

On Gödel's theorem

By Toshio NISHIMURA

(Received Nov. 17, 1959)

Introduction

By applying precisely the arguments in Richard's paradox to a formal system \mathbf{P} K. Gödel [2] proved that, if \mathbf{P} satisfies certain conditions, then the following propositions hold.

PROPOSITION 1. *If \mathbf{P} is consistent, then \mathbf{P} is ω -incomplete.*

PROPOSITION 2. *If \mathbf{P} is consistent, then the statement ' \mathbf{P} is consistent' is not provable in \mathbf{P} .*

It is well known that conditions which must be satisfied by \mathbf{P} are satisfied by many formal systems, e. g. the system in Principia Mathematica and the system of Fraenkel-v. Neumann's axiomatic set theory. From the proposition 2 it is said that, if a system including the theory of natural numbers is wide enough, then the consistency proof of the system would be very hard.

However, we must notice that the concept of 'consistency' in metamathematics and that of 'consistency' used in Gödel's proposition 2 are not the same. In the proof of Gödel's proposition 2 Gödel formulated the statement 'a formal system \mathbf{P} is consistent' in a form $\forall xC(x)$. By Gödel's proposition 1 even if formulas $C(1), C(2), C(3), \dots$ are provable in \mathbf{P} , the formula $\forall xC(x)$ is not necessarily provable in \mathbf{P} . In order to prove in our proof-theory that the system is consistent it is sufficient to show that formulas $C(1), C(2), C(3), \dots$ hold, and it is not necessary to show that $\forall xC(x)$ holds.

In §1 we give a formal system \mathbf{P} . Let $\forall xC(x)$ be a formula to formulate in \mathbf{P} the proposition that \mathbf{P} is consistent. In §2 we prove that $C(1), C(2), C(3), \dots$ are provable in \mathbf{P} and $\forall xC(x)$ is not provable in \mathbf{P} if \mathbf{P} is consistent.

In §3 and §4 we give a consistency proof of \mathbf{P} in which the transfinite induction is not applied. Our proof is a modification of W. Ackermann's consistency-proof of \mathbf{P} [1].

§1. The formal system \mathbf{P} .

To clarify the distinction between the strong form and the weak form of consistency formulated in a formal system, we give a formal system \mathbf{P} as follows.

1. Symbols. \mathbf{P} contains following fundamental symbols: the particular

symbol $\mathbf{0}$, free variables for natural numbers a, b, c etc., bound variables x, y, z , etc., function symbols $', +$, etc., the predicate symbol $=$, logical symbols \neg, \vdash , ε -symbol ε , parentheses (and).

We sometimes use several letters for abbreviation.

2. *Formulas* and *terms* are constructed inductively as follows.

(1) The particular object $\mathbf{0}$ and free variables are terms. (2) If t is a term, then t' is a term. If s and t are terms, then $s+t$ and $s \cdot t$ are terms. (3) If s and t are terms, then $s = t$ is a formula. (4) If A is a formula, then $\neg A$ is a formula. If A and B are formulas, then $A \vdash B$ is a formula. (5) If $A(a)$ is a formula and x is a bound variable not contained in $A(a)$, then $\varepsilon_x A(x)$ is a term.

In particular term of the form $\mathbf{0}^{\overbrace{t' \dots t'}^n}$ is called a *numeral* representing n and denoted by n .

3. Axioms of P are divided into the following four groups.

I) Axioms for propositional logic

- (1) $A \vdash (B \vdash A)$
- (2) $(A \vdash (B \vdash C)) \vdash ((A \vdash B) \vdash (A \vdash C))$
- (3) $((\neg A) \vdash (\neg B)) \vdash (B \vdash A)$,

where A, B and C are arbitrary formulas.

II) Arithmetical axioms.

- (1) $t = t$
- (2) $s = t \vdash t = s$
- (3) $s = t \vdash (t = u \vdash s = u)$
- (4) $s' = t' \vdash s = t$
- (5) $s = t \vdash s' = t'$
- (6) $\neg t' = \mathbf{0}$,

where s, t and u are arbitrary terms.

III) Axioms for primitive recursive functions

In the following t_1, \dots, t_n and t are arbitrary terms.

- (1) $f_1(t) = t'$
- (2) $f_{2 \cdot 11^{n \cdot 13^q}}(t_1, \dots, t_n) = q$, where q is a numeral representing q .
- (3) $f_{3 \cdot 11^{n \cdot 13^i}}(t_1, \dots, t_n) = t_i$
- (4) $f_{5 \cdot 11^{k \cdot 13^{i_1} \dots p_{m+1}^{i_m}}}(t_1, \dots, t_n) = f_k(f_{i_1}(t_1, \dots, t_n), \dots, f_{i_m}(t_1, \dots, t_n))$

where p_1 is 11, p_2 is 13, p_3 is 17 etc.

- (5) $f_{7 \cdot 11^{k \cdot 13^k}}(0, t_2, \dots, t_n) = f_k(t_2, \dots, t_n)$
 $f_{7 \cdot 11^{k \cdot 13^k}}(t', t_2, \dots, t_n) = f_k(t, f_{7 \cdot 11^{k \cdot 13^k}}(t, t_2, \dots, t_n), t_2, \dots, t_n)$

IV) Axioms for ε -symbol

- (1) $A(t) \vdash (s = \varepsilon_x A(x) \vdash A(s))$
- (2) $A(t) \vdash \neg \varepsilon_x A(x) = t'$
- (3) $\neg A(\varepsilon_x A(x)) \vdash \varepsilon_x A(x) = \mathbf{0}$
- (4) $s = t \vdash \varepsilon_x A(x, s) = \varepsilon_x A(x, t)$

where $A(a)$ is an arbitrary formula, and s and t are arbitrary terms.

4. P contains rule of inference of the form

$$\frac{\underline{A} \quad A \vdash B}{B}$$

where A and B are arbitrary formulas.

5. The concept 'proof-figure' in P is defined recursively as follows.

(1) An axiom of P is a proof-figure to the axiom. (2) Let S and T are proof-figures to A and $A \vdash B$ respectively. Then the figure of the form

$$\frac{S \quad T}{B}$$

is the proof-figure to the formula B . If we have a proof-figure to a formula A , then we say that the formula A is *provable*.

6. We introduce some abbreviations. We write $\exists x A(x)$, $\forall x A(x)$, $A \vee B$ and $A \wedge B$ for $A(\varepsilon x A(x))$, $A(\varepsilon x \neg A(x))$, $(\neg A) \vdash B$ and $\neg(A \vdash (\neg B))$ respectively.

§ 2. The concept of 'consistency' and K. Gödel's theorem.

1. In the informal number theory we can arithmetize the formal system P in the well known method. Then fundamental symbols, terms, formulas and proof-figures in P are denoted by numbers in the informal number theory.

Meta-concepts 'to be a term', 'to be a formula' and 'to be a proof-figure' etc. are represented by primitive recursive number-theoretic predicates.

In particular we denote by $B(a, b)$ the meta-statement 'a number b is a proof-figure to a formula A represented by a number a '. Then, of course, the predicate $B(a, b)$ is primitive recursive.

2. Let the symbol 0 , the predicate symbol $=$, the function symbol $'$, the numeral n , logical symbols $\exists, \forall, \neg, \vdash, \wedge$ and \vee in P correspond to the number 0 , the predicate $=$, the function $'$, the number n and \exists (there exist), $()$ (for all), \neg (not), \rightarrow (implies), \wedge (and) and \vee (or) in the informal number theory.

Let the particular function $f_1, f_{2 \cdot 11^n \cdot 13^q}$ or $f_{3 \cdot 11^n \cdot 13^t}$ correspond to primitive recursive functions φ, ψ or χ such that $\varphi(x) = x'$, $\psi(x_1, \dots, x_n) = q$ or $\chi(x_1, \dots, x_n) = x_i$ respectively. Let the particular function $f_{5 \cdot 11^k \cdot 13^{i_1} \dots p_{m+1}^{i_m}}$ correspond to the primitive recursive function φ in the informal number theory such that $\varphi(x_1, \dots, x_n) = \psi(\chi_1(x_1, \dots, x_n), \dots, \chi_m(x_1, \dots, x_m))$ where f_k corresponds to ψ , and f_{i_1}, \dots, f_{i_m} correspond to χ_1, \dots, χ_m respectively. Moreover, let the particular function symbol $f_{7 \cdot 11^h \cdot 13^k}$ correspond to the primitive recursive function φ in the informal number theory such that $\varphi(0, x_2, \dots, x_n) = \psi(x_2, \dots, x_n)$ and $\varphi(y', x_2, \dots, x_n) = \chi(y, \psi(y, x_2, \dots, x_n), x_2, \dots, x_n)$ where f_h corresponds to ψ and f_k to χ .

Now let R be a predicate in the informal number theory, and \mathbf{R} be a formula in P constructed in the same manner as in R by combination of symbols, which correspond to symbols in R . Then \mathbf{R} is called the formula representing

in the formal system \mathbf{P} the predicate R in the informal number theory.

Then the following theorem holds.

THEOREM. *Let $R(a_1, \dots, a_m)$ be a primitive recursive predicate in the informal number theory. Let the formula $\mathbf{R}(b_1, \dots, b_m)$ be the formula in \mathbf{P} representing $R(a_1, \dots, a_m)$ in the informal number theory. Then for every m -tuple of numbers a_1, \dots, a_m it is true that if $R(a_1, \dots, a_m)$, then $\vdash \mathbf{R}(\mathbf{a}_1, \dots, \mathbf{a}_m)$ and if $\bar{R}(a_1, \dots, a_m)$, then $\vdash \neg \mathbf{R}(\mathbf{a}_1, \dots, \mathbf{a}_m)$. Here $\vdash \mathbf{A}$ means that \mathbf{A} is provable in \mathbf{P} .*

3. From 2 in this section, we can arithmetize \mathbf{P} in \mathbf{P} . That is, first we arithmetize expressions in \mathbf{P} and concepts on \mathbf{P} by numbers and predicates in the informal number theory respectively, and next we arithmetize by numerals and formulas representing them in \mathbf{P} .

Let $\mathbf{B}(\mathbf{a}, \mathbf{b})$ be the formula in \mathbf{P} representing $B(a, b)$ in the informal number theory. Then the following holds.

THEOREM. *For every pair of numbers a, b
if $B(a, b)$, then $\vdash \mathbf{B}(\mathbf{a}, \mathbf{b})$
and if $\bar{B}(a, b)$, then $\vdash \neg \mathbf{B}(\mathbf{a}, \mathbf{b})$.*

Now 'the formal system \mathbf{P} is consistent' is 'the formula $\mathbf{0}' = \mathbf{0}$ is not provable in \mathbf{P} '. When the formula $\mathbf{0}' = \mathbf{0}$ is arithmetized to a number κ in the arithmetization in the informal number theory, it is arithmetized to the numeral $\boldsymbol{\kappa}$ in the arithmetization in \mathbf{P} . Then the statement

'the formal system \mathbf{P} is consistent'

is represented by infinite propositions in the informal number theory

$$\bar{B}(\kappa, 0), \bar{B}(\kappa, 1), \bar{B}(\kappa, 2), \dots \dots \dots .$$

In the informal number theory the statement that the above infinite propositions are true is equivalent to $(x)\bar{B}(\kappa, x)$. Then we have the following theorem.

THEOREM. *If \mathbf{P} is consistent, then it is provable in \mathbf{P} that \mathbf{P} is consistent (in our sense), i. e.*

if $(x)\bar{B}(\kappa, x)$, then $(x)\vdash \neg \mathbf{B}(\boldsymbol{\kappa}, \mathbf{x})$.

COROLLARY. *If \mathbf{P} is ω -consistent, then the formula $\forall \mathbf{x} \neg \mathbf{B}(\boldsymbol{\kappa}, \mathbf{x})$ is undecidable, i. e. both $\forall \mathbf{x} \neg \mathbf{B}(\boldsymbol{\kappa}, \mathbf{x})$ and $\neg \forall \mathbf{x} \neg \mathbf{B}(\boldsymbol{\kappa}, \mathbf{x})$ are not provable in \mathbf{P} .*

PROOF. By K. Gödel's proposition 2 the formula $\forall \mathbf{x} \neg \mathbf{B}(\boldsymbol{\kappa}, \mathbf{x})$ is not provable in \mathbf{P} . By the above theorem and the ω -consistency of \mathbf{P} the formula $\neg \forall \mathbf{x} \neg \mathbf{B}(\boldsymbol{\kappa}, \mathbf{x})$ is not provable in \mathbf{P} .

§ 3. W. Ackermann's reduction for proof-figure in \mathbf{P} .

In this section we give W. Ackermann's reduction for proof-figure in \mathbf{P}

and some of its properties which were given in [1]. Proofs are omitted here.

1. We prove that the formula $0' = 0$ is not provable in P . That is, we show that, if p is any proof-figure in P , then p is not a proof-figure to $0' = 0$. In order to do so we substitute numerals for all terms so that terms of the same form are substituted by the same numeral and we reduce all axioms in p to true formulas. Then the consistency proof is finished.

2. Preliminary definitions.

A combination of symbols of the form $\varepsilon_x A(x)$ is called an ε -figure. If it is a term, then it is called an ε -term.

2.1. The *rank* of an ε -figure is defined as follows. If $A(x)$ contains no ε -figures of the form $\varepsilon_y B(y)$ which contain x , then the rank of $\varepsilon_x A(x)$ is one. If $A(x)$ contains ε -figures of the form $\varepsilon_y B(y)$ which contain x , then the rank of $\varepsilon_x A(x)$ is greater by one than the maximum of ranks of such ε -figures.

For example the rank of $\varepsilon_y (y' = \varepsilon_x (x = 0'))$ is one and the rank of $\varepsilon_x (x = \varepsilon_y (y = x))$ is two.

2.2. When $\varepsilon_x A(x)$ is an ε -term, we define the *fundamental type* (W. Ackermann's Grundtypus) belonging to $\varepsilon_x A(x)$ as follows. We arrange all terms in $A(x)$ such that each term is not a part of other terms.¹⁾ If s and t are terms of the same form and occur in different places in $A(x)$, then we take up them as different terms. Let these terms in $A(x)$ be t_1, \dots, t_n . Then $\varepsilon_x A(x)$ is of the form

$$\varepsilon_x B(x, t_1, \dots, t_n)$$

where $B(x, t_1, \dots, t_n)$ contains no terms except t_1, \dots, t_n indicated above. $\varepsilon_x B(x, a_1, \dots, a_n)$ is called the fundamental type belonging to $\varepsilon_x A(x)$, where a_1, \dots, a_n are arbitrary free variables. If $A(x)$ contains no terms, then the fundamental type belonging to $\varepsilon_x A(x)$ is $\varepsilon_x A(x)$ itself.

Then the rank of an ε -term $\varepsilon_x A(x)$ and that of the fundamental type belonging to it are the same.

3. Total substitution (W. Ackermann's Gesamtersetzung).

For the consistency proof of P it is sufficient to consider proof-figures which contain no free variables. Therefore we fix a proof-figure which contains no free variables and we define a total substitution for the proof-figure.

3.1. We consider the set of all fundamental types belonging to all ε -terms contained in the proof-figure. We extend the set so that, if $\varepsilon_x B(x, a_1, \dots, a_m)$ is a fundamental type contained in the set, then the set contains all fundamental types belonging to all ε -terms contained in $B(n, n_1, \dots, n_m)$ where n_1, \dots, n_m and

1) For example, the fundamental types of $\varepsilon_\eta (0' = \varepsilon_\beta (\beta < \eta''))$ and $\varepsilon_x (0'' < x \wedge \varepsilon_\eta (0'' + 0' = \eta) = x \vdash 0' < 0'')$ are $\varepsilon_\eta (a = \varepsilon_\beta (\beta < \eta''))$ and $\varepsilon_x (a < x \wedge \varepsilon_\eta (b = \eta) = x \vdash c < b)$ respectively.

\mathbf{n} are numerals. We arrange all fundamental types in an order such that a fundamental type with smaller rank is ordered before that with greater rank. Orders between fundamental types with the same rank are arbitrary, but we fix the sequence once for all.

Let it be

$$(1) \quad \varepsilon\mathbf{B}_1(\mathbf{x}, a_1, \dots, a_{m_1}), \dots, \varepsilon\mathbf{B}_r(\mathbf{x}, a_1, \dots, a_{m_r}).$$

In the following we call this sequence the \mathfrak{f} t-sequence.

3.2. We call an operation a *total substitution*, which substitutes a suitable function $\varphi(a_1, \dots, a_m)$ for every fundamental type $\varepsilon\mathbf{B}(\mathbf{x}, a_1, \dots, a_m)$ contained in the \mathfrak{f} t-sequence. Here if $\mathbf{n}_1, \dots, \mathbf{n}_m$ are numerals, then the numerical value of $\varphi(\mathbf{n}_1, \dots, \mathbf{n}_m)$ is calculable.

By a total substitution all ε -terms in the proof-figure are substituted by numerals in a manner such that the same ε -terms are substituted by the same numeral. Then it is clear that the axioms I), II), III) and IV) 4) are reduced to true formulas by any total substitution. Therefore it is sufficient that we construct a total substitution which reduces the axioms IV) 1), 2) and 3) to true formulas.

4. We define a sequence of total substitutions.

First we arrange all axioms of the form IV) 3) in \mathfrak{p} and let them be

$$(2) \quad \mathbf{A}_1(t_1) \vdash (\mathfrak{s}_1 = \varepsilon\mathbf{A}_1(\mathbf{x}) \vdash \mathbf{A}_1(\mathfrak{s}_1)), \dots, \mathbf{A}_\xi(t_\xi) \vdash (\mathfrak{s}_\xi = \varepsilon\mathbf{A}_\xi(\mathbf{x}) \vdash \mathbf{A}_\xi(\mathfrak{s}_\xi)).$$

4.1. The first total substitution τ_1 . By the first total substitution τ_1 we substitute the numeral $\mathbf{0}$ for fundamental types without arguments and substitute the function, the value of which is always zero, for fundamental types with arguments.

4.2. A total substitution τ is said to be *normal*, when it satisfies the following conditions: (1) if $\mathbf{n}_1, \dots, \mathbf{n}_m$ are arbitrary numerals and $\varepsilon\mathbf{B}(\mathbf{x}, \mathbf{n}_1, \dots, \mathbf{n}_m)$ is reduced by τ to a numeral \mathbf{n} which is not $\mathbf{0}$, then the formula $\mathbf{B}(\mathbf{n}, \mathbf{n}_1, \dots, \mathbf{n}_m)$ is reduced by τ to a true formula, and (2) for every numeral $\mathbf{n}^* (< \mathbf{n})$ the formula $\mathbf{B}(\mathbf{n}^*, \mathbf{n}_1, \dots, \mathbf{n}_m)$ is reduced by τ to a false formula.

Then it is clear that the first total substitution τ_1 is normal. Moreover by a normal total substitution the axioms IV) 2) and 3) are reduced to true formulas.

4.3. The $(i+1)$ -st total substitution τ_{i+1} .

We assume that the i -th total substitution τ_i is already defined and that τ_i is normal. Then we define the next total substitution τ_{i+1} .

If all the axioms of the form IV) 3) in \mathfrak{p} are reduced by τ_i to true formulas, then τ_i is the last total substitution and τ_{i+1} is not defined.

If we have an axiom of the form IV) 3) which is reduced by τ_i to a false formula, then we pick up the first of such one in the sequence (2). Let it be

$$A(t) \vdash (\mathfrak{s} = \varepsilon_{\mathfrak{x}} A(\mathfrak{x}) \vdash A(\mathfrak{s})),$$

and the fundamental type belonging to $\varepsilon_{\mathfrak{x}} A(\mathfrak{x})$ be

$$\varepsilon_{\mathfrak{x}} B(\mathfrak{x}, a_1, \dots, a_m).$$

Then $\varepsilon_{\mathfrak{x}} A(\mathfrak{x})$ is of the form

$$\varepsilon_{\mathfrak{x}} B(\mathfrak{x}, t_1, \dots, t_m),$$

and $A(t)$ is of the form

$$B(t, t_1, \dots, t_m).$$

If t_1, \dots, t_m and t are reduced by τ_i to numerals n_1, \dots, n_m and n respectively, then $B(n, n_1, \dots, n_m)$ is reduced by τ_i to a true formula and $\varepsilon_{\mathfrak{x}} B(\mathfrak{x}, n_1, \dots, n_m)$ to $\mathbf{0}$.

Now let $B(n^*, n_1, \dots, n_m)$ be the first formula reduced by τ_i to true formula in

$$B(\mathbf{0}, n_1, \dots, n_m), B(\mathbf{0}', n_1, \dots, n_m), \dots, B(n, n_1, \dots, n_m).$$

Then the total substitution τ_{i+1} is defined as follows: (1) for fundamental types before $\varepsilon_{\mathfrak{x}} B(\mathfrak{x}, a_1, \dots, a_m)$ in the $\mathfrak{f}t$ -sequence we substitute the same functions as in τ_i , (2) for fundamental types after $\varepsilon_{\mathfrak{x}} B(\mathfrak{x}, a_1, \dots, a_m)$ in the $\mathfrak{f}t$ -sequence we substitute functions which have always the value 0, and (3) for the fundamental types $\varepsilon_{\mathfrak{x}} B(\mathfrak{x}, a_1, \dots, a_m)$ we substitute the function $\varphi(a_1, \dots, a_m)$ where $\varphi(l_1, \dots, l_m)$ has the same value as in τ_i if the m -tuple l_1, \dots, l_m of numerals is distinct from n_1, \dots, n_m , and has the value n if l_1, \dots, l_m coincide with n_1, \dots, n_m .

5. Definitions with respect to a total substitution.

5.1. DEFINITION.

With a total substitution τ_i we have a fundamental type which is not substituted by the function the value of which is always zero. Then we have the last such fundamental type in the $\mathfrak{f}t$ -sequence. Let m be the number of the fundamental type counted from the last in the $\mathfrak{f}t$ -sequence. We call m the *characteristic number* of the total substitution τ_i .

5.2. DEFINITION.

Let $\mathfrak{s}_0, \dots, \mathfrak{s}_k$ be a sequence of ε -terms where if $i < j$, then \mathfrak{s}_j is not a part of \mathfrak{s}_i . Moreover we assume that the fundamental types belonging to ε -terms $\mathfrak{s}_0, \dots, \mathfrak{s}_k$ are contained in the $\mathfrak{f}t$ -sequence. Then these $\mathfrak{s}_0, \dots, \mathfrak{s}_k$ are reduced by a total substitution τ to numerals. Now we define a function φ such that $\varphi(i) = 1$ if \mathfrak{s}_i is reduced by τ to 0, otherwise $\varphi(i) = 0$. The number

$$2^k \cdot \varphi(0) + 2^{k-1} \cdot \varphi(1) + \dots + 2^0 \cdot \varphi(k)$$

is called the index of τ with respect to the sequence $\mathfrak{s}_0, \dots, \mathfrak{s}_k$.

If $\mathfrak{s}_0, \dots, \mathfrak{s}_k$ are all ε -terms contained in \mathfrak{p} , then the index of τ with respect to the sequence $\mathfrak{s}_0, \dots, \mathfrak{s}_k$ is called the *first index* of τ .

Let $A(t) \vdash (\mathfrak{s} = \varepsilon_{\mathfrak{x}} A(\mathfrak{x}) \vdash A(\mathfrak{s}))$ be the first formula in the sequence (2) which is reduced by τ to a false formula, and $\varepsilon_{\mathfrak{x}} B(\mathfrak{x}, a_1, \dots, a_m)$ be the fundamental

type belonging to $\varepsilon_{\mathfrak{z}}\mathbf{A}(\mathfrak{z})$, where $\varepsilon_{\mathfrak{z}}\mathbf{A}(\mathfrak{z})$ is $\varepsilon_{\mathfrak{z}}\mathbf{B}(\mathfrak{z}, t, \dots, t_m)$. If $\mathfrak{s}_0, \dots, \mathfrak{s}_k$ are all ε -terms contained in $\mathbf{B}(\mathbf{0}, \mathbf{n}_1, \dots, \mathbf{n}_m)$, $\mathbf{B}(\mathbf{0}', \mathbf{n}_1, \dots, \mathbf{n}_m)$, \dots , $\mathbf{B}(\mathbf{n}, \mathbf{n}_1, \dots, \mathbf{n}_m)$, then the index of τ with respect to $\mathfrak{s}_0, \dots, \mathfrak{s}_k$ is called the second index of τ , where $\mathbf{n}_1, \dots, \mathbf{n}_m$ and \mathbf{n} are numerals to which t_1, \dots, t_m and t are reduced by τ respectively.

When the first index of τ is a and the second index is b , then the pair (a, b) is called the *index* of τ .

When $\alpha = (a, b)$ and $\beta = (c, d)$, then $\alpha < \beta$ if and only if $a = c$ and $b < d$, or $a < c$.

6. Properties with respect to the sequence of total substitutions.

6.1. DEFINITION. A 1-series (W. Ackermann's 1-Reihe) of total substitutions is a total substitution itself. An $(m+1)$ -series (W. Ackermann's $(m+1)$ -Reihe) of total substitutions is a connected sequence $\tau_i, \tau_{i+1}, \dots, \tau_{i+k}$ of total substitutions in which the characteristic numbers of τ_i and τ_{i+k+1} are not smaller than $m+1$. Here if τ_{i+k} is the last total substitution, then the condition for τ_{i+k+1} is not needed. And if τ_i is the first total substitution τ_1 , then the condition for τ_i is not needed.

6.2. DEFINITION. Let \mathcal{E}_1 be an m -series of connected total substitutions $\kappa_1, \dots, \kappa_k$ the indices of which are $\alpha_1, \dots, \alpha_k$ respectively, and \mathcal{E}_2 be an m -series of connected total substitutions $\delta_1, \dots, \delta_l$ the indices of which are β_1, \dots, β_l respectively. Now if $\alpha_1 = \beta_1, \dots, \alpha_k = \beta_k$ and $k = l$, then we say that \mathcal{E}_1 is *equivalent* to \mathcal{E}_2 . If we have a j ($1 \leq j \leq k, 1 \leq j \leq l$) such that $\alpha_j > \beta_j$ and $\alpha_i = \beta_i$ for i as $i < j$, then we say that \mathcal{E}_2 is *strictly progressive* to \mathcal{E}_1 . Moreover we call δ_j the *total substitution distinguishing \mathcal{E}_2 from \mathcal{E}_1* .

6.3. DEFINITION. Let \mathcal{E}_1 and \mathcal{E}_2 be the same as in Definition 6.2. Let \mathcal{E}_1 consist of connected $(m-1)$ -series $\Phi_1, \Phi_2, \dots, \Phi_\mu$ and \mathcal{E}_2 consist of connected $(m-1)$ -series $\Psi_1, \Psi_2, \dots, \Psi_\nu$. We assume that \mathcal{E}_2 is strictly progressive to \mathcal{E}_1 , where δ_j in Ψ_γ is the total substitution distinguishing \mathcal{E}_2 from \mathcal{E}_1 . Then $\Phi_1, \dots, \Phi_{\gamma-1}$ are equivalent to $\Psi_1, \dots, \Psi_{\gamma-1}$ respectively and Ψ_γ is strictly progressive to Φ_γ and δ_j is the total substitution distinguishing Ψ_γ from Φ_γ . We call Ψ_γ the *$(m-1)$ -series distinguishing \mathcal{E}_2 from \mathcal{E}_1* .

6.4. THEOREM. Let \mathcal{E}_1 and \mathcal{E}_2 be two connected m -series and the characteristic number of the first total substitution of \mathcal{E}_2 be m . Then \mathcal{E}_2 is strictly progressive to \mathcal{E}_1 .

6.5. THEOREM. Let $\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3, \dots$ be connected m -series contained in an $(m-1)$ -series. Then \mathcal{E}_{i+1} is strictly progressive to \mathcal{E}_i for every i .

§ 4. Finiteness proof for the sequence of total substitutions.

If we have the last normal total substitution of the sequence of normal total substitution given in § 3, then all the axioms in \mathfrak{p} are reduced by the

total substitution to true formulas. Hence the consistency-proof is completed.

1. **PRINCIPAL THEOREM.** *The sequence of total substitutions given in §3 is finite.*

The theorem is proved from the following Theorems 2 and 3.

2. **THEOREM.** *Let $\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3, \dots$ be a sequence, connected or not, of m -series which occur in this order. If \mathcal{E}_{i+1} is strictly progressive to \mathcal{E}_i for every i , then the sequence is finite and we can give N such that \mathcal{E}_N is the last.*

Proof is given in 4.

3. **THEOREM.** *For every m an m -series contains only finite total substitutions.*

PROOF. When $m=1$, then an m -series contains only one total substitution from the definition of 1-series. Assuming that the theorem is already proved for m -series, we prove for $(m+1)$ -series. Let \mathcal{E} be an $(m+1)$ -series consisting of connected m -series $\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3, \dots$. From Theorem 6.5 in §3 \mathcal{E}_{i+1} is strictly progressive to \mathcal{E}_i for every i , so that the sequence of m -series is finite by Theorem 2 in this section. Let it be

$$\mathcal{E}_1, \mathcal{E}_2, \dots, \mathcal{E}_N.$$

By the assumption of the induction every \mathcal{E}_i contains only finite total substitutions. Therefore \mathcal{E} contains only finite total substitutions.

4. **PROOF OF THEOREM 2.**

We prove Theorem 2 by induction on m .

4.1. **LEMMA.** *Let $\kappa_1, \kappa_2, \kappa_3, \dots$ be a sequence of total substitutions the indices of which are $\alpha_1, \alpha_2, \alpha_3, \dots$ respectively. If $\alpha_1 > \alpha_2 > \alpha_3 > \dots$, then the sequence is finite, and we can give the N such that κ_N is the last total substitution.*

PROOF. We can easily prove this by double induction on the first index and the second index of total substitutions in this order.

4.2. By Lemma 4.1 the theorem is obtained in the case $m=1$. Assuming that the theorem is proved for m , we prove the theorem for $m+1$.

Now let $\mathcal{E}(1), \mathcal{E}(2), \mathcal{E}(3), \dots$ be a sequence of $(m+1)$ -series where $\mathcal{E}(i+1)$ is strictly progressive to $\mathcal{E}(i)$ for every i and $\mathcal{E}(i)$ consists of $\Phi(i, 1), \dots, \Phi(i, k_i)$: a sequence connected of m -series. Then we construct a sequence of finite sequences of the form

$$\Phi(1, 1), \Phi(h_2, i_2), \dots, \Phi(h_n, i_n)$$

of m -series such that it satisfies the following conditions 1), 2) and 3),

1) $1 \leq h_2 \leq \dots \leq h_n$ and $1 \leq i_2 \leq \dots \leq i_n$.

2) If $h_r < h_\xi$, then $\Phi(h_r, 1)$ is equivalent to $\Phi(h_\xi, 1), \dots$, and $\Phi(h_r, i_{r-1})$ is equivalent to $\Phi(h_\xi, i_{r-1})$. Moreover if $i_r < i_\xi$ and $\Phi(h_\xi, i_r)$ is not contained in $\Phi(1, 1), \Phi(h_2, i_2), \dots, \Phi(h_n, i_n)$, then $\Phi(h_r, i_r)$ is equivalent to $\Phi(h_\xi, i_\xi)$.

3) $\Phi(h_{j+1}, i_{j+1})$ is strictly progressive to $\Phi(h_j, i_j)$.

We construct the sequence. The first finite sequence of m -series consists only of $\Phi(1, 1)$. We assume that the n -th finite sequence of m -series is already defined so that the conditions 1), 2) and 3) are satisfied. Let it be

$$\Phi(1, 1), \Phi(h_2, i_2), \dots, \Phi(h_\kappa, i_\kappa).$$

Then we define the $(n+1)$ -st finite sequence of m -series. Let $\mathcal{E}(h_\kappa)$ be the last $(m+1)$ -series of $\mathcal{E}(1), \mathcal{E}(2), \dots$. If $\Phi(h_\kappa, i_\kappa)$ is the last m -series of $\mathcal{E}(h_\kappa)$, then the n -th finite sequence of m -series is the last, otherwise the $(n+1)$ -st finite sequence of m -series is

$$\Phi(1, 1), \Phi(h_2, i_2), \dots, \Phi(h_\kappa, i_\kappa), \Phi(h_\kappa, i_\kappa+1).$$

Next let $\mathcal{E}(h_\kappa)$ be not the last $(m+1)$ -series of $\mathcal{E}(1), \mathcal{E}(2), \dots$. Then we have the m -series distinguishing $\mathcal{E}(h_\kappa+1)$ from $\mathcal{E}(h_\kappa)$. Let it be $\Phi(h_\kappa+1, j)$.

(1) If $j = i_\kappa$, then the $(n+1)$ -st is

$$\Phi(1, 1), \Phi(h_2, i_2), \dots, \Phi(h_\kappa, i_\kappa), \Phi(h_\kappa+1, j)$$

which clearly satisfies the conditions 1), 2) and 3).

(2) If $j > i_\kappa$, then the $(n+1)$ -st finite sequence is

$$\Phi(1, 1), \Phi(h_2, i_2), \Phi(h_\kappa, i_\kappa), \Phi(h_\kappa, i_\kappa+1)$$

which clearly satisfies the conditions 1), 2) and 3).

(3) In the case where $j < i_\kappa$, let i_μ be the last of $1, i_1, \dots, i_\kappa$ such that $\leq j$. (We surely have such an i_μ because $1 \leq j$). Then $i_\mu < i_{\mu+1}, \dots, i_\kappa$.

(3.1) If $i_\mu < j$, then the $(n+1)$ -st finite sequence is

$$\Phi(1, 1), \Phi(h_2, i_2), \dots, \Phi(h_\mu, i_\mu), \Phi(h_\mu, i_\mu+1)$$

which clearly satisfies the conditions 1), 2) and 3).

(3.2) If $i_\mu = j$, then the $(n+1)$ -st finite sequence is

$$\Phi(1, 1), \Phi(h_2, i_2), \Phi(h_\mu, i_\mu), \Phi(h_\kappa+1, j)$$

which clearly satisfies the conditions 1), 2) and 3).

4.3. DEFINITION. We call i_κ the *rank* of a finite sequence of m -series $\Phi(1, 1), \Phi(h_2, i_2), \dots, \Phi(h_\kappa, i_\kappa)$. Now we rearrange the sequence of finite sequence of m -series given in 4.2 in this section into a double sequences as follows: (1) in the i -th row occur all finite sequences of m -series with the rank i and do not occur finite sequences of m -series with rank j ($\neq i$), and (2) in the i -th row the order between finite sequences of m -series are the same as in the sequence given in 4.2.

4.4. LEMMA. *The j -th finite sequence of m -series in the first row is of the form*

$$\Phi(1, 1), \Phi(h_2, 1), \dots, \Phi(h_j, 1).$$

PROOF. We prove by induction on j . If $j=1$, then the lemma is clear because the first is $\Phi(1, 1)$. Now let the j -th and $(j+1)$ -st of the first row be the

M -th and $(n+1)$ -st of the previous sequence respectively. Then the n -th of the previous sequence is of the form $\Phi(1, 1), \Phi(h_2, 1), \dots, \Phi(h_j, 1), \Phi(h_{i_\mu}, i_\mu), \dots, \Phi(h_{i_\kappa}, i_\kappa)$ where $1 < i_\mu, \dots, i_\kappa$. From the definition of the $(n+1)$ -st finite sequence, therefore, it is of the form

$$\Phi(1, 1), \Phi(h_2, 1), \dots, \Phi(h_j, 1), \Phi(h_{j+1}, 1).$$

4.5. Now we consider the sequence of m -series

$$\Phi(1, 1), \Phi(h_2, 1), \Phi(h_3, 1), \dots$$

where $\Phi(h_{i+1}, 1)$ is strictly progressive to $\Phi(h_i, 1)$, from the condition 3) and Lemma 4.4 in this section. By the assumption of the induction therefore the sequence is finite and we have the last m -series $\Phi(h_{N_1}, 1)$. Then the finite sequence of m -series

$$\Phi(1, 1), \Phi(h_2, 1), \dots, \Phi(h_{N_1}, 1)$$

is the last of the first row.

4.6. LEMMA. *We assume that the last finite sequence of the ξ -th row is given and it is*

$$\begin{aligned} &\Phi(1, 1), \Phi(h_2, 1), \dots, \Phi(h_{N_1}, 1), \Phi(h_{N_1+1}, 2), \dots, \Phi(h_{N_2}, 2), \\ &\dots, \Phi(h_{N_{\xi-1}+1}, \xi), \dots, \Phi(h_{N_\xi}, \xi). \end{aligned}$$

Then we have the last of the $(\xi+1)$ -st row and it is of the form

$$\begin{aligned} &\Phi(1, 1), \Phi(h_2, 1), \dots, \Phi(h_{N_1}, 1), \Phi(h_{N_1+1}, 2), \dots, \Phi(h_{N_2}, 2), \dots, \Phi(h_{N_{\xi-1}+1}, \xi), \\ &\dots, \Phi(h_{N_\xi}, \xi), \Phi(h_{N_\xi+1}, \xi+1), \dots, \Phi(h_{N_{\xi+1}}, \xi+1). \end{aligned}$$

PROOF. If $\nu \leq \xi$ and $h_{N_\xi} < \mu$, then $\Phi(\mu, \nu)$ is equivalent to $\Phi(h_{N_\xi}, \nu)$ from the assumption of the lemma and the condition 2).

Let the last of the ξ -th row be the M -th of the previous sequence. Then the first of $(\xi+1)$ -st row after the M -th of the previous sequence is of the form

$$\begin{aligned} &\Phi(1, 1), \Phi(h_2, 1), \dots, \Phi(h_{N_1}, 1), \Phi(h_{N_1+1}, 2), \dots, \Phi(h_{N_2}, 2), \\ &\Phi(h_{N_{\xi-1}+1}, \xi), \dots, \Phi(h_{N_\xi}, \xi), \Phi(h_{N_\xi+1}, \xi+1). \end{aligned}$$

Moreover we see that the i -th of the $(\xi+1)$ -st row after the M -th of the previous sequence is of the form

$$\begin{aligned} &\Phi(1, 1), \Phi(h_2, 1), \dots, \Phi(h_{N_1}, 1), \Phi(h_{N_1+1}, 2), \dots, \Phi(h_{N_2}, 2), \dots, \Phi(h_{N_{\xi-1}+1}, \xi), \\ &\dots, \Phi(h_{N_\xi}, \xi), \Phi(h_{N_\xi+1}, \xi+1), \dots, \Phi(h_{N_{\xi+i}}, \xi+1) \end{aligned}$$

in the same way as in the proof of Lemma 4.4 in this section. Then in the sequence

$$\begin{aligned} &\Phi(1, 1), \Phi(h_2, 1), \dots, \Phi(h_{N_1}, 1), \Phi(h_{N_1+1}, 2), \dots, \Phi(h_{N_2}, 2), \dots, \Phi(h_{N_{\xi-1}+1}, \xi), \\ &\dots, \Phi(h_{N_\xi}, \xi), \Phi(h_{N_\xi+1}, \xi+1), \dots, \Phi(h_{N_{\xi+n}}, \xi+1), \dots \end{aligned}$$

the $(i+1)$ -st m -series is strictly progressive to the i -th m -series for every i from

the condition 3). By the assumption of the induction the sequence is finite and the last finite sequence of the $(\xi+1)$ -st row is of the form

$$\begin{aligned} &\Phi(1, 1), \dots, \Phi(h_{N_i}, 1), \Phi(h_{N_{i+1}}, 2), \\ &\dots, \Phi(h_{N_i}, 2), \dots, \Phi(h_{N_{\xi+1}}, \xi+1), \dots, \Phi(h_{N_{\xi+1}}, \xi+1). \quad \text{q. e. d.} \end{aligned}$$

4.7. We consider the sequence of m -series $\Phi(1, 1), \Phi(h_2, 1), \dots, \Phi(h_{N_1}, 1), \Phi(h_{N_{i+1}}, 2), \dots, \Phi(h_{N_2}, 2), \dots$. Then the $(i+1)$ -st of the sequence is strictly progressive to the i -th. By the assumption of the induction therefore the sequence is finite and we have the last. Let the total sequence be

$$\begin{aligned} &\Phi(1, 1), \Phi(h_2, 1), \dots, \Phi(h_{N_1}, 1), \Phi(h_{N_{i+1}}, 2), \dots, \Phi(h_{N_2}, 2), \\ &\dots, \Phi(h_{N_{\lambda-1+1}}, \lambda), \dots, \Phi(h_{N_\lambda}, \lambda). \end{aligned}$$

It is clear that the sequence is the last of the λ -th row. Finally we show that $\Xi(h_{N_\lambda})$ is the last $(m+1)$ -series and $\Phi(h_{N_\lambda}, \lambda)$ is the last m -series of $\Xi(h_{N_\lambda})$. Let $\Xi(h_{N_\lambda})$ be not the last and $\Phi(h_{N_{\lambda+1}}, j)$ be the m -series distinguishing $\Xi(h_{N_{\lambda+1}})$ to $\Xi(h_{N_\lambda})$. Then $\lambda < j$. In fact, if $\lambda > j$, the j -th row is not finite, and if $\lambda = j$, the λ -th row is not finite. Then the $(M+1)$ -st finite sequence of m -series of the previous sequence is $\Phi(1, 1), \dots, \Phi(h_{N_\lambda}, \lambda), \Phi(h_{N_\lambda}, \lambda+1)$ and this is the finite sequence of the $(\lambda+1)$ -st row. This is a contradiction, and completes the proof of Theorem 2.

Hosei University, Tokyo

References

- [1] Ackermann, W., Zur Widerspruchsfreiheit der Zahlentheorie. Math. Ann., 117 (1940-41), 172-194.
- [2] Gödel, K., Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I, Monatsh. Math. Phys., 38 (1931), 173-198.