to the formula $\sim\sim (\sim p \vee p)$ and compare this solution with the one given in section II.2 :

$- \sim\sim (\sim p \vee p)$	(1)	$(\sim-)'$
$+ \sim (\sim p \vee p)$	(2)	$(\sim+)'$
$- (\sim p \vee p)$	(3)	$(\vee-)'$
$-\sim p^* , -p^*$	(4)	$(\sim-)'$
$+ p, -p^*$	(5)	

We see that this proof has smaller length than the one presented before. This can be formally verified by giving a

translation function which transforms proofs obtained in the pure Beth system to proofs where the improved rule set is used and showing that in all cases the length of the former proofs is greater than the length of the latter ones.

It was shown [Bittel 1987] that these improved tableau rules are sound and complete and furnishes a more efficient tableau calculus than the ones presented in the literature ([Rautenberg 1979], [Fitting 1983]).

III.2 PROVING UNDER A THEORY

In this section we consider the typical theorem proving problem of knowing if a particular formula p is implied by a given set Γ of formulas (axioms) which are assumed to be valid. This is the same of knowing whether p is a theorem in the theory defined by Γ. Here we must check if

$$\bigwedge_{q \in \Gamma} q \supset p$$

is valid by trying to construct a closed tableau for this implication. But when we have a large set of axioms this way of proving is a very inefficient one as we know that only a few formulas of Γ are usually needed to show that p is a theorem. Next, in order to solve this problem, we present a proof search procedure which looks for the formulas needed in the proof process, i.e. to close as early as possible the intuitionistic propositional tableau. This proof search procedure is based on the modified tableau calculus given in the last section and consists of a goal-oriented, depth-first strategy with backtracking that accepts arbitrary formulas of the intuitionistic propositional logic.

We adapt here a proof procedure based on classical tableau calculus [Schoenfeld 1985] for knowledge bases consisting of arbitrary propositional formulas to the intuitionistic propositional logic. At each proof step, when a new formula is to chosen from the knowledge base, the procedure chooses in such a way that the search space is small.

First we present the following definitions. We say that a

branch of a tableau T crosses (a tableau) of a formula $q \in \Gamma$ if it contains as subpath a branch of the tableau for q. By a literal we mean a signed propositional variable indexed by m: $-p^m$. We say that two literals are linked if they form a connection, i.e. a pair $-a^m, +a^m$ where a is a propositional variable. We say that a literal is connected to a formula q if it is linked to some literal in q.

To know whether p is a theorem in the theory defined by Γ we can investigate the validity of the formula $(q_1 \& \ldots \& q_n) \supset p$. Applying the improved intuitionistic propositional tableau rules to it we get:

$$-(q_1 \& \ldots \& q_n) \supset p \qquad (1) \quad (\supset -)'$$
$$+(q_1 \& \ldots \& q_n), -p \qquad (2) \quad (\& +)'$$
$$+q_1, \ldots, +q_n, -p \qquad (3) \quad .$$

Thus we suppose that the order of Γ is not fixed and construct the tableaus for each of the formulas $+q_i$ $(1 \leq i \leq n)$. From these tableaus we can obtain a connection table showing to which formulas each literal in Γ is connected. This table associates literals in Γ to ordered formula sets C.

We start the tableau proof construction with the formula -p which is called the goal formula. Suppose that in the tableau generation process we reach a state where the tableau of another $q \in \Gamma$ has to be appended to a certain open branch θ. The idea is to choose one q so that at least one of the resulting branches contains a connection. Now, let q_j be the last formula crossed by θ, and let $\theta | q_j$ be the restriction of θ to q_j, i.e. that subpath of θ which is part of the tableau for q_j. Furthermore, let C be the set of all $q_k \in \Gamma$ such that q_k is connected to some literal on $\theta | q_j$ and q_k is not crossed by θ. C is ordered in a certain way, e.g. by respecting a

given order of Γ. This is used to organize backtracking. If backtracking occurs, the subtableau starting with the actually chosen $q_k \in C$ is removed, and the new subtableau is generated starting with the next $q_k \in C$. We say that the choice at q_j is altered. Backtracing means that we go upwards on θ up to the next q_k where such an altering of a choice is possible.

The presented proof procedure is sound and complete. Soundness follows from the fact that any tableau (by a strategy whatsoever) with allbranches closed by contradictions is a correct proof. To see completeness, note that it is guaranteed that all formulas in Γ are crossed exactly once by each open branch.

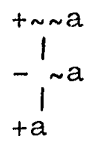
Consider the following example. Suppose the axiom set and the goal formula are given by:

$$\begin{aligned} \Gamma \quad : \quad & q_1 = \sim\sim a \\ & q_2 = b \supset a \\ & q_3 = c \supset b \\ & q_4 = d \,\&\, e \supset b \\ & q_5 = d \\ & q_6 = e \end{aligned}$$

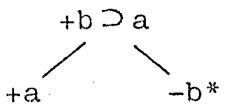
$$\text{Goal:} \quad p = a \ .$$

We want to know whether p is a theorem in the theory defined by Γ. First, we construct a tableau for each formula in this axiom set:

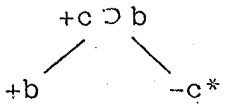
q_1 :



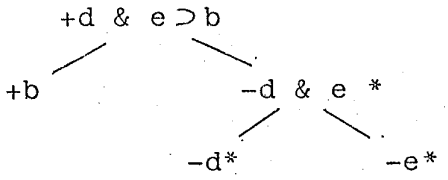
q_2 :



q_3 :



q_4 :



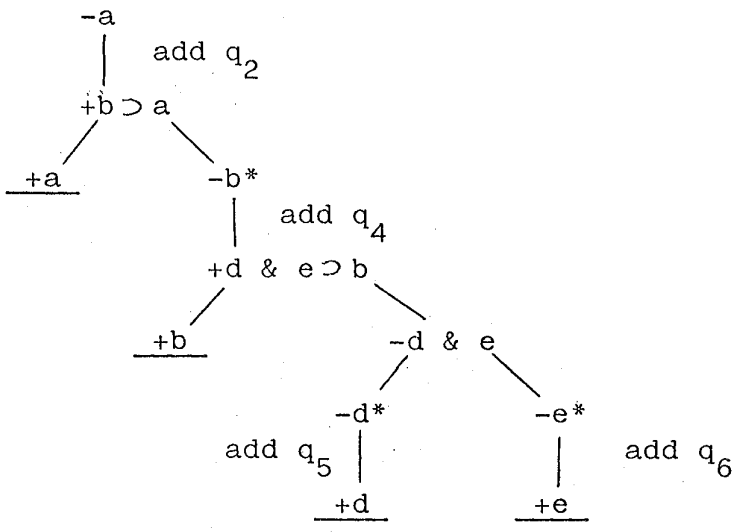
q_5 : +d

q_6 : +e

From these tableaus the following connection table is obtained. Note that this table associates literals in Γ to ordered formula sets C.

Literals	Formulas
-a	q_2
-a*	q_1, q_2
$-b^m$	q_3, q_4
$-d^m$	q_5
$-e^m$	q_6
+b	q_2
+c	q_3
+d	q_4
+e	q_4

Now the proposed proof procedure constructs the following closed tableau:



Note that we have marked the closed branches. Note also that -b* is connected to both the formulas q_3 and q_4. We have first added the formula q_3 reaching a state where the tableau could not be closed. Then backtracking occurs and the formula q_4 is added with success.

One might reformulate the above connection concept as follows. If we let θ be the actual open branch in a tableau and let $l_1 \in \theta$ be a literal in the last formula of θ, we say that a formula q is connected to l_1 by a literal l_2 if there is a path of l_1 in θ $P_1P_2\ldots P_n l_1$ and a path of l_2 in q $R_1R_2\ldots R_m l_2$ such that l_1 is linked to l_2.

III.3 THE QUANTIFIER RULES

In this section we generalize the intuitionistic proof procedure presented above to arbitrary intuitionistic first-order formulas.

We first present the whole proposed intuitionistic first-order branch extension rules which are all replacement rules as the ones in section III.1 :

Propositional Logic

$$(\&+)\quad \frac{+A \,\&\, B}{+A,\ +B} \qquad (\&-)\quad \frac{-A \,\&\, B^{\,m}}{-A^{m} \mid -B^{m}}$$

$$(\vee+)\quad \frac{+A \vee B}{+A \mid +B} \qquad (\vee-)\quad \frac{-A \vee B^{\,m}}{-A^{m}, -B^{m}}$$

$$(\sim+)\quad \frac{+\sim A}{-A^{m}} \qquad (\sim-)\quad \frac{\Gamma_1;\ X \cup -\sim A^{m}}{\Gamma_1^{+};\ X^{+} \cup \{+A\}}$$

$$(\supset+)\quad \frac{+A \supset B}{-A^{*} \mid +B} \qquad (\supset-)\quad \frac{\Gamma_1;\ X \cup -A \supset B^{\,m}}{\Gamma_1^{+};\ X^{+} \cup \{+A, -B^{m}\}}$$

where $m=\{'*','\_'\}$ and $X^{+} = \{X - \{-A \mid -A \in X\}$.

Quantifier Rules

$$(\forall+)\quad \frac{+(\forall x)A(x)\ ;\Gamma_1}{+A(a);\Gamma_1 \cup \{(\forall x)A(x)\}} \qquad (\forall-)\quad \frac{-(\forall x)A(x)^{m}\ \ X;|_1}{-A(\underline{a}) \cup X^{+};\Gamma_1^{+}}$$

$$(\exists+)\quad \frac{+\ (\exists x)A(x)}{+A(a)} \qquad (\exists-)\quad \frac{-(\exists x)A(x)^{m};\ \Gamma_1}{-A(\underline{a})^{m};\Gamma_1 \cup \{-(\exists x)A(x)^{m}\}}$$

where $a \in C_0 \cup P_0$ and $\underline{a} \in P_0$.

Axiom Introduction Rule

$$(\Gamma)\quad \frac{X\ ;\ \Gamma_1}{X \cup q\ ;\ \Gamma_1}$$

where $q \in \Gamma \cup \Gamma_1$.

We take Γ as a global axiom set; note that Γ occurs only in the axiom introduction rule. Here Γ_1 is a local axiom set that increases just in those rules in which multipliable formulas are decomposed. Negatively signed formulas in Γ must be deleted if a crucial rule is applied.

Before we give the new connection concept and the whole proof procedure description some previous definitions are necessary.

A formula tree for a signed formula is a variant of its formation tree containing additional information as to the polarity of its subformulas occurrences i.e. whether an occurrence of a subformula is negative or positive within the formula. In other words, it is built by the tableau rules but in chich all rules are taken as branching rules.

If $P_1P_2\ldots P_n l$ is a path from the root to a particular literal l in the formula tree for an arbitrary formula p, the subformula sequence is the path obtained by the previous one by keeping formulas only of the following forms:

$$+(\forall x)A \qquad -(\forall x)A^m \qquad -\sim A^m$$
$$+(\exists x)A \qquad -(\exists x)A^m \qquad -A \supset B^m \quad .$$

The deriving sequence of a literal l in a branch Θ of a tableau is either a used chain (that will be explained latter in the context of the connection concept) if there exists some, of simply the subformula sequence of l in the formula in which l occurs. The deriving sequence is computed during a tableau construction.

Now, let's see how the connection concept looks like. If we let Θ be an actual branch in a tableau and let $l_1 \in \Theta$ be a literal in the last formula of Θ and let l_2 be a literal in a formula q, we say that q is connected to l_1 by l_2 if the

following properties hold:

(i) the deriving sequence of l_1 in Θ is $P_1P_2\ldots P_{n-1}l_1$ and the subformula sequence of l_2 in q is $R_1R_2\ldots R_m l_2$;

(ii) there exists a most general unifier σ of l_1 and l_2 ;

(iii) there exists a merge $S_1S_2\ldots S_{m+n}$ of $P_1P_2\ldots P_n$ and $R_1R_2\ldots R_m$, such that

(a) $x \to y$, $S_i \in \{+(\exists x)A,\ -(\forall x)A\}$ and

$S_j \in \{+(\forall y)A,\ -(\exists y)A\} \implies S_i < S_j$;

(b) for all $P \in \{P_1,\ldots,P_n\} \cap \{-A \mid A \text{ is a formula}\}$ and

$PR_i\ldots R_{i+j} \preceq_m S_1\ldots S_{m+n} \Rightarrow$

($\preceq_m$ means the subsequence$_m$ relation)

$R_i,\ldots,R_{i+j} \notin \{-\sim A^m,\ -A \supset B^m,\ -(\forall x)A^m\}$;

(c) for all $R \in \{R_1,\ldots,R_m\} \cap \{-A\}$ and

$RP_1\ldots P_{i+j} \preceq_m S_1\ldots S_{m+n} \Rightarrow$

$P_i,\ldots,P_{i+j} \notin \{-\sim A^m,\ -A \supset B^m,\ -(\forall x)A^m\}$.

The ordered sequence of formulas $S_1S_2\ldots S_{m+n}1$ is called a chain of formulas. One minght think of this order as being the order of the rule applications in order to get a closed branch. In a further step we will show how this merge can be constructed.

Now we show how the whole proof procedure works. It can be summarized in the next six points:

1. Apply fist the non-crucial rules .
2. If there is a chain $F_1 < F_2 < \ldots < F_n$ then decompose F_1 and delete F_1 from the chain .
3. Now, apply the rules ($\sim$-) and ($\supset$-) if nothing is deleted.
4. Apply the rules ($\exists$+) and ($\forall$-) if nothing is deleted.
5. Apply the rules ($\forall$+) and ($\exists$-).
6. Choose indeterministically one of the crucial formulas and apply the corresponding rule to it,i.e. ($\sim$-), ($\supset$-) and ($\forall$-) or

choose a formula q from $\Gamma \cup \Gamma_1$ which is connected to one of the literals corresponding to the last formula . and add q to the tableau, where it is necessary, and go on from that position by using now the computed chain $F_1 < F_2 < \ldots < F_n$.

As an example consider the following formula to which we are going to apply the proposed proof procedure:

$$\sim\sim(\exists y)\ (\sim(\forall x)\sim\sim F(x) \supset \sim F(y)) \quad .$$

First, we construct its tableau:

P_1, Q_1	$-\sim\sim(\exists y)\ (\sim(\forall x)\sim\sim F(x) \supset \sim F(y))$	
	$+\sim(\exists y)\ (\ldots)$	
P_2, Q_2	$-(\exists y)\ (\ldots)^*$	
P_3, Q_3	$-\sim(\forall x)\sim\sim F(x) \supset \sim F(\underline{y})\ ^*$	$\Gamma_1 := -(\exists y)(\ldots)^*$
	$+\sim(\forall x)\sim\sim F(x)$	
Q_4	$-\sim F(\underline{y})^*$	
P_4	$-(\forall x)\sim\sim F(x)^*$	
	$+F(\underline{y})$	
P_5	$-\sim\sim F(\underline{x})$	
	$+\sim F(\underline{x})$	
	$-F(\underline{x})^*$	

The deriving sequences of $-F(\underline{x})^*$ and $+F(\underline{y})$ are $P_1P_2P_3P_4P_5$ and $Q_1Q_2Q_3Q_4$, respectively. Now we see that the subformula sequence of $+F(\underline{z})$ in $-(\exists y)(\ldots)^*$ is obtained as follows:

R_1	$-(\exists y)(\ldots)^*$
R_2	$-\sim(\forall x)\sim\sim F(x) \supset \sim F(\underline{z})^*$
R_3	$-\sim F(\underline{z})^*$
	$+F(\underline{z})$

and is given by $R_1R_2R_3$.

We note that there is a connection from $-F(\underline{x})^{*}$ to $+F(\underline{z})$ where the most general unifier is given by $\sigma(\underline{z}) = \underline{x}$ and as a result we get the chain $P_1P_2P_3P_4P_5R_1R_2R_3$. When the procedure is applied we are guided by the above order of rule applications.

As another example we consider the problem of knowing if the formula $\sim\sim(\forall x)\ A(x)\ \&\ B(x)$ is a theorem in the theory defined by the axiom set $\Gamma = \{\sim\sim(\forall y)A(y),\ \sim\sim(\forall z)B(z)\}$. First we construct the tableau for the goal formula:

P_1	$-\sim\sim(\forall x)A(x)\ \&\ B(x)$	
	$+\sim(\forall x)A(x)\ \&\ B(x)$	
P_2	$-(\forall x)A(x)\ \&\ B(x)$	
	$-A(\underline{x})\ \&\ B(\underline{x})$	
P_3	$-A(\underline{x})$	$-B(\underline{x})$ P_4

We note that the deriving sequences of $-A(\underline{x})$ and $-B(\underline{x})$ are $P_1P_2P_3$ and $P_1P_2P_4$, respectively. Now, we construct the tableaus for the formulas belonging to the axiom set:

	$+\sim\sim(\forall y)A(y)$		$+\sim\sim(\forall z)B(z)$
R_1	$-\sim(\forall y)A(y)^{*}$	S_1	$-\sim(\forall z)B(z)^{*}$
R_2	$+(\forall y)A(y)$	S_2	$+(\forall z)B(z)$
R_3	$+A(y)$	S_3	$+B(z)$

The subformula sequence of $+A(y)$ in the first formula and of $+B(z)$ in the second formula are given by $R_1R_2R_3$ and $S_1S_2S_3$, respectively. We see that there is a connection from $-A(\underline{x})$ to $+A(y)$ where the most general unifier is $\sigma(z)=\underline{x}$ and the chain $P_1R_1P_2R_2$ is obtained. From this chain we get the new tableau:

P_1 $-\sim\sim(\forall x)A(x) \;\&\; B(x)$

$+\sim(\forall x)A(x) \;\&\; B(x)$

add $+\sim\sim(\forall y)A(y)$

R_1 $-\sim(\forall y)A(y)$*

$+(\forall y)A(y)$

P_2 $-(\forall x)A(x) \;\&\; B(x)$*

$-A(\underline{x})$ $\qquad$ $-B(\underline{x})$

R_2 $+(\forall y)A(y)$

$\underline{+A(x)}$

Now the deriving sequence for $-B(\underline{x})$ is $P_1R_1P_2-B(\underline{x})$. We see that there is a connection from $-B(\underline{x})$ to $+B(z)$ where $\sigma(z)= \underline{x}$ and a resulting chain $P_1R_1S_1P_2S_2$ is obtained. Then we continue following the proof procedure in order to get a closed tableau.

IV CONCLUSION

In this work we have described an intuitionistic first-order proof procedure which is based on an improved version of the intuitionistic Beth tableau.

We note that because of the similarities between modal and intuitionistic logic, resolution proof systems (e.g. [Abadi 1986]) and matrix proof methods (e.g. [Bibel 1983] and [Wallen 1987]) for the modal logic S4 can be adapted to the intuitionistic logic. For example, if we take our special α formulas as the ν-type formulas of Wallen, our special β formulas as his π-type ones and change his path concept definition we get an intuitionistic matrix proof method. Note also that it is possible to generate connection calculi from tableau-based proofs([Wallen 1986]).

As future works some problems can be dealt with: the description of how the chain of formulas is constructed, the extension of the present proof procedure to limited second-order and the investigation of how a program can be constructed from such proofs (specially for program synthesis).

REFERENCES

[Abadi 1986] Abadi, M. and Manna, Z., Modal Theorem Proving, in J.H. Siekmann, editor, 8th International Conference on Automated Deduction, pages 172-189, July 1986. Lecture Notes in Computer Science, Volume 230, Springer-Verlag.

[Beth 1959] Beth, E. W., The Foundations of Mathematics, North-Holland Pub. Co., Amsterdam, 1959.

[Bibel 1983] Bibel, W., Matings in Matrices, Communications of the ACM 26, pp. 844-852, 1983.

[Bittel 1987] Bittel, O., A Theorem Prover for Intuitionistic Logic in ToolUse.T4, ESPRIT project, 1987.

[de Groote 1986] de Groote, Ph., Working Definition of a Kernel for a Design Calculus, Research Report in International Summer School of Programming and Calculi of Discrete Design, Marktoberdorf, 1986.

[Fitting 1983] Fitting, M. C., Proof Methods for modal and Intuitionistic Logics. Volume 169 of Synthese library, D.Reidel, Dordrecht, Holland, 1983.

[Rautenberg 1979]Rautenberg, W., Klassische und NichtKlassische Aussagenlogic, Braunscheig, 1979.

[Schoenfeld 1985] Schoenfeld, W., Prolog Extensions Based on Tableau Calculus, IJCAI, 1985.

[Sintzoff 1986] Sintzoff, M., Expressing Program Developments in a Design Calculus, Research Report in International Summer School of Programming and Calculi of Discrete Design, Marktoberdorf, 1986.

[Smullyan 1968] Smullyan, R. M., First-Order Logic. Volume 43 of Ergebnisse der Mathematik, Springer-Verlag, Berlin, 1968.

[Wallen 1986] Wallen, L. A., Generating Connection Calculi from Tableau- and Sequent-Based Proof Systems. In A. G. Cohn and J. R. Thomas, editors, Artifficial Intelligence and its Applications, pages 35-50, John Wiley & Sons Ltd., 1986.

[Wallen 1987] Wallen, L. A., Matrix Proof Methods for Modal Logics, IJCAI, 1987.