HERBRAND'S THEOREM FOR CALCULI OF SEQUENTS LK AND LJ

Gianluigi Bellin

University of Stockholm

Introduction. We give a simple proof of Herbrand's Theorem for Gentzen's Calculi of Sequents in the general case, without restriction to sequents containing only prenex formulas: this proof holds, with little modifications, both for the classical calculus LK and the intuitionistic calculus LJ. Since we deal with the general case, we must use different techniques from Gentzen's verschärfter Hauptsatz; we follow instead Herbrand's original proof more closely.

Herbrand's Theorem is a fundamental topic in Predicate Calculus, closely connected with several other basic results, for instance Cut-Elimination Theorem, Completeness Theorem, Hilbert's definition of quantification in terms of his ε-symbol and, finally, the proof procedures used in the Automatic Theorem Proving. Because of these connections, too many results are called Herbrand's Theorem today; first we give an informal account, with the attempt to make clear the connections and the differences between Herbrand's and Gentzen's results.

1. Given a formula A of Predicate Calculus, Herbrand constructs the sequence of domains $D_1, D_2, D_3, \ldots$ whose union is called Herbrand Universe or lexicon (relatively to A) and then the expansion $\mathcal{E}_p(A)$ of A over the domain D_p. There are two equivalent definitions of expansion; following the most famous one, $\mathcal{E}_p(A)$ is a disjunction of quantifier free formulas $A_1, A_2, \ldots, A_k$ whose variables are elements of D_p or terms built up with the elements of D_p.

I thank very much Prof. Dag Prawitz: he took care of me with a lot of patience. I thank also my friends in Padova, that gave me the ABC of logic: they try to study logic in the only possible way in Italy today, quite on the borders of the academic society.

Then Herbrand proves for classical logic in a Hilbert-type system:

(a) If $\vdash A$, then for some p $\mathcal{E}_p(A)$ is a tautology;

(b) If for some p, $\mathcal{E}_p(A)$ is a tautology, then there is a proof of A from $\mathcal{E}_p(A)$ in which no use is made of Modus Ponens.

Gentzen's verschärfter Hauptsatz gives, for classical sequents S containing only prenex formulas:

If $\vdash S$ then there is a cut-free proof of S of the shape

$$\begin{array}{c} \searrow \downarrow \swarrow \\ S' \\ \vdots \\ S \end{array}$$

where S' is a sequent containing no quantifiers and where all propositional inferences are above S' and all quantificational inferences are below S'.

The proof shows that it is always possible to permute the inferences of a cut-free proof of S in order to get a proof with this property.

Now we generalize the notion of expansion from formulas to sequents; (by a suitable renomination of the variables in the proof and) by adding, if necessary, some suitable quantifier free formulas to S' by Thinning, we obtain $\mathcal{E}_p(S)$ as midsequent; the new formulas disappear by Contraction after the quantification of their variables. It is not fussiness to note that, since the expansion $\mathcal{E}_p(S)$ is generated mechanically, it contains many formulas that are unnecessary in order to get a proof of S, while from Gentzen's Theorem we get more informations in order to single out the simplest midsequent S'; indeed Gentzen's Hauptsatz contains an analysis of the propositional inferences that lacks in Herbrand's Theorem.

Herbrand's Theorem holds for any formula A of the Predicate Calculus, Gentzen's verschärfter Hauptsatz for sequents S containing prenex formulas only; moreover Herbrand's expansion always separates the propositional and the quantificational parts of a proof, but this last property depends on a particularity of Herbrand's system. In fact Herbrand assumes among the primitive rules the so-called Rules of Passage, allowing to move quantifiers inside and outside a formula; hence proofs in his system have the canonical form:

$$\begin{array}{c} \mathcal{E}_p(A) \\ \vdots \\ Q_1x_1 \ldots Q_nx_n \ \mathcal{E}_p(A) \\ \vdots \\ A \end{array}$$

where first, we quantify universally or existentially the variables of $\mathcal{E}_p(A)$ and second, we obtain A by applying the Rules of Passage and then by eliminating redundant disjuncts inside a formula (Generalized Rule of Simplification).

However the use of the Rules of Passage has a very high price: firstly, a lot of complications arise in the proof of the theorem because of these rules (as Dreben and Denton experimented when they emended an error of Herbrand [DREBEN and DENTON 1966]); secondly, we cannot accept these rules if we want to prove the theorem for the intuitionistic case. Therefore we give up the Rules of Passage and consequently the property of the midsequent in the general case.

2. In the classical case, from Herbrand's Theorem we get a proof procedure for the Predicate Calculus; this procedure is complete in the sense that either (i) there exists a p such that $\mathcal{E}_p(A)$ is a tautology, or (ii) for all p, there is an assignment of truth-values to the atomic formulas of $\mathcal{E}_p(A)$ such that $\mathcal{E}_p(A)$ is false. It is well known [VAN HEIJENOORT 1967] that from Herbrand's Theorem we get Completeness Theorem just by showing that in the case (ii) it holds that (iii) A is falsifiable in a denumerable model (i.e. the set $\bigcup_{p \in N} D_p$ generated by A, with a suitable interpretation of the predicate letters, constants and functions of A).

The proofs of Completeness Theorem in Gentzen's type calculi (see for instance [KLEENE 1967]) are very elegant and straightforward; if we consider the proof procedure sketched there, however, we have to generate mechanically the subformulas of a quantified formula, as in Herbrand. The computer scientists have tackled the problem of a practical use of these procedures by giving several 'search strategies': the aim is plainly to avoid to test all the expansion $\mathcal{E}_p(A)$ for each p and to consider only the part of it that is really relevant for its validity [NILSSON 1971].

3. It is clear that from Completeness Theorem, formulated in the Calculus of Sequents, we get the Cut-Elimination Theorem as a corollary. Besides we could try to derive the Hauptsatz directly from Herbrand's Theorem: by the parts (a) and (b) together, if A is provable with Modus Ponens, then A is provable without Modus Ponens from a tautology $\mathcal{E}_p(A)$ for some p. However no treatment is given in Herbrand's work of the Cut-Elimination for propositional logic. Obviously what we obtain in this way is only a reduction of the Cut-Elimination to the Propositional Calculus.

On the contrary, our proof of Herbrand's Theorem is highly simplified having assumed the Cut-Elimination Theorem for predicate logic also.

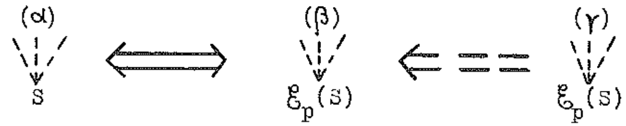
4. Gentzen's verschärfter Hauptsatz does not hold for LJ: as the counterexample $A(a) \vee A(b) \rightarrow \exists x A(x)$ shows, this depends on the non permutability of the inferences $\exists$:right/$\vee$:left [KLEENE 1952].

Of course the theorem holds for sequents whose antecedent is empty; moreover as the succedent of an intuitionistic sequent consists of at most one formula, we know immediately that $\exists x A(x)$ has one only ancestor $A(t)$.

It is evident that (as pointed out by [BOWEN 1976]) since Herbrand's Theorem holds intuitionistically for a sequent $\rightarrow A$ with A prenex, the theorem fails in general because of the intuitionistic invalidity of the Rules of Passage. But if A is

prenex, a very special property of intuitionistic logic is involved, i.e. A is decidable, and we do not suppose we shall prove so much when we try to prove Herbrand's Theorem for intuitionistic logic.

5. In order to do this, we use the alternative notion of expansion, defined by induction on the construction of the formulas. Then our method is the following: given a proof (α) in <u>LK</u> (<u>LJ</u>) of S we construct, by induction on the lenght of (α), a proof (β) of $\mathcal{E}_p(S)$ for some p in the propositional part of <u>LK</u> (<u>LJ</u>), and viceversa.



However, we cannot pass from <u>any</u> propositional proof (γ) of $\mathcal{E}_p(S)$ to a proof of S in <u>LK</u> (<u>LJ</u>); in order to construct such a proof of S we need to make the induction on a suitable proof (β) where the inferences are in a certain order, so that the applications of $\forall$: right and $\exists$: left can be carried out accordingly with the restrictions on the eigenvariables. By the Permutability Theorem [KLEENE 1952], in the classical case from any proof (γ) we can get a suitable proof (β); in the intuitionistic case, only from proofs that satisfy a certain condition and that we call <u>adequate</u>. It is easy to see that a propositional proof that is constructed by our method from a quantificational proof in <u>LJ</u> is always adequate.

It would be very interesting to express the peculiarity of the intuitionistic case by a condition on the expansions themselves instead of a condition on their proofs, i.e. to establish which kind of expansions do not have an adequate proof. We were unable to do this.

6. A proof of Herbrand's Theorem for intuitionistic logic in a manuscript of Beth (1956) is mentioned by [KREISEL 1958]. We were not able to find this proof.

In the literature Herbrand's Theorem is considered a a classical result that does not hold for intuitionistic logic. The whole idea of Herbrand's expansion is considered a finitistic version of model-theoretic concepts so that Herbrand's Theorem seems to be senseless without the classical notion of thruth (see for instance the edition of [HERBRAND 1971] by Goldfarb).

On the contrary our proof shows that any reference to the classical notion of truth is unnecessary for Herbrand's Theorem.

Definitions. Negation is defined ($\neg A$ is $A \supset \bot$). We denote always a sequent by $\Gamma \rightarrow \Delta$, where, for the intuitionistic case, Δ must contain at most one formula. We disregard the structural rules Contraction and Exchange, but it is intended that we are always able to find the ancestors and the descendants of a formula in a proof (as it is required for the proof of the Permutability Theorem). Therefore our only structural rule is Thinning (left and right). We assume that all the top sequents contain atomic formulas only.

Let us consider only sequents which contain no variable occurring both free and bound, and which contain no two occurrences of quantifiers with the same variable.

We define in a standard way the positive [negative] occurrences of a subformula in a sequent $\Gamma \rightarrow \Delta$. If A belongs to Δ then A is positive; if B belongs to Γ then B is negative. If C&D or CvD or $\forall xC(x)$ or $\exists xC(x)$ are positive [negative] then C and D or C(t) are positive [negative]. If $C \supset D$ is positive [negative] then D is positive [negative] and C is negative [positive].

Following Herbrand, we call a bound variable x and its quantifier Qx restricted if Qx is existential [universal] and its scope QxC(x) is positive [negative]; a variable y and its quantifier Qy (if any) are general either if y is free or if Qy is universal [existential] and its scope QyD(y) is positive [negative].

For any distinct general variable y_i in S we define the index function of y_i in S thus:

a) if y_i is free then the index function of y_i is y_i;

b) if y_i is bound and lies in the scope of the n ($n \geq 0$) restricted quantifiers $Qx_1, Qx_2, \dots, Qx_n$, then the index function of y_i is $y_i[x_1 x_2 \dots x_n]$.

The functional form $\mathfrak{F}(A)$ of a formula A in a sequent S is defined to be the expression obtained

a) by deleting all general quantifiers, and then

b) by replacing each general variable by its index function at each of its remaining occurrences.

The functional form $\mathfrak{F}(S)$ of a sequent S is the sequent obtained by replacing each formula of S by its functional form (in S).

Let $\mathfrak{IF}(S)$ be the finite set of all the index functions that occur in the functional form $\mathfrak{F}(S)$ of a sequent S. We define the finite sets $D_1^S, D_2^S, \dots$ by the following induction:

1) $D_1^S = \{1\}$

2) $D_{p+1} = D_p^S \cup \{y_i[t_{i,1} \dots t_{i,n}] : y_i[x_{i,1} \dots x_{i,n}]$ belongs to $\mathfrak{IF}(S)$ and $t_{i,1}, \dots, t_{i,n}$ belong to $D_p^S\}$.

We call the elements of the domains D_p^S functional terms; however a functional term must be considered as a variable, and it cannot be broken into its components.

A functional term that occurs in the domain D_p^S but not in the previous ones will be called of order p.

Now we define the p-th expansion $\mathcal{E}_p(S)$ of a sequent S over D_p^S as follows:

0) Change S into $\mathfrak{F}(S)$ (remember that only restricted quantifiers occur in $\mathfrak{F}(S)$). Then by induction on the subformulas of each $\mathfrak{F}(A)$ in $\mathfrak{F}(S)$:

1) if C is atomic, then take $\mathcal{E}_p(C) = \mathfrak{F}(C)$;

2) $\mathcal{E}_p(C \& D) = \mathcal{E}_p(C) \& \mathcal{E}_p(D)$; $\quad \mathcal{E}_p(C \vee D) = \mathcal{E}_p(C) \vee \mathcal{E}_p(D)$;

$\mathcal{E}_p(C \supset D) = \mathcal{E}_p(C) \supset \mathcal{E}_p(D)$;

3) $\mathcal{E}_p(\exists x C(x)) = \bigvee_{t \in D_p^S} \mathcal{E}_p(C(t))$; $\quad \mathcal{E}_p(\forall x C(x)) = \bigwedge_{t \in D_p^S} \mathcal{E}_p(C(t))$.

Here $\bigvee_{t \in D_p^S} \mathcal{E}_p(C(t))$ $\left[\bigwedge_{t \in D_p^S} \mathcal{E}_p(C(t))\right]$ is the finite disjunction [conjunction] of all the formulas that result from $\mathcal{E}_p(C(x))$ by replacing a $t \in D_p^S$ for x.

Let y be a general variable and let QyD(y) be its scope in S. Note that in $\mathcal{E}_p(S)$ several subformulas $\mathcal{E}_p(Qy(D(y)))$ can correspond to QyD(y), each of them having a different functional term in the place of y. We shall call these functional terms the functional terms of y.

Any sequence $S_1,\ldots,S_k$ of consecutive sequents in a branch of the proof-tree will be called a fragment (of the proof-tree).

Let S be any sequent containing a subformula QyD(y), with y general; let $\mathcal{E}_p(S)$ be the p-th expansion of S and let $\mathcal{E}_p(D(t_i))$ be an expansion of QyD(y) in $\mathcal{E}_p(S)$.

Now let us consider any cut-free proof (γ) of $\mathcal{E}_p(S)$. A fragment $S_1,\ldots,S_k$ of (γ) is crucial for (the quantification of the variable) t_i if $\mathcal{E}_p(D(t_i))$ occurs just once in each sequent $S_1,\ldots,S_k$ of the fragment, but only in S_1 as the principal formula of a rule application and only in S_k as the side formula of a rule application $\mathcal{R}_*$. Call $\mathcal{R}_*$ crucial rule application for t_i.

The end of this definition is clear: when we pass from a proof (α) of S to a proof of its expansion $\mathcal{E}_p(S)$, no inference corresponds in the new proof to any $\forall$:right or $\exists$:left application in (α). Conversely, when we pass from a proof (γ) of $\mathcal{E}_p(S)$ to a proof of S we do not find any instruction in (γ) for the $\forall$:right and $\exists$:left applications, but we know that such an inference with QyD(y) as principal formula can occur only in the part of the new proof corresponding to the crucial fragment for the variable t_i.

It can happen that there are several crucial fragments for t_i but only because of a branching in the proof. Note that if different occurrences of the same formula $\mathcal{E}_p(D(t_i))$ are concracted, then the sequent S_1 of the crucial fragment for t_i is the sequent that contains just one occurrence of $\mathcal{E}_p(D(t_i))$ as principal formula of the Contraction.

If in a proof (γ) of $\mathcal{E}_p(S)$ some $\bigvee_{t \in D_p^S} \mathcal{E}_p(C(t))$ or $\bigwedge_{t \in D} \mathcal{E}_p(C(t))$ comes from $\mathcal{E}_p(C(t_i))$ by repeated v:right or &:left applications then a critical fragment for t_i is defined to be the fragment of (γ) containing all the ancestors of $\mathcal{E}_p(C(t_i))$ in which t_i occurs.

Preliminaries. This is the basic condition for the "if" part of the theorem, both in the classic and intuitionistic cases:

(✱) A crucial fragment for the quantification of t_i is not included in a critical fragment for t_i.

It is easy to see that if the condition (✱) holds for any t_i then there is always in the fragment of the new proof corresponding to the crucial fragment for t_i a sequent where t_i occurs just once; at this point we can make the required $\forall$:right or $\exists$:left application accordingly with the restrictions on the eigenvariable.

By the Permutability Theorem, in the classical case we can always permute two propositional inferences: so from any proof (γ) of $\mathcal{E}_p(S)$ we can obtain a proof (β) having the property (✱) for all the crucial fragments, just by shifting the crucial inference for any t_i below all critical fragments for t_i.

But we have to show that there is a consistent procedure for making these permutations, i.e. a procedure that does not contain contradictory instructions.

In the classical case it can happen that a crucial fragment for t_i must be included in a critical fragment for t_j only when these conditions occur: t_i is a functional term of the variable y, t_j takes the place of the variable x and in S the scope of the quantifier Qy is included in the scope of the quantifier Qx.

By adapting an idea of Herbrand, we make this link explicit as follows.

Any array of functional terms preceded by a signe + or − and, possibly, connected with braces, will be called a schema.

We construct the schema of a proof (γ) of $\mathcal{E}_p(S)$ according to the following instructions:

i) if there is in (γ) a crucial fragment for t_i, write $+t_i$ in the schema;

ii) if there is in (γ) a critical fragment for t_j, write $-t_j$ in the schema;

iii) if the scope of the quantifier Qz, z corresponding to $\pm t_i$, lies in the scope of the quantifier Qw, w corresponding to $\pm t_j$, then write $\pm t_i$ on the right of $\pm t_j$;

iv) if two functional terms correspond to two disjoint quantifiers, then one term is below the other.

A brace can be introduced in order to make clear the dependence of several terms on one term.

For instance

$$+y_1 \left\{ \begin{array}{lll} -1 & +y_2[1] & -y_1 \\ & & \\ -y_2[1] & +y_2[y_2[1]] & -1 \end{array} \right.$$

is the schema of the following proof of $\mathcal{E}_2(S)$ with

$S: \forall y_1 \exists x_1 \forall y_2 \exists x_2 \left[P(x_1,y_1) \supset P(y_2,x_2)\right]$

$$\rightarrow P(1,y_1) \supset P(y_2[1],y_1),\ P(y_2[1],y_1) \supset P(y_2[y_2[1]],1)$$

$$\rightarrow P(1,y_1) \supset P(y_2[1],y_1),\ \bigvee_{u\in D_2^s}\left[P(y_2[1],y_1) \supset P(y_2[y_2[1]],u)\right]$$

$$\rightarrow P(1,y_1) \supset P(y_2[1],y_1),\ \bigvee_{t\in D_2^s}\ \bigvee_{u\in D_2^s}\left[P(t,y_1) \supset P(y_2[t],u)\right]$$

$$\rightarrow \bigvee_{u\in D_2^s}\left[P(1,y_1) \supset P(y_2[1],u)\right],\ \bigvee_{t\in D_2^s}\ \bigvee_{u\in D_2^s}\left[P(t,y_1) \supset P(y_2[t],u)\right]$$

$$\rightarrow \bigvee_{t\in D_2^s}\ \bigvee_{u\in D_2^s}\left[P(t,y_1) \supset P(y_2[t],u)\right],\ \bigvee_{t\in D_2^s}\ \bigvee_{u\in D_2^s}\left[P(t,y_1) \supset P(y_2[t],u)\right]$$

$$\rightarrow \bigvee_{t\in D_2^s}\ \bigvee_{u\in D_2^s}\left[P(t,y_1) \supset P(y_2[t],u)\right]$$

Now let us consider the order (see above) of the functional terms that occur in the schema of a proof: it is clear that if a negative term is of order p then all the positive

terms lying on its right have order higher than p.

We can easily establish a linear order between the functional terms of the array by ordering the lines of the schema as follows: let $t_1,\dots,t_k$ and $t'_1,\dots,t'_h$ be all the negative terms of two lines L_1 and L_2 and let $n_1,\dots,n_k$ and $m_1,\dots,m_h$ be the numbers of order of these negative terms. Then L_1 precedes L_2 if

i) either $\max(n_1\dots n_k) < \max(m_1\dots m_h)$

ii) or, if $\max(n_1\dots n_k) = \max(m_1\dots m_h)$, then $(n_1\dots n_k)$ precedes $(m_1\dots m_h)$ in the lexicographical order.

In our example, as $D_1 = \{1\}$, $D_2 = D_1 \cup \{y_1, y_2[1]\}$, the linear order of the terms of the schema is given by the sequence:

$$+y_1,\ -1,\ +y_2[1],\ -y_1,\ -y_2[1],\ +y_2[y_2[1]],\ -1$$

Now it is clear that we can permute the fragments in such a way that a fragment connected with the terms t is above all the fragment connected with the terms on the left of t.

Moreover it is clear that the proof obtained by these permutations necessarily satisfies the condition (✱): indeed if in the sequence there are two occurrences of the same term with different signes, then the rightmost occurrence has the signe − .

In the intuitionistic case there are the following exceptions to the permutability of propositional inferences: we cannot shift the following upper inferences $\mathcal{R}_a$ below the lower one $\mathcal{R}_b$

$\mathcal{R}_a$	⊃:left	$\mathcal{R}_a$	⊃:left or v:right
$\mathcal{R}_b$	⊃:right	$\mathcal{R}_b$	v:left

In this case we cannot obtain from any proof (γ) a proof (β) satisfying the condition (✱). Let us suppose that in an intuitionistic proof (γ) a crucial fragment for the quantification of t_i is included in a critical fragment for t_i.

Then we can shift the crucial inference $\mathcal{R}_*$ below the critical fragment only if it is not the case that

i) $\mathcal{R}_*$ is $\supset$:left and any application of $\supset$:right or of v:left occurs in the critical fragment below $\mathcal{R}_*$

ii) $\mathcal{R}_*$ is v:right and any application of v:left occurs in the critical fragment below $\mathcal{R}_*$.

Let us say that an intuitionistic proof (β) of $\mathcal{E}_p(S)$ is <u>adequate</u> if (β) satisfies the condition ($*$).

Then our procedure for the "if" part of the theorem in the intuitionistic case is the following. Given a sequent S and its p-th expansion $\mathcal{E}_p(S)$, for any p, first, by Gentzen's decision procedure for the propositional part of <u>LJ</u>, search for a proof of $\mathcal{E}_p(S)$. If for some p there is any proof (γ) of $\mathcal{E}_p(S)$, then consider if (γ) is adequate, or if from (γ) an adequate proof (β) can be obtained by suitable permutations.

For an instructive example, consider the following classi<u>c</u>ally but not intuitionistically provable - sequent S: $\forall x(A(x)vB) \rightarrow \forall yA(y)vB$, where, for the sake of simplicity, A(x) and B are atomic. Look at the following proof (γ) of $\mathcal{E}_2(S)$:

$$
\begin{array}{ll}
\text{v:right} & \dfrac{A(y)\rightarrow A(y)}{A(y)\rightarrow A(y)vB} \qquad \dfrac{B\rightarrow B}{B\rightarrow A(y)vB} \\
\text{v:left} & \dfrac{\qquad\qquad}{A(y)vB \rightarrow A(y)vB} \\
\text{\&:left} & \dfrac{\qquad\qquad}{(A(1)vB)\&(A(y)vB) \rightarrow A(y)vB}
\end{array}
$$

Here the crucial fragment for y (i.e. just the highermost sequent of the left branch) is included in a critical fragment for y. In the classical case we can shift the crucial inference v:right at the bottom of the proof, but in the intuitionistic case we cannot shift this inference below v:left. Therefore the above proof is intuitionistic, but not adequate.

<u>Herbrand's Theorem</u>. For all classical sequents S $\vdash_{\underline{LK}}$ S if and only if there exists a p such that $\mathcal{E}_p(S)$ is provable in the propositional part of <u>LK</u>.

For all intuitionistic sequents S $\vdash_{\underline{LJ}}$ S if and only if there exists a p such that $\mathcal{E}_p(S)$ is provable <u>with an adequate proof</u> in the propositional part of <u>LJ</u>.

PROOF. (If). By the preliminary discussion we consider both for the classical and the intuitionistic cases only proofs (β) that satisfy the condition ($*$). The Proof is by induction on the lenght of (β).

Clearly we have only to take in account the inferences of (β) in which a subformula of the shape $\mathcal{E}_p(QxC(x))$ or $\mathcal{E}_p(QyD(y))$ (with x restricted and y general) is firstly introduced as (a part of) the principal formula, as in the other cases nothing as to be changed.

Case I. If the expansion of a quantified formula is (a part of) a formula $\mathcal{E}_p(B)$ and

i) $\mathcal{E}_p(B)$ is the principal formula of a Thinning, or

ii) $\mathcal{E}_p(A)v\,\mathcal{E}_p(B)$ $[\mathcal{E}_p(A)\&\,\mathcal{E}_p(B)]$ is the principal formula of a v:right [&:left] whose side formula is $\mathcal{E}_p(A)$,

then

i) introduce B by Thinning

ii) introduce AvB [A&B] from A as side formula that is given by induction hypothesis.

Case II. $\mathcal{E}_p(QxC(x))$ is introduced from $\mathcal{E}_pC(t)$ by repeated applications of v:right [&:left]; then introduce QxC(x) by just an application of $\exists$:right [$\forall$:left] instead of these repeated propositional inferences.

Case III. The principal formula is $\mathcal{E}_p(QyDy)$, i.e. $\mathcal{E}_pD(t_i)$, so that the crucial fragment for t_i starts. Then we continue the construction accordingly with the precedent cases but we know that at a certain sequent $S^!_*$ of the new proof corresponding to a sequent S_* of the crucial fragment we have to introduce QyD(y) from $D(t_i)$ as side formula.

We know that (β) satisfies the conditions ($*$). (A critical fragment for t_i could begin inside the crucial fragment, because of an introduction of a formula containing t_i by

Thinning, but this case is treated as the case I). So let S_* be the first sequent of the crucial fragment such that all critical fragments for t_i and above it. We show that the corresponding sequent S'_* satisfies the conditions on the eigenvariable t_i.

Note that we use in the new proof the same names for the free variables as in (β); but (β) is cut-free and because of the Subformula Property the variables that occur in the proof occur in $\mathcal{E}_p(S)$ also.

Consider now any term t_j occurring in S'_*.

If in $\mathcal{E}_p(S)$ t_j is the functional term of a general variable y' different from y, then certainly $t_j \neq t_i$.

If in $\mathcal{E}_p(S)$ t_j takes the place of a restricted variable x of S, then S_* belongs to a critical fragment for t_j, so that necessarily $t_j \neq t_i$. (Indeed, let $QxC(x)$ be the scope of the restricted quantifier Qx: if $\mathcal{E}_p(D(t_i))$ is included in $\mathcal{E}_p(C(t_j))$ then t_i is of the shape $y[t_1 \ldots t_n t_j]$; if $\mathcal{E}_p(C(t_j))$ was included in $\mathcal{E}_p(D(t_i))$, t_j would have already disappeared in the new proof; if $\mathcal{E}_p(D(t_i))$ and $\mathcal{E}_p(C(t_j))$ are disjoint, $t_j \neq t_i$ is true by the condition (✱)).

(Only if). We need the following Lemma:

LEMMA I. If $\vdash \mathcal{E}_p(S)$, then $\vdash \mathcal{E}_*(S)$, where $\mathcal{E}_p(S)$ is the p-th expansion of S over D_p^S, and $\mathcal{E}_*(S)$ is an expansion of S over a D_* such that $D_p^S \subseteq D_*$

The proof is by induction on the cut-free proof (δ) of $\mathcal{E}_p(S)$.

The Theorem is proved by induction on the lenght of the cut free proof (α) of S. For the induction step we define a <u>strong analyzing function</u> for a rule of inference (see [DREBEN, DENTON and AANDERAA 1963]). The primitive recursive function χ is a strong analyzing function for the rule $\mathcal{R}$ if the following condition is satisfied: if S comes from S_1 [and S_2] by the rule $\mathcal{R}$, and if $\mathcal{E}_p(S_1)$ [and $\mathcal{E}_q(S_2)$] is [are] the provable

expansion [s] of the upper sequent [s] S_1 [and S_2], then $\mathcal{E}_{\chi(p)}(S)$ [$\mathcal{E}_{\chi(p,q)}(S)$] is a provable expansion of the lower sequent S.

We shall show that there exist strong analyzing functions for all the rules of inference of <u>LK</u> (<u>LJ</u>) (without Cut). This proves the Theorem, as the basis of the induction is trivial.

It is easy to see that Identity is a strong analyzing function for all the rules with one premise, <u>except $\exists$:right and $\forall$:left</u>; by using Lemma I we see that max(p,q) is a strong analyzing function for all the rules with two premises (except Cut).

LEMMA II. Successor is a strong analyzing function for $\forall$:left and $\exists$:right.

Let
$$S_1 \quad \frac{\Gamma, A(t) \rightarrow \Delta}{\Gamma, \forall x A(x) \rightarrow \Delta} \quad S \qquad \text{or} \qquad S_1 \quad \frac{\Gamma \rightarrow \Delta^\circ, A(t)}{\Gamma \rightarrow \Delta^\circ, \exists x A(x)} \quad S$$
(where Δ° is empty in the intuitionistic case)

be an application of $\forall$:left or $\exists$:right; by induction hypothesis we have a proof (δ) of $\mathcal{E}_p(S_1)$.

We must distinguish the cases: t occurs or t does not occur in S. If not, replace everywhere in (δ) the numeral 1 for t. Now t=1 occurs both in $D_p^{S_1}$ and in D_p^S, and the following argument holds again.

If some general quantifier lies in the scope QxA(x) of the restricted Qx introduced by this rule application, then the set of the index functions of S_1 is different from that of S, the former having some function $y_i[x_{i,1} \ldots x_{i,n}]$ where the latter has $y_i[x_{i,1} \ldots x_{i,n} x]$. (We consider this case only; otherwise the proof is trivial). So $D_i^{S_1} \neq D_i^S$ for $i \geq 2$.

But now substitute everywhere in (δ) $y_i[t_{i,1} \ldots t_{i,n} t]$ for $y[t_{i,1} \ldots t_{i,n}]$. We obtain a proof of the expansion $\mathcal{E}_*(S_1)$ over a domain D_* such that $D_* \subseteq D_{p+1}^S$. For instance, take the case of a variable y whose index function is y in S_1 and becomes $y[x]$ in S. So if the terms

$y, \quad y_i[\ldots y \ldots], \quad y_j[\ldots y_i[\ldots y \ldots] \ldots], \ldots$

that belong to $D_2^S, D_3^S, D_4^S, \ldots$ occur in $\mathcal{E}_p(S_1)$, then

$y[t]$, $y_i[\ldots y[t]\ldots]$, $y_j[\ldots y_i[\ldots y[t]\ldots]\ldots]$, ...
that belong to $D_3^S, D_4^S, D_5^S, \ldots$ will occur in $\mathcal{E}_*(S_1)$.

Now by the Lemma I and by repeated applications of &:left or v:right we get a proof of $\mathcal{E}_{p+1}(S)$.

It is immediate to see that the proof (β) of $\mathcal{E}_p(S)$ obtained by this procedure satisfies the condition ($*$), so that in the intuitionistic case (β) is adequate.

REMARK. The "only if" part of the proof is very similar to the original exposition of Herbrand. Lemma II is similar also to the Corollary 7(ii) of the Normal Form Theorem for Intuitionistic Logic in [PRAWITZ 1965].

E.W.BETH 1956
La crise de la raison et de la logique. Conférences, faites à l'Universitè de Liége dans le cadre des échanges culturels belgo-néerlandais au mois de Mai 1956. Paris-Louvain 1957

K.BOWEN 1976
An Herbrand Theorem for Prenex Formulas of LJ, Notre Dame Journal of Formal Logic

B.DREBEN, P.ANDREWS and S.AANDERAA 1963
False Lemmas in Herbrand, Bull.A.M.S. 69

B.DREBEN and S.AANDERAA 1964
Herbrand analyzing functions, Bull.A.M.S. 70

B.DREBEN and J.DENTON 1966
A supplement to Herbrand, J.S.L. 31

J.VAN HEIJENOORT (Editor) 1967
From Frege to Gödel: A source book in Mathematical Logic, 1879 - 1931, Cambridge Mass.

J.HERBRAND 1968
Écrits Logiques, J.VAN HEIJENOORT Editor, Paris

J.HERBRAND 1971
Logical Writings, W.D.GOLDFARB Editor, Cambridge Mass.

S.C.KLEENE 1952
Permutability of Inferences in Gentzen's Calculi LK and LJ Memoirs of A.M.S.

S.C.KLEENE 1967
Mathematical Logic, New York

G.KREISEL 1958
Review to BETH 1956 in J.S.L.

N.NILSSON 1971
Problem Solving Methods in Artificial Intelligence, New York

D.PRAWITZ 1965
Natural Deduction, Stockholm.