MATHEMATICS

1962

SovietRxiv

Abstract

Full Text

MATHEMATICS

G. E. Mints

AN ANALOGUE OF HERBRAND' S THEOREM FOR THE CONSTRUCTIVE PREDICATE CALCULUS

(Presented by Academician P. S. Novikov on 19 VI 1962)

1. The paper considers a sequent variant of the pure constructive (intuitionistic) predicate calculus, denoted below by G. In constructing formulas of the calculus, free variables $(x_1, x_2, \ldots)$ and bound variables $(y_1, y_2, \ldots)$ are used. The notion of a formula is defined in the same way as in (^{1}), with the addition of the following clause: if $A_1, A_2, \ldots, A_n$ are formulas, then $(A_1 \vee A_2 \vee \cdots \vee A_n)$ is a formula. All the rules of the intuitionistic calculus $G3$, described in (^{2}) (except the rule $(\rightarrow \vee)$), with the changes caused by the use of free and bound variables and of multiple disjunction, are rules of the calculus G. The rule $(\rightarrow \vee)$ of the calculus $G3$ is replaced by the sequence of rules:

$$(\rightarrow \vee_{n,i}) \quad \frac{\Gamma \rightarrow A_i}{\Gamma \rightarrow (A_1 \vee A_2 \vee \cdots \vee A_n)} \quad (n \geq 2;\ i \leq n).$$

All terms concerning the calculus G and not explained specially are understood in the same way as the corresponding terms concerning the calculus $G3$ are understood in (^{2}). Each time derivation and derivability are mentioned, derivation and derivability in the calculus G will be meant. Speaking of a derivation, we shall always assume that it is written in the form of a tree. The sign $\asymp$ will be used to denote graphical equality of words; the symbol $F_a^\alpha[R]$, where α is a bound variable and a is a free variable, denotes the result of substituting the variable a in R for all occurrences of α. The rules $(\forall \rightarrow)$ and $(\rightarrow \exists)$ will be called **minus-rules**, and the rules $(\rightarrow \forall)$ and $(\exists \rightarrow)$ **—plus-rules**.

2. Let $\{Q_1, Q_2, \ldots, Q_m\}$ $(m \geq 0)$ be a list of quantifiers, with $Q_{e_1}, Q_{e_2}, \ldots, Q_{e_r}$, where $r \geq 0$ and $e_1 < e_2 < \cdots < e_r \leq m$, being universal quantifiers, and all the other members of this list being existential quantifiers. For each s $(s \leq r)$, the complete enumeration of the universal quantifiers preceding the quantifier Q_{e_s} in the list $\{Q_1, \ldots, Q_m\}$ and arranged in increasing order of indices will be written in the form $\{Q_{d_1}, Q_{d_2}, \ldots, Q_{d_{k_s}}\}$.

Let $\{P_1, P_2, \ldots, P_\mu\}$ $(\mu \geq 0)$ also be a list of quantifiers, with $P_{\varepsilon_1}, P_{\varepsilon_2}, \ldots, P_{\varepsilon_\rho}$ $(\rho \geq 0;\ \varepsilon_1 < \varepsilon_2 < \cdots < \varepsilon_\rho \leq \mu)$ being existential quantifiers, and all the other members of the list $\{P_1, \dots, P_\mu\}$ being universal quantifiers. For each σ ($\sigma \leq \rho$), the complete enumeration of the universal quantifiers preceding in the list under consideration the quantifier P_{ε_σ} and arranged in increasing order of indices will be written in the form $\{P_{\delta_1}, P_{\delta_2}, \dots, P_{\delta_{k_{r+\sigma}}}\}$. Under these assumptions we introduce the following definition.

A **system of Skolem functions** for a prefix of the type

$$P_1 P_2 \dots P_\mu \to Q_1 Q_2 \dots Q_m$$

relative to a list of natural numbers $\{l_1, l_2, \dots, l_t\}$ $(t \geq 0)$

is called any list of arithmetic functions $\{f_1, f_2, \dots, f_r, f_{r+1}, \dots, f_{r+\rho}\}$ with numbers of arguments respectively $k_1, k_2, \dots, k_r, k_{r+1}, \dots, k_{r+\rho}$, satisfying the following conditions.

I. Whatever the numbers i and j $(i, j \leq r + \rho)$ and the collections of numbers $n_1, n_2, \dots, n_{k_i}$ and $\nu_1, \nu_2, \dots, \nu_{k_j}$ may be, the following assertions are true: a) $f_i(n_1, n_2, \dots, n_{k_i}) \neq l_\tau$ for all τ $(\tau \leq t)$; b) $f_i(n_1, \dots, n_{k_i}) \neq 1$; c) $f_i(n_1, \dots, n_{k_i}) \neq n_\chi$ for all χ $(\chi \leq k_i)$; d) if $i \neq j$, then $f_i(n_1, \dots, n_{k_i}) \neq f_j(\nu_1, \dots, \nu_{k_j})$; e) if $f_i(n_1, \dots, n_{k_i}) = f_i(\nu_1, \dots, \nu_{k_i})$, then $n_\chi = \nu_\chi$ for all χ $(\chi \leq k_i)$.

II. Whatever the lists of natural numbers $n_{11}, n_{21}, \dots, n_{i_1 1}; n_{12}, n_{22}, \dots, n_{i_2 2}; \dots; n_{1u}, n_{2u}, \dots, n_{i_u u}$ and functions $\varphi_1, \varphi_2, \dots, \varphi_u$ from the list $\{f_1, \dots, f_{r+\rho}\}$ may be, there exists a v $(v \leq u)$ such that $\varphi_v(n_{1v}, \dots, n_{i_v v})$ is different from all n_{qj} $(j \leq u;\ q \leq i_j)$.

For natural numbers define the relation of **subordination**:
a) if $p = f_i(n_1, \dots, n_{k_i})$, then for every χ $(\chi \leq k_i)$ the number n_χ is subordinated to p;
b) if $p = f_i(n_1, \dots, n_{k_i})$ and for some χ $(\chi \leq k_i)$ the number p' is subordinated to n_χ, then p' is subordinated to p.

Let A and B be formulas, $\alpha_1, \alpha_2, \dots, \alpha_m, \beta_1, \dots, \beta_\mu$ bound variables, $B \supset P_1\beta_1 P_2\beta_2 \dots P_\mu\beta_\mu B_0$, $A \supset Q_1\alpha_1 \dots Q_m\alpha_m A_0$, and suppose that neither A_0 nor B_0 contains quantifiers. Let $\{l_1, l_2, \dots, l_t\}$ $(t \geq 0)$ be the complete list of those numbers i such that the variable x_i occurs in the sequent

$$B \to A, \tag{1}$$

and let $\{f_1, \dots, f_r, f_{r+1}, \dots, f_{r+\rho}\}$ be some Skolem system of functions for the prefix of the type $P_1 \dots P_\mu \to Q_1 \dots Q_m$ with respect to the list $\{l_1, \dots, l_t\}$. Under these assumptions we introduce, by a single inductive definition, the functions I and $\mathfrak{S}$, the concept of a **number belonging to the lexicon of the sequent** (1), and the concept of a **regular list of natural numbers**. The functions I and $\mathfrak{S}$ will be defined for numbers from the lexicon of the sequent (1). Instead of the expression "the number n belongs to the lexicon of the sequent (1)" we shall write $n \in L$.

Definition. a) If $t > 0$, $\tau \leq t$, then $l_\tau \in L$, $I(l_\tau) = 1$, $\mathfrak{S}(l_\tau) = 0$; b) if $t = 0$, then $1 \in L$, $I(1) = 1$, $\mathfrak{S}(1) = 0$; c) if $n_1 \in L, n_2 \in L, \dots, n_q \in L$, and for any i, j, u, v from the fact that $i, j \leq q$, $u \neq v$, u is subordinated to n_i, v is subordinated to n_j, $u \in L$, $v \in L$, and $\mathfrak{S}(u) = \mathfrak{S}(v) = -1$, it follows that $I(u) \neq I(v)$, then $\{n_1, \dots, n_q\}$ is a regular list of numbers; d) if $\{n_1, n_2, \dots, n_{k_{r+\sigma}}\}$ $(0 \leq \sigma \leq \rho)$ is a regular list of numbers, then $f_{r+\sigma}(n_1, \dots, n_{k_{r+\sigma}}) \in L$, $I(f_{r+\sigma}(n_1, \dots, n_{k_{r+\sigma}})) = \max\{I(n_1), \dots, I(n_{k_{r+\sigma}})\}$, $\mathfrak{S}(f_{r+\sigma}(n_1, \dots, n_{k_{r+\sigma}})) = 1$; e) if $\{n_1, \dots, n_{k_s}\}$ $(s \leq r)$ is a regular list of numbers, $\max\{I(n_1), \dots, I(n_{k_s})\} \leq s$, then $f_s(n_1, \dots, n_{k_s}) \in L$, $I(f_s(n_1, \dots, n_{k_s})) = s$, $\mathfrak{S}(f_s(n_1, \dots, n_{k_s})) = -1$.

Let $q \leq m$, $n_1 \in L, n_2 \in L, \dots, n_q \in L$, and whatever s $(s \leq r)$ may be, if $e_s \leq q$, then $n_{e_s} = f_s(n_{d_1}, \dots, n_{d_{k_s}})$. Then the formula

$$\mathrm{F}^{\alpha_1 \alpha_2 \dots \alpha_q}_{x_{n_1} x_{n_2} \dots x_{n_q}} [\, Q_{q+1} \alpha_{q+1} \dots Q_m \alpha_m A_0 \,] \tag{2}$$

is called a **succedent q-example of the formula** A with respect to the sequent (1). Analogously, for any ξ not exceeding μ, the concept of an antecedent ξ-example of the formula B with respect to the sequent (1) is introduced. In what follows we shall omit, in the terms introduced here, the words "with respect to the sequent (1)." If $q = m$, then a succedent q-example of the formula A is called a **succedent lexical example** of the formula A. Analogous terminology is introduced in the case $\xi = \mu$.

Every sequent of the form

$$B_1,\ B_2, \dots,\ B_\lambda \to (A_1 \vee A_2 \vee \dots \vee A_l) \qquad (l + \lambda > 0), \tag{3}$$

where A_1 is a succedent q_1-example of the formula A; A_2 is a succedent q_2-example of the formula A; …; A_l is a succedent q_l-example of the formula A; B_1 is an antecedent-

antecedent ξ_1-example of the formula B; B_2 an antecedent ξ_2-example of the formula B; $\cdots$; B_λ an antecedent ξ_λ-example of the formula B, will be called the junction of partial examples of sequent (1). For each i $(i \leq l)$ denote by w_i the greatest of the numbers w satisfying the conditions $w \leq r$ and $e_w \leq q_i$.

Junction (3) is called regular if the following conditions are fulfilled: a) $w_i = w_j$, if $i, j \leq l$; b) $A_i \not\equiv A_j$, if $i, j \leq l,\ i \neq j$; c) $B_\eta \not\equiv B_\theta$, if $\eta, \theta \leq \lambda,\ \eta \neq \theta$; d) if the variable x_p occurs in junction (3) and the number u is subordinate to p, then x_u occurs in junction (3).

3. An application of a minus-rule of the calculus G is called normal if one of the following conditions is fulfilled: a) the (free) variable corresponding to the given application (see (2)) occurs in the conclusion; b) no free variable occurs in the conclusion of the application under consideration, and the variable corresponding to this application is x_1. A derivation is called normal if all applications of minus-rules in it are normal.

Let $\mathfrak{D}$ be a derivation whose last sequent is a junction of partial examples of sequent (1). An application of the rule $(\rightarrow \forall)$ in $\mathfrak{D}$ is called L-normal if

$$F^{\alpha_1 \dots \alpha_q}_{x_{n_1} \dots x_{n_q}} \left[Q_{q+1} \alpha_{q+1} \dots Q_m \alpha_m A_0 \right]$$

is the principal formula of this application, x_p is the variable corresponding to this application, $q + 1 = e_s$ for some s not exceeding r, and

$$p = f_s(n_{d_1}, n_{d_2}, \dots, n_{d_{k_s}}).$$

Applications of the rule $(\exists \rightarrow)$ in the derivation $\mathfrak{D}$ are defined analogously. The derivation $\mathfrak{D}$ is called lexical if it is normal and all applications of plus-rules in it are L-normal.

Theorem 1. For every derivation one can construct a normal derivation with the same last sequent.

Theorem 2. For every derivation whose last sequent is sequent (1), one can construct a lexical derivation with the same last sequent.

4. In this section $\mathfrak{D}$ denotes a derivation whose last sequent is junction (3).

An application of the rule $(\rightarrow \vee l, i)$ in the derivation $\mathfrak{D}$ is called a d-application if the following conditions are fulfilled: a) the succedent of the conclusion of this application is $(A_1 \vee A_2 \vee \dots \vee A_l)$; b) every occurrence of a sequent in the derivation $\mathfrak{D}$ lying below the premise of the rule application under consideration (with the exception of the last sequent of the given derivation) is either the right premise of an application of the rule $(\supset\rightarrow)$, or a premise (one of the premises) of an application of an antecedent rule different from $(\supset\rightarrow)$ and from $(\neg \rightarrow)$.

An occurrence of a sequent in the derivation $\mathfrak{D}$ is called a d-occurrence if it is a premise of some d-application. The derivation $\mathfrak{D}$ is called correct if below any d-application there are no applications of quantifier rules.

Let $s \leq r$, and let π be an application of a non-quantifier rule in the derivation $\mathfrak{D}$. π is called an s-singular application of a rule if above π there is at least one d-application, the principal formula of π is an antecedent lexical example of the formula B, and this lexical example contains a variable x_p such that $I(p) \geq s$.

Let $s \leq r$. The derivation $\mathfrak{D}$ is called s-regular if, whatever an s-singular application of a rule and a d-occurrence H_1 of the sequent

$$\Gamma \rightarrow F^{\alpha_1 \dots \alpha_q}_{x_{n_1} \dots x_{n_q}} \left[Q_{q+1} \alpha_{q+1} \dots Q_m \alpha_m A_0 \right]$$

and a d-occurrence H_2 of the sequent

$$\Sigma \rightarrow F^{\alpha_1 \dots \alpha_p}_{x_{\nu_1} \dots x_{\nu_p}} \left[Q_{p+1} \alpha_{p+1} \dots Q_m \alpha_m A_0 \right],$$

the following assertion is valid: if H_1 and H_2 lie above the s-singular application of the rule under consideration, $e_s \leqslant q$ and $e_s \leqslant p$, then $n_{e_s} = \nu_{e_s}$.

Definition. A derivation $\mathfrak{D}$ is called **regular** if the following conditions are satisfied: a) the junction (3) is regular; b) $\mathfrak{D}$ is regular and lexical; c) whatever s may be ($s \leqslant r$), $\mathfrak{D}$ is s-regular; d) if $l > 1$, then in $\mathfrak{D}$ there is at least one d-application of a rule.

Theorem 3. *For every derivation of the sequent (1) one can construct a regular derivation whose last sequent is some junction of lexical examples of the sequent (1).*

Theorem 4. *For every regular derivation of some junction of partial examples of the sequent (1), one can construct a derivation of the sequent (1).*

From Theorems 3 and 4 the following assertion is easily obtained.

Theorem 5. *The sequent (1) is derivable if and only if it is possible to specify some regularly derivable junction of its lexical examples.*

It is natural to regard Theorem 5 as an analogue of Herbrand' s theorem (see (^{3})) for the constructive predicate calculus.

Remark 1. One can construct an algorithm which determines, for any junction of lexical examples of a sequent of type (1), whether this junction is regularly derivable. For those sequents of type (1) for which $k_{r+1} = k_{r+2} = \dots = k_{r+\rho} = 0$, there can be only a finite number of junctions of lexical examples. Therefore for such sequents it is easy to construct a decision algorithm.

Remark 2. By modifying in the corresponding way the notion of a lexical example and the definition of regular derivability, one can formulate and prove an analogue of Theorem 5 for sequents of the form

$$\mathrm{B}_1, \mathrm{B}_2, \dots, \mathrm{B}_i \to (A_1 \vee A_2 \vee \dots \vee A_j) \qquad (i + j > 0), \tag{4}$$

where $\mathrm{B}_1, \mathrm{B}_2, \dots, \mathrm{B}_i, A_1, A_2, \dots, A_j$ are prenex formulas, and also obtain a decision algorithm for those sequents of type (4) in which all formulas $\mathrm{B}_1, \mathrm{B}_2, \dots, \mathrm{B}_i$ have prefixes of type $\exists^m \forall^n$.

In conclusion the author expresses gratitude to N. A. Shanin for his attention to the work and valuable advice.

Leningrad Branch
of the V. A. Steklov Mathematical Institute
Academy of Sciences of the USSR

Received
12 VI 1962

CITED LITERATURE

1. G. Gentzen, Math. Zs., **39**, 176 (1934).

2. S. K. Kleene, *Introduction to Metamathematics*, M., 1957.
3. J. Herbrand, Recherches sur la théorie de la demonstration, Warsaw, 1930.
4. T. Skolem, Norsk matematisk tidsskrift, **8**, 125 (1926).
5. W. V. Quine, J. Symbolic Logic, **20**, 2, 141 (1955).
6. H. Wang, Bell Syst. Techn. J., **40**, 4 (1961).

Note: Figure translations are in progress. See original paper for figures.