

CHAPTER 1

FIRST ORDER PREDICATE CALCULUS

In this chapter we shall present Gentzen's formulation of the first order predicate calculus **LK** (logistischer klassischer Kalkül), which is convenient for our purposes. We shall also include a formulation of intuitionistic logic, which is known as **LJ** (logistischer intuitionistischer Kalkül). We then proceed to the proofs of the cut-elimination theorems for **LK** and **LJ**, and their applications.

§1. Formalization of statements

The first step in the formulation of a logic is to make the formal language and the formal expressions and statements precise.

DEFINITION 1.1. A first order (formal) language consists of the following symbols.

- 1) *Constants*:
 - 1.1) Individual constants: $k_0, k_1, \dots, k_j, \dots$ ($j = 0, 1, 2, \dots$).
 - 1.2) Function constants with i argument-places ($i = 1, 2, \dots$): $f_0^i, f_1^i, \dots, f_j^i, \dots$ ($j = 0, 1, 2, \dots$).
 - 1.3) Predicate constants with i argument-places ($i = 0, 1, 2, \dots$): $R_0^i, R_1^i, \dots, R_j^i, \dots$ ($j = 0, 1, 2, \dots$).
- 2) *Variables*:
 - 2.1) Free variables: $a_0, a_1, \dots, a_j, \dots$ ($j = 0, 1, 2, \dots$).
 - 2.2) Bound variables: $x_0, x_1, \dots, x_j, \dots$ ($j = 0, 1, 2, \dots$).
- 3) *Logical symbols*:
 \neg (not), \wedge (and), \vee (or), \supset (implies), \forall (for all) and \exists (there exists). The first four are called propositional connectives and the last two are called quantifiers.
- 4) *Auxiliary symbols*:
(,) and , (comma).

We say that a first order language L is given when all constants are given. In every argument, we assume that a language L is fixed, and hence we omit the phrase "of L ".

There is no reason why we should restrict the cardinalities of various kinds of symbols to exactly \aleph_0 . It is, however, a standard approach in

elementary logic to start with countably many symbols, which are ordered with order type ω . Therefore, for the time being, we shall assume that the language consists of the symbols as stated above, although we may consider various other types of language later on. In any case it is essential that each set of variables is infinite and there is at least one predicate symbol. The other sets of constants can have arbitrary cardinalities, even 0.

We shall use many notational conventions. For example, the superscripts in the symbols of 1.2) and 1.3) are mostly omitted and the symbols of 1) and 2) may be used as meta-symbols as well as formal symbols. Other letters such as g, h, \dots may be used as symbols for function constants, while a, b, c, \dots may be used for free variables and x, y, z, \dots for bound variables.

Any finite sequence of symbols (from a language L) is called an *expression* (of L).

DEFINITION 1.2. *Terms* are defined inductively (recursively) as follows:

- 1) Every individual constant is a term.
- 2) Every free variable is a term.
- 3) If f^i is a function constant with i argument-places and t_1, \dots, t_i are terms, then $f^i(t_1, \dots, t_i)$ is a term.
- 4) Terms are only those expressions obtained by 1)–3). Terms are often denoted by t, s, t_1, \dots .

Since in proof theory inductive (recursive) definitions such as Definition 1.2 often appear, we shall not mention it each time. We shall normally omit the last clause which states that the objects which are being defined are only those given by the preceding clauses.

DEFINITION 1.3. If R^i is a predicate constant with i argument-places and t_1, \dots, t_i are terms, then $R^i(t_1, \dots, t_i)$ is called an *atomic formula*. *Formulas* and their outermost logical symbols are defined inductively as follows:

- 1) Every atomic formula is a formula. It has no outermost logical symbol.
- 2) If A and B are formulas, then $(\neg A)$, $(A \wedge B)$, $(A \vee B)$ and $(A \supset B)$ are formulas. Their outermost logical symbols are \neg , \wedge , \vee and \supset , respectively.
- 3) If A is a formula, a is a free variable and x is a bound variable not occurring in A , then $\forall x A'$ and $\exists x A'$ are formulas, where A' is the expression obtained from A by writing x in place of a at each occurrence of a in A . Their outermost logical symbols are \forall and \exists , respectively.
- 4) Formulas are only those expressions obtained by 1)–3).

Henceforth, $A, B, C, \dots, F, G, \dots$ will be metavariables ranging over formulas. A formula without free variables is called a *closed formula* or a

sentence. A formula which is defined without the use of clause 3) is called *quantifier-free*. In 3) above, A' is called the *scope* of $\forall x$ and $\exists x$, respectively.

When the language L is to be emphasized, a term or formula in the language L may be called an *L-term* or *L-formula*, respectively.

REMARK. Although the distinction between free and bound variables is not essential, and is made only for technical convenience, it is extremely useful and simplifies arguments a great deal. This distinction will, therefore, be maintained unless otherwise stated.

It should also be noticed that in clause 3) of Definition 1.3, x must be a variable which does not occur in A . This eliminates expressions such as $\forall x (C(x) \wedge \exists x B(x))$. This restriction does not essentially narrow the class of formulas, since e.g. this expression $\forall x (C(x) \wedge \exists x B(x))$ can be replaced by $\forall y (C(y) \wedge \exists x B(x))$, preserving the meaning. This restriction is useful in formulating formal systems, as will be seen later.

In the following we shall omit parentheses whenever the meaning is evident from the context. In particular the outermost parentheses will always be omitted. For the logical symbols, we observe the following convention of priority: the connective \neg takes precedence over each of \wedge and \vee , and each of \wedge and \vee takes precedence over \supset . Thus $\neg A \wedge B$ is short for $(\neg A) \wedge B$, and $A \wedge B \supset C \vee D$ is short for $(A \wedge B) \supset (C \vee D)$. Parentheses are omitted also in the case of double negations: for example $\neg\neg A$ abbreviates $\neg(\neg A)$. $A \equiv B$ will stand for $(A \supset B) \wedge (B \supset A)$.

DEFINITION 1.4. Let A be an expression, let τ_1, \dots, τ_n be distinct primitive symbols, and let $\sigma_1, \dots, \sigma_n$ be any symbols. By

$$\left(A \frac{\tau_1, \dots, \tau_n}{\sigma_1, \dots, \sigma_n} \right)$$

we mean the expression obtained from A by writing $\sigma_1, \dots, \sigma_n$ in place of τ_1, \dots, τ_n , respectively, at each occurrence of τ_1, \dots, τ_n (where these symbols are replaced simultaneously). Such an operation is called the (*simultaneous*) *replacement of (τ_1, \dots, τ_n) by $(\sigma_1, \dots, \sigma_n)$ in A* . It is not required that τ_1, \dots, τ_n actually occur in A .

PROPOSITION 1.5. (1) *If A contains none of τ_1, \dots, τ_n , then*

$$\left(A \frac{\tau_1, \dots, \tau_n}{\sigma_1, \dots, \sigma_n} \right)$$

is A itself.

(2) If $\sigma_1, \dots, \sigma_n$ are distinct primitive symbols, then

$$\left(\left(A \frac{\tau_1, \dots, \tau_n}{\sigma_1, \dots, \sigma_n} \right) \frac{\sigma_1, \dots, \sigma_n}{\theta_1, \dots, \theta_n} \right)$$

is identical with

$$\left(A \frac{\tau_1, \dots, \tau_n}{\theta_1, \dots, \theta_n} \right).$$

DEFINITION 1.6. (1) Let A be a formula and t_1, \dots, t_n be terms. If there is a formula B and n distinct free variables b_1, \dots, b_n such that A is

$$\left(B \frac{b_1, \dots, b_n}{t_1, \dots, t_n} \right),$$

then for each i ($1 \leq i \leq n$) the occurrences of t_i resulting from the above replacement are said to be indicated in A , and this fact is also expressed (less accurately) by writing B as $B(b_1, \dots, b_n)$, and A as $B(t_1, \dots, t_n)$. A may of course contain some other occurrences of t_i ; this happens if B contains t_i .

(2) We say that a term t is fully indicated in A , or every occurrence of t in A is indicated, if every occurrence of t is obtained by such a replacement (from some formula B as above, with $n = 1$ and $t = t_1$).

It should be noted that the formula B and the free variables from which A can be obtained by replacement are not unique; the indicated occurrences of some terms of A are specified relative to such a formula B and such free variables.

PROPOSITION 1.7. If $A(a)$ is a formula (in which a is not necessarily fully indicated) and x is a bound variable not occurring in $A(a)$, then $\forall x A(x)$ and $\exists x A(x)$ are formulas.

PROOF. By induction on the number of logical symbols in $A(a)$.

In the following, let Greek capital letters $\Gamma, \Delta, \Pi, \Lambda, \Gamma_0, \Gamma_1, \dots$ denote finite (possibly empty) sequences of formulas separated by commas. In order to formulate the sequential calculus, we must first introduce an auxiliary symbol \rightarrow .

DEFINITION 1.8. For arbitrary Γ and Δ in the above notation, $\Gamma \rightarrow \Delta$ is called a *sequent*. Γ and Δ are called the *antecedent* and *succedent*, respectively, of the sequent and each formula in Γ and Δ is called a *sequent-formula*.

Intuitively, a sequent $A_1, \dots, A_m \rightarrow B_1, \dots, B_n$ (where $m, n \geq 1$) means: if $A_1 \wedge \dots \wedge A_m$, then $B_1 \vee \dots \vee B_n$. For $m \geq 1$, $A_1, \dots, A_m \rightarrow$ means that $A_1 \wedge \dots \wedge A_m$ yields a contradiction. For $n \geq 1$, $\rightarrow B_1, \dots, B_n$ means that $B_1 \vee \dots \vee B_n$ holds. The empty sequent \rightarrow means there is a contradiction. Sequents will be denoted by the letter S , with or without subscripts.

§2. Formal proofs and related concepts

DEFINITION 2.1. An *inference* is an expression of the form

$$\frac{S_1}{S} \quad \text{or} \quad \frac{S_1 \quad S_2}{S},$$

where S_1, S_2 and S are sequents. S_1 and S_2 are called the *upper sequents* and S is called the *lower sequent* of the inference.

Intuitively this means that when S_1 (S_1 and S_2) is (are) asserted, we can infer S from it (from them). We restrict ourselves to inferences obtained from the following rules of inference, in which $A, B, C, D, F(a)$ denote formulas.

1) Structural rules:

1.1) *Weakening*:

$$\text{left: } \frac{\Gamma \rightarrow \Delta}{D, \Gamma \rightarrow \Delta}; \quad \text{right: } \frac{\Gamma \rightarrow \Delta}{\Gamma \rightarrow \Delta, D}.$$

D is called the *weakening formula*.

1.2) *Contraction*:

$$\text{left: } \frac{D, D, \Gamma \rightarrow \Delta}{D, \Gamma \rightarrow \Delta}; \quad \text{right: } \frac{\Gamma \rightarrow \Delta, D, D}{\Gamma \rightarrow \Delta, D}.$$

1.3) *Exchange*:

$$\text{left: } \frac{\Gamma, C, D, \Pi \rightarrow \Delta}{\Gamma, D, C, \Pi \rightarrow \Delta}; \quad \text{right: } \frac{\Gamma \rightarrow \Delta, C, D, A}{\Gamma \rightarrow \Delta, D, C, A}$$

We will refer to these three kinds of inferences as “weak inferences”, while all others will be called “strong inferences”.

1.4) *Cut*:

$$\frac{\Gamma \rightarrow \Delta, D \quad D, \Pi \rightarrow A}{\Gamma, \Pi \rightarrow \Delta, A}.$$

D is called the *cut formula* of this inference.

2) Logical rules:

$$2.1) \neg : \text{left} : \frac{\Gamma \rightarrow \Delta, D}{\neg D, \Gamma \rightarrow \Delta}; \quad \neg : \text{right} : \frac{D, \Gamma \rightarrow \Delta}{\Gamma \rightarrow \Delta, \neg D}.$$

D and $\neg D$ are called the *auxiliary formula* and the *principal formula*, respectively, of this inference.

$$2.2) \wedge : \text{left} : \frac{C, \Gamma \rightarrow \Delta}{C \wedge D, \Gamma \rightarrow \Delta} \text{ and } \frac{D, \Gamma \rightarrow \Delta}{C \wedge D, \Gamma \rightarrow \Delta};$$

$$\wedge : \text{right} : \frac{\Gamma \rightarrow \Delta, C \quad \Gamma \rightarrow \Delta, D}{\Gamma \rightarrow \Delta, C \wedge D}.$$

C and D are called the auxiliary formulas and $C \wedge D$ is called the principal formula of this inference.

$$2.3) \vee : \text{left} : \frac{C, \Gamma \rightarrow \Delta \quad D, \Gamma \rightarrow \Delta}{C \vee D, \Gamma \rightarrow \Delta};$$

$$\vee : \text{right} : \frac{\Gamma \rightarrow \Delta, C}{\Gamma \rightarrow \Delta, C \vee D} \text{ and } \frac{\Gamma \rightarrow \Delta, D}{\Gamma \rightarrow \Delta, C \vee D}.$$

C and D are called the auxiliary formulas and $C \vee D$ the principal formula of this inference.

$$2.4) \supset : \text{left} : \frac{\Gamma \rightarrow \Delta, C \quad D, \Pi \rightarrow \Lambda}{C \supset D, \Gamma, \Pi \rightarrow \Delta, \Lambda};$$

$$\supset : \text{right} : \frac{C, \Gamma \rightarrow \Delta, D}{\Gamma \rightarrow \Delta, C \supset D}.$$

C and D are called the auxiliary formulas and $C \supset D$ the principal formula.

2.1)–2.4) are called *propositional inferences*.

$$2.5) \forall : \text{left} : \frac{F(t), \Gamma \rightarrow \Delta}{\forall x F(x), \Gamma \rightarrow \Delta}, \quad \forall : \text{right} : \frac{\Gamma \rightarrow \Delta, F(a)}{\Gamma \rightarrow \Delta, \forall x F(x)},$$

where t is an arbitrary term, and a does not occur in the lower sequent. $F(t)$ and $F(a)$ are called the auxiliary formulas and $\forall x F(x)$ the principal formula. The a in $\forall : \text{right}$ is called the *eigenvariable* of this inference.

Note that in $\forall : \text{right}$ all occurrences of a in $F(a)$ are indicated. In $\forall : \text{left}$,

$F(t)$ and $F(x)$ are

$$\left(F(a) \frac{a}{t} \right) \quad \text{and} \quad \left(F(a) \frac{a}{x} \right),$$

respectively (for some free variable a), so not every t in $F(t)$ is necessarily indicated.

$$2.6) \exists : \text{left} : \frac{F(a), \Gamma \rightarrow \Delta}{\exists x F(x), \Gamma \rightarrow \Delta}, \quad \exists : \text{right} : \frac{\Gamma \rightarrow \Delta, F(t)}{\Gamma \rightarrow \Delta, \exists x F(x)},$$

where a does not occur in the lower sequent, and t is an arbitrary term.

$F(a)$ and $F(t)$ are called the auxiliary formulas and $\exists x F(x)$ the principal formula. The a in $\exists : \text{left}$ is called the eigenvariable of this inference.

Note that in $\exists : \text{left}$ a is fully indicated, while in $\exists : \text{right}$ not necessarily every t is indicated. (Again, $F(t)$ is $(F(a) \frac{a}{t})$ for some a .)

2.5) and 2.6) are called *quantifier inferences*. The condition, that the eigenvariable must not occur in the lower sequent in $\forall : \text{right}$ and $\exists : \text{left}$, is called the *eigenvariable condition* for these inferences.

A sequent of the form $A \rightarrow A$ is called an *initial sequent*, or *axiom*.

We now explain the notion of formal proof, i.e., proof in **LK**.


DEFINITION 2.2. A *proof* P (in **LK**), or **LK-proof**, is a tree of sequents satisfying the following conditions:

- 1) The topmost sequents of P are initial sequents.
- 2) Every sequent in P except the lowest one is an upper sequent of an inference whose lower sequent is also in P .

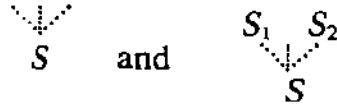
The following terminology and conventions will be used in discussing formal proofs in **LK**.

DEFINITION 2.3. From Definition 2.2, it follows that there is a unique lowest sequent in a proof P . This will be called the *end-sequent* of P . A proof with end-sequent S is called a *proof ending with S* or a *proof of S* . A sequent S is called *provable* in **LK**, or **LK-provable**, if there is an **LK-proof** of it. A formula A is called **LK-provable** (or a *theorem of **LK***) if the sequent $\rightarrow A$ is **LK-provable**. The prefix “**LK-**” will often be omitted from “**LK-proof**” and “**LK-provable**”.

A proof without the cut rule is called *cut-free*.

It will be standard notation to abbreviate part of a proof by . Thus,

for example,



denote a proof of S , and a proof of S from S_1 and S_2 , respectively. Proofs are mostly denoted by letters P, Q, \dots . An expression such as $P(a)$ means that all the occurrences of a in P are indicated. (Of course such notation is useful only when replacement of a by another term is being considered.) Then $P(t)$ is the result of replacing all occurrences of a in $P(a)$ by t .

Let us consider some slightly modified rules of inference, e.g.,

$$J \quad \frac{\Gamma \rightarrow \Delta, A \quad \Pi \rightarrow \Lambda, B}{\Gamma, \Pi \rightarrow \Delta, \Lambda, A \wedge B}.$$

This is not a rule of inference of **LK**. However, from the two upper sequents we can infer the lower sequent in **LK** using several structural inferences and an \wedge : right :

$$(*) \quad \wedge : \text{right} : \quad \frac{\frac{\Gamma \rightarrow \Delta, A}{\text{several weakenings and exchanges}} \quad \frac{\Pi \rightarrow \Lambda, B}{\text{several weakenings and exchanges}}}{\Gamma, \Pi \rightarrow \Delta, \Lambda, A \wedge B}$$

Conversely, from the sequents $\Gamma \rightarrow \Delta, A$ and $\Gamma \rightarrow \Delta, B$ we can infer $\Gamma \rightarrow \Delta, A \wedge B$ using several structural inferences and an instance of the inference-schema J :

$$J \quad \frac{\frac{\Gamma \rightarrow \Delta, A \quad \Gamma \rightarrow \Delta, B}{\Gamma, \Gamma \rightarrow \Delta, \Delta, A \wedge B}}{\text{several contractions and exchanges}} \quad \Gamma \rightarrow \Delta, A \wedge B$$

Thus we may regard J as an abbreviation of $(*)$ above. In such a case we will use the notation

$$\frac{\Gamma \rightarrow \Delta, A \quad \Pi \rightarrow \Lambda, B}{\Gamma, \Pi \rightarrow \Delta, \Lambda, A \wedge B}.$$

As in this example we often indicate abbreviation of several steps by double lines.

Another remark we wish to make here is that the restriction on bound

variables (in the definition of formulas) prohibits an unwanted inference such as

$$\frac{\frac{\frac{A(a), B(b) \rightarrow A(a) \wedge B(b)}{A(a), B(b) \rightarrow \exists x (A(x) \wedge B(b))}}{A(a), B(b) \rightarrow \exists x \exists x (A(x) \wedge B(x))}}{\exists x A(x), \exists x B(x) \rightarrow \exists x \exists x (A(x) \wedge B(x))}.$$

In our system this can never happen, since $\exists x \exists x (A(x) \wedge B(x))$ is not a formula.

The quantifier-free part of **LK**, that is, the subsystem of **LK** which does not involve quantifiers, is called the *propositional calculus*.

EXAMPLE 2.4. The following are **LK**-proofs.

$$\begin{array}{lcl} 1) & & \frac{A \rightarrow A}{\rightarrow A, \neg A} \\ & \neg : \text{right} & \\ & \vee : \text{right} & \frac{\rightarrow A, \neg A}{\rightarrow A, A \vee \neg A} \\ & \text{exchange} : \text{right} & \frac{\rightarrow A, A \vee \neg A}{\rightarrow A \vee \neg A, A} \\ & \vee : \text{right} & \frac{\rightarrow A \vee \neg A, A}{\rightarrow A \vee \neg A, A \vee \neg A} \\ & \text{contraction} : \text{right} & \frac{\rightarrow A \vee \neg A, A \vee \neg A}{\rightarrow A \vee \neg A}. \end{array}$$

2) Suppose that a is fully indicated in $F(a)$.

$$\begin{array}{lcl} & & \frac{F(a) \rightarrow F(a)}{F(a) \rightarrow \exists x F(x)} \\ & \exists : \text{right} & \\ & \neg : \text{right} & \frac{F(a) \rightarrow \exists x F(x)}{\rightarrow \exists x F(x), \neg F(a)} \\ & \forall : \text{right} & \frac{\rightarrow \exists x F(x), \neg F(a)}{\rightarrow \exists x F(x), \forall y \neg F(y)} \\ & \neg : \text{left} & \frac{\rightarrow \exists x F(x), \forall y \neg F(y)}{\neg \forall y \neg F(y) \rightarrow \exists x F(x)} \\ & \supset : \text{right} & \frac{\neg \forall y \neg F(y) \rightarrow \exists x F(x)}{\rightarrow \neg \forall y \neg F(y) \supset \exists x F(x)} \end{array}$$

It should be noted that the lower sequent of $\forall : \text{right}$ does not contain the eigenvariable a .

EXERCISE 2.5. Prove the following in **LK**.

- 1) $A \vee B \equiv \neg(\neg A \wedge \neg B)$.
- 2) $A \supset B \equiv \neg A \vee B$.
- 3) $\exists x F(x) \equiv \neg \forall y \neg F(y)$.
- 4) $\neg \forall y F(y) \equiv \exists x \neg F(x)$.
- 5) $\neg(A \wedge B) \equiv \neg A \vee \neg B$.

EXERCISE 2.6. Prove the following in **LK**.

- 1) $\exists x (A \supset B(x)) \equiv A \supset \exists x B(x)$.

- 2) $\exists x (A(x) \supset B) \equiv \forall x A(x) \supset B$, where B does not contain x .
- 3) $\exists x (A(x) \supset B(x)) \equiv \forall x A(x) \supset \exists x B(x)$.
- 4) $\neg A \supset B \rightarrow \neg B \supset A$.
- 5) $\neg A \supset \neg B \rightarrow B \supset A$.

EXERCISE 2.7. Construct a cut-free proof of $\forall x A(x) \supset B \rightarrow \exists x (A(x) \supset B)$, where $A(a)$ and B are atomic and distinct.

DEFINITION 2.8. (1) When we consider a formula, term or logical symbol together with the place that it occupies in a proof, sequent or formula respectively, we refer to it as a formula, term or logical symbol in the proof, sequent or formula, respectively.

(2) A sequence of sequents in a proof P is called a *thread* (of P) if the following conditions are satisfied:

- 2.1) The sequence begins with an initial sequent and ends with the end-sequent.
- 2.2) Every sequent in the sequence except the last is an upper sequent of an inference, and is immediately followed by the lower sequent of this inference.

(3) Let S_1 , S_2 and S_3 be sequents in a proof P . We say S_1 is *above* S_2 or S_2 is *below* S_1 (in P) if there is a thread containing both S_1 and S_2 in which S_1 appears before S_2 . If S_1 is above S_2 and S_2 is above S_3 , we say S_2 is *between* S_1 and S_3 .

(4) An inference in P is said to be *below* a sequent S (in P) if its lower sequent is below S .

(5) Let P be a proof. A part of P which itself is a proof is called a *subproof* of P . This can also be described as follows. For any sequent S in P , that part of P which consists of all sequents which are either S itself or which occur above S , is called a subproof of P (with end-sequent S).

(6) Let P_0 be a proof of the form

$$(*) \left\{ \begin{array}{c} \vdots \\ \vdots \\ \Gamma \rightarrow \Theta \\ \vdots \\ \vdots \end{array} \right.$$

where $(*)$ denotes the part of P_0 under $\Gamma \rightarrow \Theta$, and let Q be a proof ending with $\Gamma, D \rightarrow \Theta$. By a copy of P_0 from Q we mean a proof P of the form

$$(**) \left\{ \begin{array}{c} Q \\ \Gamma, D \rightarrow \Theta \\ \vdots \\ \vdots \end{array} \right.$$

where $(**)$ differs from $(*)$ only in that for each sequent in $(*)$, say $\Pi \rightarrow \Lambda$, the corresponding sequent in $(**)$ has the form $\Pi, D \rightarrow \Lambda$. That is to say, P

is obtained from P_0 by replacing the subproof ending with $\Gamma \rightarrow \Theta$ by Q , and adding an extra formula D to the antecedent of each sequent in (*). Likewise, a copy can be defined for the case of an extra formula in the succedent. We can also extend the definition to the case where there are several of these formulas.

The precise definition can be carried out by induction on the number of inferences in (*). However this notion is intuitive, simple, and will appear often in this book.

(7) Let $S(a)$, or $\Gamma(a) \rightarrow \Delta(a)$, denote a sequent of the form $A_1(a), \dots, A_m(a) \rightarrow B_1(a), \dots, B_n(a)$. Then $S(t)$, or $\Gamma(t) \rightarrow \Delta(t)$, denotes the sequent $A_1(t), \dots, A_m(t) \rightarrow B_1(t), \dots, B_n(t)$.

We can define: t is fully indicated in $S(t)$, or $\Gamma(t) \rightarrow \Delta(t)$, by analogy with Definition 1.6.

In order to prove a basic property of provability, i.e., that provability is preserved under substitution of terms for free variables, we shall first list some lemmas, which themselves assert basic properties of proofs. We first define an important concept.

DEFINITION 2.9. A proof in **LK** is called *regular* if it satisfies the condition that firstly, all eigenvariables are distinct from one another, and secondly, if a free variable a occurs as an eigenvariable in a sequent S of the proof, then a occurs only in sequents above S .

LEMMA 2.10. (1) Let $\Gamma(a) \rightarrow \Delta(a)$ be an (**LK**-)provable sequent in which a is fully indicated, and let $P(a)$ be a proof of $\Gamma(a) \rightarrow \Delta(a)$. Let b be a free variable not occurring in $P(a)$. Then the tree $P(b)$, obtained from $P(a)$ by replacing a by b at each occurrence of a in $P(a)$, is also a proof and its end-sequent is $\Gamma(b) \rightarrow \Delta(b)$.

(2) For an arbitrary **LK**-proof there exists a regular proof of the same end-sequent. Moreover, the required proof is obtained from the original proof simply by replacing free variables (in a suitable way).

PROOF. (1) By induction on the number of inferences in $P(a)$. If $P(a)$ consists of simply an initial sequent $A(a) \rightarrow A(a)$, then $P(b)$ consists of the sequent $A(b) \rightarrow A(b)$, which is also an initial sequent. Let us suppose that our proposition holds for proofs containing at most n inferences and suppose that $P(a)$ contains $n + 1$ inferences. We treat the possible cases according to the last inferences in $P(a)$. Since other cases can be treated similarly, we consider only the case where the last inference, say J , is a \forall : right. Suppose the eigenvariable of J is a , and $P(a)$ is of the form

$$Q(a) \left\{ \begin{array}{c} \vdots \\ \Gamma \rightarrow \Lambda, A(a) \\ \hline \Gamma \rightarrow \Lambda, \forall x A(x) \end{array} \right\}_J$$

where $Q(a)$ is the subproof of $P(a)$ ending with $\Gamma \rightarrow \Lambda, A(a)$. It should be remembered that a does not occur in Γ, Λ or $A(x)$. By the induction hypotheses the result of replacing all a 's in $Q(a)$ by b is a proof whose end-sequent is $\Gamma \rightarrow \Lambda, A(b)$. Γ and Λ contain no b 's. Thus we can apply a \forall : right to this sequent using b as its eigenvariable:

$$Q(b) \left\{ \frac{\Gamma \rightarrow \Lambda, A(b)}{\Gamma \rightarrow \Lambda, \forall x A(x)} \right.$$

and so $P(b)$ is a proof ending with $\Gamma \rightarrow \Lambda, \forall x A(x)$. If a is not the eigenvariable of J , $P(a)$ is of the form

$$Q(a) \left\{ \frac{\Gamma(a) \rightarrow \Lambda(a), A(a, c)}{\Gamma(a) \rightarrow \Lambda(a), \forall x A(a, x)} \right.$$

By the induction hypothesis the result of replacing all a 's in $Q(a)$ by b is a proof and its end-sequent is $\Gamma(b) \rightarrow \Lambda(b), A(b, c)$.

Since by assumption b does not occur in $P(a)$, b is not c , and so we can apply a \forall : right to this sequent, with c as its eigenvariable, and obtain a proof $P(b)$ whose end-sequent is $\Gamma(b) \rightarrow \Lambda(b), \forall x A(b, x)$.

(2) By mathematical induction on the number l of applications of \forall : right and \exists : left in a given proof P . If $l = 0$, then take P itself. Otherwise, P can be represented in the form:

$$(*) \left\{ \begin{array}{c} P_1 \quad P_2 \dots P_k \\ \quad \quad \quad \downarrow \\ \quad \quad \quad S \end{array} \right.$$

where P_i is a subproof of P of the form

$$I_i \frac{\Gamma_i \rightarrow \Delta_i, F_i(b_i)}{\Gamma_i \rightarrow \Delta_i, \forall y_i F_i(y_i)} \quad \text{or} \quad I_i \frac{F_i(b_i), \Gamma_i \rightarrow \Delta_i}{\exists y_i F_i(y_i), \Gamma_i \rightarrow \Delta_i}$$

and I_i is a lowermost \forall : right or \exists : left in P ($i = 1, \dots, k$), i.e., there is no \forall : right or \exists : left in the part of P denoted by $(*)$.

Let us deal with the case where I_i is \forall : right. P_i has fewer applications of \forall : right or \exists : left than P , so by the induction hypothesis there is a regular proof P'_i of $\Gamma_i \rightarrow \Delta_i, F_i(b_i)$. Note that no free variable in $\Gamma_i \rightarrow \Delta_i, F_i(b_i)$ (including b_i) is used as an eigenvariable in P'_i . Suppose c_1, \dots, c_m are all the eigenvariables in all the P_i 's which occur in P above $\Gamma_i \rightarrow \Delta_i, \forall y_i F_i(y_i)$, $i = 1, \dots, k$. Then change c_1, \dots, c_m to d_1, \dots, d_m , respectively, where

d_1, \dots, d_m are the first m variables which occur neither in P nor in P'_i , $i = 1, \dots, k$. If b_i occurs in P below $\Gamma_i \rightarrow \Delta_i, \forall y_i F_i(y_i)$, then change it to d_{m+i} .

Let P''_i be the proof which is obtained from P'_i by the above replacement of variables. Then P''_1, \dots, P''_k are each regular. P' is defined to be

$$(*) \left\{ \begin{array}{c} P''_1 \dots \overline{P''_i} \dots P''_n \\ \Gamma_i \rightarrow \Delta_i, \forall y_i F_i(y_i) \\ S \end{array} \right.$$

where $(*)$ is the same as in P , except for the replacement of b_i by d_{m+i} . This completes the proof.

From now on we will assume that we are dealing with regular proofs whenever convenient, and will not mention it on each occasion.

By a method similar to that in Lemma 2.10 we can prove the following.

LEMMA 2.11. *Let t be an arbitrary term. Let $\Gamma(a) \rightarrow \Delta(a)$ be a provable (in **LK**) sequent in which a is fully indicated, and let $P(a)$ be a proof ending with $\Gamma(a) \rightarrow \Delta(a)$ in which every eigenvariable is different from a and not contained in t . Then $P(t)$ (the result of replacing all a 's in $P(a)$ by t) is a proof whose end-sequent is $\Gamma(t) \rightarrow \Delta(t)$.*

LEMMA 2.12. *Let t be an arbitrary term, $\Gamma(a) \rightarrow \Delta(a)$ a provable (in **LK**) sequent in which a is fully indicated, and $P(a)$ a proof of $\Gamma(a) \rightarrow \Delta(a)$. Let $P'(a)$ be a proof obtained from $P(a)$ by changing eigenvariables (not necessarily replacing distinct ones by distinct ones) in such a way that in $P'(a)$ every eigenvariable is different from a and not contained in t . Then $P'(t)$ is a proof of $\Gamma(t) \rightarrow \Delta(t)$.*

PROOF. By induction on the number of eigenvariables in $P(a)$ which are either a or contained in t , using Lemmas 2.10 and 2.11.

We rewrite part of Lemma 2.11 as follows.

PROPOSITION 2.13. *Let t be an arbitrary term and $S(a)$ a provable (in **LK**) sequent in which a is fully indicated. The $S(t)$ is also provable.*

We will point out a simple, but useful fact about the formal proofs of our system, which will be used repeatedly.

PROPOSITION 2.14. *If a sequent is provable, then it is provable with a proof in which all the initial sequents consist of atomic formulas. Furthermore, if a sequent is provable without cut, then it is provable without cut with a proof of the above sort.*

PROOF. It suffices to show that for an arbitrary formula A , $A \rightarrow A$ is provable without cut, starting with initial sequents consisting of atomic formulas. This, however, can be easily shown by induction on the complexity of A .

DEFINITION 2.15. We say that two formulas A and B are *alphabetical variants* (of one another) if for some $x_1, \dots, x_n, y_1, \dots, y_n$

$$\left(A \frac{x_1, \dots, x_n}{z_1, \dots, z_n} \right)$$

is

$$\left(B \frac{y_1, \dots, y_n}{z_1, \dots, z_n} \right),$$

where z_1, \dots, z_n are bound variables occurring neither in A nor in B ; that is to say, if A and B are different, it is only because they have a different choice of bound variables. The fact that A and B are alphabetical variants will be expressed by $A \sim B$.

One can easily prove that the relation $A \sim B$ is an equivalence relation. Intuitively it is obvious that changing bound variables in a formula does not change its meaning. We can prove by induction on the number of logical symbols in A that if $A \sim B$, then $A \equiv B$ is provable without cut (indeed in **LJ**, which is to be defined in the next section). Thus two alphabetical variants will often be identified without mention.

§3. A formulation of intuitionistic predicate calculus

DEFINITION 3.1. We can formalize the intuitionistic predicate calculus as a sub-system of **LK**, which we call **LJ**, following Gentzen. (**J** stands for "intuitionistic".) **LJ** is obtained from **LK** by modifying it as follows (cf. Definitions 2.1 and 2.2 for **LK**):

1) A sequent in **LJ** is of the form $\Gamma \rightarrow \Delta$, where Δ consists of at most one formula.

2) Inferences in **LJ** are those obtained from those in **LK** by imposing the restriction that the succedent of each upper and lower sequent consists of at most one formula; thus there are no inferences in **LJ** corresponding to contraction : right or exchange : right.

The notions of proof, provable and other concepts for **LJ** are defined similarly to the corresponding notions for **LK**.

Every proof in **LJ** is obviously a proof in **LK**, but the converse is not true. Hence:

PROPOSITION 3.2. *If a sequent S of **LJ** is provable in **LJ**, then it is also provable in **LK**.*

Lemmas 2.10–2.12 and Propositions 2.13 and 2.14 hold, reading “**LJ**-provable” in place of “provable” or “provable (in **LK**)”. We shall refer to these results (for **LJ**) as Lemma 3.3, Lemma 3.4, Lemma 3.5, Proposition 3.6 and Proposition 3.7, respectively. We omit the statements of these.)

EXAMPLE 3.8. The following are **LJ**-proofs.

1)

$$\begin{array}{lcl}
 \wedge : \text{left} & & \frac{A \rightarrow A}{A \wedge \neg A \rightarrow A} \\
 \neg : \text{left} & & \frac{A \wedge \neg A \rightarrow A}{\neg A, A \wedge \neg A \rightarrow} \\
 \wedge : \text{left} & & \frac{\neg A, A \wedge \neg A \rightarrow}{A \wedge \neg A, A \wedge \neg A \rightarrow} \\
 \text{contraction : left} & & \frac{A \wedge \neg A, A \wedge \neg A \rightarrow}{A \wedge \neg A \rightarrow} \\
 \neg : \text{right} & & \frac{A \wedge \neg A \rightarrow}{\rightarrow \neg(A \wedge \neg A)}
 \end{array}$$

2) Suppose a is fully indicated in $F(a)$.

$$\begin{array}{lcl}
 \exists : \text{right} & & \frac{F(a) \rightarrow F(a)}{F(a) \rightarrow \exists x F(x)} \\
 \neg : \text{left} & & \frac{F(a) \rightarrow \exists x F(x)}{\neg \exists x F(x), F(a) \rightarrow} \\
 \text{exchange : left} & & \frac{\neg \exists x F(x), F(a) \rightarrow}{F(a), \neg \exists x F(x) \rightarrow} \\
 \neg : \text{left} & & \frac{F(a), \neg \exists x F(x) \rightarrow}{\neg \exists x F(x) \rightarrow \neg F(a)} \\
 \forall : \text{right} & & \frac{\neg \exists x F(x) \rightarrow \neg F(a)}{\neg \exists x F(x) \rightarrow \forall y \neg F(y)}.
 \end{array}$$

EXERCISE 3.9. Prove the following in **LJ**.

- 1) $\neg A \vee B \rightarrow A \supset B$.
- 2) $\exists x F(x) \rightarrow \neg \forall y \neg F(y)$.
- 3) $A \wedge B \rightarrow A$.
- 4) $A \rightarrow A \vee B$.
- 5) $\neg A \vee \neg B \rightarrow \neg(A \wedge B)$.
- 6) $\neg(A \vee B) \equiv \neg A \wedge \neg B$.
- 7) $(A \vee C) \wedge (B \vee C) \equiv (A \wedge B) \vee C$.
- 8) $\exists x \neg F(x) \rightarrow \neg \forall x F(x)$.

- 9) $\forall x (F(x) \wedge G(x)) \equiv \forall x F(x) \wedge \forall x G(x)$.
- 10) $A \supset \neg B \rightarrow B \supset \neg A$.
- 11) $\exists x (A \supset B(x)) \rightarrow A \supset \exists x B(x)$.
- 12) $\exists x (A(x) \supset B) \rightarrow \forall x A(x) \supset B$.
- 13) $\exists x (A(x) \supset B(x)) \rightarrow \forall x A(x) \supset \exists x B(x)$.

EXERCISE 3.10. Prove the following in **LJ**.

- 1) $\neg\neg(A \supset B), A \rightarrow \neg\neg B$.
- 2) $\neg\neg B \supset B, \neg\neg(A \supset B) \rightarrow A \supset B$.
- 3) $\neg\neg\neg A \equiv \neg A$.

EXERCISE 3.11. Define **LJ'** to be the system which is obtained from **LJ** by adding to it, as initial sequents, all sequents $\neg\neg R \rightarrow R$, where R is atomic. Let A be a formula which does not contain \vee or \exists . Then $\neg\neg A \rightarrow A$ is **LJ'**-provable. [*Hint*: By induction on the number of logical symbols in A ; cf. Exercise 3.10.]

PROBLEM 3.12. For every formula A define A^* as follows.

- 1) If A is atomic, then A^* is $\neg\neg A$.
- 2) If A is one of the forms $\neg B, B \wedge C, B \vee C$ or $B \supset C$, then A^* is $\neg B^*, B^* \wedge C^*, \neg(\neg B^* \wedge \neg C^*)$ or $B^* \supset C^*$, respectively.
- 3) If A is of the form $\forall x F(x)$ or $\exists x F(x)$, then A^* is $\forall x F^*(x)$ or $\neg\forall x \neg F^*(x)$, respectively.

(Thus A^* does not contain \vee or \exists .) Prove that for any A , A is **LK**-provable if and only if A^* is **LJ**-provable. [*Hint*: Follow the prescription given below.]

- 1) For any A , $A \equiv A^*$ is **LK**-provable.
- 2) Let S be a sequent of the form $A_1, \dots, A_m \rightarrow B_1, \dots, B_n$. Let S' be the sequent

$$A_1^*, \dots, A_m^*, \neg B_1^*, \dots, \neg B_n^* \rightarrow.$$

Prove that S is **LK**-provable if and only if S' is **LK**-provable.

- 3) $A^* \equiv \neg\neg A^*$ in **LJ**, from Exercise 3.11.
 - 4) Show that if S is **LK**-provable, then S' is **LJ**-provable. (Use mathematical induction on the number of inferences in a proof of S .)
- What must be proved is now a special case of 4).

§4. Axiom systems

DEFINITION 4.1. The basic system is **LK**.

- 1) A finite or infinite set \mathcal{A} of sentences is called an *axiom system*, and each of these sentences is called an *axiom* of \mathcal{A} . Sometimes an axiom system is called a *theory*. (Of course this definition is only significant in certain contexts.)

2) A finite (possibly empty) sequence of formulas consisting only of axioms of \mathcal{A} is called an *axiom sequence* of \mathcal{A} .

3) If there exists an axiom sequence Γ_0 of \mathcal{A} such that $\Gamma_0, \Gamma \rightarrow \Delta$ is **LK**-provable, then $\Gamma \rightarrow \Delta$ is said to be *provable from \mathcal{A}* (in **LK**). We express this by $\mathcal{A}, \Gamma \rightarrow \Delta$.

4) \mathcal{A} is *inconsistent* (with **LK**) if the empty sequent \rightarrow is provable from \mathcal{A} (in **LK**).

5) If \mathcal{A} is not inconsistent (with **LK**), then it is said to be *consistent* (with **LK**).

6) If all function constants and predicate constants in a formula A occur in \mathcal{A} , then A is said to be *dependent on \mathcal{A}* .

7) A sentence A is said to be *consistent* (*inconsistent*) if the axiom system $\{A\}$ is consistent (*inconsistent*).

8) $\mathbf{LK}_{\mathcal{A}}$ is the system obtained from **LK** by adding $\rightarrow A$ as initial sequents for all A in \mathcal{A} .

9) $\mathbf{LK}_{\mathcal{A}}$ is said to be *inconsistent* if \rightarrow is $\mathbf{LK}_{\mathcal{A}}$ -provable, otherwise it is *consistent*.

The following propositions, which are easily proved, will be used quite often.

PROPOSITION 4.2. *Let \mathcal{A} be an axiom system. Then the following are equivalent:*

- (a) \mathcal{A} is inconsistent (with **LK**) (as defined above);
- (b) for every formula A (of the language), A is provable from \mathcal{A} ;
- (c) for some formula A , A and $\neg A$ are both provable from \mathcal{A} .

PROPOSITION 4.3. *Let \mathcal{A} be an axiom system. Then a sequent $\Gamma \rightarrow \Delta$ is $\mathbf{LK}_{\mathcal{A}}$ -provable if and only if $\Gamma \rightarrow \Delta$ is provable from \mathcal{A} (in **LK**).*

COROLLARY 4.4. *An axiom system \mathcal{A} is consistent (with **LK**) if and only if $\mathbf{LK}_{\mathcal{A}}$ is consistent.*

These definitions and the propositions hold also for **LJ**.

§5. The cut-elimination theorem

A very important fact about **LK** is the cut-elimination theorem, also known as Gentzen's Hauptsatz:

THEOREM 5.1 (the cut-elimination theorem: Gentzen). *If a sequent is (**LK**)-provable, then it is (**LK**)-provable without a cut.*

This means that any theorem in the predicate calculus can be proved

without detours, so to speak. We shall come back to this point later. The purpose of the present section is to prove this theorem. We shall follow Gentzen's original proof.

First we introduce a new rule of inference, the mix rule, and show that the mix rule and the cut rule are equivalent. Let A be a formula. An inference of the following form is called a *mix* (with respect to A):

$$\frac{\Gamma \rightarrow \Delta \quad \Pi \rightarrow \Lambda}{\Gamma, \Pi^* \rightarrow \Delta^*, \Lambda} \quad (A)$$

where both Δ and Π contain the formula A , and Δ^* and Π^* are obtained from Δ and Π respectively by deleting all the occurrences of A in them. We call A the mix formula of this inference, and the mix formula of a mix is normally indicated in parentheses (as above).

Let us call the system which is obtained from **LK** by replacing the cut rule by the mix rule, **LK***. The following is easily proved.

LEMMA 5.2. ***LK** and **LK*** are equivalent, that is, a sequent S is **LK**-provable if and only if S is **LK***-provable.*

By virtue of the Lemma 5.2, it suffices to show that the mix rule is redundant in **LK***, since a proof in **LK*** without a mix is at the same time a proof in **LK** without a cut.

THEOREM 5.3 (cf. Theorem 5.1). *If a sequent is provable in **LK***, then it is provable in **LK*** without a mix.*

This theorem is an immediate consequence of the following lemma.

LEMMA 5.4. *If P is a proof of S (in **LK***) which contains (only) one mix, occurring as the last inference, then S is provable without a mix.*

The proof of Theorem 5.3 from Lemma 5.4 is simply by induction on the number of mixes occurring in a proof of S .

The rest of this section is devoted to proving Lemma 5.4. We first define two scales for measuring the complexity of a proof. The *grade* of a formula A (denoted by $g(A)$) is the number of logical symbols contained in A . The grade of a mix is the grade of the mix formula. When a proof P has a mix (only) as the last inference, we define the grade of P (denoted by $g(P)$) to be the grade of this mix.

Let P be a proof which contains a mix only as the last inference:

$$J \frac{\Gamma \rightarrow \Delta \quad \Pi \rightarrow \Lambda}{\Gamma, \Pi^* \rightarrow \Delta^*, \Lambda} (A).$$

We refer to the left and right upper sequents as S_1 and S_2 , respectively,

and to the lower sequent as S . We call a thread in P a *left (right) thread* if it contains the left (right) upper sequent of the mix J . The *rank* of a thread \mathcal{F} in P is defined as follows: if \mathcal{F} is a left (right) thread, then the rank of \mathcal{F} is the number of consecutive sequents, counting upward from the left (right) upper sequent of J , that contains the mix formula in its succedent (antecedent). Since the left (right) upper sequent always contains the mix formula, the rank of a thread in P is at least 1. The rank of a thread \mathcal{F} in P is denoted by $\text{rank}(\mathcal{F}; P)$. We define

$$\text{rank}_l(P) = \max_{\mathcal{F}}(\text{rank}(\mathcal{F}; P)),$$

where \mathcal{F} ranges over all the left threads in P , and

$$\text{rank}_r(P) = \max_{\mathcal{F}}(\text{rank}(\mathcal{F}; P)),$$

where \mathcal{F} ranges over all the right threads in P . The rank of P , $\text{rank}(P)$, is defined as

$$\text{rank}(P) = \text{rank}_l(P) + \text{rank}_r(P).$$

Notice that $\text{rank}(P)$ is always ≥ 2 .

PROOF OF LEMMA 5.4. We prove the Lemma by double induction on the grade g and rank r of the proof P (i.e., transfinite induction on $\omega \cdot g + r$). We divide the proof into two main cases, namely $r = 2$ and $r > 2$ (regardless of g).

Case 1: $r = 2$, viz. $\text{rank}_l(P) = \text{rank}_r(P) = 1$.

We distinguish cases according to the forms of the proofs of the upper sequents of the mix.

1.1) The left upper sequent S_1 is an initial sequent. In this case we may assume P is of the form

$$J \frac{A \rightarrow A \quad \Pi \rightarrow \Lambda}{A, \Pi^* \rightarrow \Lambda}.$$

We can then obtain the lower sequent without a mix:

$$\frac{\frac{\Pi \rightarrow \Lambda}{\text{some exchanges}}}{A, \dots, A, \Pi^* \rightarrow \Lambda} \text{some contractions}$$

1.2) The right upper sequent S_2 is an initial sequent. Similarly:

1.3) Neither S_1 nor S_2 is an initial sequent, and S_1 is the lower sequent of a structural inference J_1 . Since $\text{rank}_l(P) = 1$, the formula A cannot appear in the succedent of the upper sequent of J_1 , i.e., J_1 must be weakening:right, whose weakening formula is A :

$$J_1 \frac{\Gamma \rightarrow \Delta_1}{\Gamma \rightarrow \Delta_1, A} \quad \Pi \rightarrow A \quad (A), \\ J \frac{\Gamma \rightarrow \Delta_1, A \quad \Pi \rightarrow A}{\Gamma, \Pi^* \rightarrow \Delta_1, A}$$

where Δ_1 does not contain A . We can eliminate the mix as follows:

$$\frac{\Gamma \rightarrow \Delta_1}{\text{some weakenings}} \\ \frac{\Pi^*, \Gamma \rightarrow \Delta_1, A}{\text{some exchanges}} \\ \Gamma, \Pi^* \rightarrow \Delta_1, A$$

1.4) None of 1.1)–1.3) holds but S_2 is the lower sequent of a structural inference. Similarly:

1.5) Both S_1 and S_2 are the lower sequents of logical inferences. In this case, since $\text{rank}_l(P) = \text{rank}_r(P) = 1$, the mix formula on each side must be the principal formula of the logical inference. We use induction on the grade, distinguishing several cases according to the outermost logical symbol of A . We treat here two cases and leave the others to the reader.

(i) The outermost logical symbol of A is \wedge . In this case S_1 and S_2 must be the lower sequents of \wedge : right and \wedge : left, respectively:

$$\frac{\Gamma \rightarrow \Delta_1, B \quad \Gamma \rightarrow \Delta_1, C}{\Gamma \rightarrow \Delta_1, B \wedge C} \quad \frac{B, \Pi_1 \rightarrow A}{B \wedge C, \Pi_1 \rightarrow A} \quad (B \wedge C), \\ \Gamma, \Pi_1 \rightarrow \Delta_1, A$$

where by assumption none of the proofs ending with $\Gamma \rightarrow \Delta_1, B$; $\Gamma \rightarrow \Delta_1, C$ or $B, \Pi_1 \rightarrow A$ contain a mix. Consider the following:

$$\frac{\Gamma \rightarrow \Delta_1, B \quad B, \Pi_1 \rightarrow A}{\Gamma, \Pi_1^* \rightarrow \Delta_1^*, A} \quad (B),$$

where Π_1^* and Δ_1^* are obtained from Π_1 and Δ_1 by omitting all occurrences of B . This proof contains only one mix, a mix that occurs as its last inference. Furthermore the grade of the mix formula B is less than $g(A)$ ($= g(B \wedge C)$). So by the induction hypothesis we can obtain a proof which contains no mixes and whose end-sequent is $\Gamma, \Pi_1^* \rightarrow \Delta_1^*, A$. From this we can obtain a proof without a mix with end-sequent $\Gamma, \Pi_1 \rightarrow \Delta_1, A$.

(ii) The outermost logical symbol of A is \forall . So A is of the form $\forall x F(x)$ and the last part of P has the form:

$$\frac{\frac{\Gamma \rightarrow \Delta_1, F(a)}{\Gamma \rightarrow \Delta_1, \forall x F(x)} \quad \frac{F(t), \Pi_1 \rightarrow \Lambda}{\forall x F(x), \Pi_1 \rightarrow \Lambda}}{\Gamma, \Pi_1 \rightarrow \Delta_1, \Lambda} \quad (A)$$

(a being fully indicated in $F(a)$). By the eigenvariable condition, a does not occur in Γ, Δ_1 or $F(x)$. Since by assumption the proof ending with $\Gamma \rightarrow \Delta_1, F(a)$ contains no mix, we can obtain a proof without a mix, ending with $\Gamma \rightarrow \Delta_1, F(t)$ (cf. Lemma 2.12). Consider now

$$\frac{\Gamma \rightarrow \Delta_1, F(t) \quad F(t), \Pi_1 \rightarrow \Lambda}{\Gamma, \Pi_1^* \rightarrow \Delta_1^*, \Lambda} \quad (F(t)),$$

where Π_1^* and Δ_1^* are obtained from Π_1 and Δ_1 by omitting all occurrences of $F(t)$. This has only one mix. It occurs as the last inference and the grade of the mix formula is less than $g(A)$. Thus by the induction hypothesis we can eliminate this mix and obtain a proof ending with $\Gamma, \Pi_1^* \rightarrow \Delta_1^*, \Lambda$, from which we can obtain a proof, without a mix, ending with $\Gamma, \Pi_1 \rightarrow \Delta_1, \Lambda$.

Case 2. $r > 2$, i.e., $\text{rank}_l(P) > 1$ and/or $\text{rank}_r(P) > 1$.

The induction hypothesis is that from every proof Q which contains a mix only as the last inference, and which satisfies either $g(Q) < g(P)$, or $g(Q) = g(P)$ and $\text{rank}(Q) < \text{rank}(P)$, we can eliminate the mix.

2.1) $\text{rank}_r(P) > 1$.

2.1.1) Γ or Δ (in S_1) contains A . Construct a proof as follows.

$\frac{\frac{\frac{\vdots}{\vdots}}{\vdots} \Pi \rightarrow \Lambda}{\text{some exchanges and contractions}} \quad \frac{\frac{\frac{\vdots}{\vdots}}{\vdots} \Gamma \rightarrow \Delta}{\text{some exchanges and contractions}}$	$\frac{\frac{\frac{\vdots}{\vdots}}{\vdots} \Pi \rightarrow \Lambda}{\text{some exchanges and contractions}} \quad \frac{\frac{\frac{\vdots}{\vdots}}{\vdots} \Gamma \rightarrow \Delta}{\text{some exchanges and contractions}}$
$\frac{A, \Pi^* \rightarrow \Lambda}{\text{some weakenings and exchanges}}$	$\frac{\Gamma \rightarrow \Delta^*, A}{\text{some weakenings and exchanges}}$
$\Gamma, \Pi^* \rightarrow \Delta^*, \Lambda$	$\Gamma, \Pi^* \rightarrow \Delta^*, \Lambda$

2.1.2) S_2 is the lower sequent of an inference J_2 , where J_2 is not a logical inference whose principal formula is A . The last part of P looks like this:

$$\frac{\Gamma \rightarrow \Delta \quad \frac{J_2 \quad \frac{\Phi \rightarrow \Psi}{\Pi \rightarrow \Lambda}}{\Gamma, \Pi^* \rightarrow \Delta^*, \Lambda}}{\Gamma, \Pi^* \rightarrow \Delta^*, \Lambda} \quad (A),$$

where the proofs of $\Gamma \rightarrow \Delta$ and $\Phi \rightarrow \Psi$ contain no mixes and Φ contains at least one A . Consider the following proof P' :

$$\text{mix} \frac{\frac{\Gamma \rightarrow \Delta}{\Gamma, \Phi^* \rightarrow \Delta^*, \Psi} \quad \frac{\Phi \rightarrow \Psi}{\Gamma, \Phi^* \rightarrow \Delta^*, \Psi}}{\Gamma, \Phi^* \rightarrow \Delta^*, \Psi} (A).$$

In P' , the grade of the mix is equal to $g(P)$, $\text{rank}_l(P') = \text{rank}_l(P)$ and $\text{rank}_r(P') = \text{rank}_r(P) - 1$. Thus by the induction hypothesis, $\Gamma, \Phi^* \rightarrow \Delta^*, \Psi$ is provable without a mix. Then we construct the proof

$$\begin{array}{c} \frac{\Gamma, \Phi^* \rightarrow \Delta^*, \Psi}{\text{some exchanges}} \\ J_2 \frac{\Phi^*, \Gamma \rightarrow \Delta^*, \Psi}{\Pi^*, \Gamma \rightarrow \Delta^*, \Lambda} \end{array}$$

In case that the auxiliary formula in J_2 in P is a mix in Φ , we need an additional weakening before J_2 in the new proof.

2.1.3) Γ contains no A 's, and S_2 is the lower sequent of a logical inference whose principal formula is A . Although there are several cases according to the outermost logical symbol of A , we treat only two examples here and leave the rest to the reader.

(i) A is $B \supset C$. The last part of P is of the form:

$$J \frac{\Gamma \rightarrow \Delta \quad J_2 \frac{\Pi_1 \rightarrow \Lambda_1, B \quad C, \Pi_2 \rightarrow \Lambda_2}{B \supset C, \Pi_1, \Pi_2 \rightarrow \Lambda_1, \Lambda_2}}{\Gamma, \Pi_1^*, \Pi_2^* \rightarrow \Delta^*, \Lambda_1, \Lambda_2} (B \supset C)$$

Consider the following proofs P_1 and P_2 :

$$\frac{P_1 \frac{\Gamma \rightarrow \Delta \quad \Pi_1 \rightarrow \Lambda_1, B}{\Gamma, \Pi_1^* \rightarrow \Delta^*, \Lambda_1, B} (B \supset C) \quad P_2 \frac{\Gamma \rightarrow \Delta \quad C, \Pi_2 \rightarrow \Lambda_2}{\Gamma, C, \Pi_2^* \rightarrow \Delta^*, \Lambda_2} (B \supset C)}$$

assuming that $B \supset C$ is in Π_1 and Π_2 . If $B \supset C$ is not in Π_i ($i = 1$ or 2), then Π_i^* is Π_i and P_i is defined as follows.

$$\begin{array}{c} P_1 \frac{\Pi_1 \rightarrow \Lambda_1, B}{\text{weakenings and exchanges}} \\ \Gamma, \Pi_1^* \rightarrow \Delta^*, \Lambda_1, B \end{array} \quad \begin{array}{c} P_2 \frac{C, \Pi_2 \rightarrow \Lambda_2}{\text{weakenings and exchanges}} \\ \Gamma, C, \Pi_2^* \rightarrow \Delta^*, \Lambda_2 \end{array}$$

Note that $g(P_1) = g(P_2) = g(P)$, $\text{rank}_l(P_1) = \text{rank}_l(P_2) = \text{rank}_l(P)$ and $\text{rank}_r(P_1) = \text{rank}_r(P_2) = \text{rank}_r(P) - 1$. Hence by the induction hypothesis, the end-sequents of P_1 and P_2 are provable without a mix (say by P'_1 and P'_2). Consider the following proof P' :

$$J \frac{\Gamma \rightarrow \Delta \quad \frac{\frac{P'_1}{\Gamma, \Pi_1^* \rightarrow \Delta^*, \Lambda_1, B} \quad \frac{\frac{P'_2}{\Gamma, C, \Pi_2^* \rightarrow \Delta^*, \Lambda_2} \text{some exchanges}}{C, \Gamma, \Pi_2^* \rightarrow \Delta^*, \Lambda_2}}{B \supset C, \Gamma, \Pi_1^*, \Gamma, \Pi_2^* \rightarrow \Delta^*, \Lambda_1, \Delta^*, \Lambda_2}}{\Gamma, \Gamma, \Pi_1^*, \Gamma, \Pi_2^* \rightarrow \Delta^*, \Delta^*, \Lambda_1, \Delta^*, \Lambda_2} (B \supset C).$$

Then $g(P') = g(P)$, $\text{rank}_l(P') = \text{rank}_l(P)$, $\text{rank}_r(P') = 1$, for Γ contains no occurrences of $B \supset C$ and $\text{rank}(P') < \text{rank}(P)$. Thus the end-sequent of P' is provable without a mix by the induction hypothesis, and hence so is the end-sequent of P .

(ii) A is $\exists x F(x)$. The last part of P looks like this:

$$J \frac{\Gamma \rightarrow \Delta \quad \frac{F(a), \Pi_1 \rightarrow \Lambda}{\exists x F(x), \Pi_1 \rightarrow \Lambda}}{\Gamma, \Pi_1^* \rightarrow \Delta^*, \Lambda} (\exists x F(x)).$$

Let b be a free variable not occurring in P . Then the result of replacing a by b throughout the proof ending with $F(a), \Pi_1 \rightarrow \Lambda$ is a proof, without a mix, ending with $F(b), \Pi_1 \rightarrow \Lambda$, since by the eigenvariable condition, a does not occur in Π_1 or Λ (cf. Lemma 2.11).

Consider the following proof:

$$J \frac{\Gamma \rightarrow \Delta \quad F(b), \Pi_1 \rightarrow \Lambda}{\Gamma, F(b), \Pi_1^* \rightarrow \Delta^*, \Lambda} (\exists x F(x)).$$

By the induction hypothesis, the end-sequent of this proof can be proved without a mix (say by P'). Now consider the proof

$$J \frac{\Gamma \rightarrow \Delta \quad \frac{\frac{P'}{\Gamma, F(b), \Pi_1^* \rightarrow \Delta^*, \Lambda} \text{some exchanges}}{F(b), \Gamma, \Pi_1^* \rightarrow \Delta^*, \Lambda}}{\Gamma, \Gamma, \Pi_1^* \rightarrow \Delta^*, \Delta^*, \Lambda} (\exists x F(x)),$$

where b occurs in none of $\exists x F(x)$, Γ , Π_1 , Δ , A . This mix can then also be eliminated, by the induction hypothesis.

2.2) $\text{rank}_t(P) = 1$ (and $\text{rank}_t(P) > 1$).

This case is proved in the same way as 2.1) above.

This completes the proof of Lemma 5.4 and hence of the cut-elimination theorem.

It should be emphasized that the proof is constructive, i.e., a new proof is effectively constructed from the given proof in Lemma 5.2 and again in Lemma 5.4, and hence in Theorem 5.1.

The cut-elimination theorem also holds for **LJ**. Actually the above proof is designed so that it goes through for **LJ** without essential changes: we only have to keep in mind that there can be at most one formula in each succedent. The details are left to the reader; we simply state the theorem.

THEOREM 5.5. *The cut-elimination theorem holds for LJ.*

§6. Some consequences of the cut-elimination theorem

There are numerous applications of the cut-elimination theorem, some of which will be listed in this section, others as exercises. In order to facilitate discussion of this valuable, productive and important theorem, we shall first define the notion of subformula, which will be used often.

DEFINITION 6.1. By a *subformula* of a formula A we mean a formula used in building up A . The set of subformulas of a formula is inductively defined as follows, by induction on the number of logical symbols in the formula.

(1) An atomic formula has exactly one subformula, viz. the formula itself. The subformulas of $\neg A$ are the subformulas of A and $\neg A$ itself. The subformulas of $A \wedge B$ or $A \vee B$ or $A \supset B$ are the subformulas of A and of B , and the formula itself. The subformulas of $\forall x A(x)$ or $\exists x A(x)$ are the subformulas of any formula of the form $A(t)$, where t is an arbitrary term, and the formula itself.

(2) Two formulas A and B are said to be *equivalent* in **LK** if $A \equiv B$ is provable in **LK**.

(3) We shall say that in a formula A an occurrence of a logical symbol, say $\#$, is *in the scope* of an occurrence of a logical symbol, say \natural , if in the construction of A (from atomic formulas) the stage where $\#$ is the outermost logical symbol precedes the stage where \natural is the outermost logical symbol (cf. Definition 1.3). Further, a symbol $\#$ is said to be in the left scope of a \supset if \supset occurs in the form $B \supset C$ and $\#$ occurs in B .

(4) A formula is called *prenex* (in prenex form) if no quantifier in it is in the scope of a propositional connective. It can easily be seen that any

formula is equivalent (in **LK**) to a prenex formula, i.e., for every formula A there is a prenex formula B such that $A \equiv B$ is **LK**-provable.

One can easily see that in any rule of inference except a cut, the lower sequent is no less complicated than the upper sequent(s); more precisely, every formula occurring in an upper sequent is a subformula of some formula occurring in the lower sequent (but not necessarily conversely). Hence a proof without a cut contains only subformulas of the formulas occurring in the end-sequent (the "subformula property"). So the cut-elimination theorem tells us that if a formula is provable in **LK** (or **LJ**) at all, it is provable by use of its subformulas only. (This is what we meant by saying that a theorem in the predicate calculus could be proved without detours.)

From this observation, we can convince ourselves that the empty sequent \rightarrow is not **LK**- (or **LJ**-) provable. This leads us to the consistency proof of **LK** and **LJ**.

THEOREM 6.2 (consistency). ***LK** and **LJ** are consistent.*

PROOF. Suppose \rightarrow were provable in **LK** (or **LJ**). Then, by the cut-elimination theorem, it would be provable in **LK** (or **LJ**) without a cut. But this is impossible, by the subformula property of cut-free proofs.

An examination of the proof of this theorem (including the cut-elimination theorem) shows that the consistency of **LK** (and **LJ**) was proved by quantifier-free induction on the ordinal ω^2 . We shall not, however, go into the details of the consistency problem at this stage.

For convenience, we re-state the subformula property of cut-free proofs as a theorem.

THEOREM 6.3. *In a cut-free proof in **LK** (or **LJ**) all the formulas which occur in it are subformulas of the formulas in the end-sequent.*

PROOF. By mathematical induction on the number of inferences in the cut-free proof.

In the rest of this section, we shall list some typical consequences of the cut-elimination theorem. Although some of the results are stated for **LJ** as well as **LK**, we shall give proofs only for **LK**; those for **LJ** are left to the reader.

THEOREM 6.4 (1) (Gentzen's midsequent theorem for **LK**). *Let S be a sequent which consists of prenex formulas only and is provable in **LK**. Then*

there is a cut-free proof of S which contains a sequent (called a midsequent), say S' , which satisfies the following:

1. S' is quantifier-free.
2. Every inference above S' is either structural or propositional.
3. Every inference below S' is either structural or a quantifier inference.

Thus a midsequent splits the proof into an upper part, which contains the propositional inferences, and a lower part, which contains the quantifier inferences.

(2) (The midsequent theorem for **LJ** without \vee : left.) *The above holds reading “**LJ** without \vee : left” in place of “**LK**”.*

PROOF (outline). Combining Proposition 2.14 and the cut-elimination theorem, we may assume that there is a cut-free proof of S , say P , in which all the initial sequents consist of atomic formulas only. Let I be a quantifier inference in P . The number of propositional inferences under I is called the order of I . The sum of the orders for all the quantifier inferences in P is called the order of P . (The term “order” is used only temporarily here.) The proof is carried out by induction on the order of P .

Case 1: The order of a proof P is 0. If there is a propositional inference, take the lowermost such, and call its lower sequent S_0 . Above this sequent there is no quantifier inference. Therefore, if there is a quantifier in or above S_0 , then it is introduced by weakenings. Since the proof is cut-free, the weakening formula is a subformula of one of the formulas in the end-sequent. Hence no propositional inferences apply to it. We can thus eliminate these weakenings and obtain a sequent S'_0 corresponding to S_0 . By adding some weakenings under S'_0 (if necessary), we derive S , and S'_0 serves as the mid-sequent.

If there is no propositional inference in P , then take the uppermost quantifier inference. Its upper sequent serves as a midsequent.

Case 2: The order of P is not 0. Then there is at least one propositional inference which is below a quantifier inference. Moreover, there is a quantifier inference I with the following property: the uppermost logical inference under I is a propositional inference. Call it I' . We can lower the order by interchanging the positions of I and I' . Here we present just one example: say I is \forall : right.

P :

$$(*) \quad \left\{ \begin{array}{l} I \quad \frac{\Gamma \xrightarrow{\vee} \Theta, F(a)}{\Gamma \rightarrow \Theta, \forall x F(x)} \\ I' \quad \frac{\Delta \xrightarrow{\vee} \Lambda}{\Delta \rightarrow \Lambda} \end{array} \right.,$$

where the $(*)$ -part of P contains only structural inferences and Λ contains

$\forall x F(x)$ as a sequent-formula. Transform P into the following proof P' :

$$\begin{array}{c}
 \frac{\Gamma \rightarrow \Theta, F(a)}{\text{structural inferences}} \\
 \hline
 \Gamma \rightarrow F(a), \Theta, \forall x F(x) \\
 \vdots \\
 I' \frac{\Delta \rightarrow F(a), \Lambda}{\Delta \rightarrow \Lambda, \forall x F(x)} \\
 I \frac{\Delta \rightarrow \Lambda, \forall x F(x)}{\Delta \rightarrow \Lambda} \\
 \vdots
 \end{array}$$

It is obvious that the order of P' is less than that of P .

Prior to the next theorem, Craig's interpolation theorem*, we shall first state and prove a lemma which itself can be regarded as an interpolation theorem for provable sequents and from which the original form of the interpolation theorem follows immediately. We shall present the argument for **LK** only, although everything goes through for **LJ** as well.

For technical reasons we introduce the predicate symbol \top , with 0 argument places, and admit $\rightarrow \top$ as an additional initial sequent. (\top stands for "true".) The system which is obtained from **LK** thus extended is denoted by **LK#**.

LEMMA 6.5. *Let $\Gamma \rightarrow \Delta$ be **LK**-provable, and let (Γ_1, Γ_2) and (Δ_1, Δ_2) be arbitrary partitions of Γ and Δ , respectively (including the cases that one or more of $\Gamma_1, \Gamma_2, \Delta_1, \Delta_2$ are empty). We denote such a partition by $[\{\Gamma_1; \Delta_1\}, \{\Gamma_2; \Delta_2\}]$ and call it a partition of the sequent $\Gamma \rightarrow \Delta$. Then there exists a formula C of **LK#** (called an interpolant of $[\{\Gamma_1; \Delta_1\}, \{\Gamma_2; \Delta_2\}]$) such that:*

- (i) $\Gamma_1 \rightarrow \Delta_1, C$ and $C, \Gamma_2 \rightarrow \Delta_2$ are both **LK#**-provable;
- (ii) All free variables and individual and predicate constants in C (apart from \top) occur both in $\Gamma_1 \cup \Delta_1$ and $\Gamma_2 \cup \Delta_2$.

We will first prove the theorem (from this lemma) and then prove the lemma.

THEOREM 6.6 (Craig's interpolation theorem for **LK**). (1) *Let A and B be two formulas such that $A \supset B$ is **LK**-provable. If A and B have at least one predicate constant in common, then there exists a formula C , called an interpolant of $A \supset B$, such that C contains only those individual constants, predicate constants and free variables that occur in both A and B , and such*

* A strong general theory on interpolation theorems is established in N. Motohashi: Interpolation theorem and characterization theorem, Ann. Japan Assoc. Philos. Sci., 4 (1972) pp. 15-80.

that $A \supset C$ and $C \supset B$ are **LK**-provable. If A and B contain no predicate constant in common, then either $A \rightarrow$ or $\rightarrow B$ is **LK**-provable.

(2) As above, with **LJ** in place of **LK**.

PROOF. Assume that $A \supset B$, and hence $A \rightarrow B$, is provable, and A and B have at least one predicate constant in common. Then by Lemma 6.5, taking A as Γ_1 and B as Δ_1 (with Γ_2 and Δ_2 empty), there exists a formula C satisfying (i) and (ii). So $A \rightarrow C$ and $C \rightarrow B$ are **LK**#-provable. Let R be predicate constant which is common to A and B and has k argument places. Let R' be $\forall y_1 \dots \forall y_k R(y_1, \dots, y_k)$, where y_1, \dots, y_k are new bound variables. By replacing T by $R' \supset R'$, we can transform C into a formula C' of the original language, such that $A \rightarrow C'$ and $C' \rightarrow B$ are **LK**-provable. C' is then the desired interpolant.

If there is no predicate common to $\Gamma_1 \cup \Delta_1$ and $\Gamma_2 \cup \Delta_2$ in the partition described in Lemma 6.5, then by that lemma, there is a C such that $\Gamma_1 \rightarrow \Delta_1$, C and $C, \Gamma_2 \rightarrow \Delta_2$ are provable, and C consists of T and logical symbols only. Then it can easily be shown, by induction on the complexity of C , that either $\rightarrow C$ or $C \rightarrow$ is provable. Hence either $\Gamma_1 \rightarrow \Delta_1$ or $\Gamma_2 \rightarrow \Delta_2$ is provable. In particular, this applies to $A \rightarrow B$ when A is taken as Γ_1 and B as Δ_2 .

This method is due to Maehara and its significance lies in the fact that an interpolant of $A \supset B$ can be constructively formed from a proof of $A \supset B$. Note also that we could state the theorem in the following form: *If neither $\neg A$ nor B is provable, then there is an interpolant of $A \supset B$.*

A uniform form of interpolation theorem is given in

N. Motohashi: An Axiomatization Theorem, J. Math. Soc. Japan 34 (1982) 551–560.

PROOF OF LEMMA 6.5. The lemma is proved by induction on the number of inferences k , in a cut-free proof of $\Gamma \rightarrow \Delta$. At each stage there are several cases to consider; we deal with some examples only.

1) $k = 0$. $\Gamma \rightarrow \Delta$ has the form $D \rightarrow D$. There are four cases: (1) $[\{D; D\}, \{; \}]$, (2) $[\{; \}, \{D; D\}]$, (3) $[\{D; \}, \{; D\}]$, and (4) $[\{; D\}, \{D; \}]$. Take for C : $\neg T$ in (1), T in (2), D in (3) and $\neg D$ in (4).

2) $k > 0$ and the last inference is \wedge : right:

$$\frac{\Gamma \rightarrow \Delta, A \quad \Gamma \rightarrow \Delta, B}{\Gamma \rightarrow \Delta, A \wedge B}.$$

Suppose the partition is $[\{\Gamma_1; \Delta_1, A \wedge B\}, \{\Gamma_2; \Delta_2\}]$. Consider the induced partition of the upper sequents, viz. $[\{\Gamma_1; \Delta_1, A\}, \{\Gamma_2; \Delta_2\}]$ and $[\{\Gamma_1; \Delta_1, B\}, \{\Gamma_2; \Delta_2\}]$, respectively. By the induction hypotheses applied to the sub-proofs of the upper sequents, there exist interpolants C_1 and C_2 so that

$\Gamma_1 \rightarrow \Delta_1, A, C_1$; $C_1, \Gamma_2 \rightarrow \Delta_2$; $\Gamma_1 \rightarrow \Delta_1, B, C_2$; and $C_2, \Gamma_2 \rightarrow \Delta_2$ are all **LK#**-provable. From these sequents, $\Gamma_1 \rightarrow \Delta_1, A \wedge B, C_1 \vee C_2$ and $C_1 \vee C_2, \Gamma_2 \rightarrow \Delta_2$ can be derived. Thus $C_1 \vee C_2$ serves as the required interpolant.

3) $k > 0$ and the last inference is \forall : left:

$$\frac{F(s), \Gamma \rightarrow \Delta}{\forall x F(x), \Gamma \rightarrow \Delta}.$$

Suppose b_1, \dots, b_n are all the free variables and constants (possibly none) which occur in s . Suppose the partition is $[\{\forall x F(x), \Gamma_1; \Delta_1\}, \{\Gamma_2; \Delta_2\}]$. Consider the induced partition of the upper sequent and apply the induction hypothesis. So there exists an interpolant $C(b_1, \dots, b_n)$ so that

$$F(s), \Gamma_1 \rightarrow \Delta_1, C(b_1, \dots, b_n) \quad \text{and} \quad C(b_1, \dots, b_n), \Gamma_2 \rightarrow \Delta_2$$

are **LK#**-provable. Let b_{i_1}, \dots, b_{i_m} be all the variables and constants among b_1, \dots, b_n which do not occur in $\{F(x), \Gamma_1; \Delta_1\}$. Then

$$\forall y_1 \dots \forall y_m C(b_1, \dots, y_1, \dots, y_m, \dots, b_n),$$

where b_{i_1}, \dots, b_{i_m} are replaced by the bound variables, serves as the required interpolant.

4) $k > 0$ and the last inference is \forall : right:

$$\frac{\Gamma \rightarrow \Delta, F(a)}{\Gamma \rightarrow \Delta, \forall x F(x)},$$

where a does not occur in the lower sequent.

Suppose the partition is $[\{\Gamma_1; \Delta_1, \forall x F(x)\}, \{\Gamma_2; \Delta_2\}]$. By the induction hypothesis there exists an interpolant C so that $\Gamma_1 \rightarrow \Delta_1, F(a), C$ and $C, \Gamma_2 \rightarrow \Delta_2$ are provable. Since C does not contain a , we can derive

$$\Gamma_1 \rightarrow \Delta_1, \forall x F(x), C,$$

and hence C serves as the interpolant.

All other cases are treated similarly.

EXERCISE 6.7. Let A and B be prenex formulas which have only \forall and \wedge as logical symbols. Assume furthermore that there is at least one predicate constant common to A and B . Suppose $A \supset B$ is provable.

Show that there exists a formula C such that

- 1) $A \supset C$ and $C \supset B$ are provable;
- 2) C is a prenex formula;

- 3) the only logical symbols in C are \forall and \wedge ;
 4) the predicate constants in C are common to A and B .

[Hint: Apply the cut-elimination theorem and the midsequent theorem.]

DEFINITION 6.8. (1) A semi-term is an expression like a term, except that bound variables are (also) allowed in its construction. (The precise definition is left to the reader.) Let t be a term and s a semi-term. We call s a sub-semi-term of t if

- (i) s contains a bound variable (that is, s is not a term),
- (ii) s is not a bound variable itself,
- (iii) some subterm of t is obtained from s by replacing all the bound variables in s by appropriate terms.

(2) A semi-formula is an expression like a formula, except that bound variables are (also) allowed to occur free in it (i.e., not in the scope of a quantifier).

THEOREM 6.9. *Let t be a term and S a provable sequent satisfying:*

- (*) *There is no sub-semi-term of t in S .*

Then the sequent which is obtained from S by replacing all the occurrences of t in S by a free variable is also provable.

PROOF (outline). Consider a cut-free regular proof of S , say P . From the observation that if (*) holds for the lower sequent of an inference in P then it holds for the upper sequent(s), the theorem follows easily by mathematical induction on the number of inferences in P .

DEFINITION 6.10. Let R_1, \dots, R_m, R be predicate constants. Let $A(R, R_1, \dots, R_m)$ be a sentence in which all occurrences of R, R_1, \dots, R_m are indicated. Let R' be a predicate constant with the same number of argument-places as R . Let B be $\forall x_1 \dots \forall x_k (R(x_1, \dots, x_k) \equiv R'(x_1, \dots, x_k))$, where the string of quantifiers is empty if $k = 0$, and let C be $A(R, R_1, \dots, R_m) \wedge A(R', R_1, \dots, R_m)$. We say that $A(R, R_1, \dots, R_m)$ defines (in **LK**) R implicitly in terms of R_1, \dots, R_m if $C \supset B$ is (**LK**)-provable and we say that $A(R, R_1, \dots, R_m)$ defines (in **LK**) R explicitly in terms of R_1, \dots, R_m and the individual constants in $A(R, R_1, \dots, R_m)$ if there exists a formula $F(a_1, \dots, a_k)$ containing only the predicate constants R_1, \dots, R_m and the individual constants in $A(R, R_1, \dots, R_m)$ such that

$$A(R, R_1, \dots, R_m) \rightarrow \forall x_1 \dots \forall x_k (R(x_1, \dots, x_k) \equiv F(x_1, \dots, x_k))$$

is **LK**-provable.

PROPOSITION 6.11 (Beth's definability theorem for **LK**). *If a predicate constant R is defined implicitly in terms of R_1, \dots, R_m by $A(R, R_1, \dots, R_m)$, then R can be defined explicitly in terms of R_1, \dots, R_m and the individual constants in $A(R, R_1, \dots, R_m)$.*

PROOF (outline). Let c_1, \dots, c_n be free variables not occurring in A . Then

$$A(R, R_1, \dots, R_m), A(R', R_1, \dots, R_m) \rightarrow R(c_1, \dots, c_n) \equiv R'(c_1, \dots, c_n)$$

and hence also

$$A(R, R_1, \dots, R_m) \wedge R(c_1, \dots, c_k) \rightarrow A(R', R_1, \dots, R_m) \supset R'(c_1, \dots, c_n)$$

are provable. Now apply Craig's theorem (i.e., part (1) of Theorem 6.6) to the latter sequent.

We now present a version of Robinson's theorem (for **LK**).

PROPOSITION 6.12 (Robinson). *Assume that the language contains no function constants. Let \mathcal{A}_1 and \mathcal{A}_2 be two consistent axiom systems. Suppose furthermore that, for any sentence A which is dependent on \mathcal{A}_1 and \mathcal{A}_2 , it is not the case that $\mathcal{A}_1 \rightarrow A$ and $\mathcal{A}_2 \rightarrow \neg A$ (or $\mathcal{A}_1 \rightarrow \neg A$ and $\mathcal{A}_2 \rightarrow A$) are both provable. Then $\mathcal{A}_1 \cup \mathcal{A}_2$ is consistent. (See Definition 4.1 for the technical terms.)*

PROOF (outline). Suppose $\mathcal{A}_1 \cup \mathcal{A}_2$ is not consistent. Then there are axiom sequences Γ_1 and Γ_2 from \mathcal{A}_1 and \mathcal{A}_2 respectively such that $\Gamma_1, \Gamma_2 \rightarrow$ is provable. Since \mathcal{A}_1 and \mathcal{A}_2 are each consistent, neither Γ_1 nor Γ_2 is empty. Apply Lemma 6.5 to the partition $[\{\Gamma_1; \}, \{\Gamma_2; \}]$.

Let **LK'** and **LJ'** denote the quantifier-free parts of **LK** and **LJ**, respectively, viz. the formulations (in tree form) of the classical and intuitionistic propositional calculus, respectively.

THEOREM 6.13. *There exist decision procedures for **LK'** and **LJ'**.*

PROOF (outline). The following decision procedure was given by Gentzen. A sequent of **LK'** (or **LJ'**) is said to be reduced if in the antecedent the same formula does not occur at more than three places as sequent-formulas, and likewise in the succedent. A sequent S' is called a *reduct* of a sequent S if S' is reduced and is obtained from S by deleting some occurrences of formulas. Now, given a sequent S of **LK'** (or **LJ'**), let S' be any reduct of S . We note the following.

1) S is provable or unprovable according as S' is provable or unprovable.

2) The number of all reduced sequents which contain only subformulas of the formulas in S is finite.

Consider the finite system of sequents as in 2), say \mathcal{S} . Collect all initial sequents in the systems. Call this set \mathcal{S}_0 . Then examine $\mathcal{S} - \mathcal{S}_0$ to see if there is a sequent which can be the lower sequent of an inference whose upper sequent(s) is (are) one (two) sequent(s) from \mathcal{S}_0 . Call the set of all sequents which satisfy this condition \mathcal{S}_1 . Now see if there is a sequent in $(\mathcal{S} - \mathcal{S}_0) - \mathcal{S}_1$ which can be the lower sequent of an inference whose upper sequent(s) is (are) one (two) of the sequent(s) in $\mathcal{S}_0 \cup \mathcal{S}_1$. Continue this process until either the sequent S' itself is determined as provable, or the process does not give any new sequent as provable. One of the two must happen. If the former is the case, then S is provable. Otherwise S is unprovable. (Note that the whole argument is finitary.)

THEOREM 6.14 (1) (Harrop). *Let Γ be a finite sequence of formulas such that in each formula of Γ every occurrence of \vee and \exists is either in the scope of a \neg or in the left scope of a \supset (cf. Definition 6.1, part 3)). This condition will be referred to as (*) in this theorem. Then*

1) $\Gamma \rightarrow A \vee B$ is **LJ**-provable if and only if $\Gamma \rightarrow A$ or $\Gamma \rightarrow B$ is **LJ**-provable,

2) $\Gamma \rightarrow \exists x F(x)$ is **LJ**-provable if and only if for some term s , $\Gamma \rightarrow F(s)$ is **LJ**-provable.

(2) The following sequents (which are **LK**-provable) are not (in general) **LJ**-provable.

$$\begin{aligned} \neg(\neg A \wedge \neg B) &\rightarrow A \vee B; & \neg\forall x \neg F(x) &\rightarrow \exists x F(x); \\ A \supset B &\rightarrow \neg A \vee B; & \neg\forall x F(x) &\rightarrow \exists x \neg F(x); \\ \neg(A \wedge B) &\rightarrow \neg A \vee \neg B. \end{aligned}$$

PROOF. (1) part 1): The “if” part is trivial. For the “only if” part, consider a cut-free proof of $\Gamma \rightarrow A \vee B$. The proof is carried out by induction on the number of inferences below all the inferences for \vee and \exists in the given proof. If the last inference is \vee : right, there is nothing to prove. Notice that the last inference cannot be \vee , \neg , or \exists : left.

Case 1: The last inference is \wedge : left:

$$\frac{C, \Gamma \rightarrow A \vee B}{C \wedge D, \Gamma \rightarrow A \vee B}$$

It is obvious that C satisfies the condition (*). Thus the induction hypothesis applies to the upper sequent; hence either $C, \Gamma \rightarrow A$ or $C, \Gamma \rightarrow B$ is provable. In either case, the end-sequent can be derived in **LJ**.

Case 2: The last inference is \supset : left:

$$\frac{\Gamma \rightarrow C \quad D, \Gamma \rightarrow A \vee B}{C \supset D, \Gamma \rightarrow A \vee B}.$$

It is obvious that D satisfies the condition (*); thus, by the induction hypothesis applied to the right upper sequent, $D, \Gamma \rightarrow A$ or $D, \Gamma \rightarrow B$ is provable. In either case the end-sequent can be derived.

Other cases are treated likewise. The proofs of (1) part 2), and (2), are left to the reader.

§7. The predicate calculus with equality

DEFINITION 7.1. The predicate calculus with equality (denoted \mathbf{LK}_e) can be obtained from \mathbf{LK} by specifying a predicate constant of two argument places ($=$: read equals) and adding the following sequents as additional initial sequents ($a = b$ denoting $=(a, b)$):

$$\rightarrow s = s;$$

$$s_1 = t_1, \dots, s_n = t_n \rightarrow f(s_1, \dots, s_n) = f(t_1, \dots, t_n)$$

for every function constant f of n argument-places ($n = 1, 2, \dots$);

$$s_1 = t_1, \dots, s_n = t_n, R(s_1, \dots, s_n) \rightarrow R(t_1, \dots, t_n)$$

for every predicate constant R (including $=$) of n argument-places ($n = 1, 2, \dots$); where $s, s_1, \dots, s_n, t_1, \dots, t_n$ are arbitrary terms.

Each such sequent may be called an equality axiom of \mathbf{LK}_e .

PROPOSITION 7.2. Let $A(a_1, \dots, a_n)$ be an arbitrary formula. Then

$$s_1 = t_1, \dots, s_n = t_n, A(s_1, \dots, s_n) \rightarrow A(t_1, \dots, t_n)$$

is provable in \mathbf{LK}_e , for any terms s_i, t_i ($1 \leq i \leq n$). Furthermore, $s = t \rightarrow t = s$ and $s_1 = s_2, s_2 = s_3 \rightarrow s_1 = s_3$ are also provable.

DEFINITION 7.3. Let Γ_e be the set (axiom system) consisting of the following sentences:

$$\forall x(x = x),$$

$$\begin{aligned} \forall x_1 \dots \forall x_n \forall y_1 \dots \forall y_n [x_1 = y_1 \wedge \dots \wedge x_n = y_n \supset f(x_1, \dots, x_n) = f(y_1, \dots, y_n)] \end{aligned}$$

for every function constant f with n argument-places ($n = 1, 2, \dots$),

$$\forall x_1 \dots \forall x_n \forall y_1 \dots \forall y_n [x_1 = y_1 \wedge \dots \wedge x_n = y_n \wedge R(x_1, \dots, x_n) \supset R(y_1, \dots, y_n)]$$

for every predicate constant R of n argument-places ($n = 1, 2, \dots$). Each such sentence is called an equality axiom.

PROPOSITION 7.4. *A sequent $\Gamma \rightarrow \Delta$ is provable in \mathbf{LK}_e if and only if $\Gamma, \Gamma_e \rightarrow \Delta$ is provable in \mathbf{LK} .*

PROOF. Only if: It is easy to see that all initial sequents of \mathbf{LK}_e are provable from Γ_e . Therefore the proposition is proved by mathematical induction on the number of inferences in a proof of the sequent $\Gamma \rightarrow \Delta$.

If: All formulas of Γ_e are \mathbf{LK}_e -provable.

DEFINITION 7.5. If the cut formula of a cut in \mathbf{LK}_e is of the form $s = t$, then the cut is called inessential. It is called essential otherwise.

THEOREM 7.6 (the cut-elimination theorem for the predicate calculus with equality, \mathbf{LK}_e). *If a sequent of \mathbf{LK}_e is \mathbf{LK}_e -provable, then it is \mathbf{LK}_e -provable without an essential cut.*

PROOF. The theorem is proved by removing essential cuts (mixes as a matter of fact), following the method used for Theorem 5.1.

If the rank is 2, S_2 is an equality axiom and the mix formula is not of the form $s = t$, then the mix formula is of the form $P(t_1, \dots, t_n)$. If S_1 is also an equality axiom, then it has the form

$$s_1 = t_1, \dots, s_n = t_n, P(s_1, \dots, s_n) \rightarrow P(t_1, \dots, t_n).$$

From this and S_2 , i.e.,

$$t_1 = r_1, \dots, t_n = r_n, P(t_1, \dots, t_n) \rightarrow P(r_1, \dots, r_n),$$

we obtain by a mix

$$s_1 = t_1, \dots, s_n = t_n, t_1 = r_1, \dots, t_n = r_n, P(s_1, \dots, s_n) \rightarrow P(r_1, \dots, r_n).$$

This may be replaced by

$$s_i = t_i, t_i = r_i \rightarrow s_i = r_i \quad (i = 1, 2, \dots, n);$$

$$s_1 = r_1, \dots, s_n = r_n, P(s_1, \dots, s_n) \rightarrow P(r_1, \dots, r_n);$$

and then repeated cuts of $s_i = r_i$ to produce the same end-sequent. All cuts (or mixes) introduced here are inessential.

If $P(t_1, \dots, t_n)$ in S_2 is a weakening formula, then the mix inference is:

$$\frac{s_1 = t_1, \dots, s_n = t_n, P(s_1, \dots, s_n) \rightarrow P(t_1, \dots, t_n) \quad P(t_1, \dots, t_n), \Pi \rightarrow \Lambda}{s_1 = t_1, \dots, s_n = t_n, P(s_1, \dots, s_n), \Pi \rightarrow \Lambda}.$$

Transform this into:

$$\frac{\Pi \rightarrow \Lambda}{\text{end-sequent.}}$$

The rest of the argument in Theorem 5.1 goes through.

PROBLEM 7.7. A sequent of the form

$$s_1 = t_1, \dots, s_n = t_n \rightarrow s = t \quad (n = 0, 1, 2, \dots)$$

is said to be simple if it is obtained from sequents of the following four forms by applications of exchanges, contractions, cuts, and weakening left.

- 1) $\rightarrow s = s$.
- 2) $s = t \rightarrow t = s$.
- 3) $s_1 = s_2, s_2 = s_3 \rightarrow s_1 = s_3$.
- 4) $s_1 = t_1, \dots, s_m = t_m \rightarrow f(s_1, \dots, s_m) = f(t_1, \dots, t_m)$.

Prove that if $s_1 = s_1, \dots, s_m = s_m \rightarrow s = t$ is simple, then $s = t$ is of the form $s = s$. As a special case, if $\rightarrow s = t$ is simple, then $s = t$ is of the form $s = s$.

Let \mathbf{LK}'_e be the system which is obtained from \mathbf{LK} by adding the following sequents as initial sequents:

- a) simple sequents,
- b) sequents of the form

$$s_1 = t_1, \dots, s_m = t_m, R(s'_1, \dots, s'_n) \rightarrow R(t'_1, \dots, t'_n),$$

where $s_1 = t_1, \dots, s_m = t_m \rightarrow s'_i = t'_i$ is simple for each i ($i = 1, \dots, n$). First prove that the initial sequents of \mathbf{LK}'_e are closed under cuts and that if

$$R(s_1, \dots, s_n) \rightarrow R(t_1, \dots, t_n)$$

is an initial sequent of \mathbf{LK}'_e (where R is not $=$), then it is of the form $D \rightarrow D$. Finally, prove that the cut-elimination theorem (without the exception of inessential cuts) holds for \mathbf{LK}'_e .

PROBLEM 7.8. Show that if a sequent S without the $=$ symbol is \mathbf{LK}_e -provable, then it is provable in \mathbf{LK} (without $=$).

PROBLEM 7.9. Prove that Theorems 6.2–6.4, 6.6, 6.9, and 6.14, Propositions 6.11 and 6.12 and Exercise 6.7 hold for \mathbf{LK}_c when they are modified in the following way: References to \mathbf{LK} - (or \mathbf{LJ} -) provability are replaced throughout by references to \mathbf{LK}_c -provability, and further, when the statement demands that a formula can contain only certain constants, = can be added as an exception.

The general technique of proof is to change a condition that a sequent $\Gamma \rightarrow \Delta$ be provable in \mathbf{LK} to one that a sequent $\Pi, \Gamma \rightarrow \Delta$ be provable in \mathbf{LK} , where Π is a set of equality axioms, and in this way to reduce the problem to \mathbf{LK} .

§8. The completeness theorem

Although we do not intend to develop model theory in this book, we shall outline a proof of the completeness theorem for \mathbf{LK} . The completeness theorem for the first order predicate calculus was first proved by Gödel. Here we follow Schütte's method, which has a close relationship to the cut-elimination theorem. In fact the cut-elimination theorem is a corollary of the completeness theorem as formulated below. (The importance of the proof of cut-elimination in §5 lies in its constructive nature.)

DEFINITION 8.1. (1) Let L be a language as described in §1. By a *structure* for L (an L -structure) we mean a pair $\langle D, \phi \rangle$, where D is a non-empty set and ϕ is a map from the constants of L such that

- (i) if k is an individual constant, then ϕk is an element of D ;
- (ii) if f is a function constant of n arguments, then ϕf is a mapping from D^n into D ;
- (iii) if R is a predicate constant of n arguments, then ϕR is a subset of D^n .

(2) An *interpretation* of L is a structure $\langle D, \phi \rangle$ together with a mapping ϕ_0 from variables into D . We may denote an interpretation $\langle \langle D, \phi \rangle, \phi_0 \rangle$ simply by \mathfrak{I} . ϕ_0 is called an assignment from D .

(3) We say that an interpretation $\mathfrak{I} = \langle \langle C, \phi \rangle, \phi_0 \rangle$ *satisfies* a formula A if this follows from the following inductive definition. In fact we shall define the notion of "satisfying" for all semi-formulas (cf. Definition 6.8).

0) Firstly, we define $\phi(t)$, for every semi-term t , inductively as follows. We define $\phi(a) = \phi_0(a)$ and $\phi(x) = \phi_0(x)$ for all free variables a and bound variables x . Next, if f is a function constant and t is a semi-term for which ϕt is already defined, then $\phi(f(t))$ is defined to be $(\phi f)(\phi t)$.

1) If R is a predicate constant of n arguments and t_1, \dots, t_n are semi-terms, then \mathfrak{I} satisfies $R(t_1, \dots, t_n)$ if and only if $\langle \phi t_1, \dots, \phi t_n \rangle \in \phi R$.

2) \mathfrak{I} satisfies $\neg A$ if and only if it does not satisfy A ; \mathfrak{I} satisfies $A \wedge B$ if

and only if it satisfies both A and B ; \mathfrak{I} satisfies $A \vee B$ if and only if it satisfies either A or B ; \mathfrak{I} satisfies $A \supset B$ if and only if either it does not satisfy A or it satisfies B .

3) \mathfrak{I} satisfies $\forall x B$ if and only if for every ϕ'_0 such that ϕ_0 and ϕ'_0 agree, except possibly on x , $(\langle D, \phi \rangle, \phi'_0)$ satisfies B ; \mathfrak{I} satisfies $\exists x B$ if and only if for some ϕ'_0 such that ϕ_0 and ϕ'_0 agree, except possibly on x , $(\langle D, \phi \rangle, \phi'_0)$ satisfies B .

If $\mathfrak{I} = (\langle D, \phi \rangle, \phi_0)$ satisfies a formula A , we say that A is satisfied in $\langle D, \phi \rangle$ by ϕ_0 , or simply A is satisfied by \mathfrak{I} .

(4) A formula is called valid in $\langle D, \phi \rangle$ if and only if for every ϕ_0 , $(\langle D, \phi \rangle, \phi_0)$ satisfies that formula. It is called valid if it is valid in every structure.

(5) A sequent $\Gamma \rightarrow \Delta$ is satisfied in $\langle D, \phi \rangle$ by ϕ_0 (or $\mathfrak{I} = (\langle D, \phi \rangle, \phi_0)$ satisfies $\Gamma \rightarrow \Delta$) if either some formula in Γ is not satisfied by \mathfrak{I} , or some formula in Δ is satisfied by \mathfrak{I} . A sequent is valid if it is satisfied in every interpretation.

(6) A structure may also be denoted as

$$\langle D; \phi k_0, \phi k_1, \dots, \phi f_0, \phi f_1, \dots, \phi R_0, \phi R_1, \dots \rangle.$$

A structure is called a model of an axiom system Γ if every sentence of Γ is valid in it. It is called a counter-model of Γ if there is a sentence of Γ which is not valid in it.

THEOREM 8.2 (completeness and soundness). *A formula is provable in **LK** if and only if it is valid.*

NOTES. (1) The “if” part of the theorem is the statement of the completeness of **LK**. In general, a system is said to be complete if and only if every valid formula is provable in the system (for a suitable definition of validity).

Soundness means: all provable sequents are valid, i.e., the “only if” part of the theorem. Soundness ensures consistency.

(2) The theorem connects proof theory with semantics, where semantics means, very roughly, the study of the interpretation of formulas in a structure (of a language), and hence of their truth or falsity.

PROOF OF THEOREM 8.2. The “only if” part is easily proved by induction on the number of inferences in a proof of the formula. We prove the “if” part in the following generalized form:

LEMMA 8.3. *Let S be a sequent. Then either there is a cut-free proof of S , or there is an interpretation which does not satisfy S (and hence S is not valid).*

PROOF. We will define, for each sequent S , a (possibly infinite) tree, called

the reduction tree for S , from which we can obtain either a cut-free proof of S or an interpretation not satisfying S . (This method is due to Schütte.) This reduction tree for S contains a sequent at each node. It is constructed in stages as follows.

Stage 0: Write S at the bottom of the tree.

Stage k ($k > 0$): This is defined by cases:

Case I. Every topmost sequent has a formula common to its antecedent and succedent. Then stop.

Case II. Not Case I. Then this stage is defined according as

$$k \equiv 0, 1, 2, \dots, 11, 12 \pmod{13}.$$

$k \equiv 0$ and $k \equiv 1$ concern the symbol \neg ; $k \equiv 2$ and $k \equiv 3$ concern \wedge ; $k \equiv 4$ and $k \equiv 5$ concern \vee ; $k \equiv 6$ and $k \equiv 7$ concern \supset ; $k \equiv 8$ and $k \equiv 9$ concern \forall ; and $k \equiv 10$ and $k \equiv 11$ concern \exists .

Since the formation of reduction trees is a common technique and will be used several times in this text, we shall describe these stages of the so-called reduction process in detail. In order to make the discussion simpler, let us assume that there are no individual or function constants.

All the free variables which occur in any sequent which has been obtained at or before stage k are said to be "available at stage k ". In case there is none, pick any free variable and say that it is available.

0) $k \equiv 0$. Let $\Pi \rightarrow \Lambda$ be any topmost sequent of the tree which has been defined by stage $k - 1$. Let $\neg A_1, \dots, \neg A_n$ be all the formulas in Π whose outermost logical symbol is \neg , and to which no reduction has been applied in previous stages. Then write down

$$\Pi \rightarrow \Lambda, A_1, \dots, A_n$$

above $\Pi \rightarrow \Lambda$. We say that a \neg :left reduction has been applied to $\neg A_1, \dots, \neg A_n$.

1) $k \equiv 1$. Let $\neg A_1, \dots, \neg A_n$ be all the formulas in Λ whose outermost logical symbol is \neg and to which no reduction has been applied so far. Then write down

$$A_1, \dots, A_n, \Pi \rightarrow \Lambda$$

above $\Pi \rightarrow \Lambda$. We say that a \neg :right reduction has been applied to $\neg A_1, \dots, \neg A_n$.

2) $k \equiv 2$. Let $A_1 \wedge B_1, \dots, A_n \wedge B_n$ be all the formulas in Π whose outermost logical symbol is \wedge and to which no reduction has been applied yet. Then write down

$$A_1, B_1, A_2, B_2, \dots, A_n, B_n, \Pi \rightarrow \Lambda$$

above $\Pi \rightarrow \Lambda$. We say that an \wedge : left reduction has been applied to

$$A_1 \wedge B_1, \dots, A_n \wedge B_n.$$

3) $k \equiv 3$. Let $A_1 \wedge B_1, A_2 \wedge B_2, \dots, A_n \wedge B_n$ be all the formulas in Λ whose outermost logical symbol is \wedge and to which no reduction has been applied yet. Then write down all sequents of the form

$$\Pi \rightarrow \Lambda, C_1, \dots, C_n,$$

where C_i is either A_i or B_i , above $\Pi \rightarrow \Lambda$. Take all possible combinations of such: so there are 2^n such sequents above $\Pi \rightarrow \Lambda$. We say that an \wedge : right reduction has been applied to $A_1 \wedge B_1, \dots, A_n \wedge B_n$.

4) $k \equiv 4$. \wedge : left reduction. This is defined in a manner symmetric to 3).

5) $k \equiv 5$. \vee : right reduction. This is defined in a manner symmetric to 2).

6) $k \equiv 6$. Let $A_1 \supset B_1, \dots, A_n \supset B_n$ be all the formulas in Π whose outermost logical symbol is \supset and to which no reduction has been applied yet. Then write down the following sequents above $\Pi \rightarrow \Lambda$:

$$B_{i_1}, B_{i_2}, \dots, B_{i_k}, \Pi \rightarrow \Lambda, A_{j_1}, A_{j_2}, \dots, A_{j_{n-k}},$$

where $i_1 < i_2 < \dots < i_k$, $j_1 < j_2 < \dots < j_{n-k}$ and $(i_1, i_2, \dots, i_k, j_1, j_2, \dots, j_{n-k})$ is a permutation of $(1, 2, \dots, n)$. Take all possible permutations: so there are 2^n such sequents above $\Pi \rightarrow \Lambda$. We say that an \supset : left reduction has been applied to $A_1 \supset B_1, \dots, A_n \supset B_n$.

7) $k \equiv 7$. Let $A_1 \supset B_1, \dots, A_n \supset B_n$ be all the formulas in Λ whose outermost logical symbol is \supset and to which no reduction has been applied yet. Then write down

$$A_1, A_2, \dots, A_n, \Pi \rightarrow \Lambda, B_1, B_2, \dots, B_n$$

above $\Pi \rightarrow \Lambda$. We say that an \supset : right reduction has been applied to

$$A_1 \supset B_1, \dots, A_n \supset B_n.$$

8) $k \equiv 8$. Let $\forall x_1 A_1(x_1), \dots, \forall x_n A_n(x_n)$ be all the formulas in Π whose outermost logical symbol is \forall . Let a_i be the first variable available at this stage which has not been used for a reduction of $\forall x_i A_i(x)$ for $1 \leq i \leq n$. Then write down

$$A_1(a_1), \dots, A_n(a_n), \Pi \rightarrow \Lambda$$

above $\Pi \rightarrow \Lambda$. We say that a \forall : left reduction has been applied to

$$\forall x_1 A_1(x), \dots, \forall x_n A_n(x).$$

9) $k \equiv 9$. Let $\forall x_1 A_1(x_1), \dots, \forall x_n A_n(x_n)$ be all the formulas in Λ whose outermost logical symbol is \forall and to which no reduction has been applied so far. Let a_1, \dots, a_n be the first n free variables (in the list of variables) which are *not* available at this stage. Then write down

$$\Pi \rightarrow \Lambda, A_1(a_1), \dots, A_n(a_n)$$

above $\Pi \rightarrow \Lambda$. We say that a \forall :right reduction has been applied to $\forall x_1 A_1(x_1), \dots, \forall x_n A_n(x_n)$. Notice that a_1, \dots, a_n are new available free variables.

10) $k \equiv 10$. \exists :left reduction. This is defined in a manner symmetric to 9).

11) $k \equiv 11$. \exists :right reduction. This is defined in a manner symmetric to 8).

12) If Π and Λ have any formula in common, write nothing above $\Pi \rightarrow \Lambda$ (so this remains a topmost sequent). If Π and Λ have no formula in common and the reductions described in 0)–11) are not applicable, write the same sequent $\Pi \rightarrow \Lambda$ again above it.

So the collection of those sequents which are obtained by the above reduction process, together with the partial order obtained by this process, is the reduction tree (for S). It is denoted by $T(S)$. We will construct “reduction trees” like this again.

As an example of the case where the reduction process does not terminate, consider a sequent of the form $\forall x \exists y A(x, y) \rightarrow$, where A is a predicate constant.

Now a (finite or infinite) sequence S_0, S_1, S_2, \dots of sequents in $T(S)$ is called a branch if (i) $S_0 = S$; (ii) S_{i+1} stands immediately above S_i ; (3) if the sequence is finite, say S_1, \dots, S_n , then S_n has the form $\Pi \rightarrow \Lambda$, where Π and Λ have a formula in common.

Now, given a sequent S , let T be the reduction tree $T(S)$. If each branch of T ends with a sequent whose antecedent and succedent contain a formula in common, then it is a routine task to write a proof without a cut ending with S by suitably modifying T . Otherwise there is an infinite branch. Consider such a branch, consisting of sequents $S = S_0, S_1, \dots, S_n, \dots$.

Let S_i be $\Gamma_i \rightarrow \Delta_i$. Let $\cup \Gamma$ be the set of all formulas occurring in Γ_i for some i , and let $\cup \Delta$ be the set of all formulas occurring in Δ_j for some j . We shall define an interpretation in which every formula in $\cup \Gamma$ holds and no formula in $\cup \Delta$ holds. Thus S does not hold in it.

First notice that from the way the branch was chosen, $\cup \Gamma$ and $\cup \Delta$ have no atomic formula in common. Let D be the set of all the free variables. We consider the interpretation $\mathfrak{I} = (\langle D, \phi \rangle, \phi_0)$, where ϕ and ϕ_0 are defined as follows: $\phi_0(a) = a$ for all free variables a , $\phi_0(x)$ is defined arbitrarily for all bound variables x . For an n -ary predicate constant R , ϕR is any subset of D^n such that: if $R(a_1, \dots, a_n) \in \cup \Gamma$, then $(a_1, \dots, a_n) \in \phi R$, and $(a_1, \dots, a_n) \notin \phi R$ otherwise.

We claim that this interpretation \mathfrak{I} has the required property: it satisfies

every formula in $\cup \Gamma$, but no formula in $\cup \Delta$. We prove this by induction on the number of logical symbols in the formula A . We consider here only the case where A is of the form $\forall x F(x)$ and assume the induction hypothesis:

Subcase 1. A is in $\cup \Gamma$. Let i be the least number such that A is in Γ_i . Then A is in Γ_j for all $j > i$. It is sufficient to show that all substitution instances $A(a)$, for $a \in D$, are satisfied by \mathfrak{I} , i.e., all these substitution instances are in $\cup \Gamma$. But this is evident from the way we construct the tree.

Subcase 2. A is in $\cup \Delta$. Consider the step at which A was used to define an upper sequent from $\Gamma_i \rightarrow \Delta_i$ (or $\Gamma_i \rightarrow \Delta_i^1, A, \Delta_i^2$). It looks like this:

$$\frac{\Gamma_{i+1} \rightarrow \Delta_{i+1}^1, F(a), \Delta_{i+1}^2}{\Gamma_i \rightarrow \Delta_i^1, A, \Delta_i^2}.$$

Then by the induction hypothesis, $F(a)$ is not satisfied by \mathfrak{I} , so A is not satisfied by \mathfrak{I} either. This completes the proof.

PROBLEM 8.4 (Feferman). Let J be a non-empty set. Each element of J is called a *sort*. A many-sorted language for the set of sorts J , say $L(J)$, consists of the following.

- 1) Individual constants: $k_0, k_1, \dots, k_i, \dots$, where to each k_i is assigned one sort.
- 2) Predicate constants: $R_0, R_1, \dots, R_i, \dots$, where to each R_i is assigned a number n (≥ 0) (the number of arguments) and sorts j_1, \dots, j_n . We say that $(n; j_1, \dots, j_n)$ is assigned to R_i .
- 3) Function constants: $f_0, f_1, \dots, f_i, \dots$, where to each f_i is assigned a number n (≥ 1) (the number of arguments) and sorts j_1, \dots, j_n, j . We say that $(n; j_1, \dots, j_n, j)$ is assigned to f_i .
- 4) Free variables of sort j for each j in J : $a_0^j, a_1^j, \dots, a_i^j, \dots$.
- 5) Bound variables of sort j for each j in J : $x_0^j, x_1^j, \dots, x_i^j, \dots$.
- 6) Logical symbols: $\neg, \wedge, \vee, \supset, \forall, \exists$.

Terms of sort j for each j are defined as follows. Individual constants and free variables of sort j are terms of sort j ; if f is a function constant with $(n; j_1, \dots, j_n, j)$ assigned to it and t_1, \dots, t_n are terms of sort j_1, \dots, j_n , respectively, then $f(t_1, \dots, t_n)$ is a term of sort j .

If R is a predicate constant with $(n; j_1, \dots, j_n)$ assigned to it and t_1, \dots, t_n are terms of sort j_1, \dots, j_n , respectively, then $R(t_1, \dots, t_n)$ is an atomic formula. If $F(a^j)$ is a formula and x^j does not occur in $F(a^j)$, then $\forall x^j F(x^j)$ and $\exists x^j F(x^j)$ are formulas; the other steps in building formulas of $L(J)$ are as usual. The sequents of $L(J)$ are defined as usual.

The rules of inference are those of **LK**, except that in the rules for \forall and \exists , terms and free variables must be replaced by bound variables of the same sort.

Prove the following:

- (1) The cut-elimination theorem holds for the system just defined.

Next, define Sort , Ex , Un , Fr , and Pr as follows. $\text{Sort}(A)$ is the set of j in J such that a symbol of sort j occurs in A ; $\text{Ex}(A)$ and $\text{Un}(A)$ are the sets of sorts of bound variables which occur in some essentially existential, respectively universal quantifier in A . (An occurrence of \exists , say $\#$, is said to be essentially existential or universal according to the following definition. Count the number of \neg and \supset in A such that $\#$ is either in the scope of \neg , or in the left scope of \supset . If this number is even, then $\#$ is essentially existential in A , while if it is odd then $\#$ is essentially universal. Likewise, we define, dually, an occurrence of \forall to be essentially existential or universal.) $\text{Fr}(A)$ is the set of free variables in A ; $\text{Pr}(A)$ is the set of predicate constants in A .

(2) Suppose $A \supset B$ is provable in the above system and at least one of $\text{Sort}(A) \cap \text{Ex}(B)$ and $\text{Sort}(B) \cap \text{Un}(A)$ is not empty. Then there is a formula C such that $\sigma(C) \subseteq \sigma(A) \cap \sigma(B)$, where σ stands for Fr , Pr or Sort , and such that $\text{Un}(C) \subseteq \text{Un}(A)$ and $\text{Ex}(C) \subseteq \text{Ex}(B)$. [*Hint*: Re-state the above theorem for sequents and apply (1), viz. the cut-elimination theorem.]

DEFINITION 8.5. We can define a structure for a many-sorted language as follows. Let $L(J)$ be a many-sorted language. A structure for $L(J)$ is a pair $\langle D, \phi \rangle$, where D is a set of non-empty sets $\{D_j; j \in J\}$ and ϕ is a map from the constants of $L(J)$ into appropriate objects. We call D_j the domain of the structure of sort j . We leave the listing of the conditions on ϕ to the reader; we only have to keep in mind that an individual constant of sort j is a member of D_j . Let $\mathcal{M} = \langle D, \phi \rangle$ and $\mathcal{M}' = \langle D', \phi' \rangle$ be two structures for $L(J)$. We say \mathcal{M}' is an extension of \mathcal{M} and write $\mathcal{M} \subseteq \mathcal{M}'$ if

- (i) for each j in J , $D_j \subseteq D'_j$,
- (ii) for each individual constant k , $\phi'k = \phi k$,
- (iii) for each predicate constant R with $(n; j_1, \dots, j_n)$ assigned to it,

$$\phi R = \phi' R \cap (D_{j_1} \times \dots \times D_{j_n}),$$

- (iv) for each function constant f with $(n; j_1, \dots, j_n, j)$ assigned to it and $(d_1, \dots, d_n) \in D_{j_1} \times \dots \times D_{j_n}$,

$$(\phi'f)(d_1, \dots, d_n) = (\phi f)(d_1, \dots, d_n).$$

A formula is said to be existential if $\text{Un}(A)$ is empty.

COROLLARY 8.6 (Łos-Tarski). *The following are equivalent: let A be a formula of an ordinary (i.e., single-sorted) language L .*

(i) *For any structure \mathcal{M} (for L) and extension \mathcal{M}' , and any assignments ϕ, ϕ' from the domains of $\mathcal{M}, \mathcal{M}'$, respectively, which agree on the free variables of A , if (\mathcal{M}, ϕ) satisfies A , then so does (\mathcal{M}', ϕ') .*

(ii) *There exists an (essentially) existential formula B such that $A \equiv B$ is provable and the free variables of B are among those of A .*

PROOF. (Feferman) We assume (for simplicity) that the language has no individual and function constants. The major task is to write down the conditions in (1) syntactically, by considering an extended language in which we can express the relation between two structures.

Let \mathcal{M} and \mathcal{M}' be two structures of the form

$$\mathcal{M} = \langle D_1, \{R_i\}_{i \in I} \rangle, \quad \mathcal{M}' = \langle D_2, \{R'_i\}_{i \in I} \rangle.$$

Let J be $\{1, 2\}$. $(J, I, \langle k_i \rangle_{i \in I})$ will determine a 'type' of structures. Let L^+ be a corresponding language. It contains the original language L as the sublanguage of sort 1. For each bound variable u , the n th bound variable of sort 1, let u' be the n th bound variable of sort 2. If C is an L -formula, then C' denotes the result of replacing each bound variable u in C by u' ; hence $\text{Fr}(C) = \text{Fr}(C')$. With this notation, define Ext to be the sentence of the form $\forall u' \exists u (u' = u)$. Then, Ext and $\exists u'_i (u'_i = b_i)$ for $i = 1, \dots, n$ yield $A' \rightarrow A$. I.e., we have

$$\text{Ext}, \{\exists u'_i (u'_i = b_i)\}_{i=1}^n, A' \rightarrow A.$$

Now apply the result of Problem 8.4. An interpolant B can be chosen so as to satisfy:

- (i) $\text{Fr}(B) \subseteq \text{Fr}(A) = \{b_1, \dots, b_n\}$,
- (ii) $\text{Pr}(B) \subseteq \text{Pr}(A)$,
- (iii) every bound variable in B is of sort 1 i.e., in L ,
- (iv) $U_n(B)$ is empty.

Hence B is an existential formula of L . Since

$$\text{Ext}, \{\exists u'_i (u'_i = b_i)\}_{i=1}^n, A' \rightarrow B \text{ and } B \rightarrow A$$

are provable, we obtain that $A \equiv B$ is provable.

A general syntactic theory including Problem 8.6 is obtained by N. Motohashi: Interpolation Theorem and Characterization Theorem, Ann. Japan Assoc. Philos. Sci. 4 (1972) 15–80.

PROBLEM 8.7. Let \mathcal{A} be an axiom system in a language L , $\forall x \exists y A(x, y)$ a sentence of L provable from \mathcal{A} , and f a function symbol not in L . Then any L -formula which is provable from $\mathcal{A} \cup \{\forall x A(x, f(x))\}$ is also provable from \mathcal{A} in L . (That is to say, the introduction of f in this way does not essentially extend the system.) [*Hint* (Maehara's method): This is a corollary of the following lemma.]

LEMMA 8.8. Let $\forall x \exists y A(x, y)$ be a sentence of L , f a function symbol not in L , and Γ and Θ finite sequences of L -formulas. If $\forall x A(x, f(x))$, $\Gamma \rightarrow \Theta$ is (LK-) provable, then $\forall x \exists y A(x, y)$, $\Gamma \rightarrow \Theta$ is provable in L .

PROOF. Let P be a cut-free regular proof of $\forall x A(x, f(x)), \Gamma \rightarrow \Theta$. Let t_1, \dots, t_n be all the terms in P (i.e. proper terms, not semi-terms) whose outermost function symbol is f . These are arranged in an order such that t_i is not a subterm of t_j for $i < j$. Suppose t_i is $f(s_i)$ for $i = 1, \dots, n$. P is transformed in three steps.

Step (1): Let a_1, \dots, a_n be distinct free variables not occurring in P . Transform P by replacing t_1 by a_1 , then t_2 by a_2 , and so on. The resulting figure P' has the same end-sequent as P , but is not, in general, a proof (as we will see below) and must be further transformed.

Step (2): Since P is cut-free and f does not occur in Γ or Θ , it can be seen that the only occurrences of f in P are in the context. $\forall x A(x, f(x))$, and further, all these $\forall x A(x, f(x))$ occur in antecedents of sequents in P' , and the corresponding occurrences of $\forall x A(x, f(x))$ in P are introduced (in P) only by weakening : left or by some inferences of the form

$$I \quad \frac{A(s_i, f(s_i)), \Pi \rightarrow \Lambda}{\forall x A(x, f(x)), \Pi \rightarrow \Lambda}$$

(for some of the i , $1 \leq i \leq n$). Suppose the upper sequent of I is transformed into

$$A(s'_i, a_i), \Pi' \rightarrow \Lambda'$$

in P' . (So I is not transformed by step (1) into a correct inference in P' .) Now replace all occurrences of $\forall x A(x, f(x))$ in P' by

$$A(s'_1, a_1), \dots, A(s'_n, a_n)$$

(where s'_i is formed by replacing all t_j in s_i by a_j). Then the lower sequent of (the transform of) I can be derived from the upper sequent by several weakenings.

The result (after applying some contractions etc.) is a figure P'' with end-sequent

$$A(s'_1, a_1), \dots, A(s'_n, a_n), \Gamma \rightarrow \Theta.$$

However it may still not be a proof, as we now show, and must be transformed further.

Step (3): Consider a \exists : left in P :

$$J \quad \frac{B(b), \Delta \rightarrow \Psi}{\exists z B(z), \Delta \rightarrow \Psi}$$

and suppose this is transformed in P'' (by steps (1) and (2)) to

$$J' \quad \frac{B'(b), \Delta' \rightarrow \Psi'}{\exists z B'(z), \Delta' \rightarrow \Psi'}.$$

Now it may happen that for some i , the eigenvariable b occurs in s_i (and also s'_i), and further, the formula $A(s'_i, a_i)$ occurs in Δ' or Ψ' ; so that the eigenvariable condition is no longer satisfied in J' .

So we transform all J' in P'' (arising from \exists : left inferences J in P) as follows:

$$\supset : \text{left} \quad \frac{\exists z B'(z) \rightarrow \exists z B'(z) \quad B'(b), \Delta' \rightarrow \Psi'}{\exists z B'(z) \supset B'(b), \exists z B'(z), \Delta' \rightarrow \Psi'}$$

and carry the extra formula $\exists z B'(z) \supset B'(b)$ down to the end-sequent.

For the same reason, for every \forall : right in P

$$J \quad \frac{\Delta \rightarrow \Psi, B(b)}{\Delta \rightarrow \Psi, \forall z B(z)}$$

we replace its transform in P''

$$J' \quad \frac{\Delta' \rightarrow \Psi', B'(b)}{\Delta' \rightarrow \Psi', \forall z B'(z)}$$

by

$$\supset : \text{left} \quad \frac{\begin{array}{c} \forall z B'(z), \exists z \neg B'(z) \quad \frac{\Delta' \rightarrow \Psi', B'(b)}{\neg B'(b), \Delta' \rightarrow \Psi'} \\ \hline \exists z \neg B'(z) \supset \neg B'(b), \Delta' \rightarrow \Psi', \forall z B'(z) \end{array}}{\Delta' \rightarrow \Psi', \forall z B'(z)}$$

(and carry the extra formula down to the end).

The result (after some obvious adjustments with structural inferences) is a proof, without \exists : left or \forall : right, whose end-sequent has the form

$$(S_1) \quad \exists z B'(z) \supset B'(b), \dots, A(s'_i, a_i), \dots, \Gamma \rightarrow \Theta.$$

Now apply \exists : left and \forall : left inferences in a suitable order (see below) (and contractions, etc.) to derive

$$(S_2) \quad F, \dots, \forall x \exists y A(x, y), \Gamma \rightarrow \Theta,$$

where F is the formula obtained from $\exists u (\exists z B'(z) \supset B'(u))$ by universal quantification over all its free variables.

Finally, applying cuts with sequents $\rightarrow F$, we obtain a proof, as desired, of

$$\forall x \exists y A(x, y), \Gamma \rightarrow \Theta.$$

We must still check that it is indeed possible to find a suitable order for applying the quantifier inferences in proceeding from (S_1) to (S_2) above, so that they all satisfy the eigenvariable condition. To this end, we use the following (temporary) notation. For terms s and t and a formula B , $s \subset t$ means that s is a (proper) subterm of t , $s \subseteq t$ means that s is a subterm of t or t itself, and $s \subset B$ means that s is contained in B .

Now note that the following condition (C) is satisfied for any of the auxiliary formulas $B(b)$ of P with eigenvariable b , considered above, and $1 \leq i \leq n$:

$$(C) \text{ If } b \subset t_i, \text{ then } t_i \not\subset B(b).$$

(For suppose $b \in t_i$ and also t_i , which we write as $f(s_i(b))$, occurs in $B(b)$. Then in the lower sequent of the inference J with auxiliary formula $B(b)$, f would occur in the principal formula $\exists z B(z)$ (or $\forall z B(z)$) in the context of the semiterm $f(s_i(z))$, and so, since P is cut-free, f would also occur (in a similar context) in all sequents of P below this, and hence in Γ or Θ .)

Now let J_1, \dots, J_m be all the \exists : left and \forall : right inferences in P , with eigenvariables b_1, \dots, b_m and auxiliary formulas $B_1(b_1), \dots, B_m(b_m)$, respectively. Consider the partial order on $a_1, \dots, a_n, b_1, \dots, b_m$, generated by the relation $<$, which is defined by the following conditions:

- (1a) If $t_j \subset t_i$, then $a_i < a_j$.
- (1b) If $b_j \subset t_i$, then $a_i < b_j$.
- (2a) If $t_j \subset B_i(b_i)$, then $b_i < a_j$.
- (2b) If $b_j \subset B_i(b_i)$ ($j \neq i$), then $b_i < b_j$.

We will prove below that this does indeed generate a partial order, i.e., no circularities are formed. Assume this for the moment. Then, starting with sequent (S_1) , we apply, in any $<$ -increasing order, the quantifier inferences

$$\frac{A(s'_i, a_i), \dots}{\exists : \text{left and } \forall : \text{left}} \frac{}{\forall x \exists y A(x, y), \dots}$$

and

$$\frac{\exists z B_j(z, a_i, \dots, b_k, \dots) \supset B_j(b_j, a_i, \dots, b_k, \dots), \dots}{\exists : \text{left and } \forall : \text{left}} \frac{}{\forall x \dots \forall y \dots \exists u (\exists z B_j(z, x, \dots, y, \dots) \supset B_j(u, x, \dots, y, \dots)), \dots}$$

so as to obtain (S_2) . We can see that the eigenvariable condition is satisfied throughout, from the way in which $<$ was defined (and since $a_j \subset s'_i \Rightarrow t_j \subset t_i$, $b_j \subset s'_i \Rightarrow b_j \subset t_i$, $a_j \subset B'_i(b_i) \Rightarrow t_j \subset B_i(b_i)$, and $b_j \subset B'_i(b_i) \Rightarrow b_j \subset B_i(b_i)$).

Finally we must show that the relation $<$ does generate a partial order. This follows from the following two sublemmas.

SUBLEMMA 8.9 (in the notation of Lemma 8.8). (a) *For any $<$ -increasing sequence $b_i < \dots < b_j$, J_i lies above J_j in P . (So $i \neq j$.)*

(b) *For any $<$ -increasing sequence $a_i < \dots < a_j$, we have $t_i \not\subset t_j$. (So, in particular, $i \neq j$.)*

PROOF OF (a). The proof is by induction on the length of this sequence.

(i) If the length is 2, i.e., $b_1 < b_j$, this follows from the definition of $<$ (part 2b) and the eigenvariable condition in P .

(ii) For the case $b_i < a_k < b_j$: we have $t_k \subset B_i(b_i)$ (by 2a) and $b_j \subset t_k$ (by 1b). Hence $b_j \subset B_i(b_i)$. Also $i \neq j$, by condition (C). So again $b_i < b_j$ (by 2b) and J_i is above J_j .

(iii) For the case $b_i < a_k < \dots < a_l < b_j$ (with only a 's between b_i and b_j): notice that $t_l \subset t_k$ (from 1a). The argument is now similar to that in (ii).

(iv) For the remaining case, $b_i < \dots < b_k < \dots < b_j$, use the induction hypothesis.

PROOF OF (b). The proof is by induction on the length of this sequence.

(i) If the length is 2, i.e. $a_i < a_j$, this follows from the definition (part 1a).

(ii) For the case $a_i < b_k < a_j$: we have $b_k \subset t_i$ and $t_j \subset B_k(b_k)$. So $t_i \subseteq t_j$ would imply $t_i \subset B_k(b_k)$, contradicting (C).

(iii) For the case $a_i < b_k < \dots < b_l < a_j$ (with anything between b_k and b_l) we have $b_k \subset t_i$, $t_j \subset B_l(b_l)$ and J_k is above J_l (by Sublemma 8.12(a)). So $t_i \subseteq t_j$ would imply $b_k \subset B_l(b_l)$, contradicting the eigenvariable condition in P .

For the remaining two cases:

(iv) $a_i < a_k < \dots < a_j$,

(v) $a_i < \dots < a_k < a_j$,

use (1a) and the induction hypothesis.

This completes the proof of the sublemmas, and hence of Lemma 8.8.

A general syntactic theory including Lemma 8.8 and its analogue in LJ, is obtained by

N. Motohashi: Approximation Theory of Uniqueness Conditions by Existence Conditions, Fund. Math. 120 (1983) 29–44.

The following proposition is not strictly proof-theoretical in nature; however, it is useful for the next topic (in the proof of Proposition 8.13). We first give some definitions.

DEFINITION 8.10. Let R be a set and suppose a set W_p is assigned to every $p \in R$. If $R_1 \subseteq R$ and $f \in \prod_{p \in R_1} W_p$, then f is called a *partial function (over R)* with domain $\text{Dom}(f) = R_1$. If $\text{Dom}(f) = R$, then f is called a *total function (over R)*. If f and g are partial functions and $\text{Dom}(f) = D_0 \subseteq \text{Dom}(g)$ and $f(x) = g(x)$ for every $x \in D_0$, then we call g an *extension* of f and write $f < g$ and $f = g \upharpoonright D_0$.

PROPOSITION 8.11 (a generalized König's lemma). *Let R be any set. Suppose a finite set W_p is assigned to every $p \in R$. Let P be a property of partial functions f over R (defined as above) satisfying the following conditions:*

1) $P(f)$ holds if and only if there exists a finite subset N of R satisfying $P(f \upharpoonright N)$,

2) $P(f)$ holds for every total function f .

Then there exists a finite subset N_0 of R such that $P(f)$ holds for every f with $N_0 \subseteq \text{Dom}(f)$.

Note that R can have arbitrarily large cardinality. The case that R is the set of natural numbers is the original König's lemma.

PROOF. Let $X = \prod_{p \in R} W_p$, and give each W_p the discrete topology, and X the product topology. Since each W_p is compact, so is X (Tychonoff's theorem). For each g such that $\text{Dom}(g)$ is finite, let

$$N_g = \{f \mid f \text{ is total and } g < f\}.$$

Let

$$C = \{N_g \mid \text{Dom}(g) \text{ is finite, and } P(g)\}.$$

C is an open cover of X . Therefore C has a finite subcover, say

$$N_{g_1}, \dots, N_{g_k}.$$

Let $N_0 = \text{Dom}(g_1) \cup \dots \cup \text{Dom}(g_k)$. We will show that N_0 satisfies the condition of the theorem. If $N_0 \subseteq \text{Dom}(g)$, then let $g < f$, f total. Then $P(f)$ and $f \in N_{g_1} \cup \dots \cup N_{g_k}$. Say $f \in N_{g_i}$. So $g_i < f$, $P(g_i)$ and $g_i < g$. Therefore $P(g)$. This completes the proof.

What happens if we wish to apply to **LJ** the technique which has been used in proving completeness for **LK**? This leads us naturally to the study of Kripke models of **LJ**, relative to which one can prove the completeness of **LJ**. In order to simplify the discussion, we assume again that our language does not contain individual or function constants. Again, there should be no essential difficulty in extending the argument to the case where individual and function constants are included.

For technical reasons, we will deal with a system which is an equivalent modification of **LJ**. This system, invented by Maehara, will be called **LJ'**. **LJ'** is defined by restricting **LK** (rather than **LJ**) as follows: The inferences \neg :right, \supset :right and \forall :right are allowed only when the principal formulas are the only formulas in the succedents of the lower sequents. (These are called the "critical inferences" of **LJ'**.) Thus, for instance, \neg :right will take a form:

$$\frac{D, \Gamma \rightarrow}{\Gamma \rightarrow \neg D}.$$

As is obvious from the definition, the sequents of **LJ'** are those of **LK** (so the restriction on the sequents of **LJ**, that there can be at most one formula in the succedent of a sequent, is lifted here). It should be noted that all the other inferences are exactly those of **LK**. In particular, in \vee :right, the inference

$$\frac{\Gamma \rightarrow \Delta, A}{\Gamma \rightarrow \Delta, A \vee B}$$

is allowed even if Δ is not empty.

By interpreting a sequent of **LJ'**, say $\Gamma \rightarrow B_1, \dots, B_n$, as $\Gamma \rightarrow B_1 \vee \dots \vee B_n$, it is a routine matter to prove that **LJ'** and **LJ** are equivalent. Also, the cut-elimination theorem holds for **LJ'**. (Combine the proofs of cut-elimination for **LK** and **LJ**.)

The question now arises: Given a sequent of **LJ'**, say $\Gamma \rightarrow \Delta$, is there a cut-free proof of $\Gamma \rightarrow \Delta$ in **LJ'**?

Starting with a given $\Gamma \rightarrow \Delta$, we can carry out the reduction process which was defined for the classical case (cf. Lemma 8.3), except that we omit the stages 1) (\neg : right reduction), 7) (\supset : right reduction) and 9) (\forall : right reduction); in other words, all the reductions are as for the classical case, except those which concern the critical inferences of **LJ'**, which are simply omitted. We return to consider this point later.

The tree obtained by the above reduction process is (again) called the reduction tree for $\Gamma \rightarrow \Delta$.

In preparation for Kripke's semantics for intuitionistic systems and the completeness theorem for **LJ**, we will generalize the above reduction process to the case where Γ and/or Δ are infinite; i.e., we define reduction trees for infinite sequents $\Gamma \rightarrow \Delta$.

DEFINITION 8.12. Let Γ and Δ be well-ordered sequences of formulas, which may be infinite. We say that $\Gamma \rightarrow \Delta$ is provable (cut-free provable) (in **LJ'**) if there are finite subsequences of Γ and Δ , say $\tilde{\Gamma}$ and $\tilde{\Delta}$, respectively, such that $\tilde{\Gamma} \rightarrow \tilde{\Delta}$ is provable (cut-free provable).

(It is clear that $\Gamma \rightarrow \Delta$ is provable (in **LJ'**) if and only if it is provable without cut, even when Γ and/or Δ are infinite, by the cut-elimination theorem of §5, adapted to **LJ'**.)

The reduction process which has just been described can be generalized immediately to the case of infinite sequents. We shall only point out a few modifications in the stages. Note: for the reduction process, we assume that the language is augmented by uncountably many new free and bound variables (in a well-ordered sequence).

8) $k \equiv 8$. Let $\forall x_1 A_1(x_1), \dots, \forall x_\alpha A_\alpha(x_\alpha), \dots$ be all the formulas in Π whose outermost logical symbol is \forall . Let $a_1, \dots, a_\beta, \dots$ be all the free variables available at this stage. Then write down

$$A_1(a_1), \dots, A_1(a_\beta), \dots, A_\alpha(a_1), \dots, A_\alpha(a_\beta), \dots, \Pi \rightarrow \Lambda$$

above $\Pi \rightarrow \Lambda$.

10) $k \equiv 10$. Let $\exists x_1 A_1(x_1), \dots, \exists x_\alpha A_\alpha(x_\alpha), \dots$ be all the formulas in Π whose outermost logical symbol is \exists . Introduce new free variables $b_1, b_2, \dots, b_\alpha, \dots$. Then write down

$$A_1(b_1), \dots, A_\alpha(b_\alpha), \dots, \Pi \rightarrow \Lambda$$

above $\Pi \rightarrow \Lambda$.

PROPOSITION 8.13. (a) *If a sequent $\Gamma \rightarrow \Delta$ is provable (in \mathbf{LJ}'), then every sequent of the reduction tree for $\Gamma \rightarrow \Delta$ is provable.*

(b) *If a sequent $\Gamma \rightarrow \Delta$ is unprovable, then there is a branch (in the tree for $\Gamma \rightarrow \Delta$) in which every sequent is unprovable.*

PROOF. (a) is obvious. In order to prove (b), we shall first prove the following: Let $\Pi \rightarrow \Lambda$ be a sequent in the tree and let $\Pi_\lambda \rightarrow \Lambda_\lambda$, $\lambda = 1, 2, \dots, \alpha, \dots$ be all its upper sequents, given by a reduction. If each is provable, then $\Pi \rightarrow \Lambda$ is provable. In other words, if for each λ , $\lambda = 1, 2, \dots, \alpha, \dots$, there are finite subsets of Π_λ and Λ_λ , say Π'_λ respectively, such that $\Pi'_\lambda \rightarrow \Lambda'_\lambda$ is provable, then there are finite subsets of Π and Λ , say Π' and Λ' respectively, such that $\Pi' \rightarrow \Lambda'$ is provable. We shall only deal with a few cases.

1) A \exists : left reduction has been applied to $\Pi \rightarrow \Lambda$. Then its upper sequent is of the form

$$A_1(b_1), \dots, A_\alpha(b_\alpha), \dots, \Pi \rightarrow \Lambda,$$

where $\exists x_\alpha A_\alpha(x_\alpha)$ is in Π for each α , and $b_1, \dots, b_\alpha, \dots$ are newly introduced free variables. By the hypothesis, there are finite subsets of $A_1(b_1), \dots, A_\alpha(b_\alpha), \dots$ (say $B_1(c_1), \dots, B_n(c_n)$), of Π (say Π'), and of Λ (say Λ'), such that

$$B_1(c_1), \dots, B_n(c_n), \Pi' \rightarrow \Lambda'$$

is provable. By repeated \exists : left and some weak inferences, we obtain $\Pi \rightarrow \Lambda'$, which is a subsequence of $\Pi \rightarrow \Lambda$. Notice that since $B_1(c_1), \dots, B_n(c_n), \Pi' \rightarrow \Lambda'$ is provable (with a finite proof), we may regard c_1, \dots, c_n as free variables of our original language.

2) An \wedge : right reduction has been applied to $\Pi \rightarrow \Lambda$. Then all upper sequents are of the form

$$\Pi \rightarrow \Lambda, C_1, \dots, C_\alpha, \dots,$$

where $A_1 \wedge B_1, \dots, A_\alpha \wedge B_\alpha, \dots$ are all the formulas of Λ whose outermost logical symbol is \wedge and each C_α is A_α or B_α . We shall distinguish these cases by denoting C_α by $C_{0,\alpha}$ if C_α is A_α and by $C_{1,\alpha}$ if C_α is B_α . Then the upper sequents are the sequents

$$\Gamma \rightarrow \Lambda, C_{i_1,1}, \dots, C_{i_\alpha,\alpha}, \dots,$$

where $i_\alpha = 0$ or 1 , for all possible combinations of values of $i_1, \dots, i_\alpha, \dots$. Let f denote any sequence $(i_1, \dots, i_\alpha, \dots)$. By assumption, there is a finite subsequence of each sequent, say $\Pi^f \rightarrow \Lambda^f, C_1^f, \dots, C_{n_f}^f$, which is provable, where $C_1^f, \dots, C_{n_f}^f$ is a finite subset of $C_{i_1,1}, \dots, C_{i_\alpha,\alpha}, \dots$.

In order now to exploit the generalized König's lemma (Proposition 8.14), we let R be a set with the order type of the sequence $C_1, C_2, \dots, C_\alpha, \dots$ (say $R = \{1, 2, \dots, \alpha, \dots\}$). Define $W_\alpha = 2 (= \{0, 1\})$. For any subset $R_1 \subseteq R$ and any $f \in \prod_{\alpha \in R_1} W_\alpha$, we say that a finite sequence of formulas

$$(C_{f(\alpha_1), \alpha_1}, \dots, C_{f(\alpha_n), \alpha_n})$$

(with $\alpha_1, \dots, \alpha_n \in R_1$) is selected for f if there are finite subsets of Π and Λ , say Π' and Λ' , respectively, such that

$$\Pi' \rightarrow \Lambda', C_{f(\alpha_1), \alpha_1}, \dots, C_{f(\alpha_n), \alpha_n}$$

is provable. From the observation above, there is such a selected subset for any total function f . Now, for any $R_1 \subseteq R$ and any $f \in \prod_{\alpha \in R_1} W_\alpha$, we define

$$P(f) \Leftrightarrow \exists k \exists \alpha_1 \dots \exists \alpha_k (\alpha_1, \dots, \alpha_k \text{ are in the domain of } f \text{ and}$$

$$(C_{f(\alpha_1), \alpha_1}, \dots, C_{f(\alpha_k), \alpha_k}) \text{ is selected), where } k \text{ ranges}$$

over the natural numbers.

Then conditions 1 and 2 in the hypothesis of the generalized König's lemma are satisfied; hence by this lemma, there exists a finite subset of R , say $N_0 = \{\gamma_1, \dots, \gamma_l\}$, such that if $\text{Dom}(f)$ contains N_0 , then $P(f)$ holds.

Let

$$F = \{f \mid \text{Dom}(f) = N_0\} = \prod_{j=1}^l W_{\gamma_j}.$$

F is a finite set and, for every f in F , $P(f)$ holds, i.e., there is a subset of $\gamma_1, \dots, \gamma_l$, say $\alpha_1, \dots, \alpha_k$, such that $(C_{f(\alpha_1), \alpha_1}, \dots, C_{f(\alpha_k), \alpha_k})$ is selected for f ; i.e., there exist finite subsets of Π and Λ , say Π' and Λ' respectively, such that

$$\Pi' \rightarrow \Lambda', C_{f(\alpha_1), \alpha_1}, \dots, C_{f(\alpha_k), \alpha_k}$$

is provable. Therefore, for every possible combination of values of $(i_1, \dots, i_k) (= i)$, there are finite subsets of Π and Λ , say Π^i and Λ^i respectively, such that

$$\Pi^i \rightarrow \Lambda^i, C_{i_1, \alpha_1}, \dots, C_{i_k, \alpha_k}$$

is provable. Hence by weakenings and repeated \wedge : right, we obtain

$$\tilde{\Pi}' \rightarrow \tilde{\Lambda}', A_{\alpha_1} \wedge B_{\alpha_1}, \dots, A_{\alpha_k} \wedge B_{\alpha_k},$$

where $\tilde{\Pi}'$ consists of all the Π^i 's for f in F , and likewise with $\tilde{\Lambda}'$.

Now, from the argument just completed, if the given sequent $\Gamma \rightarrow \Delta$ is not provable, then there is one branch in which every sequent is unprovable.

Having finished these preparations, we now define Kripke (intuitionistic) structures (for a language L).

DEFINITION 8.14. (1) A *partially ordered structure* $P = \langle O, \leq \rangle$ consists of a set O together with a binary relation \leq satisfying the following:

- a) $p \leq p$,
- b) $p \leq q$ and $q \leq p$ imply $p = q$,
- c) $p \leq q$ and $q \leq r$ imply $p \leq r$,

where p, q and r range over elements of O .

(2) A Kripke structure for a language L is an ordered triple $\langle P, U, \phi \rangle$ such that:

1) $P = \langle O, \leq \rangle$ is a partially ordered structure.

2) U is a map which assigns to every member of O , say p , a non-empty set, say U_p , such that, if $p \leq q$, then $U_p \subseteq U_q$ (where \subseteq means set inclusion).

3) ϕ is a binary function $\phi(R, p)$, where R ranges over predicate constants in the language L and p ranges over members of O . Further:

3.1) Suppose the number of argument places of R is 0. Then $\phi(R, p) = T$ or F , and if $\phi(R, p) = T$ and $p \leq q$, then $\phi(R, q) = T$.

3.2) Suppose R is an n -ary predicate ($n \geq 1$). Then $\phi(R, p)$ is a subset of

$$U_p^n = \underbrace{U_p \times \dots \times U_p}_{n \text{ times}}$$

and $p \leq q$ implies $\phi(R, p) \subseteq \phi(R, q)$.

We define $U = \bigcup_{p \in O} U_p$. Then U can be thought of as the universe of the model or structure, and the elements of O as stages (see below).

Suppose that there is an assignment of objects of U to all the free variables; i.e., to each free variable a_i an object of U , say c_i , is assigned. Let $F(a_1, \dots, a_n)$ be a formula with free variables a_1, \dots, a_n (at most). The *interpretation* of $F(a_1, \dots, a_n)$ at (the stage) p (under this assignment) is defined as follows by induction on the number of logical symbols in $F(a_1, \dots, a_n)$, and this interpretation is expressed as $\phi(F(c_1, \dots, c_n), p)$. The value of such an interpretation is T or F .

- a) $\phi(R(c_1, \dots, c_n), p) = T$ if and only if $\langle c_1, \dots, c_n \rangle \in \phi(R, p)$ (for $n > 0$).
- b) $\phi(A \wedge B, p) = T$ if and only if $\phi(A, p) = T$ and $\phi(B, p) = T$.
- c) $\phi(A \vee B, p) = T$ if and only if $\phi(A, p) = T$ or $\phi(B, p) = T$.
- d) $\phi(A \supset B, p) = T$ if and only if for all q such that $p \leq q$, either $\phi(A, q) = F$ or $\phi(B, q) = T$.

- e) $\phi(\neg A, p) = \text{T}$ if and only if for all q such that $p \leq q$, $\phi(A, q) = \text{F}$.
- f) $\phi(\exists x A(c_1, \dots, c_n, x), p) = \text{T}$ if and only if there is a c in U_p such that $\phi(A(c_1, \dots, c_n, c), p) = \text{T}$.
- g) $\phi(\forall x F(c_1, \dots, c_n, x), p) = \text{T}$ if and only if for all q such that $p \leq q$, and for all c in U_q , $\phi(F(c_1, \dots, c_n, c), q) = \text{T}$.

We can generalize the definition of interpretation which has just been given to the case of sequents (finite or infinite). Let $\Gamma \rightarrow \Delta$ be a sequent. Then $\phi(\Gamma \rightarrow \Delta, p)$ is defined to be T if and only if, for all q such that $p \leq q$, either $\phi(A, q) = \text{F}$ for some A in Γ or $\phi(B, q) = \text{T}$ for some B in Δ .

A sequent $\Gamma \rightarrow \Delta$ is said to be valid in a Kripke structure $\langle P, U, \phi \rangle$ (with $P = \langle O, \leq \rangle$) if $\phi(\Gamma \rightarrow \Delta, p) = \text{T}$ for all p in O .

PROPOSITION 8.15. *Suppose $\Gamma \rightarrow \Delta$ is provable in \mathbf{LJ}' , and $\langle P, U, \phi \rangle$ is a Kripke structure. Then $\Gamma \rightarrow \Delta$ is valid in $\langle P, U, \phi \rangle$.*

PROOF. This is only a routine matter: by mathematical induction on the number of inferences in a proof of $\Gamma \rightarrow \Delta$ (or a subsequent of it).

Now, in order to finish the completeness proof for \mathbf{LJ}' , we shall start with an unprovable sequent $\Gamma \rightarrow \Delta$ and construct a counter-model in the sense of Kripke. This will be constructed from the reduction tree for $\Gamma \rightarrow \Delta$. Let us call this tree T . (Remember, in the construction of T , the \neg : right, \supset : right and \forall : right reductions were omitted.) This situation, i.e., with just this tree present, is called stage 0. By Proposition 8.16, there is a branch of T , say B_0 , containing (only) unprovable sequents. If B_0 is finite, let $\Gamma_0 \rightarrow \Delta_0$ be its uppermost sequent. If B_0 is infinite, let Γ_0 and Δ_0 be the union of all formulas in the antecedents and succedents respectively of the sequents in B_0 (each arranged in a well-ordered sequence), and consider the (possibly infinite) sequent $\Gamma_0 \rightarrow \Delta_0$. Single out all the formulas in Δ_0 whose outermost symbols are \neg , \supset or \forall . (If there is no such formula, then stop.) Let the symbol p range over all such formulas. We call each such p an immediate successor of 0 (and 0 an immediate predecessor of p).

Case 1. p is a formula of the form $\neg A$. Then consider the sequent $A, \Gamma_0 \rightarrow$.

Case 2. p is $B \supset C$. Then consider the sequent $B, \Gamma_0 \rightarrow C$.

Case 3. p is $\forall x F(x)$. Let a be a free variable which does not belong to U_0 .

(This can always be done by introducing a new symbol if necessary.) Then consider the sequent $\Gamma_0 \rightarrow F(a)$.

It is easily shown that (in each case) this new sequent is not provable, since otherwise $\Gamma_0 \rightarrow \Delta_0$ would be provable. Let us call this new sequent $\tilde{\Gamma}_p \rightarrow \tilde{\Delta}_p$, and let T_p be the reduction tree for $\tilde{\Gamma}_p \rightarrow \tilde{\Delta}_p$.

As before, let B_p be a branch of T_p containing unprovable sequents, and let $\Gamma_p \rightarrow \Delta_p$ be either the topmost sequent of B_p , or (if B_p is infinite) the "union" of all sequents in B_p , as before. Then follow exactly the same

process as the preceding paragraph. Namely, let q range over all formulas in Δ_p whose outermost logical symbol is \neg , \supset or \forall . (If there is no such formula, then stop.) Again, for all such q and p (with q in Δ_p as above), we call q an immediate successor of p and p an immediate predecessor of q . Then define as before the tree T_q and branch B_q .

Continue this procedure ω times. Let O be the set of all these p 's, and let \leq be the transitive reflexive relation on O generated by the immediate predecessor relation defined above. O is partially ordered by \leq . Now define U_p to be the set of all free variables occurring in B_p , for all $p \in O$, and define $U = \bigcup_{p \in O} U_p$. Notice the following.

1) If $p \leq q$, then $U_p \subseteq U_q$.

2) If q is an immediate successor of p , then all formulas in Γ_p occur in the antecedents of all sequents in T_q (and hence in B_q).

We now define the function ϕ as follows. For any n -ary predicate symbol R ($n > 0$), and any $p \in O$,

$$\phi(R, p) = \{ \langle a_1, \dots, a_n \rangle \mid a_1, \dots, a_n \in U_p \text{ and } R(a_1, \dots, a_n) \text{ occurs in } \Gamma_p \}$$

(and for $n = 0$, $\phi(R, p) = \top$ if and only if R occurs in Γ_p).

So we have defined a Kripke structure $\langle P, U, \phi \rangle$. We shall consider the interpretation of formulas in this structure relative to the (natural) assignment of each free variable to itself.

PROPOSITION 8.16 (with the above notation). *Let A be a formula in B_p . If A occurs in the antecedent of a sequent in B_p , then $\phi(A, p) = \top$; if it occurs in the succedent, then $\phi(A, p) = \text{F}$.*

PROOF. By induction on the number of logical symbols in A . First it should be noticed that if a formula occurs in the antecedent of a sequent in B_p , then it does not occur in the succedent of any sequent in B_p . The same holds with "antecedent" and "succedent" interchanged. Also, once a formula appears on one side of a sequent, it will appear on the same side of all higher sequents of B_p , and hence of the sequent $\Gamma_p \rightarrow \Delta_p$.

1) A is an atomic formula $R(a_1, \dots, a_n)$. If A occurs in an antecedent, hence in Γ_p , then by definition $\langle a_1, \dots, a_n \rangle \in \phi(R, p)$, which implies, again by definition, that $\phi(A, p) = \top$. If A occurs in a succedent, then $\langle a_1, \dots, a_n \rangle \notin \phi(R, p)$, so $\phi(A, p) = \text{F}$.

2) A is $\neg B$. Suppose A occurs in the antecedent. Then A occurs in Γ_p . This implies that, given any q such that $p \leq q$, A occurs in the antecedent of all the sequents in B_q ; hence B occurs in the succedent of a sequent in B_q ; therefore, by the induction hypothesis, $\phi(B, q) = \text{F}$. So $\phi(B, q) = \text{F}$ for any q such that $p \leq q$. This means that $\phi(A, p) = \top$.

Suppose next that A occurs in the succedent of a sequent in B_p . Then there exists a next stage, say q . It starts with $B, \Gamma_p \rightarrow$. By the induction hypothesis, $\phi(B, q) = \top$. That is to say, there is a q such that $p \leq q$ and $\phi(B, q) = \top$. Therefore by definition $\phi(A, p) = \text{F}$.

3) A is $B \wedge C$ or $B \vee C$. Those cases are easy; so they are left to the reader.

4) A is $\forall x F(x)$. Suppose A occurs in the antecedent of a sequent in B_p and suppose $p \leq q$. Then A occurs in the antecedent of a sequent in B_q . Let a be an element of U_q . Then $F(a)$ occurs in the antecedent of a sequent in B_q . Hence, by the induction hypothesis, $\phi(F(a), q) = T$. So for any q such that $p \leq q$ and any a in U_q , $\phi(F(a), q) = T$, which means that $\phi(A, p) = T$.

Suppose next that A occurs in the succedent of a sequent in B_p . So the next stage, say q , starts with $\Gamma_p \rightarrow F(a)$, where a is a (new) variable in U_q . By the induction hypothesis, $\phi(F(a), q) = F$. So there exists a q such that $p \leq q$, and a member a of U_q , such that $\phi(F(a), q) = F$. This means that

$$\phi(\forall x F(x), p) = F.$$

5) A is of the form $\exists x F(x)$. This case is left as an exercise.

6) A is of the form $B \supset C$. Suppose that A occurs in the antecedent of a sequent in B_p . Then either C occurs in Γ_p or B occurs in Δ_p . Let $p \leq q$. Then either C occurs in the antecedent or B occurs in the succedent of a sequent in B_q . So for any q , with $p \leq q$, either $\phi(C, q) = T$ or $\phi(B, q) = F$. So $\phi(B \supset C, p) = T$.

Suppose next that A occurs in the succedent of a sequent in B_p . Then the next stage, say q , starts with $B, \Gamma_p \rightarrow C$. Hence there is a q such that $p \leq q$, $\phi(B, q) = T$ and $\phi(C, q) = F$; so $\phi(B \supset C, p) = F$.

So now we can conclude that if $\Gamma \rightarrow \Delta$ is unprovable, then we can construct a Kripke structure $\langle P, U, \phi \rangle$ such that (under a suitable assignment to free variables) every formula in Γ assumes the value T and every formula in Δ assumes the value F ; in other words, there is a Kripke counter-model for $\Gamma \rightarrow \Delta$. This ends the completeness proof. Thus we have obtained:

THEOREM 8.17 (completeness of the intuitionistic predicate calculus: a generalized version; cf. Theorem 8.2). *Let $\Gamma \rightarrow \Delta$ be a sequent (finite or infinite). If $\Gamma \rightarrow \Delta$ is valid in all Kripke structures, then $\Gamma \rightarrow \Delta$ is provable. In particular, **LJ** is complete.*

(Recall that the soundness of **LJ** was established by Proposition 8.18). Notice that the method which has been prescribed here for completeness of **LJ** works even when the language is not countable, while the method for **LK** works only for a countable language. Although we could in fact use a method for **LK** similar to this one for **LJ'**, we do not attempt to do so, since Henkin's simple method is sufficient for that purpose.

EXERCISE 8.18. Construct a Kripke counter-model for each of the following sequents.

- 1) $\rightarrow P \vee \neg P$, where P is a predicate symbol.
 - 2) $\forall x (P(x) \vee Q) \rightarrow \forall x P(x) \vee Q$, where P and Q are predicate symbols of the indicated numbers of argument.
 - 3) $\rightarrow \exists x (\exists y P(y) \supset P(x))$, where P is a unary predicate.
- [Hint for 1): At stage 0:

$$\frac{\rightarrow P \vee \neg P, P, \neg P}{\rightarrow P \vee \neg P}.$$

Let p be $\neg P$. Then at stage p :

$$\frac{P \rightarrow}{\rightarrow \neg P}.$$

So define $O = \{0, p\}$, $0 \leq p$, $U_0 = U_p = \{a\}$, $\phi(P, 0) = F$. Then $\phi(P \vee \neg P, 0) = F$ can be easily proved.]

In order to discuss the completeness theorem for the intuitionistic logic further, we first discuss the complete Heyting algebras. A complete Heyting algebra (abbreviated by **cHa**) is a special kind of complete lattice. Let Ω be a complete lattice and $A \subseteq \Omega$. The least upperbound of A and the greatest lower bound of A are denoted by $\bigvee A$ and $\bigwedge A$ respectively. If $A = \{a_i \mid i \in I\}$, then $\bigvee A$ is denoted by $\bigvee_{i \in I} a_i$ or $\bigvee_i a_i$ and $\bigwedge A$ is denoted by $\bigwedge_{i \in I} a_i$ or $\bigwedge_i a_i$. For a and b in Ω , $a \vee b$ denotes the join of a and b and $a \wedge b$ denotes the meet of a and b .

DEFINITION 8.19. A **cHa** is a complete lattice Ω satisfying the following \wedge, \bigvee -distributive law:

$$p \wedge \bigvee_{i \in I} q_i = \bigvee_{i \in I} (p \wedge q_i)$$

for all $p \in \Omega$ and all subsets $\{q_i \mid i \in I\} \subseteq \Omega$. We denote the greatest element and the least element of Ω by 1 and 0 respectively. Let Ω be a **cHa** and $p, q \in \Omega$. We define $p \supset q$ as $\bigvee \{r \in \Omega \mid p \wedge r \leq q\}$ and $\neg p$ as $p \supset 0$.

A complete Boolean algebra is a **cHa**. Another typical example of **cHa** is a topological space. Let X be a topological space and $\mathcal{O}(X)$ be the set of all open sets of X . Then $\mathcal{O}(X)$ is a **cHa** by the following definition: $p \wedge q = p \cap q$ and $\bigvee_i p_i = \bigcup_i p_i$, where p, q and p_i are open sets. It is easily seen that $\neg p = (X - p)^\circ$ and $\bigwedge_i p_i = (\bigcap_i p_i)^\circ$, where q° denotes the open kernel of q .

EXERCISE 8.20. Let Ω be a **cHa** and $p, q, r \in \Omega$. Then the following equivalences hold.

- 1) $p \wedge q \leq r$ iff $q \leq (p \supset r)$.
- 2) $p \wedge q = 0$ iff $q \leq \neg p$.

Let L be a language without function constants. For any non-empty set D , $L\{D\}$ is the extended language obtained from L by introducing a new individual constant \bar{d} for every member d in D .

DEFINITION 8.21. (1) Let Ω be a **cHa**. By an Ω -valued structure for L we mean a pair $\langle D, \phi \rangle$, where D is a non-empty set and ϕ is a map from the constants of $L\{D\}$ such that:

- (i) if k is an individual constant, then ϕk is an element of D ;
- (ii) if d is an element of D , then $\phi \bar{d}$ is d ,
- (iii) if R is a predicate constant of n arguments, then ϕR is a function from D^n into Ω .

(2) Let A be a sentence in $L\{D\}$. Then the truth value $\llbracket A \rrbracket$ of A is defined by an Ω -valued structure $\langle D, \phi \rangle$ as follows.

1) If R is a predicate constant of n arguments and t_1, \dots, t_n are individual constants in $L\{D\}$, then $\llbracket R(t_1, \dots, t_n) \rrbracket$ is $\phi R(\phi t_1, \dots, \phi t_n)$. $\llbracket R(t_1, \dots, t_n) \rrbracket$ is a member of Ω .

2) If A is a sentence with a logical symbol, then $\llbracket A \rrbracket$ is defined according to its outermost logical symbols as follows.

- (i) $\llbracket \neg A \rrbracket = \neg \llbracket A \rrbracket$,
 $\llbracket A \wedge B \rrbracket = \llbracket A \rrbracket \wedge \llbracket B \rrbracket$,
 $\llbracket A \vee B \rrbracket = \llbracket A \rrbracket \vee \llbracket B \rrbracket$,
 $\llbracket A \supset B \rrbracket = \llbracket A \rrbracket \supset \llbracket B \rrbracket$,

where \neg, \wedge, \vee , and \supset in the left-hand side of $=$ are logical symbols of the language and \neg, \wedge, \vee , and \supset in the right-hand side of $=$ are operations on Ω .

- (ii) $\llbracket \forall x A(x) \rrbracket = \bigwedge_{d \in D} \llbracket A(\bar{d}) \rrbracket$,
 $\llbracket \exists x A(x) \rrbracket = \bigvee_{d \in D} \llbracket A(\bar{d}) \rrbracket$.

For every sentence A of $L\{D\}$, $\llbracket A \rrbracket$ is a member of Ω . Let \mathcal{B} be a complete Boolean algebra. Since a complete Boolean algebra is a **cHa**, the definitions of a \mathcal{B} -valued structure $\langle D, \phi \rangle$ and its truth value $\llbracket \cdot \rrbracket$ are obtained as special cases of the above definition. If \mathcal{B} is the complete Boolean algebra $\{0, 1\}$, then we can identify a \mathcal{B} -valued structure and a structure in Definition 8.1 as follows. If $\langle D, \phi \rangle$ is a structure in Definition 8.1, then we assign to $\langle D, \phi \rangle$ a $\{0, 1\}$ -valued structure $\langle D, \tilde{\phi} \rangle$ defined as follows.

- (i) For an individual constant k in L , $\tilde{\phi} k$ is ϕk .
- (ii) For any element d of D , $\tilde{\phi} \bar{d}$ is d .
- (iii) For a predicate constant R of n arguments, $\tilde{\phi} R$ is a function from D^n into $\{0, 1\}$ satisfying

$$\tilde{\phi} R(d_1, \dots, d_n) = 1 \text{ iff } \langle d_1, \dots, d_n \rangle \in \phi R.$$

It is easily proved that for every sentence A in L and for every interpretation $\mathcal{I} = (\langle D, \phi \rangle, \phi_0)$, \mathcal{I} satisfies A iff $\llbracket A \rrbracket = 1$, where $\llbracket A \rrbracket$ is the truth value of A by $\langle D, \tilde{\phi} \rangle$.

Now let Ω be again a **cHa** and $\langle D, \phi \rangle$ be an Ω -valued structure. The truth value of a closed sequent in **LJ** is defined by

$$\llbracket A_1, \dots, A_n \rightarrow B \rrbracket = \llbracket A_1 \wedge \dots \wedge A_n \supset B \rrbracket, \text{ and}$$

$$\llbracket A_1, \dots, A_n \rightarrow \rrbracket = \llbracket \neg(A_1 \wedge \dots \wedge A_n) \rrbracket.$$

A closed sequent $\Sigma \rightarrow \Delta$ of **L**{ D } is said to be valid in $\langle D, \phi \rangle$ if $\llbracket \Sigma \rightarrow \Delta \rrbracket = 1$, where $\llbracket \Sigma \rightarrow \Delta \rrbracket$ is the truth value of $\Sigma \rightarrow \Delta$ by $\langle D, \phi \rangle$. The sequent is said to be Ω -valid if it is valid in every Ω -valued structure $\langle D, \phi \rangle$.

Then Theorem 8.2 implies the following theorem.

THEOREM 8.22. *Let \mathcal{B} be a complete Boolean algebra. A closed sequent $\Gamma \rightarrow \Delta$ is provable in **LK** if and only if it is \mathcal{B} -valid.*

The proof that provability implies \mathcal{B} -validity is routine. The converse direction is immediate from Theorem 8.2 since $\{0, 1\}$ is a subalgebra of \mathcal{B} for every Boolean algebra \mathcal{B} .

Before Kripke, Rasiowa and Sikorski proved a completeness theorem for the intuitionistic predicate calculus by using the **cHa**. We shall discuss their completeness theorem and its relation with Kripke's completeness theorem. First we shall give the definition of Heyting algebra itself and another definition of **cHa**.

DEFINITION 8.23. A lattice H is said to be a Heyting algebra if \supset satisfying the following condition is defined on H

$$p \wedge q \leq r \text{ iff } q \leq (p \supset r).$$

THEOREM 8.24. *A **cHa** is a Heyting algebra and a Heyting algebra is a **cHa** if it is complete.*

PROOF. The first part is 1) of Exercise 8.20. Now we assume that Ω is a Heyting algebra and complete. It suffices to show

$$a \wedge \bigvee_i b_i \leq \bigvee_i (a \wedge b_i).$$

This is proved as follows

$$\begin{aligned} a \wedge b_i &\leq \bigvee_i (a \wedge b_i) \rightarrow b_i \leq \left(a \supset \bigvee_i (a \wedge b_i) \right) \\ &\rightarrow \bigvee_i b_i \leq \left(a \supset \bigvee_i (a \wedge b_i) \right) \\ &\rightarrow a \wedge \bigvee_i b_i \leq \bigvee_i (a \wedge b_i). \end{aligned}$$

THEOREM 8.25. (Rasiowa and Sikorski). *Let $\Gamma \rightarrow \Delta$ be a (finite or infinite) sequent in L . If $\Gamma \rightarrow \Delta$ is not provable in **LJ**, then there exists a **cHa** Ω , and a Ω -valued structure $\langle D, \phi \rangle$, such that $\llbracket A \rrbracket = 1$ for each A in Γ and $\llbracket A \rrbracket \neq 1$ for each A in Δ .*

PROOF. We assume that there are infinitely many free variables which do not occur in Γ or Δ . Let D be the set of all terms in L and $L(D)$ be the set of all formulas in L . We define an order \leq on $L(D)$ as follows.

$A \leq B$ iff $\Gamma, A \rightarrow B$ is provable in **LJ**. We also define $A \equiv B$ to be ' $A \leq B$ and $B \leq A$ '. Then \equiv is an equivalence relation on $L(D)$ and the equivalence class of A in $L(D)$ is denoted by $\llbracket A \rrbracket$. Let H be the set of $\llbracket A \rrbracket$ namely $H = \{\llbracket A \rrbracket \mid A \in L(D)\}$. The order \leq on $L(D)$ induces an order \leq on H . It is easily seen that H is a Heyting algebra. The following properties hold.

$$1) \llbracket \forall x A(x) \rrbracket = \bigwedge_{d \in D} \llbracket A(d) \rrbracket.$$

$$2) \llbracket \exists x A(x) \rrbracket = \bigvee_{d \in D} \llbracket A(d) \rrbracket.$$

Proof of 1). For every $d \in D$ $\llbracket \forall x A(x) \rrbracket \leq \llbracket A(d) \rrbracket$ since $\forall x A(x) \rightarrow A(d)$ is provable in **LJ**. Now let $\llbracket C \rrbracket \leq \llbracket A(d) \rrbracket$ for every $d \in D$. Then $\Gamma, C \rightarrow A(d)$ is provable for every $d \in D$. Take d to be a free variable which does not occur in $\Gamma, C, \forall x A(x)$. Then $\Gamma, C \rightarrow \forall x A(x)$ is provable in **LJ**.

The proof of 2) goes in the same way as 1).

For each n -ary predicate constant R , we define ϕR by $(\phi R)(d_1, \dots, d_n) = \llbracket R(d_1, \dots, d_n) \rrbracket$ for $d_1, \dots, d_n \in D$. Then $\langle D, \phi \rangle$ is a H -valued structure, $\llbracket A \rrbracket = 1$ for every A in Γ , and $\llbracket A \rrbracket \neq 1$ for every A in Δ . Therefore the theorem immediately follows from the following Rasiowa-Sikorski's embedding lemma.

EXERCISE 8.26. For every Heyting algebra A there exists a **cHa** A^* and an isomorphism of A into A^* , preserving all infinite joins and meets in A .

[Hint: Follow the prescription given below.]

1). Let J be a subset of A . J is said to be an ideal of A if it satisfies the following conditions:

$$i) a_1 \in J, a_2 \leq a_1 \rightarrow a_2 \in J;$$

$$ii) a_1 \in J, a_2 \in J \rightarrow (a_1 \vee a_2) \in J.$$

An ideal J of A is said to be a prime ideal if $1 \notin J$ and the following condition is satisfied: $(a_1 \wedge a_2) \in J \rightarrow a_1 \in J \vee a_2 \in J$. The set of all prime ideals of A is called the Stone space of A .

Let X be the Stone space of A . Then there exists an embedding $h: \langle A, \wedge, \vee \rangle \rightarrow \langle \mathcal{P}(X), \cap, \cup \rangle$, defined by $h(a) = \{x \in X \mid a \notin x\}$.

2). Let B be the Boolean subalgebra of $\mathcal{P}(X)$ generated by $h(A)$. Every element of B is of the form $((X - a_1) \cup b_1) \cap \dots \cap ((X - a_n) \cup b_n)$, where $a_1, b_1, \dots, a_n, b_n \in h(A)$. We define an interior operation $I: B \rightarrow h(A)$ by the following equation

$$I(((X - a_1) \cup b_1) \cap \dots \cap ((X - a_n) \cup b_n)) = (a_1 \supset b_1) \cap \dots \cap (a_n \supset b_n),$$

where $h(a) \supset h(b)$ denotes $h(a \supset b)$. Then $I : B \rightarrow B$ satisfies the following conditions.

- i) $I(b_1 \wedge b_2) = I(b_1) \wedge I(b_2)$.
- ii) $I(b) \leq b$.
- iii) $II(b) = I(b)$.
- iv) $I(1) = 1$.

A Boolean algebra B together with I satisfying i)–iv) is called a topological Boolean algebra. Our topological Boolean algebra $\langle B, I \rangle$ satisfies $I(B) = h(A)$.

3). Let B^* be the complete Boolean algebra of all regular open sets of the Stone space of B . Then there exists a canonical embedding $h' : B \rightarrow B^*$ which preserves infinite joins and infinite meets. We extend the interior operation $I : B \rightarrow h(A)$ to $I : B^* \rightarrow h(A)$ by the following equation

$$I\left(\bigvee_i {}^{B^*}h'(b_i)\right) = \bigvee_i {}^{B^*}h'(Ib_i).$$

Then $\langle B^*, I \rangle$ is a topological Boolean algebra and $I(B^*)$ is a **cHa** satisfying Exercise 8.26.

Now we shall consider the relation between Kripke models and **cHa**-valued structures.

Let $\langle P, U, \phi \rangle$ be a Kripke structure for L , where $P = \langle P, \leq \rangle$. For $p \in P$, we denote $\phi(A, p) = T$ by $p \Vdash A$ and $\phi(A, p) = F$ by $p \nVdash A$. Then b)–g) in Definition 8.14 are rewritten as follows.

- b) $p \Vdash A \wedge B$ iff $p \Vdash A$ and $p \Vdash B$.
- c) $p \Vdash A \vee B$ iff $p \Vdash A$ or $p \Vdash B$.
- d) $p \Vdash A \supset B$ iff $\forall q \geq p (q \nVdash A \text{ or } q \Vdash B)$.
- e) $p \Vdash \neg A$ iff $\forall q \geq p (q \nVdash A)$.
- f) $p \Vdash \exists x A(x)$ iff $\exists c \in U_p (p \Vdash A(c))$.
- g) $p \Vdash \forall x A(x)$ iff $\forall q \geq p \forall c \in U_q (q \Vdash A(c))$.

First we extend the language L to L^E by adding a new unary predicate constant E and we define

$$p \Vdash E(c) \text{ iff } c \in U_p.$$

Then the following holds

$$p \Vdash E(c), p \leq q \rightarrow q \Vdash E(c)$$

and $\langle P, U, \phi \rangle$ becomes a Kripke structure for L^E .

Let A be a sentence of $L(U)$. Then A^E is defined to be a relativization of A by E , namely, A^E is obtained from A by replacing all quantifiers $\forall x, \exists y, \dots$ in A by $\forall x (Ex \supset), \exists y (Ey \wedge), \dots$

THEOREM 8.27. *There exists a **cHa**-valued structure $\langle U, \Vdash \rangle$ of L^E , where*

$U = \bigcup_{p \in P} U_p$, such that for every sentence A of L ,

A is valid in $\langle P, U, \phi \rangle$ iff $\llbracket A^E \rrbracket = 1$ in $\langle U, \llbracket \cdot \rrbracket \rangle$.

PROOF. Let $L^E(U)$ be obtained from L^E by adding all elements of U as constants. For a sentence A in $L^E(U)$, $\llbracket A \rrbracket$ is defined by the following equation

$$\llbracket A \rrbracket = \{p \in P \mid p \Vdash A\}.$$

Then we define H by the equation

$$H = \{\llbracket A \rrbracket \mid A \text{ is a sentence of } L^E(U)\}.$$

The following properties hold.

1) $\llbracket A \rrbracket \subseteq \llbracket B \rrbracket$ iff $\forall p (p \Vdash A \supset B)$.

If $\llbracket A \rrbracket \subseteq \llbracket B \rrbracket$, then $\forall p (p \Vdash A \text{ implies } p \Vdash B)$. Therefore $q \geq p$, $q \Vdash A \rightarrow q \Vdash B$ namely

$$\forall p (p \Vdash A \supset B).$$

Now we assume $\forall p (p \Vdash A \supset B)$. Then $\forall p (p \Vdash A \text{ implies } p \Vdash B)$. Therefore $q \in \llbracket A \rrbracket$ implies $q \in \llbracket B \rrbracket$.

2) $\llbracket A \rrbracket \cup \llbracket B \rrbracket = \llbracket A \vee B \rrbracket$.

The proofs of this and the following are obvious.

3) $\llbracket A \rrbracket \cap \llbracket B \rrbracket = \llbracket A \wedge B \rrbracket$.

4) $\llbracket A \rrbracket \cap \llbracket C \rrbracket \subseteq \llbracket B \rrbracket$ iff $\llbracket C \rrbracket \subseteq \llbracket A \supset B \rrbracket$.

$$\begin{aligned} \llbracket A \rrbracket \cap \llbracket C \rrbracket \subseteq \llbracket B \rrbracket &\text{ iff } \forall p (p \Vdash A \wedge C \supset B) \text{ by 1), 3)} \\ &\text{ iff } \forall p (p \Vdash C \supset (A \supset B)) \\ &\text{ iff } \llbracket C \rrbracket \subseteq \llbracket A \supset B \rrbracket. \end{aligned}$$

5) $\bigcup_{u \in U} \llbracket Eu \wedge A(u) \rrbracket = \llbracket \exists x A(x) \rrbracket$.

$$\begin{aligned} p \in \bigcup_{u \in U} \llbracket Eu \wedge A(u) \rrbracket &\text{ iff } \exists u \in U (p \Vdash Eu \wedge A(u)) \\ &\text{ iff } \exists u \in U_p (p \Vdash A(u)) \\ &\text{ iff } p \Vdash \exists x A(x). \end{aligned}$$

$$6) \bigcap_{u \in U} [Eu \supset A(u)] = [\forall x A(x)].$$

$$p \in \bigcap_{u \in U} [Eu \supset A(u)] \text{ iff } \forall u \in U (p \Vdash Eu \supset A(u))$$

$$\text{iff } \forall u \in U \forall q \geq p (q \Vdash Eu \text{ implies } q \Vdash A(u))$$

$$\text{iff } \forall u \in U \forall q \geq p (u \in U_q \text{ implies } q \Vdash A(u))$$

$$\text{iff } \forall q \geq p \forall u \in U_q (q \Vdash A(u))$$

$$\text{iff } p \Vdash \forall x A(x).$$

From 1)–4), $\langle H, \cap, \cup \rangle$ is a Heyting algebra, where $1 = P$ and $0 = \phi$. For every n -ary predicate constant R we define

$$\llbracket R(u_1, \dots, u_n) \rrbracket = [R(u_1, \dots, u_n)].$$

Then for every sentence A in $L(U)$, $\llbracket A^E \rrbracket$ is defined as a member of H .

$$7) \llbracket A^E \rrbracket = [A].$$

If A is atomic, then this is obvious from the definition. The cases for $A \vee B$, $A \wedge B$, and $A \supset B$ are also immediate. We prove only the cases $\forall x A(x)$ and $\exists x A(x)$.

$$\begin{aligned} \llbracket (\forall x A(x))^E \rrbracket &= \llbracket \forall x (Ex \supset A^E(x)) \rrbracket \\ &= \bigcap_{u \in U} (\llbracket Eu \rrbracket \supset \llbracket A^E(u) \rrbracket) \\ &= [\forall x A(x)] \quad \text{by 6).} \end{aligned}$$

$$\begin{aligned} \llbracket (\exists x A(x))^E \rrbracket &= \llbracket \exists x (Ex \wedge A^E(x)) \rrbracket \\ &= \bigcup_{u \in U} \llbracket Eu \rrbracket \wedge \llbracket A^E(u) \rrbracket \\ &= \bigcup_{u \in U} [Eu \wedge A(u)] \\ &= [\exists x A(x)] \quad \text{by 5).} \end{aligned}$$

By Rasiowa–Sikorski's embedding lemma (Exercise 8.26) there exist a **cHa** Ω and an isomorphism $H \rightarrow \Omega$, in which all infinite joins and meets are preserved. Then $\langle U, \llbracket \cdot \rrbracket \rangle$ can be considered an Ω -valued structure and we have

$$\begin{aligned} \llbracket A^E \rrbracket = 1 \text{ in } \langle U, \llbracket \cdot \rrbracket \rangle &\text{ iff } [A] = P \\ &\text{ iff } \forall p \in P (p \Vdash A). \end{aligned}$$

Compared with the completeness theorem for **LK**, Theorem 8.26 for **LJ** is much weaker. It says only that $\Gamma \rightarrow \Delta$ is provable if and only if it is Ω -valid for every **cHa** Ω . Therefore the following open problems are very interesting.

1. Let Ω be a **cHa**. Formulate an extension **LJ** $_{\Omega}$ of **LJ** such that the following equivalence holds: $\Gamma \rightarrow \Delta$ is provable in **LJ** $_{\Omega}$ iff it is Ω -valid. An interesting special case is that Ω is the **cHa** of the n -dimensional Euclidean space.

2. Let \mathcal{F} be a class of **cHa**. Formulate an extension **LJ** $_{\mathcal{F}}$ of **LJ** such that the following equivalence holds: $\Gamma \rightarrow \Delta$ is provable in **LJ** $_{\mathcal{F}}$ iff it is Ω -valid for every **cHa** Ω in \mathcal{F} . An interesting special case is that \mathcal{F} is the class of $\mathcal{O}(X)$ where X is a certain type of topological spaces e.g. $\mathcal{F} = \{\mathcal{O}(X) \mid X \text{ is a finite topological space}\}$.

We have the impression that an axiomatization of **LJ** $_{\Omega}$ might be impossible for almost all infinite **cHa** Ω . In other words, an axiomatization of **LJ** $_{\mathcal{F}}$ is very likely only when \mathcal{F} is a large class of **cHa**. In this sense, the following example **LJ** $_I$ is very interesting since I is a single infinite **cHa** and an axiomatization of **LJ** $_I$ is possible. It seems to the author very attractive to find many such examples and to classify in what kind of Ω or \mathcal{F} **LJ** $_{\Omega}$ or **LJ** $_{\mathcal{F}}$ is axiomatizable.

In the rest of this section, we solve the first problem for a **cHa** of $[0, 1]$ (a closed interval of real numbers). Let I be the **cHa** of $[0, 1]$. The operations \wedge and \vee are defined as follows;

$a \wedge b$ is the minimum of a and b , and $\bigvee_i a_i$ is the least upper bound of a_i .

It is easily seen that I is a **cHa**. 0 and 1 are the smallest element and the greatest element of I respectively.

In order to formulate **LJ** $_I$ we introduce propositional variables $\alpha_0, \alpha_1, \alpha_2, \dots, \alpha, \beta, \gamma, \dots$ may be used for propositional variables. The formation of formulas is supplemented by the following rule.

A propositional variable only is an atomic formula.

Then **LJ** $_I$ is obtained from **LJ** by introducing the following extra axiomschemata and extra inference rule.

*Extra axiomschemata for **LJ** $_I$.*

1. $\rightarrow (A \supset B) \vee ((A \supset B) \supset B)$,
2. $(A \supset B) \supset B \rightarrow (B \supset A) \vee B$,
3. $\forall x (C \vee A(x)) \rightarrow C \vee \forall x A(x)$,
4. $\forall x A(x) \supset C \rightarrow \exists x (A(x) \supset D) \vee (D \supset C)$.

Extra inference rule

$$\frac{\Gamma \rightarrow A \vee (C \supset \alpha) \vee (\alpha \supset B)}{\Gamma \rightarrow A \vee (C \supset B)},$$

where α does not occur in the lower sequent.

We express two sequents $A \rightarrow B$ and $B \rightarrow A$ by $A \leftrightarrow B$.

PROPOSITION 8.28. *The following sequents are provable in \mathbf{LJ}_I .*

- (1) $\rightarrow (A \supset B) \vee (B \supset A)$,
- (2) $A \supset B \vee C \leftrightarrow (A \supset B) \vee (A \supset C)$,
- (3) $A \wedge B \supset C \leftrightarrow (A \supset C) \vee (B \supset C)$,
- (4) $C \supset \exists x A(x) \rightarrow (C \supset D) \vee \exists x (D \supset A(x))$,

where x does not occur in D .

PROOF. (1) follows from Extra axioms 1 and 2.

(\leftarrow) of (2) and (3) are provable in \mathbf{LJ} .

(\rightarrow) of (2)

$$\begin{aligned} A \supset B \vee C &\rightarrow (A \supset B \vee C) \wedge ((B \supset C) \vee (C \supset B)) \\ &\rightarrow (A \supset C) \vee (A \supset B) \end{aligned}$$

(\rightarrow) of (3)

$$\begin{aligned} A \wedge B \supset C &\rightarrow (A \wedge B \supset C) \wedge ((A \supset B) \vee (B \supset A)) \\ &\rightarrow (A \supset C) \vee (B \supset C) \end{aligned}$$

(4): By the use of Extra axiom 1, it suffices to prove the following sequent.

- (i) $C \supset \exists x A(x), (C \supset D) \supset D \rightarrow \exists x (D \supset A(x)) \vee (C \supset D)$.

Let Γ be $C \supset \exists x A(x), (C \supset D) \supset D$. Then we have

- (ii) $\Gamma \rightarrow (\exists x A(x) \supset D) \supset D$ and
- (iii) $(\exists x A(x) \supset D) \supset D \rightarrow \forall x (A(x) \supset D) \supset D$.

By using (ii), (iii) and Extra axiom 4, we have

- (iv) $\Gamma \rightarrow \exists x ((A(x) \supset D) \supset C) \vee (C \supset D)$.

On the other hand, from $\rightarrow (A(a) \supset D) \vee (D \supset A(a))$ we have $(A(a) \supset D) \supset C \rightarrow (D \supset A(a)) \vee C$. Hence from (iv) we have

$$\Gamma \rightarrow \exists x (D \supset A(x)) \vee C \vee (C \supset D).$$

Since $\Gamma, C \rightarrow \exists x (D \supset A(x))$, we have (i).

Since we extended the language by introducing propositional variables, we extend the definition of the truth value accordingly. We call a formula in this extended language a sentence even if it has propositional variables. So a formula is a sentence if no free variables occur in it.

DEFINITION 8.29. Let $\langle D, \phi \rangle$ be an Ω -valued structure. An interpretation of $L\{D\}$ is a structure $\langle D, \phi \rangle$ together with a mapping ρ from propositional variables into I . We may denote an interpretation $(\langle D, \phi \rangle, \rho)$ simply by \mathcal{J} . Here ρ is called an assignment from the set of all propositional variables. Now we extend the truth value of a sentence. The truth value of A depends on ρ and is denoted by $\llbracket A \rrbracket_\rho$ or simply by $\llbracket A \rrbracket$. The definition of $\llbracket A \rrbracket_\rho$ is obtained by rewriting $\llbracket A \rrbracket$ in the previous definition by $\llbracket A \rrbracket_\rho$ and adding the following rule.

$$\llbracket \alpha_i \rrbracket_\rho = \rho \alpha_i, \text{ where } \alpha_i \text{ is a propositional variable.}$$

Obviously $\llbracket A \rrbracket_\rho$ does not depend on ρ if A does not have any propositional variable. We say that $\Gamma \rightarrow \Delta$ is valid (more precisely I -valid) if $\llbracket \Gamma \rightarrow \Delta \rrbracket_\rho = 1$ for every interpretation $(\langle D, \phi \rangle, \rho)$.

PROPOSITION 8.30. *If a closed sequent $\Gamma \rightarrow \Delta$ is provable in \mathbf{LJ}_I , then it is valid.*

PROOF. We prove only the validity of the extra inference rule, since it is clear for other cases.

Let $\mathcal{J} = (\langle D, \phi \rangle, \rho)$ be an interpretation and the lower sequent of

$$\frac{\Gamma \rightarrow A \vee (C \supset \alpha) \vee (\alpha \supset B)}{\Gamma \rightarrow A \vee (C \supset B)}$$

be not valid in \mathcal{J} . Then

$$\llbracket \Gamma \rightarrow A \vee (C \supset B) \rrbracket_\rho \neq 1.$$

It follows that

$$\llbracket D \rrbracket_\rho \wedge \llbracket C \rrbracket_\rho > \llbracket B \rrbracket_\rho$$

for each $D \in \Gamma$, and so there exists $p \in [0, 1]$ such that

$$\bigvee_{D \in \Gamma} \llbracket D \wedge C \rrbracket_\rho > p > \llbracket B \rrbracket_\rho.$$

Let ρ' be an assignment which has the same values as ρ except $\rho'(\alpha) = p$. Then we have

$$\llbracket \Gamma \rightarrow A \vee (C \supset \alpha) \vee (\alpha \supset B) \rrbracket_{\rho'} \neq 1.$$

Therefore the upper sequent is not valid.

THEOREM 8.31 (Takeuti–Titani) (Completeness theorem for \mathbf{LJ}_I). *Let L*

be a countable language. A closed sequent $\Gamma \rightarrow \Delta$ is valid if and only if it is \mathbf{LJ}_I -provable.

PROOF. We have already proved the 'if-part' in Proposition 8.33. Now suppose $\Gamma \rightarrow \Delta$ is not provable in \mathbf{LJ}_I . Without loss of generality we may assume that Γ is empty and Δ consists of one formula A . We enumerate all free variables b_0, b_1, b_2, \dots and all propositional variables $\beta_0, \beta_1, \beta_2, \dots$ which do not occur in A . We write $\vdash C$ if $\rightarrow C$ is provable in \mathbf{LJ}_I and $\nvdash C$ if $\rightarrow C$ is not provable in \mathbf{LJ}_I . If S is of the form $\rightarrow C$, we write $\vdash S$ for $\vdash C$ and $\nvdash S$ for $\nvdash C$. Enumerate the set \mathcal{F} of all formulas of L , say $\mathcal{F} = \{B_1, B_2, B_3, \dots\}$. We will construct the set M_k , $k = 0, 1, 2, \dots$ of finite formulas by induction so that

$$\nvdash \bigvee M_k,$$

where $\bigvee M_k$ with $M_k = \{C_1, \dots, C_n\}$ denotes $C_1 \vee \dots \vee C_n$. Let $M_0 = \{A\}$. Then $\nvdash \bigvee M_0$. For the induction step, we assume that M_k has been defined and $\nvdash \bigvee M_k$.

Case 1. If $\vdash \bigvee M_k \vee B_{k+1}$, then put

$$M_{k+1} = M_k.$$

Case 2. If $\nvdash \bigvee M_k \vee B_{k+1}$, then put

$$M'_{k+1} = M_k \cup \{B_{k+1}, \beta_j, \beta_j \supset B_{k+1}\},$$

where β_j is the first β which does not occur in $\bigvee M_k \vee B_{k+1}$.

Case 2.1. If $\nvdash \bigvee M_k \vee B_{k+1}$ and B_{k+1} is neither of the form $C_1 \supset C_2$ nor of the form $\forall x \varphi(x)$, then let $M_{k+1} = M'_{k+1}$.

Case 2.2. If $\nvdash \bigvee M_k \vee B_{k+1}$ and B_{k+1} is of the form $C_1 \supset C_2$, then let

$$M_{k+1} = M'_{k+1} \cup \{C_1 \supset \beta_j, \beta_j \supset C_2\},$$

where β_j is the first β which does not occur in M'_{k+1} . It is clear that $\nvdash \bigvee M_{k+1}$.

Case 2.3. If $\nvdash \bigvee M_k \vee B_{k+1}$ and B_{k+1} is of the form $\forall x \varphi(x)$, then let

$$M_{k+1} = M'_{k+1} \cup \{\varphi(b_i)\},$$

where b_i is the first b which does not occur in M'_{k+1} . Then we have

$$\nvdash \bigvee M_{k+1}.$$

Now that $\{M_k\}_{k \in \omega}$ have been defined, put $M = \bigcup_{k \in \omega} M_k$.

Let $P = \{\gamma_0, \gamma_1, \gamma_2, \dots\}$ be the set of propositional variables such that $\gamma \vee \neg\gamma \in M$.

For the set M we have:

LEMMA 8.32. (1) If $C \notin M$, then there exist $C_1, \dots, C_n \in M$ such that

$$\vdash C_1 \vee \dots \vee C_n \vee C.$$

- (2) If $C_1, \dots, C_n \in M$, then $C_1 \vee \dots \vee C_n \in M$.
- (3) If $C \in M$ and $\vdash E \rightarrow C$, then $E \in M$.
- (4) If $C \in M$, then there exists $\gamma \in P$ such that $(\gamma \supset C) \in M$.
- (5) If $C_1 \wedge C_2 \in M$, then $C_1 \in M$ or $C_2 \in M$.
- (6) If $(C_1 \supset C_2) \in M$, then there exists $\gamma \in P$ such that $(C_1 \supset \gamma) \vee (\gamma \supset C_2) \in M$.
- (7) If $\forall x \varphi(x) \in M$, then there exists a free variable a such that $\varphi(a) \in M$.
- (8) If $\exists x \varphi(x) \notin M$ and $\gamma \in P$, then there exists a free variable a such that $(\gamma \supset \varphi(a)) \notin M$.
- (9) For each formula C and $\gamma \in P$, $(C \supset \gamma) \in M$ or $(C \supset \gamma) \supset \gamma \in M$.

PROOF. (1)–(7) are obvious from the construction of M .

(8) Assume $\exists x \varphi(x) \notin M$ and $\gamma \in P$. We have

$$\exists x (\gamma \supset \varphi(x)) \notin M, \exists x (\gamma \supset \varphi(x)) \supset \gamma \in M$$

and $\forall x ((\gamma \supset \varphi(x)) \supset \gamma) \in M$. Hence there exists a free variable a such that $(\gamma \supset \varphi(a)) \supset \gamma \in M$. Since $\vdash ((\gamma \supset \varphi(a)) \supset \gamma) \vee (\gamma \supset (\gamma \supset \varphi(a)))$ and $\vdash \gamma \supset (\gamma \supset \varphi(a)) \leftrightarrow \gamma \supset \varphi(a)$, we have $(\gamma \supset \varphi(a)) \notin M$.

(9) follows from $\vdash (C \supset \gamma) \wedge ((C \supset \gamma) \supset \gamma) \rightarrow \gamma$.

Now we shall construct an interpretation $(\langle D, \phi \rangle, \rho)$. Let D be the set of all terms in L . Define a relation \leq on $P = \{\gamma_0, \gamma_1, \gamma_2, \dots\}$ by

$$\gamma_i \leq \gamma_j \text{ iff } \gamma_i \supset \gamma_j \notin M.$$

Then $\gamma_i < \gamma_j$ (i.e., $\gamma_i \leq \gamma_j \wedge \gamma_j \not\leq \gamma_i$) iff $\gamma_j \supset \gamma_i \in M$.

LEMMA 8.33. P is a countable ordered set satisfying

- a) the order $<$ is dense;
- b) P has no least nor greatest element.

PROOF. 1) P is clearly ordered.

1.1) $\gamma \not\leq \gamma$ since $\gamma \supset \gamma \notin M$.

1.2) $\gamma_i < \gamma_j$ and $\gamma_j < \gamma_k$ implies $\gamma_i < \gamma_k$.

$$\begin{aligned}
\gamma_i < \gamma_j \wedge \gamma_i \not\leq \gamma_k &\rightarrow \gamma_i \supset \gamma_j \notin M \wedge \gamma_k \supset \gamma_i \notin M \\
&\rightarrow \gamma_k \supset \gamma_j \notin M \\
&\rightarrow \gamma_j \not\leq \gamma_k.
\end{aligned}$$

$\gamma_i \not\leq \gamma_j$ implies $\gamma_j < \gamma_i$ or $\gamma_j = \gamma_i$.

(a) If $\gamma_i < \gamma_j$, i.e., $\gamma_j \supset \gamma_i \in M$, then there exists α such that $(\gamma_j \supset \alpha) \vee (\alpha \supset \gamma_i) \in M$.

Since $\vdash \alpha \vee \neg \alpha \supset (\gamma_j \supset \alpha) \vee (\alpha \supset \gamma_i)$, $\alpha \vee \neg \alpha \in M$.

Therefore $\alpha \in P$ and $\gamma_j > \alpha > \gamma_i$.

(b) If $\gamma_i \in P$, then $\gamma_i \vee \neg \gamma_i \in M$, that is, $\gamma_i \rightarrow O \in M$, where O is a formula of the form $C \wedge \neg C$. By Lemma 8.35, (6), there exists $\gamma \in P$ such that $(\gamma_i \supset \gamma) \vee (\gamma \supset O) \in M$. Hence $\gamma_i > \gamma$.

If $\gamma_i \in P$, then $1 \supset \gamma_i \in M$, where 1 is a provable formula. By Lemma (6), there exists a $\gamma \in P$ such that $(1 \supset \gamma) \vee (\gamma \supset \gamma_i) \in M$. So $\gamma > \gamma_i$.

By the lemma, there exists an isomorphism τ of P onto the set of rational numbers r such that $0 < r < 1$, which is denoted by $(0, 1)_Q$. Extend the isomorphism $\tau: P \rightarrow (0, 1)_Q$ to $\rho: \{\alpha_0, \alpha_1, \dots\} \rightarrow [0, 1]$ by

$$\rho(\alpha_i) = \bigwedge \{\tau(\gamma) \mid \gamma \in P \text{ and } (\gamma \supset \alpha) \in M\}.$$

We also define ϕ by $\phi(d) = d$ for any element d of D . Finally we define ϕR for a predicate constant R with n arguments by the following equation.

$$\phi R(d_1, \dots, d_n) = \bigwedge \{\tau(\gamma) \mid \gamma \in P \text{ and } (\gamma \supset R(d_1, \dots, d_n)) \in M\}.$$

We will prove that A is not valid in the interpretation we defined. First we prove the following lemma.

LEMMA 8.34. For a formula φ of L and $\gamma \in P$,

$$\llbracket \varphi \rrbracket < \llbracket \gamma \rrbracket \text{ iff } (\gamma \supset \varphi) \in M.$$

PROOF. We prove this by induction on the complexity of φ .

(1) If φ is atomic, i.e., propositional variable α or of the form $R(t_1, \dots, t_n)$, then it is obvious from the definition.

(2) If φ is $B \vee C$, then

$$\begin{aligned}
(\gamma \supset \varphi) \in M &\text{ iff } (\gamma \supset B) \vee (\gamma \supset C) \in M \\
&\text{ iff } \llbracket \varphi \rrbracket < \llbracket \gamma \rrbracket,
\end{aligned}$$

by using induction hypothesis.

(3) If φ is $B \wedge C$, then $(\gamma \supset \varphi) \in M$ iff $\llbracket \varphi \rrbracket < \llbracket \gamma \rrbracket$. The proof is similar as in (2).

(4) Let φ be $B \supset C$. Then $(\gamma \supset \varphi) \in M$ iff $(\gamma \supset C) \vee (B \supset C) \in M$, since $\gamma \supset (B \supset C) \leftrightarrow (\gamma \wedge B) \supset C \leftrightarrow (\gamma \supset C) \vee (B \supset C)$. Hence $(\gamma \supset \varphi) \in M$ iff there exists $\gamma_i \in P$ such that $(\gamma \supset C) \vee (B \supset \gamma_i) \vee (\gamma_i \supset C) \in M$. It follows, by the induction hypothesis, that

$$(\gamma \supset \varphi) \in M \text{ iff } \llbracket \gamma \rrbracket > \llbracket C \rrbracket = \llbracket \varphi \rrbracket.$$

(5) Let φ be $\forall x B(x)$. Then

$$\llbracket \varphi \rrbracket = \bigwedge_{d \in D} \llbracket B(d) \rrbracket.$$

If $\llbracket \varphi \rrbracket < \llbracket \gamma \rrbracket$, then there exists $d \in D$ such that $\llbracket B(d) \rrbracket < \llbracket \gamma \rrbracket$ and hence, by the induction hypothesis, $(\gamma \supset \forall x B(x)) \in M$. Conversely, if $(\gamma \supset \forall x B(x)) \in M$, then $\forall x (\gamma \supset B(x)) \in M$ and so there exists a free variable a such that $\gamma \supset B(a) \in M$. Therefore

$$\llbracket \forall x B(x) \rrbracket \leq \llbracket B(a) \rrbracket < \llbracket \gamma \rrbracket.$$

(6) Let φ be $\exists x B(x)$. Then $\llbracket \varphi \rrbracket = \bigvee_{d \in D} \llbracket B(d) \rrbracket$. If $\llbracket \varphi \rrbracket < \llbracket \gamma \rrbracket$, then there exists $\gamma_i \in P$ such that $\llbracket \varphi \rrbracket < \llbracket \gamma_i \rrbracket < \llbracket \gamma \rrbracket$ and hence $\gamma \supset (\gamma_i \supset B(d)) \in M$ for each $d \in D$, since

$$\gamma \supset (\gamma_i \supset B(d)) \leftrightarrow \gamma \wedge \gamma_i \supset B(d) \leftrightarrow (\gamma \supset B(d)) \vee (\gamma_i \supset B(d)).$$

Therefore by (8) of Lemma 8.35

$$\exists x (\gamma_i \supset B(x)) \in M \quad \text{and} \quad \gamma \supset \gamma_i \in M.$$

Consequently $(\gamma \supset \gamma_i) \vee \exists x (\gamma_i \supset B(x)) \in M$. So, by Proposition 8.31 (4) $\gamma \supset \exists x B(x) \in M$. Conversely, let $\gamma \supset \exists x B(x) \in M$. Then there exists γ_i such that

$$(\gamma \supset \gamma_i) \vee (\gamma_i \supset \exists x B(x)) \in M.$$

If $\llbracket \exists x B(x) \rrbracket = \bigvee_{d \in D} \llbracket B(d) \rrbracket > \llbracket \gamma \rrbracket$, then there exists $d \in D$ such that $\llbracket B(d) \rrbracket > \llbracket \gamma \rrbracket$, hence, by the induction hypothesis, $\gamma_i \supset B(d) \notin M$. This is a contradiction, since $\gamma_i \supset \exists x B(x) \in M$. Therefore, $\llbracket \gamma_i \rrbracket \geq \llbracket \exists x B(x) \rrbracket$, and so $\llbracket \gamma \rrbracket > \llbracket \exists x B(x) \rrbracket$.

PROOF OF $\llbracket A \rrbracket \neq 1$. By the construction of M , A is in M . Hence there exists $\gamma \in P$ such that

$$\gamma \supset A \in M,$$

thus $\llbracket A \rrbracket \neq 1$.

CHAPTER 2

PEANO ARITHMETIC

In this chapter we shall formulate first-order Peano arithmetic, prove Gödel's incompleteness theorem, develop a constructive theory of ordinals up to the first ε -number ε_0 , and then present a consistency proof of the system, due to Gentzen.

§9. A formulation of Peano arithmetic

DEFINITION 9.1. The language of the system, which will be called L_n , contains finitely many constants, as follows. (See also Definition 1.1.)

Individual constant: 0;

Function constants: ', +, ·;

Predicate constant: =;

where ' is unary while the other constants are binary.

The intended interpretation of the above constants should be obvious. We shall use expressions like $s = t$, $s + t$, $s \cdot t$ and s' rather than formal expressions like $+(s, t)$.

A numeral is an expression of the form $0' \cdots'$, i.e., zero followed by n primes for some n , which is used as a formal expression for the natural number n , and is denoted by \bar{n} . Further, if s is a closed term of L_n denoting a number m (in the intended interpretation), then \bar{s} denotes the numeral \bar{m} (e.g., if s is $\bar{2} + \bar{3}$, then \bar{s} denotes $\bar{5}$).

DEFINITION 9.2. The first axiom system of Peano arithmetic which we consider, CA, consists of Γ_e for L_n in Definition 7.3 and the following sentences.

$$A1 \quad \forall x \forall y (x' = y' \supset x = y);$$

$$A2 \quad \forall x (\neg x' = 0);$$

$$A3 \quad \forall x (x + 0 = x);$$

$$A4 \quad \forall x \forall y (x + y' = (x + y)');$$

$$A5 \quad \forall x (x \cdot 0 = 0);$$

$$A6 \quad \forall x \forall y (x \cdot y' = x \cdot y + x).$$

The second axiom system of Peano arithmetic which we consider, VJ,

consists of all sentences of the form

$$\forall z_1 \dots \forall z_n \forall x (F(0, z) \wedge \forall y (F(y, z) \supset F(y', z)) \supset F(x, z)),$$

where z is an abbreviation for the sequence of variables z_1, \dots, z_n ; and all the variables which are free in $F(x, z)$ are among x, z .

The basic logical system of Peano arithmetic is **LK**. Then $\text{CA} \cup \text{VJ}$ is an axiom system with equality, regarding $=$ as the distinguished predicate constant in §7. Furthermore, $\forall x \forall y (x = y \supset (F(x) \equiv F(y)))$ is provable for every formula of Ln (cf. Proposition 7.2).

As an example of the strength of $\text{CA} \cup \text{VJ}$, we mention that the theory of primitive recursive functions can be developed in this system. Although this point will not be discussed further here, such knowledge is assumed.

DEFINITION 9.3. The system **PA** (Peano arithmetic) is obtained from **LK** (in the language Ln) by adding extra initial sequents (called the *mathematical initial sequents*) and a new rule of inference called "*ind*", stated below.

1) Mathematical initial sequents: additional initial sequents of **LK_e** for Ln in Definition 7.1 and the following sequents

$$\begin{aligned} s' = t' &\rightarrow s = t; \\ s' = 0 &\rightarrow ; \\ \rightarrow s + 0 &= s; \\ \rightarrow s + t' &= (s + t)'; \\ \rightarrow s \cdot 0 &= 0; \\ \rightarrow s \cdot t' &= s \cdot t + s, \end{aligned}$$

where s, t, r are arbitrary terms of Ln .

2) Ind:

$$\frac{F(a), \Gamma \rightarrow \Delta, F(a')}{F(0), \Gamma \rightarrow \Delta, F(s)}$$

where a is not in $F(0)$, Γ or Δ ; s is an arbitrary term (which may contain a); and $F(a)$ is an arbitrary formula of Ln .

$F(a)$ is called the *induction formula*, and a is called the *eigenvariable* of this inference. Further, we call $F(a)$ and $F(a')$ the *left* and *right auxiliary formula*, respectively, and $F(0)$ and $F(s)$ the *left* and *right principal formula*, respectively, of this inference.

The initial sequents of the form $D \rightarrow D$ are called *logical* initial sequents (in contrast to the mathematical initial sequents defined above).

To summarize, then: there are two kinds of initial sequents of **PA**: logical and mathematical; and three kinds of inference rules: structural, logical and ind (cf. Definition 2.1).

Finally, a *weak inference* is a structural inference other than cut.

We shall adapt the concepts concerning proofs which were defined in Chapter 1 with some modifications; the new inference “ind” must be taken into account in every definition. In particular, the successor of $F(a)$ (respectively, $F(a')$) in ind is $F(0)$ (respectively, $F(s)$). Otherwise all definitions in Chapter 1 are relevant here.

As an easy corollary of the definitions we have

PROPOSITION 9.4. *A sequent is provable from $CA \cup VJ$ (in **LK**) if and only if it is provable in **PA**. Hence the axiom system $CA \cap VJ$ is consistent if and only if \rightarrow is not provable in **PA**.*

Thus we can restrict our attention to the system **PA**. In the rest of this chapter, “provability” means provability in **PA**. It was Gentzen’s great development to formulate first-order arithmetic in the form of **PA**.

Similarly to Lemma 2.11, we can prove the following proposition, which we shall use without mention.

PROPOSITION 9.5. *Let P be a proof in **PA** of a sequent $S(a)$, where all the occurrences of a in $S(a)$ are indicated. Let s be an arbitrary term. Then we may construct a **PA**-proof P' of $S(s)$ such that P' is regular (cf. Lemma 2.9, part (2)) and P' differs from P only in that some free variables are replaced by some other free variables and some occurrences of a are replaced by s .*

The following lemma will be used later.

LEMMA 9.6. (1) *For an arbitrary closed term s , there exists a unique numeral \bar{n} such that $s = \bar{n}$ is provable without an essential cut and without ind. (See Definition 7.5 for “essential cut”).*

(2) *Let s and t be closed terms. Then either $\rightarrow s = t$ or $s = t \rightarrow$ is provable without an essential cut or ind.*

(3) *Let s and t be closed terms such that $s = t$ is provable without an essential cut or ind and let $q(a)$ and $r(a)$ be two terms with some occurrences of a (possibly none). Then $q(s) = r(s) \rightarrow q(t) = r(t)$ is provable without an essential cut or ind.*

(4) *Let s and t be as in (3). For an arbitrary formula $F(a): s = t$, $F(s) \rightarrow F(t)$ is provable without an essential cut or ind.*

PROOF. (1) By induction on the complexity of s .

We defined some notions concerning formal proofs in §2. In order to

carry out the consistency proof for **PA**, however, we need some more of these. We shall list them all here.

DEFINITION 9.7. When we consider a formula or a logical symbol together with the place that it occupies in a proof, in a sequent or in a formula, we refer to it (respectively) as a formula or a logical symbol in the proof, in the sequent or in the formula. A formula in a sequent is also called a *sequent-formula*.

- (1) **Successor.** If a formula E is contained in the upper sequent of an inference using one of the rules of inference in §1 or “ind”, then the *successor* of E is defined as follows:
 - (1.1) If E is a cut formula, then E has no successor.
 - (1.2) If E is an auxiliary formula of any inference other than a cut or exchange, then the principal formula is the successor of E . (For the case of ind, see above.)
 - (1.3) If E is the formula denoted by C (respectively, D) in the upper sequent of an exchange (in Definition 2.1), then the formula C (respectively, D) in the lower sequent is the successor of E .
 - (1.4) If E is the k th formula of Γ , Π , Δ , or Λ in the upper sequent (in Definition 2.1), then the k th formula of Γ , Π , Δ or Λ , respectively, in the lower sequent is the successor of E .
- (2) **Thread.** The notion of a sequence of sequents in a proof, called a *thread*, has been defined in Definition 2.8.
- (3) The notions of a sequent being above or below another, and of a sequent being between two others, were defined in Definition 2.8; so was the notion of an inference being below a sequent.
- (4) A sequent formula is called an *initial formula* or an *end-formula* if it occurs, respectively, in an initial sequent or an end-sequent.
- (5) **Bundle.** A sequence of formulas in a proof with the following properties is called a *bundle*:
 - (5.1) The sequence begins with an initial formula or a weakening formula.
 - (5.2) The sequence ends with an end-formula or a cut-formula.
 - (5.3) Every formula in the sequence except the last is immediately followed by its successor.
- (6) **Ancestor and descendant.** Let A and B be formulas. A is called an *ancestor* of B and B is called a *descendant* of A if there is a bundle containing both A and B in which A appears above B .
- (7) **Predecessor.** Let A and B be formulas. If A is the successor of B , then B is called a *predecessor* of A .

Some principal formulas, e.g. of \wedge : right, has two predecessors. In such cases we call a predecessor the *first* or the *second* predecessor of A , according as it is in the left or right upper sequent.

- (8) The concepts of explicit and implicit.
 - (8.1) A bundle is called *explicit* if it ends with an end formula.

(8.2) It is called *implicit* if it ends with a cut-formula.

A formula in a proof is called explicit or implicit according as the bundles containing the formula are explicit or implicit.

A sequent in a proof is called implicit or explicit according as this sequent contains an implicit formula or not.

A logical inference in a proof is called explicit or implicit according as the principal formula of this inference is explicit or implicit.

(9) End-piece. The *end-piece* of a proof is defined as follows:

(9.1) The end-sequent of the proof is contained in the end-piece.

(9.2) The upper sequent of an inference other than an implicit logical inference is contained in the end-piece if and only if the lower sequent is contained in it.

(9.3) The upper sequent of an implicit logical inference is not contained in the end-piece.

We can rephrase this definition as follows: A sequent in a proof is in the end-piece of the proof if and only if there is no implicit logical inference below this sequent.

(10) An inference of a proof is said to be *in the end-piece* of the proof if the lower sequent of the inference is in the end-piece.

(11) Boundary. Let J be an inference in a proof. We say J *belongs to the boundary* (or J is a *boundary inference*) if the lower sequent of J is in the end-piece and the upper sequent is not. It should be noted that if J belongs to the boundary, then it is an implicit logical inference.

(12) Suitable cut. A cut in the end-piece is called *suitable* if each cut formula of this cut has an ancestor which is the principal formula of a boundary inference.

(13) Essential and inessential cuts. A cut is called *inessential* if the cut formula contains no logical symbol; otherwise it is called essential.

In **PA**, the cut formulas of inessential cuts are of the form $s = t$.

(14) A proof P is *regular* if: (i) the eigenvariables of any two distinct inferences (\forall : right, \exists : left or induction) in P are distinct from each other; and (ii) if a free variable a occurs as an eigenvariable of a sequent S of P , then a only occurs in sequents above S .

PROPOSITION 9.8. *For an arbitrary proof of **PA**, there exists a regular proof of the same end-sequent, which can be obtained from the original proof by simply replacing free variables.*

PROOF. The proof is as for Lemma 2.10, part (2).

§10. The incompleteness theorem

In this section we shall prove the incompleteness of **PA**. This is a celebrated result of Gödel. We shall actually consider any axiomatizable system which contain **PA** as a subsystem.

DEFINITION 10.1. An axiom system \mathcal{A} (cf. §4) is said to be *axiomatizable* if there is a finite set of schemata such that \mathcal{A} consists of all the instances of these schemata. A formal system S is called *axiomatizable* if there is an axiomatizable axiom system \mathcal{A} such that S is equivalent to $\mathbf{LK}_{\mathcal{A}}$ (cf. §4). (Two systems are called equivalent if they have exactly the same theorems.)

A system S is called an *extension* of \mathbf{PA} if every theorem of \mathbf{PA} is provable in S . Throughout this section we deal with axiomatizable systems which are extensions of \mathbf{PA} . They are denoted by S . Such an S is arbitrary but fixed; so is the language of S , say L (which will always extend L_n).

DEFINITION 10.2. The class of primitive recursive functions is the smallest class of functions generated by the following schemata. (These can be thought of as the clauses of an inductive definition, or as the defining equations of the function being defined.)

- (i) $f(x) = x'$, where $'$ is the successor function.
- (ii) $f(x_1, \dots, x_n) = k$, where $n \geq 1$ and k is a natural number.
- (iii) $f(x_1, \dots, x_n) = x_i$, where $1 \leq i \leq n$.
- (iv) $f(x_1, \dots, x_n) = g(h_1(x_1, \dots, x_n), \dots, h_m(x_1, \dots, x_n))$, where g, h_1, \dots, h_m are primitive recursive functions.
- (v) $f(0) = k, f(x') = g(x, f(x))$, where k is a natural number and g is a primitive recursive function.
- (vi) $f(0, x_2, \dots, x_n) = g(x_2, \dots, x_n), f(x', x_2, \dots, x_n) = h(x, f(x, x_2, \dots, x_n), x_2, \dots, x_n)$, where g and h are primitive recursive functions.

This formulation is due to Kleene.

An n -ary relation R (of natural numbers) is said to be *primitive recursive* if there is a primitive recursive function f which assumes values 0 and 1 only such that $R(a_1, \dots, a_n)$ is true if and only if $f(a_1, \dots, a_n) = 0$.

EXERCISE 10.3. We define $+$ and \cdot as follows:

$$\begin{aligned} a + 0 &= a, & a \cdot 0 &= 0, \\ a + b' &= (a + b)', & a \cdot b' &= a \cdot b + a. \end{aligned}$$

Prove the following from the above equations in \mathbf{PA} .

- (1) $a + b = b + a$.
- (2) $a \cdot b = b \cdot a$.
- (3) $a \cdot (b + c) = a \cdot b + a \cdot c$.

EXERCISE 10.4. Prove that $=$ and $<$ are primitive recursive relations of natural numbers.

Here we shall state a basic metamathematical lemma without proof, which we shall use later.

LEMMA 10.5. *The consistency of S (i.e., S -unprovability of \rightarrow) is equivalent to the S -unprovability of $0 = 1$. In other words, $0 = 1$ is S -provable if and only if every formula of L is S -provable. (Cf. Proposition 4.2.)*

PROPOSITION 10.6 (Gödel). (1) *The graphs of all the primitive recursive functions can be expressed in Ln , so that (the translations of) their defining equations are provable in PA .*

Thus the theory of primitive recursive functions can be translated into our formal system of arithmetic. We may therefore assume that PA (or any of its extensions) actually contains the function symbols for primitive recursive functions and their defining equations, as well as predicate symbols for the primitive recursive relations.

We must distinguish between informal objects and their formal expressions (although this will lead to notational complications). For example, the formal expression (function symbol) for a primitive recursive function f will be denoted by \bar{f} ; if R is a predicate (of natural numbers) which can be expressed in the formal language, then its formal expression will be denoted by \bar{R} . Also, as stated earlier, for any closed term t , \bar{t} is the numeral of the number denoted by t . Although in later sections we may omit such a rigorous distinction between formal and informal expressions, it is essential in this section.

(2) *Let R be a primitive recursive relation of n arguments. It can be represented in PA by a formula $\bar{R}(a_1, \dots, a_n)$, namely $\bar{f}(a_1, \dots, a_n) = \bar{0}$, where f is the characteristic function of R . Then, for any n -tuple of numbers (m_1, \dots, m_n) , if $R(m_1, \dots, m_n)$ is true, then $\bar{R}(\bar{m}_1, \dots, \bar{m}_n)$ is PA -provable.*

PROOF. The proof of (1) is by induction on the inductive definition of the primitive recursive functions (i.e., by induction on their construction).

The proof of (2) is carried out as follows. We prove that for any primitive recursive function f (of n arguments) and any numbers m_1, \dots, m_n, p , if $f(m_1, \dots, m_n) = p$, then $\bar{f}(\bar{m}_1, \dots, \bar{m}_n) = \bar{p}$ is PA -provable. The proof is by induction on the construction of f (according to its defining equations). Then, finally, if f is a primitive recursive function which is the characteristic function of R , we have, for all m_1, \dots, m_n , if $R(m_1, \dots, m_n)$ is true, then $\bar{f}(\bar{m}_1, \dots, \bar{m}_n) = \bar{0}$ is PA -provable.

Since the rest of the argument depends heavily on this proposition, we shall use it without quoting it each time.

Note that the converse proposition (i.e., for primitive recursive R , if $\bar{R}(\bar{m}_1, \dots, \bar{m}_n)$ is PA -provable, then $R(m_1, \dots, m_n)$ is true) follows from the consistency of PA .

DEFINITION 10.7 (Gödel numbering). We shall define a one-to-one map from the formal expressions of the language L , such as symbols, terms,

formulas, sequents and proofs, to the natural numbers. (The following is only one example of a suitable map.) For an expression X , we use ' X ' to denote the corresponding number, which we call the Gödel number of X .

(1) First assign different odd numbers to the symbols of L_n . (We include \rightarrow and $-$ among the symbols of the language here.)

(2) Let X be a formal expression $X_0 X_1 \dots X_n$, where each X_i , $0 \leq i \leq n$, is a symbol of L . Then ' X ' is defined to be $2^{x_0} 3^{x_1} \dots p_n^{x_n}$, where p_n is the n th prime number.

(3) If P is a proof of the form

$$\frac{Q}{S} \quad \text{or} \quad \frac{Q_1 \quad Q_2}{S}$$

then ' P ' is $2^{q_1} 3^{r-1} 5^{s_1}$ or $2^{q_1} 3^{r_2} 5^{r-1} 7^{s_1}$, respectively.

If an operation or relation defined on a class of formal objects (e.g., formulas, proofs, etc.) is thought of in terms of the corresponding number-theoretic operation or relation on their Gödel numbers, we say that the operation or relation has been *arithmetized*. More precisely, suppose ψ is an operation defined on n -tuples of formal objects of a certain class, and f is a number-theoretic function such that for all formal objects X_1, \dots, X_n, X (of the class considered), if ψ applied to X_1, \dots, X_n produces X , then $f('X_1', \dots, 'X_n') = 'X'$. Then f is called the *arithmetization* of ψ . Similarly with relations.

LEMMA 10.8. (1) *The operation of substitution can be arithmetized primitive recursively, i.e., there is a primitive recursive function sb of two arguments such that if $X(a_0)$ is an expression of L (where all occurrences of a_0 in X are indicated), and Y is another expression, then $sb('X(a_0)', 'Y') = 'X(Y)'$, where $X(Y)$ is the result of substituting Y for a_0 in X .*

(2) *There is a primitive recursive function ν such that $\nu(m) =$ 'the m th numeral'. In terms of our notation, $\nu(m) = 'm'$.*

(3) *The notion that P is a proof (of the system S) of a formula A (or a sequent S) is arithmetized primitive recursively; i.e., there is a primitive recursive relation $\text{Prov}(p, a)$ such that $\text{Prov}(p, a)$ is true if and only if there is a proof P and a formula A (or a sequent S) such that $p = 'P'$, $a = 'A'$ (or $a = 'S'$) and P is a proof of A (or S).*

(4) *Prov may be written as Prov_S to emphasize the system S .*

(5) *As was mentioned before, the formal expression for Prov will be denoted by Prov .*

We shall not prove this lemma. It is important to note that the axiomatizability of S is used in (3); (3) is crucial in the subsequent argument. We also use the following fact about Gödel numbering: we can go effectively from formal objects to their Gödel numbers, and back again

(i.e., decide effectively whether a given number is a Gödel number, and if so, of what formal object).

$\exists x \overline{\text{Prov}}(x, \ulcorner A \urcorner)$ is often abbreviated to $\overline{\text{Pr}}(\ulcorner A \urcorner)$ or $\vdash \ulcorner A \urcorner$.

PROPOSITION 10.9. (1) *If A is S -provable, then $\vdash \ulcorner A \urcorner$ is S -provable.*

(2) *If $A \leftrightarrow B$ is S -provable, then $\overline{\text{Pr}}(\ulcorner A \urcorner) \leftrightarrow \overline{\text{Pr}}(\ulcorner B \urcorner)$, i.e., $\vdash \ulcorner A \urcorner \leftrightarrow \vdash \ulcorner B \urcorner$, is S -provable.*

(3) $\vdash \ulcorner A \urcorner \rightarrow (\vdash \ulcorner \ulcorner A \urcorner \urcorner)$ is S -provable.

PROOF. (1) Suppose A is provable with a proof P . Then by (3) of Lemma 10.5, $\overline{\text{Prov}}(\ulcorner P \urcorner, \ulcorner A \urcorner)$ is true, which implies, by (2) of Proposition 10.6, that $\exists x \overline{\text{Prov}}(x, \ulcorner A \urcorner)$, i.e., $\vdash \ulcorner A \urcorner$, is S -provable.

(2) Suppose $A \equiv B$ is provable with a proof P and A is provable with a proof Q . There is a prescription for constructing a proof of B from P and Q , uniform in P and Q , which can be arithmetized by a primitive recursive function f . Thus $\overline{\text{Prov}}(q, \ulcorner A \urcorner) \rightarrow \overline{\text{Prov}}(f(p, q), \ulcorner B \urcorner)$ is true, from which it follows by (2) of Proposition 10.6 that $\vdash \ulcorner A \urcorner \rightarrow \vdash \ulcorner B \urcorner$ is provable. The same argument works for $\vdash \ulcorner B \urcorner \rightarrow \vdash \ulcorner A \urcorner$.

(3) If P is a proof of A , then we can construct a proof Q of $\vdash \ulcorner A \urcorner$ by (1). This process is uniform in P ; in other words, there is a uniform prescription for obtaining Q from P . Thus

$$\overline{\text{Prov}}(p, \ulcorner A \urcorner) \rightarrow \overline{\text{Pr}}(\ulcorner \ulcorner A \urcorner \urcorner)$$

is true for some primitive recursive function f , from which it follows that $\vdash \ulcorner A \urcorner \rightarrow \vdash \ulcorner \ulcorner A \urcorner \urcorner$ is provable.

We shall now consider the notion of truth definition and Tarski's theorem concerning it.

DEFINITION 10.10. A formula of L (the language of S) with one free variable, say $T(a_0)$, is called a *truth definition* for S if every sentence A of L ,

$$T(\ulcorner A \urcorner) \equiv A$$

is S -provable.

THEOREM 10.11 (Tarski). *If S is consistent, then it has no truth definition.*

PROOF. Suppose otherwise. Then there is a formula $T(a_0)$ of L such that for every sentence A of L , $T(\ulcorner A \urcorner) \equiv A$ is provable in S . Consider the formula $F(a_0)$, with sole free variable a_0 , defined as: $\neg T(\text{sb}(a_0, \bar{v}(a_0)))$. Put $p = \ulcorner F(a_0) \urcorner$, and let A_T be the sentence $F(\bar{p})$. Then by definition:

$$A_T \equiv \neg T(\text{sb}(\bar{p}, \bar{v}(\bar{p}))). \quad (1)$$

Also, since $\ulcorner A_T \urcorner = \text{sb}(p, \nu(p))$, we can prove in **S** the equivalences:

$$\begin{aligned} A_T &\equiv T(\overline{\ulcorner A_T \urcorner}) \quad (\text{by assumed property of } T) \\ &\equiv T(\overline{\text{sb}(\bar{p}, \bar{\nu}(\bar{p}))}). \end{aligned} \quad (2)$$

(1) and (2) together contradict the consistency of **S**.

An interesting consequence of Theorem 10.11 is the following. First note that in the proof of Theorem 10.11, we need *not* assume that **S** is axiomatizable (cf. Def. 10.1). So we may take as the axioms of **S** the set of all sentences of L_n which are *true* in the intended interpretation (or standard model) \mathcal{M} of **PA** (using the ordinary semantic or model-theoretic definition of truth in \mathcal{M}). We then obtain that there is no formula $T(a_0)$ of L_n such that for any sentence A of L_n :

$$A \text{ is true} \Leftrightarrow T(\overline{\ulcorner A \urcorner}) \text{ is true}$$

(i.e., true in \mathcal{M}). This corollary of Theorem 10.11 can be stated in the form: "The notion of arithmetical truth is not arithmetical" (i.e., cannot be expressed by a formula of L_n). This is often taken as the statement of Tarski's theorem.

DEFINITION 10.12. **S** is called *incomplete* if for some sentence A , neither A nor $\neg A$ is provable in **S**.

Next we introduce "Gödel's trick" for use in Theorem 10.16.

DEFINITION 10.13. Consider a formula $F(\alpha)$ with a metavariable α (i.e., a new predicate variable, not in L , which we only use temporarily for notational convenience), where α is regarded as an atomic formula in $F(\alpha)$ and $F(\alpha)$ is closed. $F(\ulcorner \text{sb}(\bar{a}_0, \bar{\nu}(\bar{a}_0)) \urcorner)$ is a formula with \bar{a}_0 as its sole free variable. Define $p = \ulcorner F(\ulcorner \text{sb}(\bar{a}_0, \bar{\nu}(\bar{a}_0)) \urcorner) \urcorner$ and A_F as $F(\ulcorner \text{sb}(\bar{p}, \bar{\nu}(\bar{p})) \urcorner)$. Note that A_F is a sentence of L .

LEMMA 10.14. $A_F \equiv F(\overline{\ulcorner A_F \urcorner})$ is provable in **S**.

PROOF. Since $\ulcorner A_F \urcorner = \text{sb}(p, \nu(p))$ by definition,

$$\overline{\ulcorner A_F \urcorner} = \overline{\text{sb}(\bar{p}, \bar{\nu}(\bar{p}))} \text{ is provable in } \mathbf{S}.$$

Hence $A_F \equiv F(\overline{\ulcorner A_F \urcorner})$ is provable in **S**.

From now on, we shall use the abbreviation $\vdash A$ for $\vdash \overline{\ulcorner A \urcorner}$.

DEFINITION 10.15. S is called ω -consistent if the following condition is satisfied. For every formula $A(a_0)$, if $\neg A(\bar{n})$ is provable in S for every $n = 0, 1, 2, \dots$, then $\exists x A(x)$ is not provable in S . Note that ω -consistency of S implies consistency of S .

THEOREM 10.16 (Gödel's first incompleteness theorem). *If S is ω -consistent, then S is incomplete.*

PROOF. There exists a sentence A_G of L such that $A_G \equiv \neg \vdash A_G$ is provable in S . (Any such sentence will be called a Gödel sentence for S .) This follows from Lemma 10.14, by taking $F(\alpha)$ in Definition 10.13 to be $\neg \alpha$. Then $A_G \equiv \neg \vdash A_G$ is provable in S . First we shall show that A_G is not provable in S , assuming only the consistency of S (but without assuming the ω -consistency of S). Suppose that A_G were provable in S . Then by (1) of Proposition 10.9, $\vdash A_G$ is provable in S ; thus by the definition of Gödel sentence, $\neg A_G$ is provable in S , contradicting the consistency of S .

Next we shall show that $\neg A_G$ is not provable in S , assuming the ω -consistency of S . Since we have proved that A_G is not provable in S , for each $n = 0, 1, 2, \dots$, $\neg \text{Prov}(\bar{n}, \ulcorner A_G \urcorner)$ is provable in S . By the ω -consistency of S , $\exists x \text{Prov}(x, \ulcorner A_G \urcorner)$ is not provable in S . Since $\neg A_G \equiv \vdash A_G$ is provable in S , $\neg A_G$ is not provable in S .

REMARK. In fact, A_G , although unprovable, is (intuitively) true, since it asserts its own unprovability.

DEFINITION 10.17. $\overline{\text{Consis}}_S$ is the sentence $\neg \vdash 0 = 1$. (So $\overline{\text{Consis}}_S$ asserts the consistency of S .)

THEOREM 10.18. (Gödel's second incompleteness theorem). *If S is consistent, then $\overline{\text{Consis}}_S$ is not provable in S .*

PROOF. Let A_G be a Gödel sentence. In the proof of Theorem 10.16, we proved that A_G is not provable, assuming only consistency of S . Now we shall prove a stronger theorem: that $A_G \equiv \overline{\text{Consis}}_S$ is provable in S .

(1) To show $A_G \rightarrow \overline{\text{Consis}}_S$ is provable in S . By Lemma 10.5, $\neg \overline{\text{Consis}}_S \equiv \forall' A' (\vdash A)$ is provable (where $\forall' A'$ means: for all Gödel numbers of formulas A). Therefore, $A_G \rightarrow \neg \vdash A_G \rightarrow \neg \forall' A' (\vdash A) \rightarrow \overline{\text{Consis}}_S$.

(2) To show $\overline{\text{Consis}}_S \rightarrow A_G$ is provable in S . Again by Lemma 10.5, $\overline{\text{Consis}}_S, \vdash A_G \rightarrow \neg \vdash \neg A_G \rightarrow \neg \vdash \vdash A_G$, since $\neg A_G \equiv \vdash A_G$ (of (3) of Lemma 10.8). But $\vdash A_G \rightarrow \vdash \vdash A_G$, by Proposition 10.9. So $\overline{\text{Consis}}_S, \vdash A_G \rightarrow \neg \vdash \vdash A_G \wedge \vdash \vdash A_G$, and so $\overline{\text{Consis}}_S \rightarrow \neg \vdash A_G \rightarrow A_G$.

EXERCISE 10.19. Define the system **QA** as the quantifier-free part of **PA**.

Show that the following are provable in **QA** for free variables a, b, c .

- (1) $a = a$,
- (2) $a = b \rightarrow b = a$,
- (3) $a + b = b + a$,
- (4) $a \cdot b = b \cdot a$,
- (5) $a \cdot (b + c) = a \cdot b + a \cdot c$.

EXERCISE 10.20. In Gödel's trick (cf. Definition 10.13) we may replace $\text{sb}(a_0, \nu(a_0))$ by $e(\text{sb}(a_0, \nu(a_0)))$ for some primitive recursive function e which satisfies that if A is a formula then $e('A')$ is Gödel number of a formula obtained from A by adding some more stages of the definition of formula; for example, $e('A') = '\neg A'$. Show that if $e('A') = '\neg A'$, $p = 'F(\vdash \bar{e}(\text{sb}(a_0, \bar{\nu}(a_0))))'$ and B_F is $F(\vdash \bar{e}(\text{sb}(\bar{p}, \bar{\nu}(\bar{p}))))$, then $'B_F' = \text{sb}(p, \nu(p))$, i.e., B_F is $F(\vdash \neg B_F)$.

PROBLEM 10.21 (Löb). Show that for any sentence A , if $(\vdash A) \rightarrow A$ is **PA**-provable, then A is itself provable. [*Hint:* By Gödel's trick there is a sentence B such that $B \equiv (\vdash B \supset A)$. For such B , if B is provable then $\vdash B$ is provable (cf. Proposition 10.9) and $(\vdash B) \rightarrow A$ is provable; thus A is provable. This procedure is uniform in the proofs of B ; hence by formalizing the entire process we obtain $(\vdash B) \rightarrow (\vdash A)$. This and the assumption $(\vdash A) \rightarrow A$ imply $(\vdash B) \rightarrow A$. But, by the definition of B , the last sequent implies B itself, and hence $\vdash B$ (Proposition 10.9). So, since $\vdash B$ and $(\vdash B) \rightarrow A$ are both provable, so is A .]

PROBLEM 10.22 (Rosser). Let e be a primitive recursive function satisfying $e('A') = '\neg A'$ as in Exercise 10.20. Let $F(a_{10})$ be

$$\forall x_1 (\overline{\text{Prov}}(x_1, \text{sb}(a_0, \bar{\nu}(a_0))) \supset \exists x_2 (x_2 \leq x_1 \vee \overline{\text{Prov}}(x_2, \bar{e}(\text{sb}(x_1, \bar{\nu}(x_0)))))).$$

Define $p = 'F(a_0)'$ and A_R as $F(\bar{p})$. Prove that if **S** is consistent, then neither A_R nor $\neg A_R$ is provable in **S**.

REMARK. This strengthens Gödel's first incompleteness theorem. Namely, the hypothesis of the ω -consistency in Theorem 10.16 is weakened to the consistency.

§11. A discussion of ordinals from a finitist standpoint

When one is concerned with consistency proofs, their philosophical interpretation is always a paramount problem. There is no doubt that Hilbert's "finitist standpoint" which considers only a finite number of

symbols concretely given and arguments concretely given about finite sequences of these symbols (called expressions) is an ideal standpoint in proving consistency. From this standpoint, one defines expressions in the following way (as we have, in fact, done already).

(0) Firstly, we give a finite set of symbols, called an alphabet.

(1) Next, we give a finite set of finite sequences of these symbols, called initial expressions.

(2) Next, we give a finite set of concrete operations, for constructing or generating expressions from expressions already obtained.

(3) Finally, we restrict ourselves to considering only expressions obtained by starting with step (1) and iterating step (2).

As a special case of the above, let us suppose that we are given symbols a_1, \dots, a_n by (1), and concrete operations f_1, \dots, f_j , to obtain new expressions from expressions we already have, and let \mathcal{D} be the collection of all expressions thus obtained. Then the definition of \mathcal{D} is as follows:

(0) The alphabet consists of $\{a_1, \dots, a_n\}$.

(1) a_1, \dots, a_n (considered as sequences of length 1) are in \mathcal{D} .

(2) If x_1, \dots, x_{k_i} are in \mathcal{D} , then $f_i(x_1, \dots, x_{k_i})$ is in \mathcal{D} ($i = 1, \dots, j$).

(3) \mathcal{D} consists of only these objects (expressions) obtained by (1) and (2).

This is called a *recursive* or *inductive definition* of the class \mathcal{D} . Corresponding to this inductive definition, we have a principle of “*proof by induction*” on (the elements of) \mathcal{D} , namely, let A be any property (of expressions), and suppose we can do the following.

(1) Prove that $A(a_1), \dots, A(a_n)$ hold;

(2) Assuming $A(x_1), \dots, A(x_k)$ hold for x_1, \dots, x_k in \mathcal{D} , infer that

$$A(f_1(x_1, \dots, x_{k_1})), \dots, A(f_j(x_1, \dots, x_{k_j}))$$

hold.

Then we conclude that $A(x)$ holds for all x in \mathcal{D} . This follows since for any x in \mathcal{D} that is concretely given, one can show that $A(x)$ holds by following the steps in constructing this x , by applying (1) and (2) above step by step. According to this viewpoint, we can regard “induction” simply as a general statement of a concrete method of proof applicable for any given expression x , and not as an axiom that is accepted a priori.

Though nobody denies that the above way of thinking is contained in Hilbert’s standpoint, there are many opinions about where to set the boundary of this standpoint: for example, assuming that transfinite induction up to each of $\omega, \omega \cdot 2, \omega \cdot 3, \dots$ is accepted, whether transfinite induction up to ω^2 should also be accepted; or, assuming that transfinite induction up to each of $\omega, \omega^\omega, \omega^{\omega^\omega}, \dots$ is accepted, whether transfinite induction up to the first ε -number (denoted by ε_0) should be. If we consider each concretely given expression (in this case an ordinal less than ε_0), then it must be less than some ω_n , and so should be accepted—or

should it? Here ω_n denotes the ordinal

$$\omega \cdot \left. \begin{matrix} \omega \\ \vdots \\ \omega \end{matrix} \right\} n.$$

When one thinks about this in a very skeptical way, how far can one accept induction? One might even perhaps doubt whether induction up to ω itself is already beyond Hilbert's standpoint.

However, if we interpret Hilbert's finitist standpoint in an extremely pure and restricted way so as to forbid both transfinite induction and all abstract notions such as Gödel's primitive recursive functionals of finite types, then by Gödel's incompleteness theorem, it is clear that *the consistency of PA cannot be proved if one adheres to this standpoint*, since (presumably) such strictly finitist methods can be formalized in PA (in fact, in "primitive recursive arithmetic": see below).

Therefore in a consistency proof it is always very interesting to see what is used that goes beyond Hilbert's finitist standpoint, and on what basis it can be justified.

At present, the methods used mainly for consistency proofs are firstly those using transfinite induction (initiated by Gentzen), and, secondly, those using higher type functionals (initiated by Gödel).

We explain the first method, that of Gentzen. First, in order to make sure of our standpoint, let us consider an inductive definition of natural numbers that adheres most closely to the above scheme:

N 1 1 is a natural number.

N 2 If a is a natural number, then $a1$ is a natural number.

N 3 Only those objects obtained by N 1 and N 2 are natural numbers.

Although we normally consider a definition like this to be obvious, it seems that this is because much knowledge is often unconsciously presupposed. In order to clarify our unconsciously-arrived-at standpoint, let us ask ourselves questions that a person E who has no understanding of N 1–N 3 might ask.

First, E might say he did not understand N 2 and N 3. For E it is impossible to understand N 2 using the notion of natural number when one does not understand "natural numbers" (a "vicious circle"). Moreover, E cannot understand in N 3 what "those objects obtained by N 1 and N 2" means. There are many possible answers to these doubts. The most practical one from the didactic point of view will be as follows: 1 is a natural number by N 1. Now that we know 1 is a natural number, 11 is a natural number by N 2; now that we know 11 is a natural number, 111 is a natural number by N 2. Everything obtained in this way by starting with N 1 and iterating the operation N 2 is a natural number. N 3 says on the other hand, that only those things obtained in this way are natural

numbers. Of course E might ask more questions about the above explanation: "What do you mean by 'iterating the operation $N2$ '?", "What do you mean by 'everything obtained in this way'?" etc., and this kind of discussion can be continued endlessly. I hope that E will finally get the idea. The important fact is that the general concept of a (potentially) infinite process of creating new things by iterating a concrete operation a finite number of times is presupposed in order to understand the definition $N1$ – $N3$ of natural numbers, and that the purpose of the definition $N1$ – $N3$ is to specify the process of defining natural numbers by such a procedure.

When we analyze precisely the discussion repeated endlessly with E , we will realize that we must accept or presuppose to some extent the notion of finite sequence (or finite iteration of an operation) as our basic notion. Here an important remark should be made: this does not mean that we must accept large amounts of knowledge about sequences and finiteness separately; only that which seems absolutely necessary to understand the single notion of finite sequence.

In order to clarify our standpoint further, let us consider the inductive definition of the finite (non-empty) sequences of natural numbers:

- S 1 If n is a natural number, then n itself is a finite sequence of natural numbers.
- S 2 If m is a natural number and s is a finite sequence of natural numbers, then $s * m$ is a finite sequence of natural numbers.
- S 3 Only those objects obtained by S 1 and S 2 are finite sequences of natural numbers.

It should be realized that this kind of definition is regarded as basic and clear, no matter what standpoint one assumes.

We shall present some more examples of such inductively defined classes of concrete objects, and properties of them.

For instance, the notion of length of a finite sequence of natural numbers is defined inductively as follows:

- L 1 If s is a sequence of natural numbers consisting of a natural number n only, then the length of s is 1.
- L 2 If s is a sequence of natural numbers of the form $s_0 * n$, and the length of s_0 is l , then the length of s is $l + 1$.

We can certainly take an alternative definition: given a sequence of natural numbers, say s , examine s and count the number of $*$'s in it. If the number of $*$'s is l , then the length of s is $l + 1$. (Each of these definitions presents an operation which applies to the concretely given figures in a general form.)

These finitist inferences often present striking similarities to the arguments in the following formalism, which we call primitive recursive arithmetic.

- (1) The basic logical system is the propositional calculus.
- (2) The defining equations of primitive recursive functions are assumed as axioms.

- (3) No quantifiers are introduced.
 (4) Mathematical induction (for quantifier-free formulas) is admitted:

$$\frac{A(a), \Gamma \rightarrow \Delta, A(a')}{A(0), \Gamma \rightarrow \Delta, A(t)}$$

where a does not occur in $A(0)$, Γ or Δ , and t is an arbitrary term.

From the above discussion, it seems quite reasonable to characterize Hilbert's finitist standpoint as that which can be formalized in *primitive recursive arithmetic*. This standpoint shall be called the "purely finitist standpoint". It is therefore of paramount importance to clarify where a consistency proof exceeds this formalism, i.e., the purely finitist standpoint. (Thus, in the following, we shall not bother with arguments which can be carried out within the above formalism.) In order to pursue this point, we shall first present the recursive definition of ordinal numbers up to ε_0 (the first ε -number); temporarily, by "ordinal" we mean: ordinal less than ε_0 .

O 1 0 is an ordinal.

O 2 Let μ and $\mu_1, \mu_2, \dots, \mu_n$ be ordinals. Then $\mu_1 + \mu_2 + \dots + \mu_n$ and ω^μ are ordinals.

O 3 Only those objects obtained by O 1 and O 2 are ordinals.

ω^0 will be denoted by 1. Regarding 1 as the natural number 1, $1 + 1$ as 2, etc., we may assume that the natural numbers are included in the ordinals. (We may also include 0 among the natural numbers if we wish.)

We can now define the relations $=$ and $<$ on ordinals so that they match the notions of equality and the natural ordering of ordinals which we know from set theory, and develop the theory of ordinals for these relations within the purely finitist standpoint. We can actually inductively define $=$, $<$, $+$, and \cdot simultaneously so that they satisfy the following.

(1) $<$ is a linear ordering and 0 is its least element.

(2) $\omega^\mu < \omega^\nu$ if and only if $\mu < \nu$.

(3) Let μ be an ordinal containing an occurrence of the symbol 0 but not 0 itself, and let μ' be the ordinal obtained from μ by eliminating this occurrence of 0 as well as excessive occurrences of $+$. Then $\mu = \mu'$.

As a consequence of (3) it can be easily shown that

(4) Every ordinal which is not 0 can be expressed in the form

$$\omega^{\mu_1} + \omega^{\mu_2} + \dots + \omega^{\mu_n},$$

where each of $\mu_1, \mu_2, \dots, \mu_n$ which is not 0 has the same property. (Each term ω^{μ_i} is called a monomial of this ordinal.)

(5) Let μ and ν be of the forms

$$\omega^{\mu_1} + \omega^{\mu_2} + \dots + \omega^{\mu_k} \quad \text{and} \quad \omega^{\nu_1} + \omega^{\nu_2} + \dots + \omega^{\nu_l},$$

respectively. Then $\mu + \nu$ is defined as

$$\omega^{\mu_1} + \omega^{\mu_2} + \dots + \omega^{\mu_k} + \omega^{\nu_1} + \omega^{\nu_2} + \dots + \omega^{\nu_l}.$$

(6) Let μ be an ordinal which is written in the form of (4) and contains two consecutive terms ω^{μ_i} and $\omega^{\mu_{i+1}}$ with $\mu_i < \mu_{i+1}$, i.e., μ is of the form

$$\dots + \omega^{\mu_i} + \omega^{\mu_{i+1}} + \dots,$$

and let μ' be an ordinal obtained from μ by deleting " $\omega^{\mu_i} +$ ", so that μ' is of the form

$$\dots \omega^{\mu_{i+1}} + \dots$$

Then $\mu = \mu'$.

As a consequence of (6) we can show that

(7) For every ordinal μ (which is not 0) there is an ordinal of the form

$$\omega^{\mu_1} + \omega^{\mu_2} + \dots + \omega^{\mu_n},$$

where $\mu_1 \geq \dots \geq \mu_n$ such that $\mu = \omega^{\mu_1} + \dots + \omega^{\mu_n}$, where $\mu \geq \nu$ means: $\nu < \mu$ or $\nu = \mu$. The latter is called the normal form of μ . (This normal form of μ is unique, since the same holds for every ordinal which is used in constructing μ : see O 2.)

Suppose $\mu = \omega^{\mu_1} + \dots + \omega^{\mu_n}$ and $\nu = \omega^{\nu_1} + \dots + \omega^{\nu_m}$ are in the normal form. Then, $\mu < \nu$ if and only if $\omega^{\mu_i} < \omega^{\nu_i}$ for some i and $\omega^{\mu_j} = \omega^{\nu_j}$ for all $j < i$, or $n < m$ and $\omega^{\mu_i} = \omega^{\nu_i}$ for all $i \leq n$.

(8) Let μ have the normal form

$$\omega^{\mu_1} + \omega^{\mu_2} + \dots + \omega^{\mu_n}$$

and ν be > 0 . Then $\mu \cdot \omega^\nu = \omega^{\mu_1 + \nu}$.

(9) Let μ and ν be as in (5). Then

$$\mu \cdot \nu = \mu \cdot \omega^{\nu_1} + \mu \cdot \omega^{\nu_2} + \dots + \mu \cdot \omega^{\nu_l}.$$

(10) $(\omega^\mu)^n$ is defined as $\omega^\mu \dots \omega^\mu$ (n times) for any natural number n . Then $(\omega^\mu)^n = \omega^{\mu \cdot n}$.

As a consequence of our definitions, it can easily be shown that for an arbitrary ordinal μ an ordinal of the form ω_n which satisfies $\mu < \omega_n$ can be constructed.

It is obvious that for any given natural number n the length of a strictly decreasing sequence of ordinals which starts with n is at most $n + 1$; in other words, there can be no strictly decreasing sequence of ordinals which starts with n and has length $n + 2$. This fact tells us that the notion of

arbitrary, strictly decreasing sequences of ordinals which start with n is a clear notion.

At this point it is not very meaningful to object to this on the grounds that if we write the statement that a strictly decreasing sequence terminates, in terms of expressions in the Kleene hierarchy, it turns out to belong to the Π_1^1 -class. The important fact is not to which class of the hierarchy it belongs but how evident it is. We shall come to this point later.

In the following section, a consistency proof (for **PA**) will be given in the following way. In order to emphasize the concrete or "figurative" aspect of the arguments, we say "proof-figure" for formal proof.

1) We present a uniform method such that, if a proof-figure P is concretely given, then the method enables us to concretely construct another proof-figure P' ; furthermore, the end-sequent of P' is the same as that of P if the end-sequent of P does not contain quantifiers. The process of constructing P' from P is called the "reduction" (of P) and may be denoted by r . Thus $P' = r(P)$.

2) There is a uniform method by which every proof-figure is assigned an ordinal $< \varepsilon_0$. The ordinal assigned to P (the ordinal of P) may be denoted by $o(P)$.

3) o and r satisfy: whenever a proof-figure P contains an application of ind or cut, then $o(P) > \omega$ and $o(r(P)) < o(P)$, and if P does not contain any such application, then $o(P) < \omega$.

Suppose we have concretely shown that any strictly decreasing sequence of natural numbers is finite, and that whenever a concrete method of constructing decreasing sequences of ordinals $< \varepsilon_0$ is given it can be recognized that any decreasing sequence constructed this way is finite (or such a sequence terminates). (By "decreasing sequence" we will always mean strictly decreasing sequence.) We can then conclude, in the light of 1)–3) above, that, for any given proof-figure P whose end-sequent does not contain quantifiers, there is a concrete method of transforming it into a proof-figure with the same end-sequent and containing no applications of the rules cut and ind. It can be easily seen, on the other hand, that no proof-figure without applications of a cut or ind can be a proof of the empty sequent. Thus we can claim that the consistency of the system has been proved.

The crucial point in the process described above is to demonstrate:

- (*) Whenever a concrete method of constructing decreasing sequences of ordinals is given, any such decreasing sequence must be finite.

We are going to represent a version of such a demonstration, which the author believes represents the most illuminating approach to the consistency proof.

Suppose $a_0 > a_1 > \dots$ is a decreasing sequence concretely given.

(I) Assume $a_0 < \omega$, or a_0 is a natural number.

Consider a decreasing sequence which starts with a concretely given

natural number. As soon as one writes down its first term n , one can recognize that its length must be at most $n + 1$. Hence we can assume that a_0 is not a natural number.

In order to deal with all ordinals $< \varepsilon_0$, we shall define the concept of α -sequence and α -eliminator for all $\alpha < \varepsilon_0$. We start, however, with a simple example rather than the general definition.

(II) Suppose each a_i in $a_0 > a_1 > \dots$ is written in the canonical form; a_i has the form

$$\omega^{\mu_1^i} + \omega^{\mu_2^i} + \dots + \omega^{\mu_{r_i}^i} + k_i,$$

where $\mu_j^i > 0$ and k_i is a natural number. (This includes the case where $+k_i$ does not actually appear.) A sequence in which k_i does not appear for any a_i will be called a 1-sequence. We call $\omega^{\mu_1^i} + \omega^{\mu_2^i} + \dots + \omega^{\mu_{r_i}^i}$ in a_i the 1-major part of a_i . We shall give a concrete method (M_1) which enables us to do the following: given a descending sequence $a_0 > a_1 > \dots$, where each a_i is written in its canonical form, the method M_1 concretely produces a (decreasing) 1-sequence $b_0 > b_1 > \dots$ so as to satisfy the condition

(C₁) b_0 is the 1-major part of a_0 , and we can concretely show that if $b_0 > b_1 > \dots$ is a finite sequence, then so is $a_0 > a_1 > \dots$.

This method M_1 (a 1-eliminator) is defined as follows. Put $a_i = a'_i + k_i$, where a'_i is the 1-major part of a_i . Then $a_0 > a_1 > a_2 > \dots$ can be expressed as $a'_0 + k_0 > a'_1 + k_1 > a'_2 + k_2 > \dots$.

Put $b_0 = a'_0$. Suppose $b_0 > b_1 > \dots > b_m$ has been constructed in such a manner that b_m is a'_j for some j . Then either $a'_j = a'_{j+1} = \dots = a'_{j+p}$ for some p and a'_{j+p} is the last term in the sequence, or $a'_j = a'_{j+1} = \dots = a'_{j+p} > a'_{j+p+1}$. This is so, since $a'_j = a'_{j+1} = \dots = a'_{j+p} = \dots$ implies $k_j > k_{j+1} > \dots > k_{j+p} > \dots$, but such a sequence (of natural numbers) must stop (cf. (I)). Therefore, as stated above, either the whole sequence stops, or $a'_{j+p} > a'_{j+p+1}$ for some p . If the former is the case, then stop. If the latter holds, then put $b_{m+1} = a'_{j+p+1}$.

From the definition, it is obvious that $b_0 > b_1 > \dots > b_m > \dots$. Suppose this sequence is finite, say $b_0 > b_1 > \dots > b_m$. Then according to the prescribed construction of b_{m+1} the original sequence is finite. Thus the sequence $b_0 > b_1 > \dots$ satisfies (C₁), and we have completed the definition of M_1 .

(III) Suppose we are given a decreasing sequence $a_0 > a_1 > \dots$, in which $a_0 < \omega^2$. Then by a 1-eliminator M_1 applied to this sequence, we can construct a 1-sequence $b_0 > b_1 > \dots$, where $b_0 \leq a_0$. Then $b_0 > b_1 > \dots$ can be written in the form $\omega \cdot k_0 > \omega \cdot k_1 > \dots$, which implies $k_0 > k_1 > \dots$. Then by (I), $k_0 > k_1 > \dots$ must be finite, which successively implies that $b_0 > b_1 > \dots$ and $a_0 > a_1 > \dots$ are finite.

(IV) We now define " n -sequences" as follows. Let $a_0 > a_1 > \dots$ be a descending sequence which is written in the form $a'_0 + c_0 > a'_1 + c_1 > \dots$,

where if $a_i = a'_i + c_i$, then each monomial in a'_i is $\geq \omega^n$ and each monomial in c_i is $< \omega^n$. (a'_i is called the n -major part of a_i .) Such a sequence is called an n -sequence if every c_i is empty.

Now assume (as an induction hypothesis) that any descending sequence $d_0 > d_1 > \dots$, with $d_0 < \omega^n$, is finite. We shall define a concrete method M_n (an n -eliminator) such that, given a decreasing sequence $a_0 > a_1 > \dots$, M_n concretely produces an n -sequence, say $b_0 > b_1 > \dots$, which satisfies:

(C_n) b_0 is the n -major part of a_0 , and if $b_0 > b_1 > \dots$ is finite then we can concretely show that $a_0 > a_1 > \dots$ is also finite.

The prescription for M_n is as follows. Write each a_i as $a'_i + c_i$, where a'_i is the n -major part of a_i . The definition now proceeds very much like that for 1-sequences in (II). Namely, put $b_0 = a'_0$. Suppose $b_0 > b_1 > \dots > b_m$ has been constructed and b_m is a'_j . If $a'_j = a'_{j+1} = \dots = a'_{j+p}$ and a'_{j+p} is the last term in the given sequence, then stop. Otherwise $a'_j = a'_{j+1} = \dots = a'_{j+p} > a'_{j+p+1}$ for some p , since $a'_j = a'_{j+1} = \dots = a'_{j+p}$ implies that $c_j > c_{j+1} > \dots > c_{j+p}$, which, by the induction hypothesis, is finite; hence for some p , $c_{j+p+1} \geq c_{j+p}$, which implies $a'_{j+p} > a'_{j+p+1}$. Then define $b_m = a'_{j+p+1}$. Then the sequence $b_0 > b_1 > \dots$ satisfies (C_n), and so we have successfully defined M_n .

(V) By means of the n -eliminator M_n , we shall prove that a decreasing sequence $a_0 > a_1 > \dots$, where $a_0 < \omega^{n+1}$, must be finite. By applying M_n to $a_0 > a_1 > \dots$, we can construct concretely an n -sequence, say $b_0 > b_1 > \dots$, where $b_0 \leq a_0$. Moreover, b_i can be written as $\omega^n \cdot k_i$, where k_i is a natural number. So, $\omega^n \cdot k_0 > \omega^n \cdot k_1 > \dots$, and this implies $k_0 > k_1 > \dots$, which is a finite sequence by (I), hence $b_0 > b_1 > \dots$ is finite, which in turn implies that $a_0 > a_1 > \dots$ is finite.

(VI) From (III) and (V) we conclude: given (concretely) any natural number n , we can concretely demonstrate that any decreasing sequence $a_0 > a_1 > \dots$ with $a_0 < \omega^n$ is finite.

(VII) Any decreasing sequence $a_0 > a_1 > \dots$ is finite if $a_0 < \omega^\omega$, for this means that $a_0 < \omega^n$ for some n , and hence (VI) applies.

(VIII) Now the general theory of α -sequences and (α, n) -eliminators will be developed, where α ranges over all ordinals $< \epsilon_0$ and n ranges over natural numbers > 0 . A descending sequence $d_0 > d_1 > \dots$ is called an α -sequence if in each d_i all the monomials are $\geq \omega^\alpha$. If $a = a' + c$ where each monomial in a' is $\geq \omega^\alpha$ and each monomial in c is $< \omega^\alpha$, then we say that a' is the α -major part of a . An α -eliminator has the property that given any concrete descending sequence, say $a_0 > a_1 > \dots$, it concretely produces an α -sequence $b_0 > b_1 > \dots$ such that

- (i) b_0 is the α -major part of a_0 ,
- (ii) if $b_0 > b_1 > \dots$ is a finite sequence then we can concretely demonstrate that $a_0 > a_1 > \dots$ is finite.

(Clearly $a_0 \geq b_0$.)

We delay the definition of α -eliminators. Assuming that an α -eliminator has been defined for every α , we can show that any decreasing sequence is finite. For consider $a_0 > a_1 > \dots$. There exists an α such that $a_0 < \omega^{\alpha+1}$. An α -eliminator concretely gives an α -sequence $b_0 > b_1 > \dots$ satisfying (i) and (ii) above. Since $b_0 \leq a_0$, each b_i can be written in the form $\omega^\alpha \cdot k_i$; thus $\omega^\alpha \cdot k_0 > \omega^\alpha \cdot k_1 > \dots$, which implies $k_0 > k_1 > \dots$. By (I) this means that $k_0 > k_1 > \dots$ is finite, hence so is $b_0 > b_1 > \dots$; so $a_0 > a_1 > \dots$ is finite. This proves our objective (*). Therefore, what must be done is to define (construct) α -eliminators for all $\alpha < \varepsilon_0$.

(IX) We rename an α -eliminator to be an $(\alpha, 1)$ -eliminator. Suppose that (α, n) -eliminators have been defined. A $(\beta, n+1)$ -eliminator is a *concrete* method for constructing an $(\alpha \cdot \omega^\beta, n)$ -eliminator from any given (α, n) -eliminator. We must go through the following procedure.

(X) Suppose $\{\mu_m\}_{m < \omega}$ is an increasing sequence of ordinals whose limit is μ (where there is a concrete method for obtaining μ_m for each m), and suppose g_m is a μ_m -eliminator. Then the g defined as follows is a μ -eliminator. Suppose $a_0 > a_1 > \dots$ is a concretely given sequence. If a_0 is written as $a'_0 + c_0$, where a'_0 is the μ -major part of a_0 , then there exists an m for which $c_0 < \omega^{\mu_m}$, so we may assume that each a_i is written as $a'_i + c_i$, where a'_i is the μ_m -major part of a_i . Then g_m can be applied to the sequence $a_0 > a_1 > \dots$ and hence it concretely produces a μ_m -sequence

$$b_{10} > b_{11} > b_{12} > \dots \quad (1)$$

satisfying (i) and (ii) above (with μ_m in place of α), with $b_{10} = a'_0$, so that in fact b_{10} is the μ -major part of a_0 . Write $b_0 = b_{10}$.

Now consider the sequence $b_{11} > b_{12} > \dots$. Suppose $b_{11} \geq \omega^\mu$. Then repeat the above procedure: i.e., for the sequence (1), write $b_{10} = b'_{10} + c_{10}$, where b'_{10} is the μ -major part of b_{10} . Then there exists an m_1 such that $c_{10} < \omega^{\mu_{m_1}}$. So apply g_{m_1} to the sequence $b_{11} > b_{12} > b_{13} > \dots$, to obtain a μ_{m_1} -sequence

$$b_{21} > b_{22} > b_{23} > \dots$$

satisfying (i) and (ii) (with μ_{m_1} in place of α), with b_{21} the μ -major part of b_{10} . Put $b_1 = b_{21}$. Suppose $b_{22} \geq \omega^\mu$. Then repeat this procedure with the sequence $b_{22} > b_{23} > \dots$ to obtain a sequence

$$b_{32} > b_{33} > b_{34} > \dots,$$

and put $b_2 = b_{32}$. Continuing in this way, we obtain a μ -sequence

$$b_0 > b_1 > b_2 > \dots$$

If this sequence is finite with last term (say) $b_l = b_{l+1,l}$, then it follows that

in the sequence

$$b_{l+1,l} > b_{l+1,l+1} > b_{l+1,l+2} > \dots \quad (2)$$

we must have $b_{l+1,l+1} < \omega^\mu$. So $b_{l+1,l+1} < \omega^{\mu_{m'}}$ for some m' . Apply $g_{m'}$ to the sequence (2); we then obtain a finite $\mu_{m'}$ -sequence with only the term 0; hence the sequence (2) is finite (by definition of $\mu_{m'}$ -eliminator); hence the sequence $b_{l,l-1} > b_{l,l} > \dots$ is finite; and so on (backwards), until we deduce that the original sequence $a_0 > a_2 > \dots$ is finite.

(XI) Suppose $\{\mu_m\}_{m < \omega}$ is a sequence of ordinals whose limit is μ and suppose for each m , a $(\mu_m, n+1)$ -eliminator is concretely given. Then we can define a $(\mu, n+1)$ -eliminator g as follows. The definition is by induction on n . For $n = 0$ (so $n+1 = 1$), (X) applies. Assume (XI) for n ; so there is an operation k_n such that for any sequence $\{\gamma_m\}_{m < \omega}$ with limit γ and (γ_m, n) -eliminator g'_m , k_n applied to g'_m concretely produces a (γ, n) -eliminator. Now for $n+1$, suppose a sequence $\{\beta_m\}_{m < \omega}$ with limit β and an (α, n) -eliminator p are given. Since g_m is a $(\beta_m, n+1)$ -eliminator, it produces concretely an $(\alpha \cdot \omega^{\beta_m}, n)$ -eliminator from p , which we denote by $g_m(p)$. So, by taking $\alpha \cdot \omega^{\beta_m}$ for γ_m , $g_m(p)$ for g'_m and $\alpha \cdot \omega^\beta$ for γ , we can apply the induction hypothesis; thus k_n applied to $\{g'_m\}$ defines an $(\alpha \cdot \omega^\beta, n)$ -eliminator q . This procedure for defining q from p is concrete, and so serves as a $(\beta, n+1)$ -eliminator.

(XII) Suppose g is a $(\mu, n+1)$ -eliminator. Then we will construct a $(\mu \cdot \omega, n+1)$ -eliminator. In virtue of (XI) it suffices to show that we can concretely construct (from g) a $(\mu \cdot m, n+1)$ -eliminator for every $m < \omega$. Suppose an (α, n) -eliminator, say f , is given. Note that

$$\alpha \cdot \omega^{\mu \cdot m} = \alpha \cdot \underbrace{\omega^\mu \cdot \omega^\mu \cdot \dots \cdot \omega^\mu}_m.$$

Since g is a $(\mu, n+1)$ -eliminator, g concretely constructs an $(\alpha \cdot \omega^\mu, n)$ -eliminator from f , which we denote by $g(f)$. Now apply g to this, to obtain an $(\alpha \cdot \omega^\mu \cdot \omega^\mu, n)$ -eliminator $g(g(f))$. Repeating this procedure m times, we obtain the $(\alpha \cdot \omega^{\mu \cdot m}, n)$ -eliminator $g(\dots g(f) \dots)$.

(XIII) We can now construct a $(1, m+1)$ -eliminator for every $m \geq 0$. The construction is by induction on m . We may take M_1 as a $(1, 1)$ -eliminator. For $m = 1$, the construction of a $(1, 2)$ -eliminator is reduced to the construction of an $(\alpha + \alpha)$ -eliminator from an α -eliminator. Given $a_0 > a_1 > \dots$, apply an α -eliminator to obtain $b_0 > b_1 > \dots$, where $\{b_i\}$ is an α -sequence, b_0 is the α -major part of a_0 , and if $\{b_i\}$ is finite, then so is $\{a_i\}$. Each b_i can be written in the form $\omega^\alpha \cdot c_i$, where $\{c_i\}$ is decreasing and, if $\{c_i\}$ is finite, then so is $\{b_i\}$. $a_0 = b_0 + e_0$ where $e_0 < \omega^\alpha$. Apply and α -eliminator to $\{c_i\}$ to obtain $d_0 > d_1 > \dots$, where $\{d_i\}$ is an α -sequence, d_0 is the α -major part of c_0 and, if $\{d_i\}$ is finite, then so is $\{c_i\}$. $\{\omega^\alpha \cdot d_i\}$ is an

$(\alpha + \alpha)$ -sequence and decreasing. If $\{\omega^\alpha d_i\}$ is finite, then so are $\{d_i\}$, $\{c_i\}$, $\{b_i\}$, $\{a_i\}$ successively, and

$$\begin{aligned}\omega^\alpha \cdot d_0 &= \omega^\alpha \cdot (\text{the } \alpha\text{-major part of } c_0) \\ &= (\alpha + \alpha)\text{-major part of } b_0 \\ &= (\alpha + \alpha)\text{-major part of } a_0.\end{aligned}$$

So $\{\omega^\alpha d_i\}$ is the $(\alpha + \alpha)$ -sequence which was desired for $\{a_i\}$.

For $m > 1$, suppose f is an (α, m) -eliminator. Then, by (XII) (with $n + 1 = m$), we can construct an $(\alpha \cdot \omega, m)$ -eliminator concretely from f . Hence we have a $(1, m + 1)$ -eliminator.

(XIV) Conclusion: An (α, n) -eliminator can be constructed for every α of the form ω_m , i.e.,

$$\left. \begin{array}{c} \omega \\ \cdot \\ \cdot \\ \cdot \\ \omega \end{array} \right\} m.$$

The construction is by induction on m . If $m = 0$, then we define α to be $1 = \omega^0$. Then an (α, n) -eliminator has been defined in (XIII) for every n . Suppose f is a $(1, n)$ -eliminator, and g is an $(\alpha, n + 1)$ -eliminator, which we assume to have been defined. Then g operates on f and produces the required $(1 \cdot \omega^\alpha, n) = (\omega^\alpha, n)$ -eliminator. This completes the proof.

NOTE. We can also develop the theory of eliminators if we define a $(\beta, n + 1)$ -eliminator to be a concrete method for constructing an $(\alpha + \omega^\beta, n)$ -eliminator from any given (α, n) -eliminator. (Compare this with (IX).)

Our standpoint, which has been discussed above, is like Hilbert's in the sense that both standpoints involve "Gedankenexperimente" only on clearly defined operations applied to some concretely given figures and on some clearly defined inferences concerning these operations. An α -eliminator is a concrete operation which operates on concretely given figures. A $(\beta, 2)$ -eliminator is a concrete method which enables one to exercise a Gedanken-experiment in constructing an $\alpha \cdot \omega^\beta$ -eliminator from any concretely given α -eliminator. So if an ordinal, say ω_k is given, then we have a method for concretely constructing an ω_k -eliminator.

We believe that the most illuminating way to view the consistency proof of **PA**, to be described in §12, is in terms of the notion of eliminators, as described above. (In fact, it is not difficult to generalize this notion, so as to include, say, the concept of (α, ω) -eliminator, and so on; however, this is unnecessary for the consistency proof for **PA**.)

The ideas we have presented are normally formulated in terms of the

notion of accessibility. It may be helpful to reformulate our ideas in terms of this notion, which (we believe) is a rough but convenient way of expressing the idea of eliminators.

We say that an ordinal μ is accessible if it has been demonstrated that every strictly decreasing sequence starting with μ is finite. More precisely, we consider the notion of accessibility only when we have actually seen, or demonstrated constructively, that a given ordinal is accessible. Therefore we never consider a general notion of accessibility, and hence we do not define the negation of accessibility as such. If we mention "the negation of accessibility", it means that we are concretely given an infinite, strictly decreasing sequence.

First, we assume we have arithmetized the construction of the ordinals (less than ε_0) given by clauses O 1–O 3. In other words, we assume a Gödel numbering of these (expressions for) ordinals, with certain nice properties: namely, the induced number-theoretic relations and functions corresponding to the ordinal relations and functions $=$, $<$, $+$, \cdot , and exponentiation by ω (which we will often continue to denote by the same symbols) are primitive recursive; also we can primitive recursively represent any (Gödel number of an) ordinal in its normal form, and hence decide primitive recursively whether it represents a limit or successor ordinal, etc. The ordering of the natural numbers corresponding to $<$ (on the ordinals) will be called a "standard well-ordering of type ε_0 ", or just "standard ordering of ε_0 ".

Our method for proving the accessibility of ordinals will be as follows. (We work with our standard well-ordering of type ε_0 .)

(1) When it is known that $\mu_1 < \mu_2 < \mu_3 \dots \rightarrow \nu$ (i.e., ν is the limit of the increasing sequence $\{\mu_i\}$) and that every μ_i is accessible, then ν is also accessible.

(2) A method is given by which, from the accessibility of a subsystem, one can deduce the accessibility of a larger system.

(3) By repeating (1) and (2), we show that every initial segment of our ordering is accessible, and hence so is the whole ordering.

The fact that every decreasing sequence which starts with a natural number is finite can be proved as in (I) above.

Let us proceed to the next stage: decreasing sequences of ordinals less than $\omega + \omega$. Here we can again see that every decreasing sequence terminates. This is done as follows. Consider the first term μ_0 of such a sequence. We can effectively decide whether it is of the form n or of the form $\omega + n$, where n is a natural number. If it is of the form n , then it suffices to repeat the above argument for natural numbers. If it is of the form $\omega + n$, consider the first $n + 2$ terms of the sequence

$$\mu_{n+1} < \dots < \mu_2 < \mu_1 < \mu_0.$$

It is easily seen that μ_{n+1} cannot be of the form $\omega + m$ for any natural

number m and hence must be a natural number, so we now repeat the proof for natural numbers. This method can be extended to the cases of decreasing sequences of ordinals less than $\omega \cdot n$, less than ω^2 , less than ω^ω , etc.

A more mathematical presentation of this idea now follows.

LEMMA 11.1. *If μ and ν are accessible, then so is $\mu + \nu$.*

PROOF. We just generalize the proof that $\omega + \omega$ is accessible and make use of the following fact which is easily seen: given ordinals μ, ξ, ν such that $\mu \leq \xi < \nu$, we can effectively find a ν_0 such that $\nu_0 < \nu$ and $\xi = \mu + \nu_0$.

LEMMA 11.2. *If μ is accessible, then so is $\mu \cdot \omega$.*

PROOF. We use the following fact, which is easy to show: if $\nu < \mu \cdot \omega$, then we can find an n such that $\nu < \mu \cdot n$.

With these lemmas, let us prove that all ordinals less than ε_0 are accessible. First we introduce the technical term: " n -accessible", for every n , by induction on n .

DEFINITION 11.3. μ is said to be 1-accessible if μ is accessible. μ is said to be $(n+1)$ -accessible if for every ν which is n -accessible, $\nu \cdot \omega^\mu$ is n -accessible.

It should be emphasized that " ν being n -accessible" is a clear notion only when it has been concretely demonstrated that ν is n -accessible.

LEMMA 11.4. *If μ is n -accessible and $\nu < \mu$, then ν is n -accessible.*

LEMMA 11.5. *Suppose $\{\mu_m\}$ is an increasing sequence of ordinals with limit μ . If each μ_m is n -accessible, then so is μ .*

LEMMA 11.6. *If ν is $(n+1)$ -accessible, then so is $\nu \cdot \omega$.*

PROOF. We must show that for any n -accessible μ , $\mu \cdot \omega^{\nu \cdot \omega}$ is n -accessible. For this purpose it suffices so show that $\mu \cdot \omega^{\nu \cdot m}$ is n -accessible for each m (cf. Lemma 11.5). This is, however, obvious, since

$$\mu \cdot \omega^{\nu \cdot m} = \mu \cdot (\omega^\nu)^m = \mu \cdot \omega^\nu \dots \omega^\nu$$

and ν is $(n+1)$ -accessible.

PROPOSITION 11.7. *1 is $(n+1)$ -accessible.*

PROOF. Suppose μ is n -accessible. Then by Lemma 11.6, $\mu \cdot \omega = \mu \cdot \omega^1$ is n -accessible, which means by definition that 1 is $(n+1)$ -accessible.

DEFINITION 11.8. $\omega_0 = 1$; $\omega_{n+1} = \omega^{\omega_n}$.

PROPOSITION 11.9. ω_k is $(n-k)$ -accessible for an arbitrary $n > k$.

PROOF. By induction on k . If $k = 0$, then $\omega_k = 1$ and hence is n -accessible for all n (cf. Proposition 11.7). Suppose ω_k is $(n-k)$ -accessible. Since 1 is $[n-(k+1)]$ -accessible, $1 \cdot \omega^{\omega_k}$ is $[n-(k+1)]$ -accessible by Definition 11.3, i.e., ω_{k+1} is $[n-(k+1)]$ -accessible.

As a special case of Proposition 11.9 we have:

PROPOSITION 11.10. ω_k is accessible for every k .

Given any decreasing sequence of ordinals (less than ε_0), there is an ω_k such that all ordinals in the sequence are less than ω_k . Therefore the sequence must be finite by Proposition 11.10. Thus we can conclude:

PROPOSITION 11.11. ε_0 is accessible.

An important point to note is this. Our proof of the accessibility of ε_0 (by the method of eliminators, (I)–(XIV), or by the method of Proposition 11.11) depends essentially on the fact that we are using a standard well-ordering of type ε_0 , for which the successive steps in the argument are evident. Of course this is not so for an arbitrary well-ordering of type ε_0 , nor for the general notion of well-ordering or ordinal.

Comparison of our standpoint with some other standpoints may help one to understand our standpoint better. First, consider set theory. Our standpoint does not assume the absolute world as set theory does, which we can think of as being based on the notion of an "infinite mind". It is obvious that, on the contrary, it tries to avoid the absolute world of an "infinite mind" as much as possible. It is true that in the study of number theory, which does not involve the notion of sets, the absolute world of numbers $0, 1, 2, \dots$ is not such a complicated notion; to an infinite mind it would be quite clear and transparent. Nevertheless, our minds being finite, it is, after all, an imaginary world to us, no matter how clear and transparent it may appear. Therefore we need reassurance of such a world in one way or another.

Next, consider intuitionism. Although our standpoint and that of intuitionism have much in common, the difference may be expressed as follows.

Our standpoint avoids abstract notions as much as possible, except those which are eventually reduced to concrete operations or Gedankenex-

perimente on concretely given sequences. Of course we also have to deal with operations on operations, etc. However, such operations, too, can be thought of as Gedankenexperimente on (concrete) operations.

By contrast, intuitionism emphatically deals with abstract notions. This is seen by the fact that its basic notion of "construction" (or "proof") is absolutely abstract, and this abstract nature also seems necessary for its impredicative concept of "implication". It is not the aim of intuitionism to reduce these abstract notions to concrete notions as we do.

We believe that our standpoint is a natural extension of Hilbert's finitist standpoint, similar to that introduced by Gentzen, and so we call it the Hilbert-Gentzen finitist standpoint.

Now a Gentzen-style consistency proof is carried out as follows:

- (1) Construct a suitable standard ordering, in the strictly finitist standpoint.
- (2) Convince oneself, in the Hilbert-Gentzen standpoint, that it is indeed a well-ordering.
- (3) Otherwise use only strictly finitist means in the consistency proof.

We now present a consistency proof of this kind for **PA**.

§12. A consistency proof of **PA**

We assume from now on that **PA** is formalized in a language which includes a constant f for every primitive recursive function f . We call this language **L**.

As initial sequents of **PA** we will also take from now on the defining equations for all primitive recursive functions, as well as all sequents $\rightarrow s = t$, where s, t are closed terms of **L** denoting the same number, and all sequents $s = t \rightarrow$, where s, t are closed terms of **L** denoting different numbers.

We shall follow Gentzen's second version of his consistency proof for first order arithmetic. This involves a "reduction method". Since this method will recur often, we shall abstract the concept here. (We assume that the ordinals less than ε_0 are represented as notations in a fixed standard well-ordering, as described in §11.)

First, suppose that ordinals less than ε_0 are effectively assigned to proofs. Now let **R** be a property of proofs such that:

- (*) For any proof P satisfying **R**, we can find (effectively from P) a proof P' satisfying **R** such that P' has a smaller ordinal than P .

We can then infer from (*), and the accessibility of ε_0 :

- (**) No proof satisfies **R**.

The procedure of finding (or constructing) P' from P in (*) is called: a *reduction of P to P'* (for the property R).

The property R of proofs that we will be interested in, is the property of having \rightarrow as an end-sequent.

By giving a uniform reduction procedure for this property (Lemma 12.8), we will have shown (by (**)) that no proof of **PA** ends with \rightarrow ; in other words:

THEOREM 12.1. *The system **PA** is consistent.*

Of course the importance of this theorem exists in its proof, which, apart from the assumption of the accessibility of ε_0 , is strictly finitist. (Nobody suspects the consistency of Peano arithmetic!)

Theorem 12.1 follows from Lemma 12.8 (as just stated). First, we need:

DEFINITION 12.2. A proof in **PA** is *simple* if no free variables occur in it, and it contains only mathematical initial sequents, weak inferences and inessential cuts.

(Recall that a weak inference is a structural inference other than a cut. Cf. §9 for other definitions.)

LEMMA 12.3. *There is no simple proof of \rightarrow .*

PROOF. Let P be any simple proof. All the formulas in P are of the form $s = t$ with s and t closed. Note that with the natural interpretation of the constants, it can be determined (finitistically) whether $s = t$ is true or false (since this only involves the evaluation of certain primitive recursive functions). A sequent in P is then given the value **T** if at least one formula in the antecedent is false, or at least one formula in the succedent is true, and it is given the value **F** otherwise. It is easy to see that all mathematical initial sequents take the value **T**, and weak inferences and inessential cuts preserve the value **T** downward for sequents. So all sequents of P have the value **T**. But \rightarrow has the value **F**.

DEFINITION 12.4. (1) The *grade of a formula*, is (as defined in §5) the number of logical symbols it contains. The *grade of a cut* is the grade of the cut formula; the *grade of an ind inference* is the grade of the induction formula.

(2) The *height of a sequent S* in a proof P (denoted by $h(S; P)$ or, for short, $h(S)$) is the maximum of the grades of the cuts and ind's which occur in P below S .

PROPOSITION 12.5. (1) *The height of the end-sequent of a proof is 0.*

(2) If S_1 is above S_2 in a proof, then $h(S_1) \geq h(S_2)$; if S_1 and S_2 are the upper sequents of an inference, then $h(S_1) = h(S_2)$.

Before defining the assignment of ordinals to proofs, we introduce the following notation. For any ordinal α and natural number n , $\omega_n(\alpha)$ is defined by induction on n ; $\omega_0(\alpha) = \alpha$, $\omega_{n+1}(\alpha) = \omega^{\omega_n(\alpha)}$. So

$$\omega_n(\alpha) = \underbrace{\omega^{\cdot^{\cdot^{\cdot^{\omega^\alpha}}}}}_n$$

DEFINITION 12.6. Assignment of ordinals (less than ε_0) to the proofs of **PA**. First we assign ordinals to the sequents in a proof. The ordinal assigned to a sequent S in a proof P is denoted by $o(S; P)$ or $o(S)$. Now suppose a proof P is given. We shall define $o(S) = o(S; P)$, for all sequents S in P .

We shall henceforth assume that the ordinals are expressed in normal form (cf. §11). If μ and ν are ordinals of the form $\omega^{\mu_1} + \omega^{\mu_2} + \dots + \omega^{\mu_m}$ and $\omega^{\nu_1} + \omega^{\nu_2} + \dots + \omega^{\nu_n}$ respectively (so that $\mu_1 \geq \mu_2 \geq \dots \geq \mu_m$ and $\nu_1 \geq \nu_2 \geq \dots \geq \nu_n$), then $\mu \# \nu$ denotes the ordinal $\omega^{\lambda_1} + \omega^{\lambda_2} + \dots + \omega^{\lambda_{m+n}}$, where $\{\lambda_1, \lambda_2, \dots, \lambda_{m+n}\} = \{\mu_1, \mu_2, \dots, \mu_m, \nu_1, \nu_2, \dots, \nu_n\}$ and $\lambda_1 \geq \dots \geq \lambda_{m+n}$. $\mu \# \nu$ is called the natural sum of μ and ν .

- (1) An initial sequent (in P) is assigned the ordinal 1.
- (2) If S is the lower sequent of a weak inference, then $o(S)$ is the same as the ordinal of its upper sequent.
- (3) If S is the lower sequent of \wedge : left, \vee : right, \supset : right, \neg : right, \neg : left or an inference involving a quantifier, and the upper sequent has the ordinal μ , then $o(S) = \mu + 1$.
- (4) If S is the lower sequent of \wedge : right, \vee : left, or \supset : left and the upper sequents have ordinals μ and ν , then $o(S) = \mu \# \nu$.
- (5) If S is the lower sequent of a cut and its upper sequents have the ordinals μ and ν , then $o(S)$ is $\omega_{k-l}(\mu \# \nu)$, i.e.,

$$\left. \begin{array}{c} \omega^{\mu \# \nu} \\ \cdot \\ \cdot \\ \omega \end{array} \right\} k-l,$$

where k and l are the heights of the upper sequents and of S , respectively.

- (6) If S is the lower sequent of an ind and its upper sequent has the

ordinal μ , then $o(S)$ is $\omega_{k-l+1}(\mu_1 + 1)$, i.e.,

$$\omega^{\omega^{\mu_1+1}} \left\} (k-l)+1,$$

where μ has the normal form $\omega^{\mu_1} + \omega^{\mu_2} + \dots + \omega^{\mu_n}$ (so that $\mu_1 \geq \mu_2 \geq \dots \geq \mu_n$), and k and l are the heights of the upper sequent and of S , respectively.

(7) The ordinal of a proof P , $o(P)$, is the ordinal of its end-sequent.

We use the notation

$$P: \begin{array}{c} \downarrow \downarrow \downarrow \\ \Gamma \xrightarrow{\mu} \Delta \end{array}$$

to denote a proof P of $\Gamma \rightarrow \Delta$ such that $o(\Gamma \rightarrow \Delta; P) = o(P) = \mu$.

LEMMA 12.7. Suppose P is a proof containing a sequent S_1 , there is no ind below S_1 , P_1 is the subproof of P ending with S_1 , P'_1 is any other proof of S_1 , and P' is the proof formed from P by replacing P_1 by P'_1 :

$$P: \begin{array}{c} P_1 \left\{ \begin{array}{c} \downarrow \downarrow \downarrow \\ S_1 \end{array} \right. \end{array} \quad P': \begin{array}{c} P'_1 \left\{ \begin{array}{c} \downarrow \downarrow \downarrow \\ S_1 \end{array} \right. \end{array}$$

Suppose also that $o(S_1; P') < o(S_1; P)$. Then $o(P') < o(P)$.

PROOF. Consider a thread of P passing through S_1 . We show that for any sequent S of this thread at or below S_1 : if S' is the sequent "corresponding to" S in P' , then

$$(*) \quad o(S'; P') < o(S; P).$$

This is true for $S = S_1$ by assumption, and this property $(*)$ is preserved downwards by all the inference rules, as can be checked. (We use the fact that the natural sum is strictly monotonic in each argument, i.e., $\alpha < \beta \Rightarrow \alpha \# \gamma < \beta \# \gamma$, etc.) Finally, letting S be the end-sequent of P , we obtain the desired conclusion.

This lemma is used repeatedly in the consistency proof.

Now let R be the property of proofs of ending with the sequent \rightarrow ; i.e., for any proof P , $R(P)$ holds if and only if P is a proof of \rightarrow .

Notice first that if P is a proof of \rightarrow , then every logical inference of P is

implicit! (cf. Definition 9.7) (since otherwise a bundle containing the principal formula of this inference would end with an end formula).

Hence the definition of end-piece for such proofs can be simply stated as follows.

The end-piece of a proof of \rightarrow consists of all those sequents that are encountered as we ascend each thread from the end-sequent and stop as soon as we arrive at a logical inference. (Then the upper sequent of this inference no longer belongs to the end-piece, but the lower sequent, and all sequents below it, do.) This inference belongs to the boundary.

LEMMA 12.8. *If P is a proof of \rightarrow , then there is another proof P' of \rightarrow such that $o(P') < o(P)$.*

PROOF. Let P be a proof of \rightarrow . We can assume, by Proposition 9.8, that P is regular. We describe a "reduction" of P to obtain the desired P' . The reduction consists of a number of steps, described below. Each step is performed, perhaps finitely often (as will be clear), and at each step, we assume that the previous steps have been performed (as often as possible).

At each step, the ordinal of the resulting proof does not increase, and at least at one step, the ordinal decreases.

Step 1. Suppose the end-piece of P contains a free variable, say a , which is not used as an eigenvariable. Then replace a by the constant 0. This results in a proof of \rightarrow (using the analogue of Lemma 2.10 for **PA**), with the same ordinal.

Step 1 is performed repeatedly until there is no free variable in the end-piece which is not used as an eigenvariable.

Step 2. Suppose the end-piece of P contains an ind. Then take a lowermost one, say I . Suppose I is of the following form:

$$\begin{array}{c} P_0(a) \\ I \quad \left\{ \begin{array}{c} \vdots \\ F(a), \Gamma \xrightarrow{\mu} \Delta, F(a') \\ \hline F(0), \Gamma \rightarrow \Delta, F(s) \end{array} \right. \\ \vdots \\ \rightarrow \end{array}$$

where P_0 is the subproof ending with $F(a), \Gamma \rightarrow \Delta, F(a')$, and let l and k be the heights of the upper sequent (call it S) and the lower sequent (call it S_0) of I , respectively. Then

$$o(S_0) = \omega_{l-k+1}(\mu_1 + 1),$$

where $\mu = o(S) = \omega^{\mu_1} + \omega^{\mu_2} + \dots + \omega^{\mu_n}$ and $\mu_n \leq \dots \leq \mu_2 \leq \mu_1$. Since no

free variable occurs below I , s is a closed term and hence there is a number m such that $\rightarrow s = \bar{m}$ is **PA**-provable without an essential cut or ind (cf. Lemma 9.6); hence there is a proof Q of $F(\bar{m}) \rightarrow F(s)$ without an essential cut or ind (cf. Lemma 9.6). Let $P_0(\bar{n})$ be the proof which is obtained from P_0 by replacing a by \bar{n} throughout. Consider the following proof P' .

$$\begin{array}{c}
 \begin{array}{c}
 P_0(\bar{0}) \quad P_0(\bar{1}) \quad P_0(\bar{2}) \\
 \downarrow \quad \downarrow \quad \downarrow \\
 S_1 \quad F(0), \Gamma \rightarrow \Delta, F(0') \quad F(0'), \Gamma \rightarrow \Delta, F(0'') \quad F(0''), \Gamma \rightarrow \Delta, F(0''') \\
 S_2 \quad \frac{F(0), \Gamma \rightarrow \Delta, F(0')}{F(0), \Gamma \rightarrow \Delta, F(0'')} \quad F(0''), \Gamma \rightarrow \Delta, F(0''') \\
 S_3 \quad \frac{F(0), \Gamma \rightarrow \Delta, F(0'')}{F(0), \Delta \rightarrow \Delta, F(0''')}
 \end{array} \\
 \\
 \begin{array}{c}
 Q \\
 \downarrow \\
 S_m \quad \frac{F(0), \Gamma \rightarrow \Delta, F(\bar{m}) \quad F(\bar{m}) \rightarrow F(s)}{F(0), \Gamma \rightarrow \Delta, F(s)} \\
 S_0 \quad \frac{F(0), \Gamma \rightarrow \Delta, F(s)}{\rightarrow}
 \end{array}
 \end{array}$$

where S_1, S_2, \dots, S_0 denote the sequents shown on their right, S_1, \dots, S_m all have height l , since the formulas $F(\bar{n})$, $n = 0, \dots, m$, all have the same grade. Therefore,

$$o(F(\bar{n}), \Gamma \rightarrow \Delta, F(\bar{n}'); P') = \mu \quad \text{for } n = 0, 1, \dots, m.$$

Since Q has no essential cut or ind, $o(F(\bar{m}) \rightarrow F(s); P') = q$ (say) $< \omega$, $o(S_2) = \mu \# \mu$; $o(S_3) = \mu \# \mu \# \mu$; \dots , and in general, writing $\mu * n = \mu \# \mu \# \dots \# \mu$ (n times), $o(S_n) = \mu * n$ for $n = 1, 2, \dots, m$. Thus

$$o(S_0) = \omega_{l-k}(\mu * m + q)$$

and $\mu * m + q < \omega^{\mu_1+1}$, since $q < \omega$. Therefore

$$o(S_0; P') = \omega_{l-k}(\mu * m + q) < \omega_{l-k+1}(\mu_1 + 1) = o(S_0; P).$$

Thus $o(S_0; P') < o(S_0; P)$, and hence by Lemma 12.7, $o(P') < o(P)$.

Thus, if P has an ind in the end-piece, we are done: we have reduced P to a proof P' of \rightarrow with $o(P') < o(P)$. Otherwise, we assume from now on that P has no ind in its end-piece, and go to Step 3.

Step 3. Suppose the end-piece of P contains a logical initial sequent $D \rightarrow D$. Since the end-sequent is empty, both D 's (or more strictly, descendants of both D 's) must disappear by cuts. Suppose that (a descendant of) the D in the antecedent is a cut formula first (viz. in the

following figure a descendant of the D in the succedent of $D \rightarrow D$ occurs in Ξ).

$$\begin{array}{c}
 \begin{array}{ccc}
 & & D \rightarrow D \\
 & \swarrow \downarrow \searrow & \swarrow \downarrow \searrow \\
 \Gamma \rightarrow \Delta, D & & D, \Pi \rightarrow \Xi \\
 \hline
 S \quad \Gamma, \Pi \rightarrow \Delta, \Xi
 \end{array} \\
 \swarrow \downarrow \searrow \\
 \rightarrow
 \end{array}$$

P is reduced to the following P' :

$$\begin{array}{c}
 \begin{array}{c}
 \swarrow \downarrow \searrow \\
 \Gamma \rightarrow \Delta, D \\
 \hline
 \text{weakenings and exchanges} \\
 \hline
 S' \quad \Gamma, \Pi \rightarrow \Delta, \Xi
 \end{array} \\
 \swarrow \downarrow \searrow \\
 \rightarrow
 \end{array}$$

Note that there is a cut whose cut formula is D below S since both D 's in $D \rightarrow D$ must disappear by cuts. Hence, the height of $\Gamma \rightarrow \Delta, D$ does not change when we transform P into P' : $o(S'; P') < o(S; P)$.

Hence, by Lemma 12.7, $o(P') < o(P)$.

The other case is proved likewise.

So, if the end-piece of P contained a logical initial sequent, we have found a P' as desired. Otherwise, we assume from now on that the end-piece of P contains no logical initial sequents, and go on to Step 4.

Step 4. Suppose there is a weakening in the end-piece. Let I be the lower most weakening inference in the end-piece. Since the end-sequent is empty, there must exist a cut, J , below I and the cut formula is the descendent of the principal formula of I .

$$\begin{array}{c}
 \begin{array}{c}
 \swarrow \downarrow \searrow \\
 \Pi' \rightarrow \Xi' \\
 \hline
 D, \Pi' \rightarrow \Xi' \quad I
 \end{array} \\
 \begin{array}{ccc}
 & & \\
 & \swarrow \downarrow \searrow & \swarrow \downarrow \searrow \\
 J \quad \Gamma \rightarrow \Delta, D & & D, \Pi \rightarrow \Xi(k) \\
 \hline
 \Gamma, \Pi \rightarrow \Delta, \Xi(l)
 \end{array} \\
 \swarrow \downarrow \searrow \\
 \rightarrow
 \end{array}$$

Case (1)

If no contraction is applied to D from the inference I through J , by deleting some exchanges from P if necessary, reduce P into the following proof P' :

$$\begin{array}{c}
 \vdots \\
 \Pi' \rightarrow \Xi' \\
 \vdots \\
 \hline \hline \Pi \rightarrow \Xi \quad (l) \\
 \hline \text{weakenings and exchanges} \\
 \hline \Gamma, \Pi \rightarrow \Delta, \Xi \quad (l) \\
 \vdots \\
 \rightarrow
 \end{array}$$

Let $h(\Gamma, \Pi \rightarrow \Delta, \Xi; P) = l$ and $h(D, \Pi \rightarrow \Xi; P) = k$. Then, $l \leq k$ and $h(\Pi \rightarrow \Xi; P') = h(\Gamma, \Pi \rightarrow \Delta, \Xi; P') = l$. Let S be a sequent in P above $D, \Pi \rightarrow \Xi$, and let S' be the corresponding sequent in P' . Then, by the induction on number of inferences up to $D, \Pi \rightarrow \Xi$, we can show

$$\omega_{k_1 - k_2}(o(S; P)) \geq o(S'; P'),$$

where $k_1 = h(S; P)$ and $k_2 = h(S'; P')$. Hence, if $o(\Gamma \rightarrow \Delta, D; P) = \mu_1$, $o(D, \Pi \rightarrow \Xi; P) = \mu_2$, $o(\Gamma, \Pi \rightarrow \Delta, \Xi) = \nu$, $o(\Pi \rightarrow \Xi; P) = \mu'_2$ and $o(\Gamma, \Pi \rightarrow \Delta, \Xi) = \nu'$, then

$$\omega_{k-1}(\mu_2) \geq \mu'_2$$

and further,

$$\nu = \omega_{k-1}(\mu_2 \# \mu_1) > \omega_{k-1}(\mu_2) \geq \mu'_2 = \nu'.$$

Thus, $o(P) > o(P')$.

Case (2)

If not the Case (1), let the uppermost contraction applied to D be I' . Reduce P into the following proof Q :

P:

$$\begin{array}{c}
 \vdots \\
 \Pi' \rightarrow \Xi' \\
 \hline D, \Pi' \rightarrow \Xi' \\
 \vdots \\
 \hline \hline D, D, \Pi'' \rightarrow \Xi'' \\
 \hline D, \Pi'' \rightarrow \Xi'' \\
 \vdots \\
 \hline D, \Pi \rightarrow \Xi
 \end{array}$$

Q:

$$\begin{array}{c}
 \vdots \\
 \Pi' \rightarrow \Xi' \\
 \vdots \\
 \hline \hline D, \Pi'' \rightarrow \Xi'' \\
 \vdots \\
 \hline D, \Pi \rightarrow \Xi.
 \end{array}$$

Apparently, $o(P) = o(P')$. Hence, we can assume that the end-piece of P contains no weakening.

Step 5. We can now assume that P is not its own end-piece, since otherwise it would be simple (Definition 12.2), as is easily seen, and hence by Lemma 12.3, could not end with \rightarrow .

Under these assumptions, we shall prove that the end-piece of P contains a suitable cut (cf. Definition 9.7). We actually prove a stronger result, which is used again later (for Problem 12.11):

SUBLEMMA 12.9. *Suppose that a proof in \mathbf{PA} , say P , satisfies the following.*

- (1) *P is not its own end-piece.*
- (2) *The end-piece of P does not contain any logical inference, ind or weakening.*
- (3) *If an initial sequent belongs to the end-piece of P , then it does not contain any logical symbol.*

Then there exists a suitable cut in the end-piece of P .

(Notice that we do not assume here that the end-sequent is \rightarrow .)

PROOF. This is proved by induction on the number of essential cuts in the end-piece of P . The end-piece of P contains an essential cut, since P is not its own end-piece. Take a lowermost such cut, say I . If I is a suitable cut, then the sublemma is proved. Otherwise, let P be of the form

$$I \quad \frac{P_1 \left\{ \begin{array}{c} \vdots \\ \vdots \\ \Gamma \rightarrow \Delta, D \end{array} \right. \quad P_2 \left\{ \begin{array}{c} \vdots \\ \vdots \\ D, \Pi \rightarrow \Lambda \end{array} \right.}{\Gamma, \Pi \rightarrow \Delta, \Lambda}.$$

Since I is not a suitable cut, one of two cut formulas of I is not a descendant of the principal formula of a boundary inference. Suppose that D in $\Gamma \rightarrow \Delta, D$ is not a descendant of the principal formula of a boundary inference. Now we prove:

- (i) P_1 contains a boundary inference of P .

Suppose otherwise. Then D in $\Gamma \rightarrow \Delta, D$ is a descendant of D in an initial sequent in the end-piece of P , by (2). This contradicts the assumption that I is an essential cut, by (3).

- (ii) If an inference J in P_1 is a boundary inference of P , then J is a boundary inference of P_1 .

This is easily seen by the fact that I is a lowermost essential cut of P and D is not a descendant of the principal formula of a boundary inference.

- (iii) P_1 is not its own end-piece and the end-piece of P_1 is the intersection of P_1 and the end-piece of P .

This follows immediately from (i), (ii) and (1).

Now from the induction hypothesis, the end-piece of P_1 has a suitable cut. This cut is a suitable cut in the end-piece of P .

Returning to our proof P of \rightarrow which satisfies the conclusion of steps 1–4, we have, as an immediate consequence of Sublemma 12.9, that the end-piece of P contains a suitable cut. We now define an *essential reduction* of P .

Take a lowermost suitable cut in the end-piece of P , say I .

Case 1. The cut formula of I is of the form $A \wedge B$. Suppose P is of the form

$$\begin{array}{c}
 I_1 \quad \frac{\Gamma' \rightarrow \Theta', A \quad \Gamma' \rightarrow \Theta', B}{\Gamma' \rightarrow \Theta', A \wedge B} \quad I_2 \quad \frac{A, \Pi' \rightarrow \Lambda'}{A \wedge B, \Pi' \rightarrow \Lambda'} \\
 \downarrow \quad \downarrow \\
 I \quad \frac{\Gamma \xrightarrow{\mu} \Theta, A \wedge B \quad A \wedge B, \Pi \xrightarrow{\nu} \Lambda}{\Gamma, \Pi \rightarrow \Theta, \Lambda} \quad (l) \\
 \downarrow \\
 \Delta \xrightarrow{\lambda} \Xi \quad (k) \\
 \downarrow \\
 \rightarrow
 \end{array}$$

where $\Delta \rightarrow \Xi$ denotes the uppermost sequent below I whose height is less than that of the upper sequents of I . Let l be the height of each upper sequent of I , and k that of $\Delta \rightarrow \Xi$. Then $k < l$. Notice that $\Delta \rightarrow \Xi$ may be the lower sequent of I , or the end-sequent. The existence of such a sequent follows from Proposition 12.5.

$\Delta \rightarrow \Xi$ must be the lower sequent of a cut J (since there is no ind below I). Let $\mu = o(\Gamma \rightarrow \Theta, A \wedge B)$, $\nu = o(A \wedge B, \Pi \rightarrow \Lambda)$, $\lambda = o(\Delta \rightarrow \Xi)$ as shown. Consider the following proofs:

$$\begin{array}{c}
 P_1: \quad \frac{\frac{\Gamma' \rightarrow \Theta', A}{\Gamma' \rightarrow A, \Theta'} \quad (\text{weakening : right})}{\Gamma' \rightarrow A, \Theta', A \wedge B} \\
 \downarrow \\
 J_1 \quad \frac{\Gamma \xrightarrow{\mu_1} A, \Theta, A \wedge B \quad A \wedge B, \Pi \xrightarrow{\nu_1} \Lambda \quad (l)}{\Gamma, \Pi \rightarrow A, \Theta, \Lambda} \\
 \downarrow \\
 \frac{\Delta \xrightarrow{\lambda_1} A, \Xi}{\Delta \rightarrow \Xi, A} \quad (m)
 \end{array}$$

$$\begin{array}{c}
 P_2: \\
 \frac{\frac{\frac{A, \Pi' \rightarrow \Lambda'}{\Pi', A \rightarrow \Lambda'} \text{ (weakening : left)}}{A \wedge B, \Pi', A \rightarrow \Lambda'}}{\frac{\frac{\Gamma \xrightarrow{\mu_2} \Theta, A \wedge B \quad A \wedge B, \Pi, A \xrightarrow{\nu_2} \Lambda}{\Gamma, \Pi, A \rightarrow \Theta, \Lambda} \text{ (l)}}{\Delta, A \xrightarrow{\lambda_2} \Xi} \text{ (m)}}
 \end{array}$$

(where l and m are the heights of the sequents shown, not in P_1 and P_2 , but in P' , defined below, which contains these as subproofs).

Define P' to be the proof:

$$\begin{array}{c}
 \frac{\frac{P_1}{\Delta \xrightarrow{\lambda_1} \Xi, A} \text{ (m)} \quad \frac{P_2}{A, \Delta \xrightarrow{\lambda_2} \Xi} \text{ (m)}}{\frac{\Delta, \Delta \xrightarrow{\lambda_0} \Xi, \Xi}{\Delta \rightarrow \Xi} \text{ (k)}} \text{ (cut for } A\text{)} \\
 \rightarrow
 \end{array}$$

So m is the height of the upper sequents of I' (the cut for A). Note that the height of the lower sequent of I' is k .

It is obvious that $m = k$ if $k > \text{grade of } A$ and $m = \text{grade of } A$ otherwise. In either case $k \leq m < l$.

$$h(\Gamma \rightarrow A, \Theta, A \wedge B; P') = h(A \wedge B, \Pi \rightarrow \Lambda; P') = l,$$

since all cut formulas below I in P occur in P' below J_1 , all cut formulas below J_1 in P' except A occur in P under I , and $\text{grade of } A < \text{grade of } A \wedge B \leq l$. Similarly,

$$h(\Gamma \rightarrow \Theta, A \wedge B; P') = h(A \wedge B, \Pi, A \rightarrow \Lambda; P') = l.$$

Let

$$\begin{aligned}\mu_1 &= o(\Gamma \rightarrow A, \Theta, A \wedge B; P'), & \nu_1 &= o(A \wedge B, \Pi \rightarrow \Lambda; P'), \\ \lambda_1 &= o(\Delta \rightarrow A, \Xi; P'), & \mu_2 &= o(\Gamma \rightarrow \Theta, A \wedge B; P'), \\ \nu_2 &= o(A \wedge B, \Pi, A \rightarrow \Lambda; P'), & \lambda_2 &= o(\Delta, A \rightarrow \Xi; P'), \\ \lambda_0 &= o(\Delta, \Delta \rightarrow \Xi, \Xi; P').\end{aligned}$$

Then $\mu_1 < \mu$, $\nu_1 = \nu$, $\mu_2 = \mu$ and $\nu_2 < \nu$.

Now let

$$J' \frac{S'_1 \ S'_2}{S'} \begin{matrix} (k_1) \\ (k_2) \end{matrix}$$

be an arbitrary inference between J_1 and $\Delta \rightarrow A, \Xi$ and let

$$J \frac{S_1 \ S_2}{S}$$

be the corresponding inference between I and $\Delta \rightarrow \Xi$. Let

$$\begin{aligned}\alpha'_1 &= o(S'_1; P'), & \alpha'_2 &= o(S'_2; P'), & \alpha' &= o(S'; P'), \\ \alpha_1 &= o(S_1; P), & \alpha_2 &= o(S_2; P), & \alpha &= o(S; P), \\ k_1 &= h(S'_1, P') = h(S'_2, P'), & k_2 &= h(S', P').\end{aligned}$$

Then $\alpha = \alpha_1 \# \alpha_2$ if S is not $\Delta \rightarrow A, \Xi$, and $\alpha = \omega_{l-k}(\alpha_1 \# \alpha_2)$ if S' is $\Delta \rightarrow A, \Xi$. On the other hand $\alpha' = \omega_{k_1-k_2}(\alpha'_1 \# \alpha'_2)$.

Starting with $\mu_1 < \mu$ and $\nu_1 = \nu$, it is easily seen by induction on the number of inferences between J_1 and S that

$$\alpha' < \omega_{l-k_2}(\alpha), \tag{1}$$

if S is not $\Delta \rightarrow A, \Xi$. Let $\lambda = \omega_{l-k}(\kappa)$. Then (1) implies that $\lambda_1 < \omega_{l-m}(\kappa)$. Similarly, $\lambda_2 < \omega_{l-m}(\kappa)$. Hence

$$\omega_{m-k}(\lambda_1 \# \lambda_2) < \omega_{l-k}(\kappa),$$

since $l - k = (l - m) + (m - k)$. Therefore $\lambda_0 < \lambda$. Finally, from $\lambda_0 < \lambda$ it follows that $o(P') < o(P)$.

Case 2. The cut formula of I is of the form $\forall x F(x)$. So P has the form:

$$\begin{array}{c}
 \begin{array}{cc}
 \begin{array}{c} \Downarrow \\ I_1 \quad \frac{\Gamma' \rightarrow \Theta', F(a)}{\Gamma' \rightarrow \Theta', \forall x F(x)} \end{array} & \begin{array}{c} \Downarrow \\ I_2 \quad \frac{F(s), \Pi' \rightarrow \Lambda'}{\forall x F(x), \Pi' \rightarrow \Lambda'} \end{array} \\
 \\
 \begin{array}{c} \Downarrow \\ I \quad \frac{\Gamma \rightarrow \Theta, \forall x F(x) \quad \forall x F(x), \Pi \rightarrow \Lambda}{\Gamma, \Pi \rightarrow \Theta, \Lambda} \end{array} \\
 \\
 \begin{array}{c} \Downarrow \\ \Delta \rightarrow \Xi \\ \Downarrow \\ \rightarrow \end{array}
 \end{array}$$

The definition of $\Delta \rightarrow \Xi$ is the same as in case 1. The proof P' is then defined in terms of the following two subproofs P_1 and P_2 :

$$\begin{array}{c}
 P_1: \quad \frac{\frac{\frac{\Gamma' \rightarrow \Theta', F(s)}{\Gamma' \rightarrow F(s), \Theta'}}{\Gamma' \rightarrow F(s), \Theta', \forall x F(x)}}{\Gamma \rightarrow F(s), \Theta, \forall x F(x) \quad \forall x F(x), \Pi \rightarrow \Lambda} \\
 \frac{\Gamma \rightarrow F(s), \Theta, \forall x F(x) \quad \forall x F(x), \Pi \rightarrow \Lambda}{\Gamma, \Pi \rightarrow F(s), \Theta, \Lambda} \\
 \frac{\Gamma, \Pi \rightarrow F(s), \Theta, \Lambda}{\Delta \rightarrow F(s), \Xi} \\
 \frac{\Delta \rightarrow F(s), \Xi}{\Delta \rightarrow \Xi, F(s)}
 \end{array}$$

$$\begin{array}{c}
 P_2: \quad \frac{\frac{\frac{F(s), \Pi' \rightarrow \Lambda'}{\Pi', F(s) \rightarrow \Lambda'}}{\forall x F(x), \Pi', F(s) \rightarrow \Lambda'}}{\Gamma \rightarrow \Theta, \forall x F(x) \quad \forall x F(x), \Pi, F(s) \rightarrow \Lambda} \\
 \frac{\Gamma \rightarrow \Theta, \forall x F(x) \quad \forall x F(x), \Pi, F(s) \rightarrow \Lambda}{\Gamma, \Pi, F(s) \rightarrow \Theta, \Lambda} \\
 \frac{\Gamma, \Pi, F(s) \rightarrow \Theta, \Lambda}{\Delta, F(s) \rightarrow \Xi} \\
 \frac{\Delta, F(s) \rightarrow \Xi}{F(s), \Delta \rightarrow \Xi}
 \end{array}$$

P' is defined to be

$$\frac{\frac{\frac{P_1}{\Delta \rightarrow \Xi, F(s)} \quad \frac{P_2}{F(s), \Delta \rightarrow \Xi}}{\Delta, \Delta \rightarrow \Xi, \Xi}}{\Delta \rightarrow \Xi}.$$

Note that $o(\Gamma' \rightarrow \Theta', F(s); P') = o(\Gamma' \rightarrow \Theta', F(a); P)$. The argument on ordinals goes through as in case 1.

For the other cases, the proof is similar.

This completes the proof of Lemma 12.8 and hence the consistency proof for **PA** (Theorem 12.1).

REMARK 12.10. We wish to point out the following. One often says that the consistency of **PA** is proved by transfinite induction on the ordinals of proofs, as if we were using a general principle of transfinite induction in order to prove the consistency of mathematical induction.

This is misleading, however. The point is that the consistency proof uses the notion of accessibility of ε_0 , as explained in §11, and otherwise strictly finitist method. To re-state the matter from a more formal viewpoint:

The principle of *transfinite induction* on some (definable) well-ordering $<$ of the natural numbers can be expressed (in first-order formal systems) by the schema

$$TI(<, F(x)): \quad \forall x [\forall y (y < x \supset F(y)) \supset F(x)] \rightarrow \forall x F(x)$$

for arbitrary formulas $F(x)$ of the system considered.

Now Gentzen's consistency proof of **PA** can be formalized in the system of primitive recursive arithmetic, together with the axiom $TI(<, F(x))$, where $<$ is the standard well-ordering of type ε_0 and $F(x)$ is a certain *quantifier-free* formula.

PROBLEM 12.11. We can extend the reduction procedure of Lemma 12.8 to the following situation.

A sequent S (of the language of **PA**) is said to satisfy the property P if:

- (1) All sequent-formulas of S are closed;
- (2) Each sequent-formula in the succedent of S is either quantifier-free or of the form $\exists y_1, \dots, \forall y_m R(y_1, \dots, y_m)$, where $R(y_1, \dots, y_m)$ is quantifier-free;
- (3) Each sequent formula in the antecedent of S is either quantifier-free or of the form $\forall y_1, \dots, \forall y_m R(y_1, \dots, y_m)$, where $R(y_1, \dots, y_m)$ is quantifier-free.

Show that if a sequent satisfying P is provable in **PA**, then it is provable without an essential cut or ind. [*Hint*: We may assume that there is no free variable which is not used as an eigenvariable in the end-piece of a proof of such a sequent.]

If the end-piece has an explicit logical inference, take the lowermost explicit logical inference I . Without loss of generality, we assume that the proof is of the following form:

$$I \quad \frac{\begin{array}{c} \vdots \\ \Gamma \rightarrow \Delta, \exists y_2 \dots \exists y_m R(t, y_2, \dots, y_m) \end{array}}{\Gamma \rightarrow \Delta, \exists y_1 \dots \exists y_m R(y_1, y_2, \dots, y_m)} \\ \frac{\vdots}{\Gamma_0 \rightarrow \Delta_0, \forall y_1 \dots \forall y_m R(y_1, \dots, y_m), \Delta_1}$$

where $\Gamma_0 \rightarrow \Delta_0, \exists y_1 \dots \exists y_m R(y_1, \dots, y_m), \Delta_1$ is the end-sequent of the proof. We can eliminate I by replacing the proof by a proof whose end-sequent is either of the form

$$\Gamma_0 \rightarrow \Delta_0, \exists y_2 \dots \exists y_m R(t, y_2, \dots, y_m), \Delta_1$$

or of the form

$$\Gamma_0 \rightarrow \Delta_0, \exists y_1 \dots \exists y_m R(y_1, \dots, y_m), \Delta_1, \exists y_2 \dots \exists y_m R(t, y_2, \dots, y_m).$$

PROBLEM 12.12. Intuitionistic arithmetic can be formalized as the subsystem of **PA** defined by the condition that in the succedent of every sequent there can be at most one sequent-formula which contains quantifiers. This system may be called **HA** (for Heyting arithmetic). The reduction method for **PA** works for **HA** with a slight modification: roughly, in an essential reduction, if the cut formula of the suitable cut under consideration contains a quantifier then the weakening : right will not be introduced.

Define the reduction for **HA** precisely, thus proving the consistency of **HA** directly (not as a subsystem of **PA**).

PROBLEM 12.13. Let (*) be the property of formulas defined in Theorem 6.14, i.e., a formula satisfies (*) if every \vee and \exists in it is either in the scope of a \neg or in the left scope of a \supset . Show that, if each formula in Γ satisfies (*) and all formulas in Γ , A , B and $\exists x F(x)$ are closed, then in **HA** (cf. Problem 12.12):

- (1) $\Gamma \rightarrow A \vee B$ if and only if $\Gamma \rightarrow A$ or $\Gamma \rightarrow B$,
- (2) $\Gamma \rightarrow \exists x F(x)$ if and only if for some closed term s , $\Gamma \rightarrow F(s)$.

[*Hint* (B. Scarpellini): By transfinite induction on the ordinal of a proof P of $\Gamma \rightarrow A \vee B$ (for 1) or $\Gamma \rightarrow \exists x F(x)$ (for 2), respectively, following the

reduction method for the consistency of **PA**. First deal with explicit logical inferences in the end-piece of P .]

REMARK 12.14. As an application of Gentzen's reduction method, one can easily prove the following.

The consistency of arithmetic in which the induction formulas are restricted to those which have at most k quantifiers can be proved by transfinite induction on ω_{k+1} .

The outline of the proof is as follows. Suppose there is a proof of \rightarrow in this system. We shall carry out a reduction of such a proof.

(1) We assume that the induction formulas are in prenex normal form.

(2) A formula A in a proof (in this system) will be temporarily called free if either it has no ancestor which is an induction formula, or it has an induction formula as an ancestor but a logical symbol is introduced in an ancestor of A between any such induction formula and A itself. A cut is called free if both cut formulas are free. Notice that if a formula is not free, then it is in prenex form with at most k quantifiers. Now we can prove the following partial cut-elimination theorem:

If a sequent is provable in our system, then it is provable without free cuts.

(We simply adapt the cut-elimination proof for **LK**.)

Thus we obtain a proof of \rightarrow in which there are no free cuts, and so all the cut formulas, as well as induction formulas, are in prenex form with at most k quantifiers. We assume $k \geq 1$.

(3) Further we can assume, for convenience, that the inference rules are modified in such a way that all formulas in the proof are in prenex form, with at most k quantifiers.

This system is called **PA_k**.

We must now modify some notions slightly. The grade of a formula A is now defined to be: the number of quantifiers in A , minus 1; the grade of a cut or induction inference is the grade of the cut formula or the induction formula, respectively. The height of a sequent in a proof is defined as before, using the new definition of grade. The ordinals are assigned as before, except that the initial sequents are assigned the ordinal 0 and the propositional inferences as well as quantifier-free cuts are treated in the same manner as the weak inferences, i.e., the ordinals do not change. (In case there are two upper sequents, take the maximum of the two ordinals.) It can easily be seen that the ordinal of a proof (of the kind we are considering) is less than $\omega_k(l)$ for some natural number l .

A boundary inference is defined to be an inference which introduces a quantifier and is a boundary inference in the previous sense. A suitable cut is a cut whose cut formula contains quantifiers and which is suitable in the previous sense. In eliminating initial sequents from the end-piece, one eliminates only those which have quantifiers. The existence of a suitable cut (under certain conditions) can be proved just as before.

(4) In an essential reduction, if the suitable cut is of grade > 0 , then we can proceed as before (Step 5 in the proof of Lemma 12.8). If its grade is 0, then the cut formula is either of the form $\forall x F(x)$ or $\exists x F(x)$, where F is quantifier-free. Let us take the first case as an example. Let $F(s)$ be the auxiliary formula of a boundary inference which is an ancestor of the cut formula $\forall x F(x)$. s is a closed term, and so either $\rightarrow F(s)$ or $F(s) \rightarrow$ is a mathematical initial sequent (with ordinal 0). Suppose $\rightarrow F(s)$ is a mathematical initial sequent. Consider the proof:

$$\begin{array}{c}
 \frac{\frac{\frac{\rightarrow F(s)}{\quad} \quad \frac{F(s), \Pi' \rightarrow \Lambda'}{\quad}}{\Pi' \rightarrow \Lambda'}}{\forall x F(x), \Pi' \rightarrow \Lambda'} \\
 \frac{\frac{\Gamma \rightarrow \Theta, \forall x F(x)}{\quad} \quad \frac{\forall x F(x), \Pi \rightarrow \Lambda}{\quad}}{\Gamma, \Pi \rightarrow \Theta, \Lambda} \\
 \rightarrow
 \end{array}$$

(taking $\Gamma, \Pi \rightarrow \Theta, \Lambda$ as the sequent $\Delta \rightarrow \Xi$ shown in Lemma 12.8, Step 5). It is easy to see that the ordinal decreases again.

REMARK 12.15. Here we define an extended notion of primitive recursiveness. Let $<\cdot$ be a primitive recursive well-ordering of natural numbers. The class of $<\cdot$ -primitive recursive functions is defined as the class of functions f generated by the following schemata:

- (i) $f(a) = a + 1$,
- (ii) $f(a_1, \dots, a_n) = 0$,
- (iii) $f(a_1, \dots, a_n) = a_i$ ($1 \leq i \leq n$),
- (iv) $f(a_1, \dots, a_n) = g(h_1(a_1, \dots, a_n), \dots, h_m(a_1, \dots, a_n))$,
where g and h_i ($1 \leq i \leq m$) are $<\cdot$ -primitive recursive.
- (v) $f(0, a_2, \dots, a_n) = g(a_2, \dots, a_n)$,
 $f(a + 1, a_2, \dots, a_n) = h(a, f(a, a_2, \dots, a_n), a_2, \dots, a_n)$,
where g and h are $<\cdot$ -primitive recursive.
- (vi) (Definition by $<\cdot$ -recursion.)

$$f(a_1, \dots, a_n) = \begin{cases} h(f(\tau(a_1, \dots, a_n), a_2, \dots, a_n), a_1, \dots, a_n) \\ \quad \text{if } \tau(a_1, \dots, a_n) < a_1, \\ g(a_1, \dots, a_n) & \text{otherwise,} \end{cases}$$

where g , h and τ are $<\cdot$ -primitive recursive.

The idea of (vi) is that $f(a, a_2, \dots, a_n)$ is defined either outright or in terms of $f(b, a_2, \dots, a_n)$ for certain $b < a$.

The consistency proof for \mathbf{PA}_k which has just been presented has the following application.

COROLLARY 12.16. *Suppose R is a primitive recursive predicate and there is a proof of $\rightarrow \exists x R(a, x)$ in \mathbf{PA}_k , with ordinal $< \omega_k(l)$ for some numbers k and l (as defined just above Definition 12.6). Then the number-theoretic function f defined by*

$$f(m) = \text{the least } n \text{ such that } R(m, n)$$

is $<\cdot$ -primitive recursive, where $<\cdot$ is the initial segment of the standard ordering of ε_0 , of order type $\omega_k(l)$.

PROOF. We divide the proof into steps.

(i) Let $P(a)$ be a proof in \mathbf{PA}_k of $\rightarrow \exists x R(a, x)$ (where all occurrences of a are indicated). Then for all m , $P(\bar{m})$ is a proof in \mathbf{PA}_k of $\rightarrow \exists x R(\bar{m}, x)$ with the same ordinal, and with Gödel number primitive recursive in m . Also note that $\rightarrow \exists x R(\bar{m}, x)$ satisfies property P of Problem 12.11.

(ii) We (temporarily) call a proof *reducible* if it is a proof in \mathbf{PA}_k , with ordinal $< \omega_k(l)$, containing an essential cut or ind, and with end-sequent satisfying P . If P is reducible, then by applying repeatedly the reduction procedure of Lemma 12.8 (modified for \mathbf{PA}_k as in Remark 12.14), we obtain a proof in \mathbf{PA}_k of the same sequent, without an essential cut or ind. Let r be the function such that if p is a Gödel number of a reducible proof, then $r(p)$ is the Gödel number of the proof obtained by applying this reduction procedure (once), otherwise $r(p) = p$. Clearly r is primitive recursive.

Let O be the reduction such that if p is a Gödel number of a proof in \mathbf{PA}_k with ordinal $< \omega_k(l)$, then $O(p)$ is the Gödel number of its ordinal (and, say $O(p) = 0$ otherwise). Clearly O is primitive recursive. Note also that for all p , $O(r(p)) < \cdot O(p) \Leftrightarrow p$ is the Gödel number of a reducible proof.

(iii) Now given a proof P of $\rightarrow \exists x R(\bar{m}, x)$ without an essential cut or ind, we can effectively find from P a number n such that $R(m, n)$ holds (and in fact the least such n). This is done in the following way.

First, we may assume that no free variables appear in P . Hence if $\Gamma \rightarrow \Delta$ is a sequent in P , every formula in Γ is a closed atomic formula and every formula in Δ is either $\exists x R(\bar{m}, x)$ or a closed atomic formula.

Now consider the following property Q of sequents: Every atomic formula in the antecedent is true and every atomic formula in the succedent is false.

Notice that the end-sequent of P satisfies Q ; and if the lower sequent of a cut in P satisfies Q , then so does one upper sequent (since the cut formula is closed and atomic). Now start to construct a thread of sequents in P satisfying Q , working from the bottom upwards: the end-sequent is in the thread, and if the lower sequent of an inference is in the thread, take an upper sequent which satisfies Q . Since no initial sequent of P satisfies Q ,

this procedure must stop before we reach an initial sequent. The only way for this to happen is in the following case:

$$\frac{\Gamma \rightarrow \Delta, R(\bar{m}, \bar{k})}{\Gamma \rightarrow \Delta, \exists x R(\bar{m}, x)}$$

where $R(\bar{m}, \bar{k})$ is true. Finally, take the least $n \leq k$ for which $R(m, n)$ holds. Clearly there is a primitive recursive function h such that if P is a proof of $\rightarrow \exists x R(\bar{m}, x)$ without an essential cut or ind, then $h('P')$ is the number n found as above.

(iv) Now we can define a $<\cdot$ -primitive recursive function g such that if P is a proof of $\rightarrow \exists x R(\bar{m}, x)$ in \mathbf{PA}_k , with ordinal $< \omega_k(l)$, then $g('P') =$ the least n such that $R(m, n)$ holds:

$$g(p) = \begin{cases} g(r(p)) & \text{if } O(r(p)) < \cdot O(p), \\ h(p) & \text{otherwise.} \end{cases}$$

Then it is easily seen that g is $<\cdot$ -primitive recursive function.

(v) Finally, let $P(a)$ be a proof of $\rightarrow \exists x R(a, x)$ in \mathbf{PA}_k , with ordinal $< \omega_k(l)$ as stated. Then we define f by:

$$f(m) = g('P(\bar{m})').$$

As a special case of Corollary 12.16 we have: if $\rightarrow \exists x R(x, a)$ is provable within the system whose induction formulas have at most one quantifier, then f (defined as above) is primitive recursive (by a theorem of R. Peter that ω^l -primitive recursiveness implies primitive recursiveness for any finite l).

The following corollary is a more precise statement of Corollary 12.16.

COROLLARY 12.17. *In the same situation of Corollary 12.16 there exists a function g_0 and primitive recursive functions h, r, s , such that g_0 is defined by*

$$g_0(x) = \begin{cases} g_0(r(x)) & \text{if } O(r(x)) < \cdot O(x) \\ x & \text{otherwise} \end{cases}$$

and

$$f(x) = h(g_0(s(x))),$$

where $<\cdot$ is the initial segment of the standard ordering of ε_0 , of order type $\omega_k(l)$.

PROOF. Let g , h , r and P be same as in the proof of Corollary 12.16. In the proof of Corollary 12.16 we used different reduction and ordinal assignment from Gentzen's original reduction and ordinal assignment. In this proof, we can also use Gentzen's original reduction and ordinal assignment. Define s by $s(x) = 'P(\bar{x})'$. Then $f(x) = g(s(x))$. It is easily seen that $g(x) = h(g_0(x))$.

DEFINITION 12.18. A function f is provably recursive in \mathbf{PA} if there exist a primitive recursive predicate R and a primitive recursive function g such that $\forall x_1 \dots \forall x_n \exists y R(x_1, \dots, x_n, y)$ is provable in \mathbf{PA} and f satisfies

$$f(a_1, \dots, a_n) = g(\mu y R(a_1, \dots, a_n, y)),$$

where $\mu y R(a_1, \dots, a_n, y)$ is the least y such that $R(a_1, \dots, a_n, y)$. (See also the definition immediately before Problem 13.8.)

Corollary 12.16 gives a characterization of the provably recursive functions in \mathbf{PA} by $<\cdot$ -primitive recursive functions, where $<\cdot$ is some proper initial segment of the standard ordering of ϵ_0 .

S. S. Wainer gave a finer characterization of the provably recursive functions in \mathbf{PA} by the use of Hardy functions. For the development of the theory of Hardy functions we need a formal treatment of ordinals less than ϵ_0 . In the rest of this section by an ordinal we mean an ordinal less than ϵ_0 and let α, β, \dots be ordinals.

DEFINITION 12.19. (1) If $\omega^{\alpha_1} + \dots + \omega^{\alpha_n}$ is the normal form of α (namely $\alpha_1 \geq \dots \geq \alpha_n$) and $\omega^{\beta_1} + \dots + \omega^{\beta_m}$ is the normal form of β and $\alpha_n \geq \beta_1$, then we use $\alpha \dot{+} \beta$ to express $\alpha + \beta$. Whenever we use the expression $\alpha \dot{+} \beta$, we assume $\alpha_n \geq \beta_1$. We also use $\alpha \dot{+} \beta$ when α is empty. If α is empty, then $\alpha \dot{+} \beta$ is β itself.

(2) If α is a limit ordinal, we define a fixed fundamental sequence of α , $\{\alpha\}(0), \{\alpha\}(1), \{\alpha\}(2), \dots$ as follows.

(i) If α is of the form $\beta \dot{+} \omega^{\gamma+1}$, then $\{\alpha\}(n) = \beta \dot{+} \omega^{\gamma} \cdot n$.

(ii) If α is of the form $\beta \dot{+} \omega^{\gamma}$ and γ is a limit ordinal, then $\{\alpha\}(n) = \beta \dot{+} \omega^{\{\gamma\}(n)}$.

PROPOSITION 12.20. (1) If $\alpha > 1$ and $n > 0$, then $\{\omega^{\alpha}\}(n)$ is a limit ordinal.

(2) If α is a limit ordinal and x is a positive natural number, then there exist limit ordinals $\alpha = \alpha_1 > \alpha_2 > \dots > \alpha_k$ such that α_{i+1} ($1 \leq i \leq k$) is either $\{\alpha_i\}(0)$ or $\{\alpha_i\}(x)$ and $\alpha_{k+1} = 0$.

(3) Let α be a limit ordinal and not of the form $\alpha_0 \dot{+} \omega$. If j and x are positive natural numbers, then there exist limit ordinals

$$\{\alpha\}(j) = \alpha_1 > \alpha_2 > \dots > \alpha_k,$$

such that α_{i+1} ($1 \leq i \leq k$) is either $\{\alpha_i\}(0)$ or $\{\alpha_i\}(x)$ and $\alpha_{k+1} = \{\alpha\}(j-1)$.

PROOF. (1) This is proved by induction on α . We may assume $\alpha = \omega^\beta$. If $\beta = \beta_0 + 1$ and $\beta_0 \neq 0$, then $\{\omega^{\beta_0+1}\}(n) = \omega^{\beta_0} \cdot n$. If β is a limit ordinal and not of the form $\beta_1 + \omega$, then $\{\alpha\}(n) = \omega^{(\beta)(n)}$ and $\{\beta\}(n)$ is a limit ordinal by the induction hypothesis. If $\beta = \beta_1 + \omega$, then $\{\alpha\}(n) = \omega^{\beta_1+n}$.

(2) This is proved by induction on α . If α is of the form $\alpha_0 + \omega$, then the problem is reduced to $\alpha_0 = \{\alpha\}(0)$. If α is not of the form $\alpha_0 + \omega$, then by (1) the problem is reduced to $\{\alpha\}(x)$.

(3) This is proved by induction on α . We may assume that $\alpha = \omega^\beta$ and $\beta > 1$. If $\beta = \beta_0 + 1$, then $\{\alpha\}(j) = \omega^{\beta_0} \cdot j$ and $\{\alpha\}(j-1) = \omega^{\beta_0} \cdot (j-1)$. If β_0 is a successor ordinal, then $\{\alpha\}(j-1) = \{\{\alpha\}(j)\}(0)$. If β_0 is a limit ordinal and not of the form $\beta_1 + \omega$, then by the induction hypothesis $\{\beta_0\}(j-1)$ is obtained from $\{\beta_0\}(j)$ by successive applications of $\{\ \}(0)$ and $\{\ \}(x)$. Therefore $\{\alpha\}(j-1) = \omega^{(\beta_0)(j-1)}$ is obtained from $\{\alpha\}(j) = \omega^{(\beta_0)(j)}$ by successive applications of $\{\ \}(0)$ and $\{\ \}(x)$. Finally let $\alpha = \omega^{\beta_1+\omega}$. Then $\{\alpha\}(j) = \omega^{\beta_1+j}$ and $\{\alpha\}(j-1) = \omega^{\beta_1+j-1}$. Then $\{\{\alpha\}(j)\}(x) = \omega^{\beta_1+(j-1)} \cdot x$. If $x = 1$, then $\{\alpha\}(j-1) = \{\{\alpha\}(j)\}(x)$. If $x > 1$, then by (2) $\{\alpha\}(j-1)$ is obtained from $\{\{\alpha\}(j)\}(x)$ by successive applications of $\{\ \}(0)$ and $\{\ \}(x)$.

DEFINITION 12.21. (1) The Hardy function h_α is defined by induction on α as follows.

$$h_0(x) = x$$

$$h_{\beta+1}(x) = h_\beta(x+1)$$

$$h_\alpha(x) = h_{\{\alpha\}(x)}(x) \text{ if } \alpha \text{ is a limit ordinal.}$$

(2) For each unary function f , f^n denotes the n th iterate of f , defined by $f^0(x) = x$, $f^{m+1}(x) = f(f^m(x))$.

(3) A k -ary function g is said to be majorized by a unary function f if there is a number n such that

$$g(x_1, \dots, x_k) < f(\max(x_1, \dots, x_k)),$$

whenever $\max(x_1, \dots, x_k) \geq n$.

LEMMA 12.22. If α is a limit ordinal, then $h_{\alpha+\beta}(x) = h_\alpha(h_\beta(x))$.

PROOF. This is easily proved by induction on β . From this lemma, the following equations can be seen immediately.

$$h_{\omega^0}(x) = h_1(x) = x + 1$$

$$h_{\omega^{\beta+1}}(x) = h_{\omega^\beta}^x(x)$$

$$h_{\omega^\gamma}(x) = h_{\omega^{(\gamma)(x)}}(x) \text{ if } \alpha \text{ is a limit ordinal.}$$

LEMMA 12.23. For every α ,

- (1) h_α is strictly increasing.
- (2) If α is a limit ordinal and $i < j \leq x$, then

$$h_{\{\alpha\}(i)}(x) \leq h_{\{\alpha\}(j)}(x).$$
- (3) If $\beta < \alpha$, then h_β is majorized by h_α .

PROOF. This is proved by induction on α . If $\alpha = 0$, then the lemma is obvious. Therefore we assume that for every $\alpha_0 < \alpha$ the lemma holds. Now we assume (2) and prove (1) and (3). If α is a successor ordinal, then (1) and (3) are obvious by the induction hypothesis. Now let α be a limit ordinal, then (1) is proved as follows:

$$h_\alpha(x) = h_{\{\alpha\}(x)}(x) < h_{\{\alpha\}(x)}(x+1) \leq h_{\{\alpha\}(x+1)}(x+1) = h_\alpha(x+1),$$

where the strict inequality holds by the induction hypothesis and the second inequality holds by (2).

Now we prove (3) from (2) under the hypothesis that α is a limit ordinal. If $\beta < \alpha$, then there exists i such that $\beta < \{\alpha\}(i)$. Then h_β is majorized by $h_{\{\alpha\}(i)}$. If $x > i$, then $h_{\{\alpha\}(i)}(x) \leq h_{\{\alpha\}(x)}(x) = h_\alpha(x)$ by (2).

Now we prove (2). We may assume $i = j - 1$. If α is $\alpha_1 + \omega$, then

$$\begin{aligned} h_{\{\alpha\}(j)}(x) &= h_{\alpha_1+j}(x) = h_{\alpha_1+(j-1)}(x+1) \\ &> h_{\alpha_1+(j-1)}(x) = h_{\{\alpha\}(i)}(x). \end{aligned}$$

If α is not of the form $\alpha_1 + \omega$, then by Proposition 12.20 $\{\alpha\}(j-1)$ is obtained from $\{\alpha\}(j)$ by successive applications of $\{\ \ \}(0)$ and $\{\ \ \}(x)$. We denote this series of ordinals by

$$\{\alpha\}(j) = \alpha_0 > \alpha_1 > \dots > \alpha_n = \{\alpha\}(i),$$

where α_{k+1} is either $\{\alpha_k\}(0)$ or $\{\alpha_k\}(x)$. It suffices to show $h_{\alpha_{k+1}}(x) \leq h_{\alpha_k}(x)$. If $\alpha_{k+1} = \{\alpha_k\}(0)$, then by the induction hypothesis

$$h_{\alpha_{k+1}}(x) = h_{\{\alpha_k\}(0)}(x) \leq h_{\{\alpha_k\}(x)}(x) = h_{\alpha_k}(x).$$

If $\alpha_{k+1} = \{\alpha_k\}(x)$, then

$$h_{\alpha_{k+1}}(x) = h_{\{\alpha_k\}(x)}(x) = h_{\alpha_k}(x).$$

COROLLARY 12.24. If $\alpha > 0$ and $x > 0$, then $h_\alpha(x) > x$.

PROOF. Is easily done by induction on α .

LEMMA 12.25. If α is a limit ordinal, $\delta = \omega^{\delta_0}$ and $\omega^\delta > \alpha$, then

$$\omega^\delta \cdot \{\alpha\}(n) = \{\omega^\delta \cdot \alpha\}(n).$$

PROOF. This is proved by induction on α . Let $\alpha = \omega^{\alpha_1} + \dots + \omega^{\alpha_n}$ be a normal form. Then $\omega^\delta \cdot (\omega^{\alpha_1} + \dots + \omega^{\alpha_n}) = \omega^{\delta+\alpha_1} + \dots + \omega^{\delta+\alpha_n}$. The lemma is now obvious.

DEFINITION 12.26. The *complexity* $c(\alpha)$ of α is defined as follows.

$$c(0) = 0, \quad c(\omega^\alpha) = c(\alpha) + 1, \quad c(\alpha + \beta) = c(\alpha) + c(\beta).$$

LEMMA 12.27. Let β be a limit ordinal, $\alpha < \beta$ and $c(\alpha) < n$. Then $\alpha < \{\beta\}(n)$.

PROOF. Let $\alpha = \delta + (\omega^{\alpha_1} \cdot a_1 + \dots + \omega^{\alpha_s} \cdot a_s)$ ($\alpha_1 > \dots > \alpha_s$); $\beta = \delta + (\omega^{\beta_1} \cdot b_1 + \dots + \omega^{\beta_r} \cdot b_r)$ ($\beta_1 > \dots > \beta_r$) and $\omega^{\beta_1} \cdot b_1 > \omega^{\alpha_1} \cdot a_1$. Then $\{\beta\}(n) \geq \delta + \omega^{\beta_1}(b_1 - 1) + \{\omega^{\beta_1}\}(n)$.

Case (1). $\beta_1 > \alpha_1$.

If β_1 is a successor ordinal, then $\{\omega^{\beta_1}\}(n) \geq \omega^{\alpha_1} \cdot n$. Since $n > c(\alpha) \geq a_1$, $\{\omega^{\beta_1}\}(n) \geq \omega^{\alpha_1} \cdot (a_1 + 1)$. If β_1 is a limit ordinal and $\alpha = \delta$ (i.e., $a_1 = 0$), then this is obvious since $\{\omega^{\beta_1}\}(n) > 0$ by Proposition 12.20. If β_1 is a limit ordinal and $a_1 > 0$, then $\{\beta_1\}(n) > \alpha_1$ by the induction hypothesis since $n > c(\alpha_1)$. Therefore $\{\omega^{\beta_1}\}(n) = \omega^{\{\beta_1\}(n)} > \omega^{\alpha_1}$.

Case (2). $\beta_1 = \alpha_1$ and $b_1 > a_1$.

If $\beta_1 (= \alpha_1)$ is a successor ordinal, then $\omega^{\beta_1}(b_1 - 1) \geq \omega^{\alpha_1} \cdot a_1$ and $\{\omega^{\beta_1}\}(n) > \omega^{\alpha_1} \cdot a_2 + \dots + \omega^{\alpha_s} \cdot a_s$ since

$$n > c(\alpha) > c(\omega^{\alpha_2} \cdot a_2 + \dots + \omega^{\alpha_s} \cdot a_s).$$

If $\beta_1 (= \alpha_1)$ is a limit ordinal and $a_2 = a_3 = \dots = a_s = 0$, then

$$\begin{aligned} \{\beta\}(n) &\geq \delta + \omega^{\alpha_1} \cdot a_1 + \{\omega^{\alpha_1}\}(n) \\ &> \delta + \omega^{\alpha_1} \cdot a_1 = \alpha. \end{aligned}$$

If $\beta_1 (= \alpha_1)$ is a limit ordinal and $a_2 > 0$, then $\{\beta_1\}(n) > \alpha_2$ since $n > c(\alpha_2)$. Therefore $\{\beta\}(n) \geq \delta + \omega^{\alpha_1} \cdot a_1 + \omega^{\{\beta_1\}(n)} > \alpha$.

LEMMA 12.28. Let $\delta = \omega^{\delta_0}$, $\alpha < \beta < \omega^\delta$ and $c(\alpha) < x$. Then $h_{\omega^\delta, \alpha}(x) < h_{\omega^\delta, \beta}(x)$.

PROOF. This is proved by induction on β . If $\beta = \beta_0 + 1$, then

$$h_{\omega^\delta, \alpha}(x) \leq h_{\omega^\delta, \beta_0}(x) < h_{\omega^\delta, \beta_0}(h_{\omega^\delta}(x)) = h_{\omega^\delta, \beta}(x).$$

If β is a limit ordinal, then by Lemma 12.27 $c(\alpha) < x$ implies $\alpha < \{\beta\}(x)$. Therefore by the induction hypothesis and Lemma 12.25

$$h_{\omega^\delta, \alpha}(x) < h_{\omega^\delta, \{\beta\}(x)}(x) = h_{\{\omega^\delta, \beta\}(x)}(x) = h_{\omega^\delta, \beta}(x).$$

LEMMA 12.29. (1) If $f(x_1, \dots, x_m)$ and $g_1(x_1, \dots, x_n), \dots, g_m(x_1, \dots, x_n)$ are majorized by h_{ω^α} , then $f(g_1(x_1, \dots, x_n), \dots, g_m(x_1, \dots, x_n))$ is majorized by $h_{\omega^\alpha \cdot 2}$.

(2) If $h(x)$ and $g(x, y, z)$ are majorized by h_{ω^α} and $f(x, y)$ is obtained by a primitive recursion from h and g , namely, $f(0, y) = h(y)$ and $f(x+1, y) = g(x, y, f(x, y))$, then $f(x, y)$ is majorized by $h_{\omega^{\alpha+1}+1}$.

PROOF. First $f(x_1, \dots, x_n)$ is majorized by h_α iff there exists p such that for every x_1, \dots, x_n

$$f(x_1, \dots, x_n) < \max(h_\alpha(\max(x_1, \dots, x_n)), p).$$

(1) Let $x = \max(x_1, \dots, x_n)$ and p be such that for every y_1, \dots, y_m and x_1, \dots, x_n ,

$$f(y_1, \dots, y_m) \leq \max(h_{\omega^\alpha}(\max(y_1, \dots, y_m)), p)$$

$$g_1(x_1, \dots, x_n) \leq \max(h_{\omega^\alpha}(x), p)$$

$$\vdots$$

$$g_m(x_1, \dots, x_n) \leq \max(h_{\omega^\alpha}(x), p).$$

Then

$$\begin{aligned} & f(g_1(x_1, \dots, x_n), \dots, g_m(x_1, \dots, x_n)) \\ & \leq \max(h_{\omega^\alpha}(\max(h_{\omega^\alpha}(x), p)), p) \\ & \leq \max(h_{\omega^\alpha} \cdot h_{\omega^\alpha}(x), p') = \max(h_{\omega^{\alpha \cdot 2}}(x), p'), \end{aligned}$$

where $p' = h_{\omega^\alpha}(p)$.

(2) Let p satisfy the following inequality for every x, y , and z ,

$$h(x) < \max(h_{\omega^\alpha}(x), p)$$

$$g(x, y, z) < \max(h_{\omega^\alpha}(\max(x, y, z)), p).$$

We prove the following inequality by induction on x ,

$$f(x, y) < h_{\omega^{\alpha+1}}^x(\max(x, y, p)).$$

If $x = 0$, then the inequality is obvious. The case for $x+1$ is proved as follows.

$$\begin{aligned} f(x+1, y) & < \max(h_{\omega^\alpha}(\max(x, y, h_{\omega^{\alpha+1}}^x(\max(x, y, p))), p), p) \\ & \leq h_{\omega^\alpha} \cdot h_{\omega^{\alpha+1}}^x(\max(x, y, p)) \\ & \leq h_{\omega^{\alpha+2}}^{x+1}(\max(x+1, y, p)). \end{aligned}$$

Since $h_{\omega^{\alpha+1}}^{x+1} = h_{\omega^{\alpha+1} \cdot (x+1)}$, (2) is proved as follows.

$$\begin{aligned} f(x, y) &< h_{\omega^{\alpha+1} \cdot (x+1)}(\max(x, y, p)) \\ &\leq h_{\omega^{\alpha+1}}(\max(x, y, p) + 1) \\ &\leq h_{\omega^{\alpha+1} + 1}(\max(x, y, p)). \end{aligned}$$

COROLLARY 12.30. *All primitive recursive functions are majorized by $h_{\omega^{\omega}}$.*

DEFINITION 12.31. The Hardy class \mathcal{H} is the smallest class of functions containing 0, all h_{α} , all projection functions $(I_{n,i}(x_1, \dots, x_n) = x_i)$, and closed under primitive recursion and substitution.

By Lemma 12.23 and Lemma 12.29, every function in \mathcal{H} is majorized by $h_{\omega_n}(n)$.

From now on, we fix a representation of ordinals less than ε_0 by natural numbers. We assume that the natural number 0 does not represent any ordinal. The following theorem is easily seen from our discussion in §11. However we give here another formal proof which is also given by Gentzen.

THEOREM 12.32. *Let n be a natural number. Then transfinite induction up to ω_n is provable in **PA**.*

PROOF. Let $<$ express the order of ordinals in this proof. Then we shall show that

$$(*) \quad \forall \alpha (\forall \beta < \alpha A(\beta) \supset A(\alpha)) \rightarrow \forall \alpha \leq \omega_n A(\alpha)$$

Is provable in **PA** for every formula $A(\alpha)$ in **PA**. We show this by induction on n . The case $n = 1$ is obvious since **PA** has mathematical induction. Now we assume that $(*)$ for n is provable in **PA**. Let $A^*(\alpha)$ and φ denote $\forall \beta \leq \alpha A(\beta)$ and $\forall \alpha (\forall \beta < \alpha A(\beta) \supset A(\alpha))$ respectively. Then it is easily seen that $\varphi \rightarrow \forall \alpha (\forall \beta < \alpha A^*(\beta) \supset A^*(\alpha))$. Let $\psi(\alpha)$ denote $\forall \gamma (A^*(\gamma) \supset A^*(\gamma + \omega^{\alpha}))$. Let $\alpha = \alpha_0 + 1$. Then it is easily seen that

$$\forall \gamma < \alpha \psi(\gamma), \quad A^*(\beta + \omega^{\alpha_0} \cdot a) \rightarrow A^*(\beta + \omega^{\alpha_0} \cdot (a + 1)).$$

By mathematical induction on a , we have

$$\forall \gamma < \alpha \psi(\gamma), \quad A^*(\beta) \rightarrow A^*(\beta + \omega^{\alpha_0} \cdot a).$$

Therefore we have

$$\forall \gamma < \alpha \psi(\gamma), \quad A^*(\beta) \rightarrow \forall \gamma < \beta + \omega^{\alpha} A^*(\gamma)$$

and $\varphi, \forall \gamma < \alpha \psi(\gamma), A^*(\beta) \rightarrow A^*(\beta + \omega^\alpha)$
 and $\varphi, \forall \gamma < \alpha \psi(\gamma) \rightarrow \psi(\alpha)$.

It is also easily seen that

$$\text{Lim}(\alpha), \forall \gamma < \alpha \psi(\gamma) \rightarrow \psi(\alpha),$$

where $\text{Lim}(\alpha)$ is a formula expressing “ α is a limit ordinal”. Hence we have $\forall \gamma < \alpha \psi(\gamma) \rightarrow \psi(\alpha)$. By the induction hypothesis we have $\psi(\omega_n)$ namely $\forall \gamma (A^*(\gamma) \supset A^*(\gamma + \omega^n))$. Therefore we have $A^*(0) \rightarrow A^*(\omega_{n+1})$. Since $\varphi \rightarrow A^*(0)$ is provable, we have $\varphi \rightarrow A^*(\omega_{n+1})$.

COROLLARY 12.33. *For every α , Hardy function h_α is provably recursive in **PA**.*

LEMMA 12.34. *Let f be provably recursive in **PA**. Then there exist h_α and a primitive recursive function $u(x)$ such that for every x , $f(x) < h_\alpha(u(x))$.*

PROOF. By Corollary 12.17 and Lemma 12.29 we may assume that $f(x)$ is $g_0(x)$ in Corollary 12.17 namely

$$f(x) = \begin{cases} f(r(x)) & \text{if } O(r(x)) < O(x) < \omega_n \\ x & \text{otherwise,} \end{cases}$$

where $r(x)$ is the Gödel number of the result of Gentzen's reduction of x , if x is the Gödel number of a proof, and $O(x)$ is the ordinal assigned to x . The usual assignment of ordinal satisfies the condition $x > c(O(x))$ if x is the Gödel number of a proof. We assume that this condition is satisfied. We also assume that the ordinal of the proof of $\rightarrow \exists x R(a, x)$ is smaller than ω_n . We define an ordinal $|x|$ as follows.

$$|x| = \begin{cases} O(x) & \text{if } O(r(x)) < O(x) < \omega_n \\ x & \text{otherwise.} \end{cases}$$

Since $r(x)$ is primitive recursive, there exists b such that $b \geq 2$ and

$$\max(x, \max(r(x), r(r(x))), y) + y \geq h_{\omega_n}(\max(x, y)) + b.$$

We define $u(x)$ as follows.

$$u(x) = \max(x, r(x), b) + b.$$

Then we have

$$\begin{aligned}
 \max(x, u(r(x))) &= \max(x, \max(r(x), r(r(x)), b) + b) \\
 &\leq h_{\omega_n}(\max(x, b)) + b \\
 &\leq h_{\omega_n}(\max(x, b) + b) \\
 &\leq h_{\omega_n}(u(x)).
 \end{aligned}$$

By induction on $|x|$, we prove

$$f(x) \leq h_{\omega_n \cdot |x|}(u(x)).$$

If $|x| = 0$, then $f(x) = x \leq u(x) = h_0(u(x))$. So we assume that $|x| > 0$ and the inequality holds for y satisfying $|y| < |x|$. Then we have

$$\begin{aligned}
 f(x) &\leq \max(x, f(r(x))) \\
 &\leq \max(x, h_{\omega_n \cdot |r(x)|}(u(r(x)))) \\
 &\leq h_{\omega_n \cdot |r(x)|}(\max(x, u(r(x)))) \\
 &\leq h_{\omega_n \cdot |r(x)|}(h_{\omega_n}(u(x))) \\
 &\leq h_{\omega_n \cdot (|r(x)|+1)}(u(x)) \\
 &\leq h_{\omega_n \cdot |x|}(u(x)).
 \end{aligned}$$

The last inequality holds since

$$c(|r(x)| + 1) \leq c(|r(x)|) + 1 \leq r(x) < u(x).$$

Since $c(|x|) < x < u(x)$, we have

$$f(x) < h_{\omega_n \cdot \omega_n}(u(x)).$$

THEOREM 12.35 (Wainer). \mathcal{H} is the class of all provably recursive functions in PA.

PROOF. It suffices to show that the following function f is in \mathcal{H} .

$$f(x) = \begin{cases} f(r(x)) & \text{if } 0(r(x)) < 0(x) < \omega_n \\ x & \text{otherwise.} \end{cases}$$

We define primitive recursive functions $t(x)$ and $g(x, y)$ as follows.

$$t(x) = \begin{cases} r(x) & \text{if } 0(r(x)) < 0(x) < \omega_n \\ x & \text{otherwise.} \end{cases}$$

$$q(0, x) = x, \quad q(y + 1, x) = t(q(y, x)).$$

Then $p(x) = \mu y(q(y+1, x) = q(y, x))$ is provably recursive in **PA**. Therefore there exist β and a primitive recursive function $u(x)$ such that $p(x) < h_\beta(u(x))$. Then $p(x) = \mu y(y < h_\beta(u(x)) \wedge q(y+1, x) = q(y, x))$ and $p(x)$ is in \mathcal{H} . Since $f(x) = q(p(x), x)$, $f(x)$ is also in \mathcal{H} .

Now we are going to discuss Kirby and Paris' result on Goodstein's Theorem.

DEFINITION 12.36. Let m and n be natural numbers, $n > 1$. We define the *pure base n representation* of m as follows. First write m as the sum of powers of n . For example, if $m = 26$, $n = 2$, write $26 = 2^4 + 2^3 + 2$. Now write each exponent as a sum of powers of n . Repeat with exponents of exponents and so on until the representation stabilizes. For example the pure base 2 representation of 26 is $2^{2^2} + 2^{2^{+1}} + 2$.

We now define the Goodstein number $g_n(m)$ as follows. If $m = 0$ set $g_n(m) = 0$. Otherwise set $g_n(m)$ to be the number produced by replacing every n in the pure base n representation of m by $n+1$ and then subtracting 1. For example $g_2(26) = 3^{3^3} + 3^{3^{+1}} + 3 - 1$. Now define the Goodstein sequence for m by

$$m_0 = m, \quad m_k = g_{k+1}(m_{k-1}) \quad (k > 1).$$

So, for example,

$$\begin{aligned} 26_0 &= 26 = 2^{2^2} + 2^{2^{+1}} + 2, \\ 26_1 &= 3^{3^3} + 3^{3^{+1}} + 3 - 1 = 3^{3^3} + 3^{3^{+1}} + 2, \\ 26_2 &= 4^{4^4} + 4^{4^{+1}} + 2 - 1 = 4^{4^4} + 4^{4^{+1}} + 1, \\ 26_3 &= 5^{5^5} + 5^{5^{+1}} + 1 - 1 = 5^{5^5} + 5^{5^{+1}}. \end{aligned}$$

The general Goodstein sequence $m_{n,k}$ for $n \geq 2$ is defined as follows.

$$m_{n,0} = m, \quad m_{n,k} = g_{n+k-1}(m_{n,k-1}) \quad (k > 1).$$

Obviously $m_k = m_{2,k}$.

THEOREM 12.37. (1) (Goodstein) $\forall m \forall n \geq 2 \exists k m_{n,k} = 0$. Namely the general Goodstein sequence $m_{n,0}, m_{n,1}, m_{n,2}, \dots$ eventually terminates with 0.

(2) (Kirby and Paris) Goodstein's theorem for $n = 2$ namely $\forall m \exists k m_k = 0$ is not provable in **PA**.

Our proof is due to Cichon. We need several preparation.

DEFINITION 12.38. Let $x < \omega$ and $\alpha < \varepsilon_0$.

(1) $G_x(\alpha)$ is defined as follows.

$$\begin{aligned} G_x(0) &= 0, & G_x(\alpha + 1) &= G_x(\alpha) + 1; \\ G_x(\alpha) &= G_x(\{\alpha\}(x)) \quad \text{for a limit ordinal } \alpha. \end{aligned}$$

(2) $P_x(\alpha)$ is defined as follows.

$$\begin{aligned} P_x(0) &= 0, & P_x(\alpha + 1) &= \alpha; \\ P_x(\alpha) &= P_x(\{\alpha\}(x)) \quad \text{for a limit ordinal } \alpha. \end{aligned}$$

LEMMA 12.39. *For $x < \omega$ and $\alpha < \varepsilon_0$, the following equations hold.*

- (1) $G_x(\alpha + \beta) = G_x(\alpha) + G_x(\beta)$
- (2) $G_x(\omega^\alpha) = x^{G_x(\alpha)}$.

PROOF. (1) is easily proved by induction on β . (2) is proved by induction on α . If α is 0 or a limit ordinal, then the equation is obvious. For $\alpha + 1$,

$$\begin{aligned} G_x(\omega^{\alpha+1}) &= G_x(\omega^\alpha \cdot x) = G_x(\overbrace{\omega^\alpha + \dots + \omega^\alpha}^x) \\ &= \underbrace{x^{G_x(\alpha)} + \dots + x^{G_x(\alpha)}}_x = x^{G_x(\alpha)+1} = x^{G_x(\alpha+1)}. \end{aligned}$$

COROLLARY 12.40. $G_x(\alpha)$ is the result of replacing ω by x in the canonical normal form of α .

LEMMA 12.41. *For $x < \omega$ and $\alpha < \varepsilon_0$, the following equation holds*

$$G_x P_x(\alpha) = P_x G_x(\alpha).$$

PROOF. Is immediate by induction on α .

Now let $n \geq 2$. We are going to form $m_{n,0}, m_{n,1}, m_{n,2}, \dots$ by using G_x and P_x . Let α be obtained from the pure base n expression of m by replacing n by ω . Then $m_{n,0} = m = G_n(\alpha)$.

$$\begin{aligned} m_{n,1} &= G_{n+1}(\alpha) - 1 = P_{n+1} G_{n+1}(\alpha) = G_{n+1} P_{n+1}(\alpha), \\ m_{n,2} &= G_{n+2}(P_{n+1}(\alpha)) - 1 \\ &= P_{n+2} G_{n+2} P_{n+1}(\alpha) \\ &= G_{n+2} P_{n+2} P_{n+1}(\alpha), \\ m_{n,k} &= G_{n+k} P_{n+k} P_{n+k-1} \dots P_{n+1}(\alpha). \end{aligned}$$

It is easily seen by induction on α that for $x \neq 0$, $G_x(\alpha) = 0$ iff $\alpha = 0$.

Therefore, (1) of Theorem 12.37 $\forall m \forall n \geq 2 \exists k m_{n,k} = 0$ is implied by $\forall \alpha \forall n \geq 2 \exists k P_{n+k} \dots P_{n+1}(\alpha) = 0$ which is obvious since $\alpha > 0$ then $P_x(\alpha) < \alpha$.

LEMMA 12.42. If $0 < \alpha < \varepsilon_0$ and $1 \leq n < \omega$, then $(\mu x)(P_x P_{x-1} \dots P_{n+1}(\alpha) = 0) = h_\alpha(n+1) - 1$, where $\mu x \varphi(x)$ is the least x satisfying $\varphi(x)$ and h_α is a Hardy function.

PROOF. If $\alpha = 1$, then the lemma is obvious. If $\alpha = \beta + 1$, then

$$\begin{aligned} (\mu x)(P_x P_{x-1} \dots P_{n+1}(\beta + 1) = 0) &= (\mu x)(P_x P_{x-1} \dots P_{n+2}(\beta) = 0) \\ &= h_\beta(n+2) - 1 = h_\alpha(n+1) - 1. \end{aligned}$$

If α is a limit ordinal, then

$$\begin{aligned} (\mu x)(P_x P_{x-1} \dots P_{n+1}(\alpha) = 0) &= (\mu x)(P_x \dots P_{n+2} P_{n+1}(\{\alpha\}(n+1))) \\ &= h_{\{\alpha\}(n+1)}(n+1) - 1 = h_\alpha(n+1) - 1. \end{aligned}$$

Now we prove (2) of Theorem 12.36. We define a_n by $a_0 = 1$, $a_{k+1} = 2^{a_k}$ and b_n by $b_n = a_n + a_{n-1} + \dots + a_0$. Define $\alpha_n = \omega_n + \omega_{n-1} + \omega_{n-2} + \dots + 1$. Then $G_2(\alpha_n) = b_n$. Then $\forall m \exists k m_k = 0$ implies that $h_{\alpha_n}(3)$ as a function of n is provably recursive in \mathbf{PA} . However $h_{\alpha_n}(3) \geq h_{\omega_n}(n)$. Since $h_{\omega_n}(n)$ is not majorized by any h_α ($\alpha < \varepsilon_0$), this is a contradiction.

DEFINITION 12.43. Let A be a set and m be a natural number. $A^{[m]}$ is the collection of subset of A of cardinality m . If $F: A^{[m]} \rightarrow X$, a subset B of A is homogeneous for F if F is constant on $B^{[m]}$. We identify a natural number n with the set $\{0, 1, \dots, n-1\}$.

We state the following Ramsey's theorem without proof.

THEOREM 12.44. Let A be an infinite set and m and n be natural numbers. Then for every function $F: A^{[m]} \rightarrow n$, there exists an infinite subset B of A which is homogeneous for F .

DEFINITION 12.45. (1) Let S be a set of natural numbers. S is *large* if S is non-empty, and letting s be its least element, S has at least s elements.
(2) Let a, b, c be positive natural numbers. Then $a \rightarrow (\text{large})_c^b$, if for every map $F: a^{[b]} \rightarrow c$, there is a large homogeneous set for F of cardinality greater than b .

THEOREM 12.46. Let a, b, c range over the natural numbers. Then the following holds

$$\forall b, c \geq 1 \exists a \geq 1 (a \rightarrow (\text{large})_c^b).$$

PROOF. Suppose the theorem were false. Then there exist fixed $b, c \geq 1$ such that

$$\forall a \geq 1 (a \not\rightarrow (\text{large})_c^b).$$

Let T be the set of all F such that $F: a^{[b]} \rightarrow c$ for some a and there are no large homogeneous set for F of cardinality greater than b . For F_1, F_2 we define $F_1 \leq F_2$ if F_2 is an extension of F_1 . Then T is a tree. Then the condition $\forall a \geq 1 (a \not\rightarrow (\text{large})_c^b)$ implies that for every a , there exists a branch (a maximal linearly ordered subset) of T with length at least a . By König's lemma, there exists an infinite branch in T . Such a branch produces a function $F: \mathbb{N}^{[b]} \rightarrow C$ such that there are no large homogeneous sets for F of cardinality greater than b . This is a contradiction because of Ramsey's theorem.

Paris and Harrington proved that $\forall b, c \geq 1 \exists a \geq 1 (a \rightarrow (\text{large})_c^b)$ is not provable in **PA**. Let $\sigma(b, c)$ be the least natural number a such that $a \rightarrow (\text{large})_c^b$. Paris and Harrington proved the following stronger theorem.

THEOREM (Paris, Harrington). *The function $\sigma(n, n)$ majorizes all provably recursive functions in **PA**.*

Ketonen and Solovay investigated upper and lower bounds of $\sigma(n, n)$. As a lower bound, they proved that $\sigma(n, 7)$ majorizes all provably recursive functions in **PA**. J. Quinsey improved the result by showing that $\sigma(n, 3)$ majorizes all provably recursive functions in **PA**. We shall discuss their results. We shall not discuss an upperbound of $\sigma(n, n)$. We simply note that one can get an upperbound of $\sigma(n, n)$ in the form of an ordinal recursive function by the method of §30 if one checks the second order system in which the proof of

$$\forall b, c \geq 1 \exists a \geq 1 (a \rightarrow (\text{large})_c^b)$$

can be carried out.

First we discuss more on Ramsey's theorem. In his paper: Ramsey's Theorem and Recursion Theory, The Journal of Symbolic Logic, Vol. 37; pp. 268–280, 1972, C. Jockusch proved that Ramsey's Theorem namely Theorem 12.44 is not provable in the second order arithmetic with the arithmetical comprehension axioms and the arithmetical mathematical inductions. It is also easily seen from his paper that if m is a fixed natural number but not a variable, then Ramsey's theorem for this fixed m is provable in the second order arithmetic with the arithmetical comprehension axioms and the arithmetical mathematical inductions. This fact together with the proof of Theorem 12.44 implies that for any fixed natural number $b \geq 1$,

$$\forall c \geq 1 \exists a \geq 1 (a \rightarrow (\text{large})_c^b)$$

is provable in second order arithmetic with the arithmetical comprehension axioms and the arithmetical mathematical inductions. As is proved in §16, second order arithmetic with the arithmetical comprehension axioms and the arithmetical mathematical inductions is a conservative extension of **PA**. Therefore for every fixed natural number $b \geq 1$,

$$\forall c \geq 1, \exists a \geq 1 (a \rightarrow (\text{large})_c^b)$$

is provable in **PA**.

DEFINITION 12.47. Let a, b, c , and k be natural numbers. By $a \rightarrow (k)_c^b$, we mean the following statement: for every function $f: [a]^b \rightarrow c$, there exists a subset A of a such that A is homogeneous for f and the cardinality of A is k .

It is well-known in combinatorics that there exists a primitive recursive function $g(b, c, k)$ such that $g(b, c, k) \rightarrow (k)_c^b$.

DEFINITION 12.48. A function $f: \mathbb{N}^n \rightarrow \mathbb{N}$ is said to be monotone if for $x_1, \dots, x_n, y_1, \dots, y_n \in \mathbb{N}$, the following holds:

$$\text{if } x_1 \leq y_1, \dots, x_n \leq y_n, \text{ then } f(x_1, \dots, x_n) \leq f(y_1, \dots, y_n).$$

Our strategy is expressed by the following simple proposition.

PROPOSITION 12.49. Let $g(x)$, $p(x)$ and $h(x)$ be monotone functions from \mathbb{N} into \mathbb{N} satisfying the following conditions.

- (1) Every provably recursive function in **PA** is majorized by g .
- (2) $p(x)$ is provably recursive.
- (3) For every $x \in \mathbb{N}$, $g(x) \leq h(p(x))$.

Then every provably recursive function in **PA** is majorized by h .

PROOF. By replacing $p(x)$ by $\max(p(x), x)$ if necessary, we may assume that $\forall x (x \leq p(x))$, therefore that $\forall x \exists y (x \leq p(y))$. Let $f(x)$ be a provably recursive function in **PA**. We define $q(x)$ and $q_0(x)$ by the following equations:

$$\begin{aligned} q(x) &= \text{the least } y \leq x \text{ such that } x \leq p(y) \\ q_0(x) &= q(x) - 1. \end{aligned}$$

Since $x \leq p(q_0(x) + 1)$ we have

$$f(x) \leq f(p(q_0(x) + 1)).$$

Since $f(p(x + 1))$ is provably recursive in **PA** and $p(q_0(x)) < x$ for any

large x , we have the following inequality for any large x

$$f(p(q_0(x) + 1)) < g(q_0(x)) \leq h(p(q_0(x))) \leq h(x).$$

In the following, we shall find two primitive recursive functions $p(x)$ and $q(x)$ such that $h_{\omega_n}(n) \leq \sigma(p(n), p(n))$ and $\sigma(n, n) \leq \sigma(q(n), 3)$.

For a while, we shall use capital letters to denote subsets of \mathbb{N} and lower case letters to denote elements of \mathbb{N} . If X is a set, $|X|$ is the cardinality of X ; if $|X| = m$, and we write $X = \{x_0, \dots, x_{m-1}\}$, it is always tacitly understood that $x_0 < x_1 < \dots < x_{m-1}$.

DEFINITION 12.50. (1) Let n and c be positive natural numbers. An (n, c) -algebra is a map $G: \mathbb{N}^{[n]} \rightarrow C$, where C is a finite set of cardinality c . Also n is called the dimension of G and c is called the number of colors.

(2) A finite subset S of \mathbb{N} is suitable for the (n, c) -algebra G if S is large and homogeneous for G and $|S| \geq n + 1$.

(3) An algebra G_2 is said to simulate an algebra G_1 if every S suitable for G_2 is suitable for G_1 .

(4) Let F_1 and F_2 be (n, c_1) -algebra and (n, c_2) -algebra respectively. An $(n, c_1 c_2)$ -algebra F defined by $F(u) = \langle F_1(u), F_2(u) \rangle$ is called the *product algebra* of F_1 and F_2 .

PROPOSITION 12.51. (1) If F is the product algebra of F_1 and F_2 , then F simulates F_1 and F_2 .

(2) Every $(n, c_1 c_2)$ -algebra is isomorphic to the product of an (n, c_1) -algebra and an (n, c_2) -algebra.

(3) If $c_1 \leq c_2$, any (n, c_1) -algebra can be construed as an (n, c_2) -algebra.

(4) Let G be (n, c) -algebra and $S \subseteq \mathbb{N}$. If every subset T of S with $|T| = n + 1$ is homogeneous for G , then S is homogeneous for G .

PROOF. (1), (2), and (3) are obvious.

(4) Let $X, Y \in \mathbb{N}^{[n]}$. We prove by induction on $|X \cup Y|$ that $G(X) = G(Y)$. If $|X \cup Y| \leq n + 1$, then it is obvious. Let $|X \cup Y| > n + 1$, $x \in X - Y$, and $y \in Y - X$. Let $X_0 = (X - \{x\}) \cup \{y\}$. By the induction hypothesis, $G(X) = G(X_0) = G(Y)$.

LEMMA 12.52. (1) Let $G_i: \mathbb{N}^{[n]} \rightarrow C_i$ be an (n, c_i) -algebra ($1 \leq i \leq k$). If $G: \mathbb{N}^{[n]} \rightarrow C_1 \times \dots \times C_k$ be the product algebra, then G can be simulated by an $(n + 1, c_1 + \dots + c_k + 1)$ -algebra.

(2) Let $c \leq c_1 c_2 \dots c_k$. Then any (n, c) -algebra can be simulated by an $(n + 1, c_1 + \dots + c_k + 1)$ -algebra.

(3) Any $(n, 7)$ -algebra can be simulated by an $(n + 1, 7)$ -algebra.

PROOF. (1) Define an algebra $G^*: \mathbb{N}^{[n+1]} \rightarrow \{0\} \cup \bigcup_{1 \leq i \leq k} \{i\} \times C_i$ as follows. If $X \in \mathbb{N}^{[n+1]}$ is homogeneous for each of the G_i 's, then $G^*(X) = 0$.

Otherwise, let i be least such that X is not homogeneous for G_i . Let Y be the first n elements of X . Set $G^*(X) = \langle i, G_i(Y) \rangle$.

We show that G^* simulates G . It suffices to show that S is homogeneous for G if S is suitable for G^* .

Suppose first that the constant value assumed by S is 0. Then by (4) of Proposition 12.49, S is homogeneous for each G_i , and hence for G .

Next suppose that the constant value of G^* is $\langle i, t \rangle$. So each size $n+1$ subset of S is homogeneous for G_j if $1 \leq j < i$, is not homogeneous for G . As a special case the first $n+1$ elements of S is not homogeneous for G . Since S is suitable for G^* , $|S| \geq n+2$. Let s_0, \dots, s_{n+1} be the first $n+2$ elements of S . Let Y be an n element subset of $\{s_0, \dots, s_n\}$. Since $G^*(Y \cup \{s_{n+1}\}) = \langle i, t \rangle$, $G_i(Y) = t$. Thus G_i takes the constant value t on the size n subsets of $\{s_0, \dots, s_n\}$. This is a contradiction.

(2) follows immediately from (1).

(3) This is immediate from the case $k=2$ of (2), since $7 < 3 \cdot 3$ and $3+3+1=7$.

We shall construct many (n, c) -algebras satisfying several properties. As is suggested by Proposition 12.49, the exact values of n and c are not necessary in the end as far as they can be primitive recursively calculated. So we shall skip the calculations of n and c . In this sense, some of the following lemmas are not necessary since what we need is primitive recursive functions. Nevertheless we keep them because of their beauty.

LEMMA 12.53. (1) *Let G be an (n, c) -algebra and d be a natural number ≥ 1 . Then there is an $(n, c+d)$ -algebra G^* which simulates G and such that any S suitable for G^* has $\min S \geq d$.*

(2) *Let $n \geq 2$. Then there is an $(n, 7)$ -algebra G such that if S is suitable for G , then $\min S \geq 2n+3$.*

PROOF. (1) Let $G: \mathbb{N}^{[n]} \rightarrow C$. Define $G^*: \mathbb{N}^{[n]} \rightarrow (\{0\} \times d) \cup (\{1\} \times C)$ as follows. Let $X \in \mathbb{N}^{[n]}$. If $\min X < d$, set $G^*(X) = \langle 0, \min X \rangle$; otherwise, let $G^*(X) = \langle 1, G(X) \rangle$.

Let $S = \{s_0, \dots, s_m\}$ be suitable for G^* . Since S is suitable, $m \geq n$. We show first that $s_0 \geq d$. For, otherwise $G^*(\{s_0, \dots, s_{n-1}\}) = \langle 0, s_0 \rangle$. Then $G^*(\{s_1, \dots, s_n\}) = \langle 0, s_0 \rangle$ since S is homogeneous for G^* . So $s_0 = s_1$ which is a contradiction.

Hence G^* must have constant value $\langle 1, z \rangle$ for some z . But then G has constant value z on $S^{[n]}$ and S is suitable for G .

(2) Define a $(1, 4)$ -algebra G_1 as follows:

$$\begin{array}{ll} \text{if } 0 \leq m < n, & G_1(m) = 0; \\ \text{if } n \leq m < 2n, & G_1(m) = 1; \\ \text{if } 2n < m < 4n-1, & G_1(m) = 2; \\ \text{if } 4n-1 \leq m, & G_1(m) = 3. \end{array}$$

By (3) of Lemma 12.52, let G be an $(n, 7)$ -algebra which simulates G_1 . Let S be suitable for G . We shall show that $\min S \geq 2n + 3$.

Let $S = \{s_0, \dots, s_m\}$. Then $m \geq n$ and $m \geq s_0 - 1$ since S is suitable for G . Since G simulates G_1 , S is homogeneous for G_1 . Now $m \geq n$ implies $G_1(s_m) \geq 1$, so $G_1(s_0) \geq 1$. That is $s_0 \geq n$. Since $m \geq n$, $s_n \geq n + s_0 \geq 2n$, whence $G_1(s_n) \geq 2$. So $G_1(s_0) \geq 2$ namely $s_0 \geq 2n$. Now $m \geq s_0 - 1 \geq 2n - 1$, whence $s_m \geq 4n - 1$; so $G_1(s_0) = G_1(s_m) = 3$. That is $s_0 \geq 4n - 1$. Finally $2n + 3 \leq 4n - 1$ since $n \geq 2$.

DEFINITION 12.54. Define functions $E_m: \mathbb{N} \rightarrow \mathbb{N}$ as follows:

$$E_0(n) = n \quad \text{and} \quad E_{m+1}(n) = 2^{E_m(n)}.$$

LEMMA 12.55. Let $h: \mathbb{N}^{[n]} \rightarrow \mathbb{N}$. Suppose that whenever $1 \leq x_0 < \dots < x_{n-1}$, $h(x_0, \dots, x_{n-1}) < E_m(x_0)$. Then there is an $(n + m + 1, 10^{2^{m+2}})$ -algebra G such that for any S suitable for G , there is a function $g_s: S \rightarrow \mathbb{N}$ such that for any $X \in S^{[n]}$, $h(X) = g_s(x_0)$. We express this last as "on $S^{[n]}$, h depends only on the first coordinate".

PROOF. By induction on m .

Case 1. $m = 0$.

The algebra G will be chosen to simulate a finite number of simpler algebras: G_1 is the $(n, 7)$ -algebra provided by (2) of Lemma 12.53 that guarantees $\min S \geq 2n + 3$.

G_2 is an $(n, 2)$ -algebra. $G_2(X) = 0$ if $h(X) < [\frac{1}{2}x_0]$; otherwise $G_2(X) = 1$, where $[a]$ is Gauss's symbol.

G_3 is an $(n + 1, 3)$ -algebra. $G_3(X) = 0, 1, 2$ respectively if $h(x_0, x_1, \dots, x_{n-1}) =, >, < h(x_0, x_2, \dots, x_n)$ respectively.

G_4 is an $(n + 1, 2)$ -algebra. $G_4(X) = 0$ if on $X^{[n]}$, h depends only on the first coordinates. Otherwise $G_4(X) = 1$.

Let G be an $(n + 1, 100)$ -algebra which simulates G_1, G_2, G_3 , and G_4 .

Let $S = \{s_0, \dots, s_k\}$ be suitable for G . We shall prove that on $S^{[n]}$, h depends on the first coordinates.

1. Since G simulates each G_i , S is homogeneous for each G_i . By an argument totally similar to the proof of (4) of Proposition 12.51, it suffices to show that G_4 is identically zero on $S^{[n+1]}$. Since S is homogeneous for G_4 , it suffices to show that $G_4(s_0, \dots, s_n) = 0$.

2. Let $W = \{m \mid m < [\frac{1}{2}s_0]\}$ if G_2 has constant value 0 on $S^{[n]}$, i.e., $h(X) < [\frac{1}{2}x_0]$; otherwise let $W = \{m \mid [\frac{1}{2}s_0] \leq m < s_0\}$. Then W has at most $[\frac{1}{2}s_0] + 1$ elements. Moreover, if $A \in S^{[n]}$ and $\min A = s_0$, then $h(A) \in W$ since S is homogeneous for G_2 .

3. We shall show $[\frac{1}{2}s_0] + 1 < s_0 - n$. Since $s_0 - [\frac{1}{2}s_0] = [\frac{1}{2}(s_0 + 1)]$, it suffices to show $n + 1 < [\frac{1}{2}(s_0 + 1)]$ or equivalently $n + 2 \leq [\frac{1}{2}(s_0 + 1)]$. This is again equivalent to $n + 2 \leq \frac{1}{2}(s_0 + 1)$, i.e., $2n + 3 \leq s_0$. This follows from S being suitable for G_1 .

4. For $1 \leq i \leq s_0 + 1 - n$, let $A_i = \{s_0, s_i, \dots, s_{i+n-2}\}$. Then $A_i \in S^{[n]}$. Let $w_i = h(A_i)$; then $w_i \in W$. By the inequality of 3 and the pigeonhole principle, there are i, j with $1 \leq i < j \leq s_0 + 1 - n$ with $w_i = w_j$.

5. Since G simulates G_3 , G_3 takes some constant value on $S^{[n+1]}$. We claim this value is 0. If, for example, the value were 1, then $w_1 > w_2 > \dots > w_{s_0+1-n}$, contrary to the conclusion of 4.

6. Since $s_0 \geq 2n + 3$, s_{2n+2} is defined. We claim that if $Y \in \{s_0, \dots, s_n\}^{[n]}$ and $\min Y = s_0$, then $h(Y) = h(s_0, s_{n+1}, \dots, s_{2n-1})$.

To see this, let $\{t_0, \dots, t_{2n-2}\} = Y \cup \{s_{n+1}, \dots, s_{2n-1}\}$. Using the fact that G_3 is identically zero on $S^{[n+1]}$, we get

$$\begin{aligned} h(Y) &= h(t_0, t_1, \dots, t_{n-1}) = h(t_0, t_2, \dots, t_n) \\ &= h(t_0, t_i, t_{i+1}, \dots, t_{i+n-2}) = \dots = h(t_0, t_n, \dots, t_{2n-2}) \\ &= h(s_0, s_{n+1}, \dots, s_{2n-1}). \end{aligned}$$

7. Now there is precisely one $Y \in \{s_0, \dots, s_n\}^{[n]}$ with $\min Y \neq s_0$. Hence 6 implies $G_4(s_0, \dots, s_n) = 0$. This completes the proof of Case 1.

Case 2. $m = k + 1$.

Let $h: \mathbb{N}^{[n]} \rightarrow \mathbb{N}$ such that $h(X) < E_m(x_0)$. We define an auxiliary function $g: \mathbb{N}^{[n+1]} \rightarrow \mathbb{N}$ such that $g(Y) < E_k(y_0)$.

Let $Y = \{y_0, \dots, y_n\}$. If $h(\{y_0, \dots, y_{n-1}\}) = h(\{y_0, y_2, \dots, y_n\})$, set $g(Y) = 0$. Otherwise, let $g(Y)$ be the largest j at which the binary expansions of the two just stated values of h differ. Clearly $g(Y) < E_k(y_0)$.

As before G will be chosen so as to simulate a finite number of simpler algebras:

G_1 is the $(n, 7)$ -algebra provided by (2) of Lemma 12.53 which guarantees $\min S \geq 2n + 3$.

G_2 is the $(n + m + 1, 10^{2m})$ -algebra obtained by applying the induction hypothesis to the function g just introduced.

G_3 is an $(n + 1, 3)$ -algebra. $G_3(y_0, \dots, y_n) = 0, 1, 2$ respectively if $h(y_0, \dots, y_{n-1})$ is $=, >, < h(y_0, y_2, \dots, y_n)$ respectively.

G_4 is an $(n + 1, 2)$ -algebra. $G_4(Y) = 0$ iff h depends only on its first coordinates on $Y^{[n]}$; otherwise $G_4(Y) = 1$.

G is an $(n + m + 1, 10^{2m+2})$ -algebra which simulates G_1, G_2, G_3 , and G_4 .

Let S be suitable for G . We show that the constant value taken by G_3 on $S^{[n+1]}$ is 0. It will then follow, exactly as in Case 1, that the value of $h(X)$ for $X \in S^{[n]}$ depends only on $\min X$.

Suppose then that G_3 takes the constant value 1. (The case when G_3 's constant value is 2 is totally analogous.) We shall derive a contradiction.

Let $S = \{s_0, \dots, s_r\}$. Since G simulates G_1 , $r \geq n + 1$. For $1 \leq i \leq 3$, let $z_i = h(s_0, s_i, \dots, s_{n-2+i})$. Since $G_3 = 1$ on $S^{[n+1]}$, $z_1 > z_2 > z_3$.

Let $j_0 = g(s_0, \dots, s_n)$, $j_1 = g(s_0, s_2, \dots, s_{n+1})$. Since G simulates G_2 , $j_0 = j_1 = j$, say. By the definition of g , the j th digit is the highest order

binary digit at which z_1, z_2 differ. Since $z_1 > z_2$, z_2 's j th digit is a 0. On the other hand, the j th digit is the highest order binary digit at which z_2, z_3 differ. Since $z_2 > z_3$, z_2 's j th digit must be 1. This gives the desired contradiction.

LEMMA 12.56. *Let $g: \mathbb{N}^{[n]} \rightarrow \mathbb{N}$ satisfying $g(x_0, \dots, x_{n-1}) \leq x_0$. Then there an $(n+1, 10^4)$ -algebra G such that if S is suitable for G :*

- (1) *On $S^{[n]}$, g depends only on its first coordinates.*
- (2) *If $X, Y \in S^{[n]}$ and $\min X < \min Y$, then $g(X) \leq g(Y)$.*

PROOF. G is chosen to simulate a finite number of simpler algebras:

G_1 is an $(n, 2)$ -algebra. $G_1(X) = 0$ if $g(X) < \min X$, otherwise $G_1(X) = 1$.

Define $g': \mathbb{N}^{[n]} \rightarrow \mathbb{N}$ as follows: if $g(X) < \min X$, $g'(X) = g(X)$. Otherwise, $g'(X) = 0$. Let G_2 be the $(n+1, 100)$ -algebra obtained by applying Lemma 12.55 to g' ($m = 0$ in that lemma).

G_3 is an $(n+1, 2)$ -algebra. $G_3(X) = 0$ if $g(x_1, \dots, x_n) < [\frac{1}{2}x_0]$; otherwise $G_3(X) = 1$.

G_4 is an $(n+1, 2)$ -algebra. $G_4(x_0, \dots, x_n) = 0$ if $g(x_0, \dots, x_{n-1}) \leq g(x_1, \dots, x_n)$. Otherwise $G_4(x_0, \dots, x_n) = 1$.

G_5 is the $(n, 7)$ -algebra provided by (2) of Lemma 12.53. It insures that any S suitable for G_5 satisfies $\min S \geq 2n+3$.

Let G be an $(n+1, 10^4)$ -algebra that simulates G_1, \dots, G_5 . Let S be suitable for G . We show that on S , g satisfies (1) and (2) of the lemma.

First suppose that on $S^{[n]}$, G_1 takes the constant value 1. Then on $S^{[n]}$, $g(X) = \min X$ and (1) and (2) are clear. So from now on we may assume that on $S^{[n]}$, G_1 takes the constant value 0. Hence $g = g'$ on $S^{[n]}$, so claim (1) is clear since G simulates G_2 .

Let $S = \{s_0, \dots, s_m\}$. For $0 \leq i \leq m-n+1$, let $z_i = g(s_i, \dots, s_{i+n-1})$. If G_4 takes the constant value 0 on $S^{[n+1]}$, then $z_0 \leq z_1 \leq z_2 \leq \dots \leq z_{m-n+1}$, and claim (2) is clear. So suppose, towards a contradiction, that G_4 takes the constant value 1 on $S^{[n+1]}$ so that

$$s_0 > z_0 > z_1 > \dots > z_{m-n+1}.$$

Let $W = \{i \mid i < [\frac{1}{2}s_0]\}$ if G_3 has constant value 0; otherwise let $W = \{i \mid [\frac{1}{2}s_0] \leq i < s_0\}$. By the definition of G_3 , we have $z_i \in W$ for $1 \leq i \leq m-n+1$. But for $i < j$, $z_i > z_j$; moreover since $m \geq s_0 - 1$ and $s_0 \geq 2n+3$, we have $|W| < m-n+1$. (Cf. Lemma 12.55, Case 1, Claim 3.) But this contradicts the pigeonhole principle.

In Definition 12.19, we defined $\{\alpha\}(n)$ only when α is a limit ordinal. Now we extend the definition of $\{\alpha\}(n)$ for all ordinals less than ε_0 . We assume that the ordinals are $< \varepsilon_0$ in this section without explicit mention.

DEFINITION 12.57. (1) In addition to (2) of Definition 12.19, $\{\alpha\}(n)$ is defined as follows:

$$\{\alpha + 1\}(n) = \alpha \quad \text{and} \quad \{0\}(n) = 0.$$

(2) Let $\alpha < \beta$. Then $\beta \rightarrow_{\pi} \alpha$ if for some sequence of ordinals $\gamma_0, \dots, \gamma_r$ we have $\gamma_0 = \beta$, $\gamma_{i+1} = \{\gamma_i\}(n)$ for $0 \leq i < r$, and $\gamma_r = \alpha$.

PROPOSITION 12.58. (1) If $\alpha > 0$, then $\alpha \rightarrow_{\pi} 0$.

(2) Let $n \geq 1$. If $\alpha_1 \rightarrow_{\pi} \alpha_2$, then $\omega^{\alpha_1} \rightarrow_{\pi} \omega^{\alpha_2}$.

(3) If α is a limit ordinal, $i < j < \omega$, and $0 < n < \omega$, then $\{\alpha\}(j) \rightarrow_{\pi} \{\alpha\}(i)$.

(4) If $n > i$ and $\alpha \rightarrow_{\pi} \beta$, then $\alpha \rightarrow_{\pi} \beta$.

(5) If $\alpha \rightarrow_{\pi} \beta$, then $h_{\beta}(n) \leq h_{\alpha}(n)$.

PROOF. (1) is obvious since $\{\alpha\}(n) < \alpha$ for $\alpha > 0$.

(2) We may assume $\alpha_2 = \{\alpha_1\}(n)$. If α_1 is a limit ordinal, then $\{\omega^{\alpha_1}\}(n) = \omega^{\{\alpha_1\}(n)} = \omega^{\alpha_2}$. If $\alpha_1 = \beta + 1$, then $\alpha_2 = \beta$ and $\{\omega^{\alpha_1}\}(n) = \omega^{\alpha_2} \cdot n$. We can easily prove $\omega^{\alpha_1} \rightarrow_{\pi} \omega^{\alpha_2}$ reducing $\omega^{\alpha_2} \cdot (n-1)$ to 0 by successive application of (1).

(3) It suffices to show the case $i = j-1$. Since $\alpha \rightarrow_{\pi} \beta$ implies $\gamma + \alpha \rightarrow_{\pi} \gamma + \beta$, we may assume that α is of the form ω^{β} . If $\alpha = \omega$, then $\{\alpha\}(j) = \{\alpha\}(i) + 1$ and $\{\{\alpha\}(j)\}(n) = \{\alpha\}(i)$. If $\beta = \beta_0 + 1$ and $\beta_0 \neq 0$, then $\{\alpha\}(j) = \omega^{\beta_0}(j-1) + \omega^{\beta_0}$ and $\{\alpha\}(i) = \omega^{\beta_0}(j-1)$. Then $\{\alpha\}(j) \rightarrow_{\pi} \{\alpha\}(i)$ is obvious because of (1). If β is a limit ordinal, then $\{\beta\}(j) \rightarrow_{\pi} \{\beta\}(i)$. Then $\{\omega^{\beta}\}(j) \rightarrow_{\pi} \{\omega^{\beta}\}(i)$ because of (2).

(4) We may assume $\beta = \{\alpha\}(i)$. Then by (3) $\{\alpha\}(n) \rightarrow_{\pi} \{\alpha\}(i) = \beta$ and $\alpha \rightarrow_{\pi} \beta$.

(5) We may assume $\beta = \{\alpha\}(n)$. Then $h_{\beta}(n) \leq h_{\alpha}(n)$ is obvious if α is a limit ordinal. It is also obvious if α is a successor ordinal.

DEFINITION 12.59. For $n, x \in \mathbb{N}$, we define

$$T(\omega_n, x) = \{\alpha \mid \omega_n \rightarrow_{\pi} \alpha\}.$$

PROPOSITION 12.60. (1) $T(\omega_n, x)$ has cardinality at most

$$\left. \begin{matrix} m \\ m \dots m \end{matrix} \right\} n \text{ (} n \text{ } m\text{'s; } m = x+1)$$

(2) If $\alpha \in T(\omega_n, x)$ and $\alpha = \omega^{\beta_1} \cdot k_1 + \dots + \omega^{\beta_l} \cdot k_l$ ($\beta_1 < \dots < \beta_l$) is its Cantor normal form, then all coefficients $k_1, \dots, k_l \leq x$.

PROOF. We proceed by induction on n . The case $n = 0$ is trivial. For $n = n_0 + 1$, define $M = \{\dot{\alpha} \mid \text{all exponents in the Cantor normal form for } \alpha$

lie in $T(\omega_n, x)$ and all coefficient in the Cantor normal form for $\alpha \leq x$. It is easily checked that if $\alpha \in M$, so is $\{\alpha\}(x)$, and that $\{\omega_n\}(x)$ lies in M . Whence $T(\omega_n, x) \subseteq M$. So

$$|T(\omega_n, x)| \leq |M| \leq (x+1)^{|T(\omega_n, x)|}.$$

(2) is also clear from $T(\omega_n, x) \subseteq M$.

DEFINITION 12.61. For $m, n \in \mathbb{N}$, $E(m, n)$ is defined by $E(m, 0) = 1$ and $E(m, n+1) = m^{E(m, n)}$. Therefore Proposition 12.60 implies $|T(\omega_n, x)| \leq E(m, n)$, where $m = x+1$.

We need an upperbound for $|T(\omega_n, x)|$ in the form of $E_k(x)$. In their paper, Ketonen and Soloray proved that $|T(\omega_n, x)| \leq E_{n-1}(x^6)$. We use the following trivial estimate.

PROPOSITION 12.62. For $x \geq 1$, $|T(\omega_n, x)| \leq E_{2n}(x)$.

PROOF. It suffices to show $E(m, n) \leq E_{2n}(x)$, where $m = x+1$. Obviously $(1+n) \leq 2^n$. So $2(n+1) \leq 2 \cdot 2^n \leq 2^{n+1}$ and $2n \leq 2^n$. Therefore $n \cdot 2^n \leq 2^{2n} \leq 2^{2^n}$. Now we prove $E(m, n) \leq E_{2n}(x)$ by induction on n . The case $n = 0$ is obvious. The case $n = k+1$ is proved as follows.

$$\begin{aligned} \log_2 E(m, k+1) &= E(m, k) \log_2 m \leq x E_{2k}(x) \\ &\leq E_{2k-1}(x) \cdot E_{2k}(x) \\ &\leq 2^{E_{2k}(x)} = E_{2k+1}(x). \end{aligned}$$

DEFINITION 12.63. Let $g: \mathbb{N}^{[n]} \rightarrow \varepsilon_0$. Then g is weakly controlled by an algebra G if whenever S is suitable for G . On $S^{[n]}$, g depends only on its first coordinate (i.e., if $X, Y \in S^{[n]}$ and $\min X = \min Y$, then $g(X) = g(Y)$). If g is weakly controlled by G , and S is suitable for G , then we define a function g_s from a subset of S into ε_0 by putting $g_s(x_0) = g(x_0, \dots, x_{i-1})$.

We say that g is controlled by G if g is weakly controlled by g and if whenever S is suitable for G , and $x_0, x_1 \in S$ are such that $x_0 < x_1$ and $g_s(x_0), g_s(x_1)$ are defined, then $g_s(x_0) \leq g_s(x_1)$.

As is remarked before, the exact numbers n and c of (n, c) -algebra is not necessary as far as they are primitive recursively calculated. In the following we simply skip c by saying an adequate n -algebra when c can be primitive recursively calculated.

LEMMA 12.64. Let $g: \mathbb{N}^{[n]} \rightarrow \varepsilon_0$. Suppose that $g(x_0, \dots, x_{n-1}) \in T(\omega_k, x_0)$ for all $x \in \mathbb{N}^{[n]}$. Then g is weakly controlled by an $n+2k+1$ -algebra.

PROOF. The case $k = 0$ is trivial. So assume $k \geq 1$. By Lemma 12.55 and

Proposition 12.62, we can choose an adequate $n + 2k + 1$ -algebra that insures that $g(x_0, \dots, x_{n-1})$ depends only on x_0 , provided $x_0 \geq 1$. By (1) of Lemma 12.53, we can find an adequate $n + 2k + 1$ -algebra G that simulate the algebra just mentioned and such that if S is suitable for G , $\min S \geq 1$. This G weakly controls g .

LEMMA 12.65. *Let $k \geq 1$. Let $g: \mathbb{N}^{[n]} \rightarrow \varepsilon_0$ satisfy $g(x_0, \dots, x_{n-1}) \in T(\omega_k, x_0)$. Then g can be controlled by an adequate $n + 2k + 1$ -algebra.*

PROOF. The proof is by induction on k . The case $k = 1$ follows from Lemma 12.56. So assume $k \geq 2$ and fix g as in the statement of the lemma.

Let G_0 be an adequate $n + 2k + 1$ -algebra which weakly controls g (cf. Lemma 12.64).

Let G_1 be an $(n + 1, 2)$ -algebra. $G_1(x_0, \dots, x_n) = 0$ if $g(x_0, \dots, x_{n-1}) \leq g(x_1, \dots, x_n)$. Otherwise $G_1(x_0, \dots, x_n) = 1$.

We define an auxiliary function $h: \mathbb{N}^{[n+1]} \rightarrow \varepsilon_0$ as follows. If $g(x_0, \dots, x_{n-1}) \leq g(x_1, \dots, x_n)$, $h(x) = 0$. If $g(x_0, \dots, x_{n-1}) > g(x_1, \dots, x_n)$, write $g(x_0, \dots, x_{n-1})$ and $g(x_1, \dots, x_n)$ in the Cantor normal form $\omega^{\alpha_1} n_1 + \dots + \omega^{\alpha_k} n_k$ and $h(x)$ is the largest α_i at which $g(x_0, \dots, x_{n-1})$ differs from $g(x_1, \dots, x_n)$, i.e.,

$$g(x_0, \dots, x_{n-1}) = \omega^{\alpha_1} n_1 + \dots + \omega^{\alpha_{i-1}} n_{i-1} + \omega^{\alpha_i} n_i + \dots$$

and

$$g(x_1, \dots, x_n) = \omega^{\alpha_1} n_1 + \dots + \omega^{\alpha_{i-1}} n_{i-1} + \omega^{\beta_i} m_i + \dots$$

and $\alpha_i > \beta_i$ or $\alpha_i = \beta_i \wedge n_i > m_i$. Let $r = k - 1$. Note that $h(x_0, \dots, x_n) \in T(\omega_r, x_0)$. Let G_2 be an adequate $n + 2k + 1$ -algebra that controls h . (This exists by our induction hypothesis.)

Define an auxiliary function $h': \mathbb{N}^{[n+1]} \rightarrow \mathbb{N}$ as follows: $h'(x)$ is the coefficient of $\omega^{h(x)}$ in the Cantor normal form of $g(x_0, \dots, x_{n-1})$. (Set $h'(x) = 0$ if $g(x_0, \dots, x_{n-1}) \leq g(x_1, \dots, x_n)$.) Since $g(x_0, \dots, x_{n-1}) \in T(\omega_k, x_0)$, $h'(x) \leq x_0$. Let G_3 be an adequate $n + 3$ -algebra that controls h' (cf. Lemma 12.56).

Let G be an adequate $n + 2k + 1$ -algebra which simulates G_0, \dots, G_3 . We shall show that G controls g .

Let $S = \{s_0, \dots, s_m\}$ be suitable for G . Since G simulates G_3 , $m \geq n + 3$. Let $S' = \{s_i \mid i \leq m - n + 1\}$. Let $g_s: S' \rightarrow \varepsilon_0$ be given by $g_s(s_i) = g(s_i, \dots, s_{i+n-1})$. Since G simulates G_0 , if $X \in S^{[n]}$, $g(X) = g_s(x_0)$.

Since G simulates G_1 , we know that G_1 takes a constant value $v \leq 1$ on $S^{[n+1]}$. We will be done if $v = 0$. Towards a contradiction, assume $v = 1$, i.e., if $x_0 < x_1$, $x_0, x_1 \in S'$, then $g_s(x_0) > g_s(x_1)$. Moreover there is an ordinal $\eta_s(x_0) (= h(x_0, x_1, \dots))$ with coefficient $m_s(x_0) (= h'(x_0, x_1, \dots))$ such that the Cantor normal forms of $g_s(x_0)$ and $g_s(x_1)$ agree at exponents above

$\eta_s(x_0)$, but not at $\eta_s(x_0)$. (The fact that $\eta_s(x_0)$ does not depend on x_1 comes from G simulating G_2 which weakly controls h . Similarly since G simulates G_3 , $m_s(x_0)$ does not depend on x_1 .)

Since G simulates G_2 and G_3 which control h and h' respectively, the following is true. If $x_0, x_1 \in S'$ with $x_0 < x_1$, then $\eta_s(x_0) \leq \eta_s(x_1)$ and $m_s(x_0) \leq m_s(x_1)$.

Since $m \geq n + 2$, $\{s_0, s_1, s_2\} \subseteq S'$. Now $g_s(s_0)$ and $g_s(s_1)$ agree at exponents above $\eta_s(s_0)$ as do $g_s(s_0)$ and $g_s(s_2)$. Hence $g_s(s_1)$ and $g_s(s_2)$ agree at exponents above $\eta_s(s_0)$; i.e., $\eta_s(s_1) \leq \eta_s(s_0)$. Also, by the preceding paragraph, $\eta_s(s_0) \leq \eta_s(s_1)$; so $\eta_s(s_0) = \eta_s(s_1)$. But then $g_s(s_0) > g_s(s_1)$ implies $m_s(s_1) < m_s(s_0)$, contradicting the observation of the preceding paragraph that $m_s(s_0) \leq m_s(s_1)$.

DEFINITION 12.66. An algebra $G: \mathbb{N}^{[n]} \rightarrow C$ captures a function $f: \mathbb{N} \rightarrow \mathbb{N}$ if whenever S is suitable for G , and $x < y$ are elements of S , then $f(x) \leq y$.

THEOREM 12.67. Let $n \geq 1$. Then h_{ω_n} can be captured by an adequate $2n+3$ -algebra G .

PROOF. Let G_0 be a $(2,2)$ -algebra. $G_0(x_0, x_1) = 0$ if $x_1 \geq h_{\omega_n}(x_0)$; otherwise $G_0(x_0, x_1) = 1$.

Let G_1 be a $(2,5)$ -algebra that simulates G_0 and such that any S suitable for G_1 has $\min S \geq 3$.

Define an auxiliary function $f: \mathbb{N}^{[2]} \rightarrow \varepsilon_0$ as follows: If there is a $\xi \in T(\omega_n, x_0)$ such that $h_\xi(x_0) \geq x_1$, let $f(x_0, x_1)$ be the least such. Otherwise $f(x_0, x_1) = 0$. Let G_2 be an adequate $2n+3$ -algebra that controls f .

Let G be an adequate $2n+3$ -algebra which simulates G_1 and G_2 . We show that G captures h_{ω_n} . Let $S = \{s_0, \dots, s_m\}$ be suitable for G . Since S is large, $m \geq s_0 - 1$. Let v be the constant value taken by G_0 on $S^{[2]}$. We have to show $v = 0$. Towards a contradiction, assume $v = 1$.

Let $\{x_0, x_1\} \in S^{[2]}$. Since $G_0(x_0, x_1) = 1$, $x_1 < h_{\omega_n}(x_0)$. Let $\xi_0 = \{\omega_n\}(x_0)$. Then $x_1 < h_{\xi_0}(x_0)$ and $\xi_0 \in T(\omega_n, x_0)$. It follows that if $\xi_1 = f(x_0, x_1)$, then ξ_1 is the least ordinal in $T(\omega_n, x_0)$ such that $x_1 \leq h_{\xi_1}(x_0)$.

Now ξ_1 cannot be a limit ordinal. For then, letting $\xi_2 = \{\xi_1\}(x_0)$, we have $\xi_2 < \xi_1$, $\xi_2 \in T(\omega_n, x_0)$ and $x_1 \leq h_{\xi_2}(x_0) = h_{\xi_1}(x_0)$. Also ξ_1 cannot equal 0.

Thus $\xi_1 = f(x_0, x_1)$ has the form $\delta + 1$. Note next that since G simulates G_2 and G_2 controls f , on $S^{[2]}$, f depends only on its first coordinates. Say $f(x_0, x_1) = \delta(x_0) + 1$ (for $\{x_0, x_1\} \in S^{[2]}$). Moreover if $\{x_0, x_1\} \in S^{[2]}$ and $\delta(x_1)$ is defined, then $\delta(x_0) \leq \delta(x_1)$. Finally, by the minimal choice of $f(x_0, x_1)$ and the fact that $f(x_0, x_1) \xrightarrow{x_1} \delta(x_0)$, we have $\delta(x_0) \in T(\omega_n, x_0)$ and $x_1 > h_{\delta(x_0)}(x_0)$.

Let $0 \leq i < s_0 - 1$. We claim $s_{i+1} > h_{\delta(s_0)}(s_i)$. By the preceding paragraph, $s_{i+1} > h_{\delta(s_i)}(s_i)$. Also $\delta(s_0) \leq \delta(s_i)$. If $\delta(s_0) = \delta(s_i)$, our claim is clear. So suppose $\delta(s_i) > \delta(s_0)$. Now $\omega_n \xrightarrow{s_0} \delta(s_0)$. Hence by (4) of Proposition 12.58

$\omega_n \xrightarrow{s_i} \delta(s_0)$. But then by (5) of Proposition 12.58 $h_{\delta(s_0)}(s_i) \leq h_{\delta(s_1)}(s_i) < s_{i+1}$, establishing our claim.

Now we have

$$h_{\delta(s_0)+1}(s_0) = h_{\delta(s_0)}(s_0 + 1) \leq h_{\delta(s_1)}(s_1) < s_2.$$

But $\delta(s_0) + 1 = f(s_0, s_2)$ and this contradicts the definition of f .

THEOREM 12.68. *Let $n \geq 1$. Then there is an adequate $2n+3$ -algebra G such that if S is suitable for G , $\max S > h_{\omega_n}(n)$. Hence there exists a primitive recursive function $p(n)$ such that*

$$h_{\omega_n}(n) < \sigma(2n+3, p(n)).$$

*Therefore every provably recursive function in **PA** is majorized by $\sigma(n, n)$.*

PROOF. Let G_0 be an adequate $2n+3$ -algebra that captures h_{ω_n} . Let G_1 be an $(n+2, 7)$ -algebra that insures that if S is suitable for G_1 , $\min S \geq 2n+3$. There exist a primitive recursive function $p(n)$ and an $(2n+3, p(n))$ -algebra G that simulates G_0 and G_1 . But then, if S is suitable for G ,

$$\max S \geq s_2 \geq s_1 \geq h_{\omega_n}(s_0) \geq h_{\omega_n}(n).$$

Hence if we take the restriction of G to $N^{[2n+3]}$, where $N = h_{\omega_n}(n)$, then no subset of N is suitable for G . Hence $N < \sigma(2n+3, p(n))$. Now the last statement of the lemma follows from Proposition 12.49.

We need a lower bound of m satisfying $m \rightarrow (k+1)_2^k$. J. Quinsey noted in his disertation that $2k+6 \not\rightarrow (k+1)_2^k$. But the following trivial estimate suffices for our purpose.

PROPOSITION 12.69. $2k \not\rightarrow (k+1)_2^k$.

PROOF. Let $M = \{0, 1, 2, \dots, 2k-1\}$. Define $G: M^{[k]} \rightarrow 2$ as follows. Let $X = \{x_0, \dots, x_{k-1}\} \in M^{[k]}$. $G(x_0, \dots, x_{k-1}) = 0$ if $x_0 + \dots + x_{k-1}$ is even. $G(x_0, \dots, x_{k-1}) = 1$ otherwise. Suppose that $S \in M^{[k]}$ is homogeneous and $|S| = k+1$. Since there are only k many even numbers and only k many odd numbers in M , there exist an even number x and an odd number y in S . Then

$$G(S - \{x\}) \neq G(S - \{y\})$$

contradicting the homogeneity of S .

THEOREM 12.70. *If $m \rightarrow (e+1)_c^e$ and $N \rightarrow (\text{large})_3^m$, then $N \rightarrow (\text{large})_c^e$. Hence every provably recursive function in **PA** is majorized by $\sigma(n, 3)$.*

PROOF. We can suppose that $e, c \geq 2$. By Proposition 12.69, $m \geq 2e + 1$. Let $F: N^{[e]} \rightarrow c$ be given. Let $k = m - e - 1$ and $t = 2m$. By Proposition 12.69 we can choose $g: t^{[m]} \rightarrow 2$ with no homogeneous set of cardinality $m + 1$. Define $f: N^{[e+1]} \rightarrow 2$ by

$$f(x_0, \dots, x_e) = \begin{cases} 1 & \text{if } x_0, \dots, x_e \text{ is homogeneous for } F, \\ 0 & \text{otherwise.} \end{cases}$$

Define $G: N^{[m]} \rightarrow 3$ as follows. Let $X = \{x_0, \dots, x_{m-1}\} \in N^{[m]}$. Let i be the least i such that $x_i \geq t$, if there exists such, and m otherwise. Let

$$G(x_0, \dots, x_{m-1}) = \begin{cases} g(x_0, \dots, x_{m-1}) & \text{if } i = m, \\ 2 & \text{if } i = 1 \text{ or } m-1, \\ \frac{1}{2}(1 - (-1)^i) & \text{if } 1 < i < m-1, \\ f(x_0 - k, \dots, x_e - k) & \text{if } i = 0. \end{cases}$$

Let $S \subseteq N$ be suitable for G . Then $|S| \geq \min S$ and $|S| \geq m + 1$. We show that $\min S \geq t$. Toward a contradiction suppose $\min S < t$. Let s_0, \dots, s_m be the first $m + 1$ elements of S and $S_0 = \{s_0, \dots, s_m\}$.

Case 1. $s_m < t$.

In this case $G(X) = g(X)$ for $X \in S_0^{[m]}$. This is a contradiction since S_0 is homogeneous for G and g has no homogeneous set of cardinality $m + 1$.

Case 2. $S_i < t \leq S_{i+1}$ for some i with $0 \leq i \leq m - 1$.

In this case

$$G(S - \{s_i\}) \neq G(S - \{s_{i+1}\})$$

contradicting the homogeneity of S for G .

Therefore we have $\min S \geq t$ and for every $X \in S^{[m]}$, $G(x_0, \dots, x_{m-1}) = f(x_0 - k, \dots, x_e - k)$.

Now let $S = \{s_0, \dots, s_{a-1}\}$. Then $a \geq t = 2m$. Let $Y = \{s_0, \dots, s_{m-1}\}$ be the first m elements of S . Define $H: Y^{[e]} \rightarrow C$ by

$$H(y_0, \dots, y_{e-1}) = F(y_0 - k, \dots, y_{e-1} - k).$$

Since $m \rightarrow (e+1)_c^e$, there exists $Z \subseteq Y$ which is homogeneous for H and has the cardinality $e + 1$. Now the cardinality of $Z \cup \{s_m, \dots, s_{m+k-1}\}$ is m and $G(Z \cup \{s_m, \dots, s_{m+k-1}\}) = 1$. Since S is suitable for G , G has the constant value 1 on $[S]^m$. Since $a \geq s_0$, let $X' = \{s_0 - k, \dots, s_{s_0-k-1} - k\}$.

Then

$$|X'| \geq \min X' \geq 2m - k \geq e + 1.$$

We claim that X' is homogeneous for F . For if $\{x'_0 - k, \dots, x'_e - k\}$ is any subset of cardinality $e + 1$, then the cardinality of $\{x'_0, \dots, x'_e\} \cup \{s_{s_0-k}, \dots, s_{s_0-1}\}$ is m and $G(x'_0, \dots, x'_e, s_{s_0-k}, \dots, s_{s_0-1}) = 1$. Therefore $\{x'_0, \dots, x'_e\}$ is homogeneous for F .

Now let $p(e, c)$ be a primitive recursive function such that $p(e, c) \rightarrow (e + 1)^c$. Then we have $\sigma(e, c) \leq \sigma(p(e, c), 3)$ and $\sigma(n, n) \leq \sigma(p(n, n), 3)$. Therefore from Proposition 12.49 follows that every provably recursive function in **PA** is majorized by $\sigma(n, 3)$.

H. Friedman proved that Kruskal's theorem on finite trees is not provable in a certain second order extension of Peano's arithmetic. In the following, we prove a weaker version of Friedman's theorem.

DEFINITION 12.71. (1) A *finite tree* is a finite partially ordered set T satisfying the following conditions:

- (i) It has the minimum called its root.
- (ii) For every $b \in T$, $\{a \in T; a \leq b\}$ is linearly ordered by \leq , where \leq is the order of T .

(2) Let T_1 and T_2 be finite trees. A function $f: T_1 \rightarrow T_2$ is an embedding iff f is one-to-one, order-preserving and satisfies the equation

$$f(a \wedge b) = f(a) \wedge f(b) \quad \text{for every } a, b \in T_1,$$

where $a \wedge b$ denotes the greatest lower bound of a and b . We denote $T_1 \leq T_2$ iff there exists an embedding $f: T_1 \rightarrow T_2$.

(3) The set of all finite trees is denoted by \mathcal{T} . A mapping $o: \mathcal{T} \rightarrow \varepsilon_0$ is defined as follows, where ε_0 is the set of all ordinal, less than ε_0 as usual.

If T consists of its root alone, then $o(T) = 0$. If T has some member other than its root, let T^1, \dots, T^n be all component of $T - \{\text{root}(T)\}$, where $\text{root}(T)$ is the root of T . Without loss of generality we assume that $o(T^1), \dots, o(T^n)$ have been assigned and $o(T^1) \geq o(T^2) \geq \dots \geq o(T^n)$. Then $o(T)$ is defined by the following equalities

$$o(T) = \begin{cases} \alpha & \text{if } n = 1, \\ \alpha + \beta & \text{if } n = 2, \\ \omega^\alpha & \text{if } n \geq 3, \end{cases}$$

where $\alpha = o(T^1)$ and $\beta = o(T^2)$.

DEFINITION 12.72. We define $\tilde{c}(\alpha)$ to be the number of symbols to

represent α in a canonical form, namely, $\bar{c}(0) = 1$, $\bar{c}(\omega^\alpha) = \bar{c}(\alpha) + 1$ and $\bar{c}(\alpha + \beta) = \bar{c}(\alpha) + \bar{c}(\beta) + 1$.

LEMMA 12.73. (1) For every $\alpha < \varepsilon_0$, there exists a tree $T \in \mathcal{T}$ such that $o(T) = \alpha$ and $|T| \leq 3\bar{c}(\alpha)$.

(2) Let $T \in \mathcal{T}$ and $c \in T$. We define $T^c = \{d \in T \mid d \geq c\}$. For every $c, d \in T$, $c \leq d \rightarrow o(T^c) \geq o(T^d)$.

(3) Let $T_1, T_2 \in \mathcal{T}$ and $f: T_1 \rightarrow T_2$ be an embedding. Then for every $a \in T_1$,

$$o(T_1^a) \leq o(T_2^{f(a)}).$$

(4) Let $T_1, T_2 \in \mathcal{T}$. If $T_1 \leq T_2$, then $o(T_1) \leq o(T_2)$.

PROOF. (1) and (2) are obvious. (3) is proved by induction on the number of elements in T_1^a which is denoted by $|T_1^a|$. If $|T_1^a| = 1$, then $o(T_1^a) = 0 \leq o(T_2^{f(a)})$. Now let $|T_1^a| > 1$ and $T_1^{b_1}, \dots, T_1^{b_n}$ be all the components of $T_1^a - \{a\}$. Let c_i be an immediate successor of $f(a)$ satisfying $f(a) \leq c_i \leq f(b_i)$. Then c_i is uniquely determined and by the induction hypothesis we have

$$o(T_1^{b_i}) \leq o(T_2^{f(b_i)}) \leq o(T_2^{c_i}).$$

From this follows $o(T_1^a) \leq o(T_2^{f(a)})$ immediately. (4) follows from (3).

Kruskal proved the following theorem on finite trees.

THEOREM (Kruskal). Let $\langle T_k \mid k \leq \omega \rangle$ be a sequence of finite trees, then there exist $i < j < \omega$ such that $T_i \leq T_j$.

Kruskal's theorem and Lemma 12.73 immediately imply the accessibility of ε_0 . However the statements of Kruskal's theorem and the accessibility of ε_0 are of second order. Using Friedman's device, we will make the first order miniature of Kruskal's theorem.

DEFINITION 12.74. By the finite version of Kruskal's theorem we mean the following statement:

For every natural number n , there exists k such that for every sequence $\langle T_0, \dots, T_k \rangle$ of finite trees satisfying $|T_i| \leq n(i+1)$ there exist $i < j \leq k$ such that $T_i \leq T_j$.

The finite version of Kruskal's theorem denoted by **FKT** is an immediate corollary of Kruskal's theorem itself. In order to see this, suppose that **FKT** were false. Then there exists n such that for every k , there exists $\langle T_0, T_1, \dots, T_k \rangle$ with $|T_i| \leq n \cdot (i+1)$ such that for every $i < j \leq k$

$k, T_i \neq T_j$. We fix one such n and define \mathcal{H} to be the collection of $\langle T_0, T_1, \dots, T_k \rangle$ satisfying $|T_i| \leq n \cdot (i+1)$ for every $i < k$ and $\forall i \forall j (i < j \leq k \supset T_i \neq T_j)$. Then by König's lemma, there exists an infinite sequence T_0, T_1, T_2, \dots such that $\forall i \forall j (i < j \supset T_i \neq T_j)$ which contradicts to Kruskal's theorem.

Remark that **FKT** is of the first order. Our weaker version of Friedman's theorem is the following.

THEOREM 12.75 (H. Friedman). **FKT** is not provable in **PA**.

In order to prove the theorem, we need several preparations.

DEFINITION 12.76. (1) A sequence $\langle \beta_i \mid i < \omega \rangle$ from ε_0 is slow iff $\exists n \forall i (\bar{c}(\beta_i) \leq n \cdot (i+1))$.

(2) **SWO**(ε_0) is the statement that for every n there exists k such that for every sequence $\langle \beta_0, \beta_1, \dots, \beta_k \rangle$ from ε_0 ,

$$\forall i \leq k (\bar{c}(\beta_i) \leq n \cdot (i+1)) \supset \neg(\beta_0 > \beta_1 > \dots > \beta_k).$$

SWO(ε_0) is a first order statement.

LEMMA 12.77. **FKT** \rightarrow **SWO**(ε_0) is provable in **PA**.

PROOF. Is immediate from (1) of Lemma 12.73.

DEFINITION 12.78. **PRWO**(ε_0) is the statement that there are no primitive recursive strictly descending sequence from ε_0 . **PRWO**(ε_0) is also a first order statement.

LEMMA 12.79. **PRWO**(ε_0) \rightarrow **Cons**(**PA**) is provable in **PA**, where **Cons**(**PA**) is the consistency of **PA**.

PROOF. If there exists (a Gödel number of) a proof p to a contradiction in **PA**, then $f(n) = O(r^n(p))$ is a primitive recursive strictly descending sequence from ε_0 , where r is the Gentzen's reduction and $O(p)$ is the ordinal assigned to p .

LEMMA 12.80. Let $f: \mathbb{N} \rightarrow \mathbb{N}$ be primitive recursive. Then there exists a primitive recursive function $g: \mathbb{N}^2 \rightarrow \omega^\omega$ such that

- (1) $g(n, m) > g(n, m+1)$ if $m < f(n)$,
- (2) $\bar{c}(g(n, m)) \leq \text{constant}(n+m+1)$, where constant means that there exists some constant k such that $\bar{c}(g(n, m)) \leq k \cdot (n+m+1)$ for every n and m .

PROOF. We are going to define $g: \mathbb{N}^2 \rightarrow \omega^k$ for some $k < \omega$, where k depends on f .

Case (1). $f(n) = n + 1$.
Define g by

$$g(n, m) = n + 2 + m.$$

Case (2). Let $g: \mathbb{N}^2 \rightarrow \omega^k$ satisfy the conditions (1) and (2) for f and f' be defined by $f'(n) = f^n(n)$. Then define g' by

$$g'(n, m) = \omega^k \cdot (n - i) + g(f^i(n), m),$$

where $m = f(n) + f^2(n) + \dots + f^i(n) + j$, $i < n$ and $j < f^{i+1}(n)$. g' satisfies the conditions (1) and (2) for f' . For example,

$$\begin{aligned} \bar{c}(g'(n, m)) &\leq \text{constant} \cdot n + \text{constant}(f^i(n) + m + 1) \\ &\leq \text{constant}(n + m + 1). \end{aligned}$$

Case (3). For an arbitrary primitive recursive function f , there exists f_k such that $\forall n (f(n) \leq f_k(\text{constant} + n))$, where f_k is defined in Grzegorzcz hierarchy namely $f_0(n) = n + 1$, $f_{k+1}(n) = f_k^n(n)$. For f_k , there exists $g_k: \mathbb{N}^2 \rightarrow \omega^{k+1}$ satisfying (1) and (2) for f_k . We define g by $g(n, m) = g_k(\text{constant} + n, m)$. Then g satisfies the conditions (1) and (2) for f .

LEMMA 12.81. *For a given primitive recursive strictly descending sequence $\langle \beta_n \mid n \in \mathbb{N} \rangle$ from ε_0 , one can find a slow primitive recursive strictly descending sequence $\langle \alpha_m \mid m \in \mathbb{N} \rangle$.*

PROOF. Let a primitive recursive function $g: \mathbb{N}^2 \rightarrow \omega^\omega$ satisfy the conditions that $g(n, j) > g(n, j+1)$ for every $j < \bar{c}(\beta_{n+1})$ and $\bar{c}(g(n, j)) \leq \text{constant}(n + j + 1)$. Define $\alpha_m = \omega^\omega \cdot \beta_n + g(n, j)$, where $m = \bar{c}(\beta_1) + \bar{c}(\beta_2) + \dots + \bar{c}(\beta_n) + j$, $j < \bar{c}(\beta_{n+1})$. Then we have

$$\begin{aligned} \bar{c}(\alpha_m) &\leq \text{constant} \cdot \bar{c}(\beta_n) + \text{constant}(n + j + 1) \\ &\leq \text{constant}(m + 1). \end{aligned}$$

PROOF OF THEOREM 12.75. Now the theorem follows immediately from Lemmas 12.77, 12.79 and 12.81.

§13. Provable well-orderings

In this section, in order to distinguish between the natural ordering of natural numbers and the order relation on numbers given by the standard ordering of type ε_0 , we denote the latter by $<$ in this section.

A partial function is a number-theoretic function that may not be defined at all arguments.

DEFINITION 13.1. (1) The class of *partial recursive functions* is the class of partial functions generated by the schemata (i)–(vi) for primitive recursive functions (cf. Definition 10.2), and also the schema:

(vii) $f(x_1, \dots, x_n) \approx \mu y [g(x_1, \dots, x_n, y) = 0]$, where g is partial recursive; the right-hand side means the least y such that $\forall z < y (g(x_1, \dots, x_n, z) \text{ is defined and } \neq 0)$ and $g(x_1, \dots, x_n, y) = 0$, if such a y exists, and undefined otherwise; and \approx means that the left-hand side is defined if and only if the right-hand side is, in which case they are equal.

(2) A *general recursive* or *total recursive* or *recursive* function is a partial recursive function which is *total*, i.e., defined at all arguments.

(3) A relation on natural numbers, say R , is called *recursive* if there is a recursive function f which assumes values 0 and 1 only such that $R(x_1, \dots, x_n)$ holds if and only if $f(x_1, \dots, x_n) = 0$.

(4) A Σ_1^0 -formula of the language L is a formula of the form

$$\exists y (\bar{f}(x_1, \dots, x_n, y) = 0),$$

\bar{f} a primitive recursive function symbol. A Π_1^0 -formula is similarly of the form $\forall y (\bar{f}(x_1, \dots, x_n, y) = 0)$, \bar{f} primitive recursive.

It can be shown that any recursive relation R can be represented in **PA** by a Σ_1^0 -formula, i.e., there is a Σ_1^0 -formula $\bar{R}(x_1, \dots, x_n)$ of the language L such that, for all m_1, \dots, m_n :

$$R(m_1, \dots, m_n) \text{ holds} \leftrightarrow \bar{R}(\bar{m}_1, \dots, \bar{m}_n) \text{ is PA-provable.}$$

Also, any recursive relation can be represented in **PA** by a Π_1^0 -formula.

DEFINITION 13.2. Let ε be a new predicate constant. $L(\varepsilon)$ is the language extending L (cf. §12), formed by admitting $\varepsilon(t)$ as an atomic formula for all terms t .

PA(ε) is the system **PA** in the language $L(\varepsilon)$; more precisely, we extend **PA** by admitting as mathematical initial sequents $s = t, \varepsilon(s) \rightarrow \varepsilon(t)$ for all terms s, t and applying the rule ind to all formulas of $L(\varepsilon)$.

DEFINITION 13.3. Let $<\cdot$ be a recursive (infinite) linear ordering of the natural numbers which is actually a well-ordering. (Without loss of generality we may assume that the domain of $<\cdot$ is the set of all natural numbers and the least element with respect to $<\cdot$ is 0.) We use the same symbol $<\cdot$ in order to denote the Σ_1^0 -formula in **PA** which represents the ordering $<\cdot$.

Consider the sequent

$$TI(<\cdot): \quad \forall x (\forall y <\cdot x (\varepsilon(y)) \supset \varepsilon(x)) \rightarrow \varepsilon(a)$$

(cf. the formula $TI(<, F(x))$ of Remark 12.10). If $TI(< \cdot)$ is provable in $\mathbf{PA}(\varepsilon)$, then we say that $< \cdot$ is a *provable well-ordering* of \mathbf{PA} .

The following theorem is proved by analyzing Gentzen's proof of the unprovability of the well-ordering of $<$ (where $<$ was defined at the beginning of this section).

THEOREM 13.4 (Gentzen). *If $< \cdot$ is a provable well-ordering of \mathbf{PA} , then there exists a recursive function which is a $< \cdot - <$ order-preserving map into an initial segment of ε_0 . That is to say, there is a recursive function f such that $a < \cdot b$ if and only if $f(a) < f(b)$, and there is an ordinal $\mu (< \varepsilon_0)$ such that for every a , $f(a) < \bar{\mu}$ (where $\bar{\mu}$ is the Gödel number of μ).*

This section is devoted to Gentzen's proof, and the arithmetization of it, which proves Theorem 13.4.

From now on, let $< \cdot$ be a fixed provable well-ordering of \mathbf{PA} .

13.1) First we define **TJ**-proofs, where **TJ** stands for "transfinite induction". **TJ**-proofs are defined as $\mathbf{PA}(\varepsilon)$ -proofs with some modifications:

- (1) The initial sequents of a **TJ**-proof are those of $\mathbf{PA}(\varepsilon)$, and the following sequents, called **TJ**-initial sequents:

$$\forall x(x < \cdot t \supset \varepsilon(x)) \rightarrow \varepsilon(t)$$

for arbitrary terms t .

- (2) The end-sequent of a **TJ**-proof must be of the form

$$\rightarrow \varepsilon(\bar{m}_1), \dots, \varepsilon(\bar{m}_n),$$

where $\bar{m}_1, \dots, \bar{m}_n$ are numerals.

Let $|m|_{< \cdot}$ be the ordinal denoted by m with respect to $< \cdot$, i.e., the order type of the initial segment of $< \cdot$ determined by m . Then the minimum of $|m_1|_{< \cdot}, \dots, |m_n|_{< \cdot}$ is called the end-number of the **TJ**-proof.

13.2) Since $< \cdot$ is a provable well-ordering of \mathbf{PA} , the sequent $TI(< \cdot)$ (Definition 13.3) is $\mathbf{PA}(\varepsilon)$ -provable, and hence we can obtain in the system formed from $\mathbf{PA}(\varepsilon)$ by adjoining **TJ**-initial sequents, a proof $P(a)$ of $\rightarrow \varepsilon(a)$ (for a free variable a). Note that for each number m , $P(\bar{m})$ is a **TJ**-proof of $\rightarrow \varepsilon(\bar{m})$.

13.3) A **TJ**-proof is called non-critical if one of the reduction steps for \mathbf{PA} (in the proof of Lemma 12.8) which lower the ordinal (i.e., step 2, 3 or 5) applies to it. Otherwise it is called critical.

13.4) We shall assign ordinals (less than ε_0) to **TJ**-proofs and define a reduction for **TJ**-proofs following the reduction method for \mathbf{PA} given in the proof of Lemma 12.8: if a **TJ**-proof is critical, then more manipulation is required. The reduction is defined in such a manner that a **TJ**-proof P

with end-number > 0 is reduced to another with the same end-number if P is not critical and with an arbitrary end-number which is smaller than the original one if P is critical. At the same time the ordinal decreases.

13.5) If we can define an ordinal assignment and a reduction method with the properties stated in 13.4), we can prove:

LEMMA 13.5 (Fundamental Lemma). *For any **TJ**-proof, its end-number is not greater than its ordinal.*

PROOF. By transfinite induction on the ordinal of the proof. Let P be a **TJ**-proof with ordinal μ and end-number σ . We assume as the induction hypothesis that the lemma is true for any **TJ**-proof whose ordinal is less than μ and show that $\sigma \leq \mu$. If P is non-critical then P is reduced to a **TJ**-proof P' with the same end-number σ and an ordinal $\nu < \mu$. By the induction hypothesis $\sigma \leq \nu$, and hence $\sigma \leq \mu$. Now suppose P is critical. If σ were greater than μ , we could reduce P to a **TJ**-proof whose end-number is μ and whose ordinal is less than μ , contradicting the induction hypothesis.

Now let us proceed to the reduction method for **TJ**-proofs.

13.6) The ordinals are assigned to the sequents of the **TJ**-proofs as in §12; the ordinal of a **TJ**-initial sequent is $\bar{7}$, i.e., $\omega^0 + \dots + \omega^0$ (7 times). The lower sequent of a term-replacement inference is assigned the same ordinal as the upper sequent. For convenience, the formula in the succedent of a **TJ**-initial sequent will be considered as a principal formula.

13.7) We can follow the reduction steps given for the consistency proof of **PA** up to Step 4 (in the proof of Lemma 12.8), i.e., until we reach a **TJ**-proof P with the following properties p 1–p 4.

- p 1. The end-piece of P contains no free variable.
- p 2. The end-piece of P contains no induction.
- p 3. The end-piece of P contains no logical initial sequent.
- p 4. If the end-piece of P contains a weakening I , then any inference below I is a weakening.

REMARK. Since the end-piece of a **TJ**-proof is not empty, the end-sequent S' of the proof obtained from P by eliminating weakenings in the end-piece (in Step 4) may be different from the end-sequent of P . In this case we add weakenings below S' so that the end-sequent becomes the same as the end-sequent of P .

13.8) We can easily show the following. Let P be a **TJ**-proof satisfying p 1–p 4. Then P contains at least one logical inference (which must be implicit) or **TJ**-initial sequent. Therefore the end-piece of P contains a principal formula at the boundary or in a **TJ**-initial sequent.

13.9) Let P be a **TJ**-proof satisfying p 1–p 4. By 13.8), the end-piece of P contains a principal formula either at the boundary or in a **TJ**-initial

sequent. We call a formula A in the end-piece of P a principal descendant or a principal **TJ**-descendant, according as A is a descendant of a principal formula at the boundary or a descendant of the principal formula of a **TJ**-initial sequent in the end-piece of P .

Note that a principal **TJ**-descendant in the end-piece of P always occurs in the succedent of a sequent, and has the form $\varepsilon(t)$.

13.10) Let P be a **TJ**-proof satisfying p 1–p 4, and S a sequent in the end-piece of P . If S contains a formula B with a logical symbol, then there exists a formula A in S or in a sequent above S such that A is a principal descendant or a principal **TJ**-descendant.

PROOF. Suppose S contains a formula with a logical symbol. Then S is above the uppermost weakening in the end-piece. The property of sequents, of containing a logical symbol, is preserved upwards, to one of the upper sequents of each inference in the end-piece (but not necessarily beyond a boundary inference), or a **TJ**-initial sequent, when we follow upward the string to which S belongs. Notice that B may not be A , since B may be a descendant of a formula which is “passive” at a boundary inference.

13.11) Let P be a **TJ**-proof satisfying p 1–p 4 and not containing a suitable cut. Then its end-sequent contains a principal **TJ**-descendant.

PROOF. It suffices to prove that the end-sequent of P contains a principal descendant or a principal **TJ**-descendant, since the end-sequent contains no logical symbol. Suppose not. Since the end-piece contains a principal descendant or a principal **TJ**-descendant by 13.8), let us consider the following property (P) of cuts in the end-piece of P : A cut in the end-piece of P is said to have the property (P) if (at least) one of its upper sequents contains such a formula and its lower sequent contains no such formula. Since the end-piece contains such a formula, but the end-sequent does not (by assumption), there must be such a cut. Let I be an uppermost cut with the property (P) in the end-piece of P :

$$I \quad \frac{\Gamma \rightarrow \Delta, D \quad D, \Pi \rightarrow \Lambda}{\Gamma, \Pi \rightarrow \Delta, \Lambda}.$$

Let S_1 and S_2 be the left and right upper sequents of I , respectively. By our assumption one of the cut formulas is a principal descendant or a principal **TJ**-descendant. First suppose D in S_1 has this property. If D contains a logical symbol, then it is a principal descendant. Then also, S_2 contains a formula with a logical symbol (namely D). Therefore, by 13.10), there is a formula A in S_2 or above it such that A is a principal descendant or a principal **TJ**-descendant. If there is no such formula in S_2 , there must be a cut having the property (P) above I , contradicting our

choice of I . If such a formula A is in S_2 , A must be D itself, which contradicts our assumption that P does not contain a suitable cut. Thus D must be of the form $\varepsilon(t)$. Now suppose S_2 contains a logical symbol. Then there exists a principal descendant or a principal **TJ**-descendant either in S_2 or above it. If it is in S_2 , it cannot be D (since D is $\varepsilon(t)$ and is in the left side of a sequent, it cannot be a principal **TJ**-descendant), and so it must also appear in the lower sequent of I , contradicting our assumption that I has the property (P). This means that such a formula is in a sequent above S but not in S itself, contradicting our assumption that I is an uppermost cut with the property (P). Thus S_2 cannot contain a formula with a logical symbol. Since I is an uppermost cut with the property (P), no logical inference at the boundary or **TJ**-initial sequent in the end-piece is above S_2 . Therefore the proof down to S_2 is included in the end-piece and no logical initial sequents or **TJ**-initial sequents occur there and it is impossible that S_2 contains $\varepsilon(t)$, and so D cannot be $\varepsilon(t)$. Hence we have shown that D in S_1 cannot be a principal descendant or principal **TJ**-descendant. Next, suppose that the cut formula in S_2 is a principal descendant or principal **TJ**-descendant. As was seen above, D cannot be a principal **TJ**-descendant: D must contain a logical symbol. Hence there is a principal descendant or a principal **TJ**-descendant either in S_1 or in a sequent above S_1 . If such a formula is not in S_1 , there must be a cut having the property (P) above S_1 , which contradicts our assumption about I . Therefore D in S_1 must have that property, since the lower sequent of I cannot contain such a formula. This again contradicts our assumption that P does not contain a suitable cut.

13.12) Now let P be a critical **TJ**-proof to which the reduction of Lemma 12.8 has been applied as far as possible (i.e., up to Step 4). Then P satisfies p 1–p 4 and does not contain a suitable cut (since it is critical). We define the notion of critical reduction. By 13.11), the end-sequent of P contains a principal **TJ**-descendant, $\varepsilon(\bar{m}_i)$, say, the descendant of a principal formula $\varepsilon(r)$ (where the closed term r denotes the number m_i). Let \bar{m} be any number such that $|\bar{m}|_<$ is less than the end-number of P . Then $\bar{m} < \cdot r$ is a true Σ_1^0 -sentence of \mathbf{PA} , and hence the sequent $\rightarrow \bar{m} < \cdot r$ can be derived from a mathematical initial sequent of \mathbf{PA} (say $\rightarrow F$) by one application of \exists : right. So we replace the **TJ**-initial sequent

$$\forall x (x < \cdot r \supset \varepsilon(x)) \rightarrow \varepsilon(r)$$

in P by an ordinary proof in $\mathbf{PA}(\varepsilon)$:

$$\frac{\frac{\frac{\rightarrow F}{\rightarrow \bar{m} < \cdot r} \quad \varepsilon(\bar{m}) \rightarrow \varepsilon(\bar{m})}{\bar{m} < \cdot r \supset \varepsilon(\bar{m}) \rightarrow \varepsilon(\bar{m})} \quad \forall x (x < \cdot r \supset \varepsilon(x)) \rightarrow \varepsilon(\bar{m})}{\forall x (x < \cdot r \supset \varepsilon(x)) \rightarrow \varepsilon(\bar{m}), \varepsilon(r)}.$$

The ordinal of this proof is 4 and is less than that of a **TJ**-initial sequent (which is 7). By this replacement and some obvious changes, P is transformed into a **TJ**-proof P' whose end-sequent is

$$\rightarrow \varepsilon(\bar{m}), \varepsilon(\bar{m}_1), \dots, \varepsilon(\bar{m}_n),$$

where $\rightarrow \varepsilon(\bar{m}_1), \dots, \varepsilon(\bar{m}_n)$ is the end-sequent of P , and such that the ordinal of P' is less than that of P and the end-number of P' is $|m|_{<}$. We shall refer to P' as the proof obtained from P by an application of a critical reduction at m .

Now suppose P is any **TJ**-proof (not necessarily critical), and $|m|_{<}$ is less than the end-number of P . We shall define what is meant by the proof obtained from P be an application of a critical reduction at m .

If P is critical, the definition is as above. Otherwise, apply a sequence of reductions (as in the proof of Lemma 12.8). At each reduction, the ordinal of the proof *decreases*, so this process must terminate after a finite number of steps with a *critical* proof satisfying p 1–p 4. Now take the proof obtained from *this* proof as above.

13.13) Adjoining the reduction in 13.12) to the previous reductions, and applying the fundamental lemma in 13.5), we obtain the original form of Gentzen's theorem:

THEOREM 13.6. *The order type of $<\cdot$ is less than ε_0 .*

13.14) Let $P(a)$ be a proof of $\rightarrow \varepsilon(a)$, obtained as described in 13.2. Let us define for each number k a **TJ**-proof P_k by induction on k , where the end-number of P_k is $|k|_{<}$.

- (1) The case where $\forall n < k$ ($n < \cdot k$). We define P_k to be the proof $P(\bar{k})$ obtained from $P(a)$ by replacing a by the numeral \bar{k} throughout $P(a)$.
- (2) The case where $\exists n < k$ ($k < \cdot n$). Let

$$(**) \quad n_0 < \dots < \cdot n_{j-1} < \cdot n_j (= k) < \cdot n_{j+1} < \dots < \cdot n_k$$

be the re-ordering of the numbers $\leq k$ with respect to $<\cdot$. Then we define P_k to be the proof obtained from $P_{n_{j+1}}$ by applying a critical reduction at k (cf. 13.12)). It is obvious that this definition is recursive.

13.15) We now define a map f , which will turn out to be an order-preserving recursive map as required for Theorem 13.4, by making use of the P_k . Define $f(k)$ by induction on k :

$$f(0) = \omega^{o(P_0)},$$

and for $k > 0$, $f(k) = f(n_{j-1}) + \omega^{o(P_k)}$ where $o(P)$ is (the Gödel number of) the ordinal of P , $+$ is (the primitive recursive function representing)

addition of ordinals, ω^a is (the primitive recursive function representing) exponentiation by ω , and n_{j-1} is an in $(**)$ (such a number always existing if $k > 0$).

13.16) Let $m_0 < \cdot m_1 < \cdot \dots < \cdot m_i$ be the re-ordering of the numbers $< i + 1$ with respect to $< \cdot$. Then

$$f(m_{j+1}) = f(m_j) + \omega^{o(P_{m_{j+1}})},$$

where $0 \leq j < i$. This is proved by mathematical induction on i . For $i = 0$, this is trivial. Assume it for i . For the case of $i + 1$, it is sufficient to show (with m_0, \dots, m_i as above):

$$f(i + 1) = f(m_j) + \omega^{o(P_{i+1})} \quad (1)$$

and

$$f(m_{j+1}) = f(i + 1) + \omega^{o(P_{m_{j+1}})}, \quad (2)$$

where $m_j < \cdot i + 1 < \cdot m_{j+1}$. Here (1) holds by definition of f , and (2) follows from (1) and $f(m_{j+1}) = f(m_j) + \omega^{o(P_{m_{j+1}})}$ (by induction hypothesis) and $o(P_{i+1}) < o(P_{m_{j+1}})$ (by definition of P_{i+1}). The second point of Theorem 13.4 is also easily seen if one puts $\mu = \omega^{o(P(a))+1}$. This completes the proof of Theorem 13.4.

To end this section, another result of Gentzen will be stated. The proof is straightforward.

THEOREM 13.7. *Let $<_n$ be the standard well-ordering of ϵ_0 , restricted to ω_n . Then $<_n$ is a provable well-ordering of \mathbf{PA} .*

Kleene's T -predicate (for unary, i.e., one-argument functions) is a primitive recursive relation T such that for an arbitrary partial recursive function f (of one argument) there exists a number e for which

$$f(x) = U(\mu y T(e, x, y))$$

for all x . (U is a fixed primitive recursive function). Such an e is called a Gödel number of f . The definition can be extended to functions of many arguments.

If e is the Gödel number of a unary partial recursive function, then clearly

$$f \text{ is (total) recursive if and only if } \forall x \exists y T(e, x, y).$$

Further, f is called *provably recursive* (in \mathbf{PA}) if it has a Gödel number e

such that $\forall x \exists y T(\bar{e}, x, y)$ is **PA**-provable. Having discussed the Gödel numbering of recursive functions, we can now state a problem which should, in its correct context, actually have been placed in §12. The idea is due to Schütte.

PROBLEM 13.8. Let **PA**^{*} be the system obtained by modifying **PA** as follows. The language is the same as that of **PA**; the initial sequents are those of **PA**; the rules of inference are those of **PA** except cut, \forall : right and ind; the constructive ω -rule, which is described below, is added as a new rule of inference:

$$\frac{P_1 \dots P_i \dots}{\Gamma \rightarrow \Delta, \forall x A(x)} \quad (i < \omega),$$

where P_i is a proof ending with $\Gamma \rightarrow \Delta, A(\bar{i})$, and there is a recursive function f such that $f(i) = \ulcorner P_i \urcorner$. Let e be a Gödel number of f . Then the proof ending with $\Gamma \rightarrow \Delta, \forall x A(x)$ is assigned the number

$$5^e \cdot 7^{\ulcorner \Gamma \rightarrow \Delta, \forall x A(x) \urcorner}.$$

Show that if a sequent S is **PA**-provable and contains no free variable, then S is provable in **PA**^{*}. [*Hint:* We adapt the method of the consistency proof of **PA** as follows. Let P be a (regular) proof in **PA**, with ordinal α (according to the assignment of Definition 12.4). Then assign $\omega^\alpha + m$ to P , where m is the number of free variables in the end-piece of P . The reduction process for the consistency proof goes through almost unchanged, except that if P contains an explicit logical inference and the lowermost such is a \forall : right, then replace it by the ω -rule, which is applied at the end of the proof.]

PROBLEM 13.9. Let f be a provably recursive function in **PA**. Then there exists an ordinal μ (less than ε_0) such that f is $<^\mu$ -primitive recursive, where $<^\mu$ is the standard ordering of ε_0 restricted to μ . [*Hint:* Let e be a Gödel number of f such that $\forall x \exists y T(\bar{e}, x, y)$ is **PA**-provable. Then there is a proof, say $P(a)$, of $\exists y T(\bar{e}, a, y)$, with free variable a . Let μ be the ordinal assigned to $P(a)$, and let P_m denote $P(\bar{m})$ for each natural number m . By the method of Problem 13.8, P_m can be transformed into a cut-free proof in **PA**^{*} of the same end-sequent. It can be easily shown that the resulting proof does not contain the ω -rule, since $P(\bar{m})$ does not contain any explicit \forall : right. The transformation is actually $<^\mu$ -primitive recursive. Thus there is a $<^\mu$ -primitive recursive function τ such that $\tau(\ulcorner P_m \urcorner)$ is (the Gödel number of) a cut-free proof of $\exists y T(\bar{e}, \bar{m}, y)$. By examining this proof, we can find (primitive recursively in its Gödel number) a number n satisfying $T(e, m, n)$. Then n is a $<^\mu$ -primitive recursive function of m and $f(m) = U(n)$. Thus f is $<^\mu$ -primitive recursive.]

§14. An additional topic

Here we assume again that all the primitive recursive functions are included in the language of **PA** and their defining equations are included as initial sequents.

PROPOSITION 14.1. *Let Φ_n be the set of sentences of **PA** which have at most n logical symbols. Then there exists a truth definition for Φ_n in **PA**, i.e., a formula $T_n(a)$ of **PA** such that for every sentence A of Φ_n*

$$T_n(\overline{A}) \equiv A$$

*is **PA**-provable.*

PROOF. T_n is defined by induction on n . We shall present only the induction step, in passing from T_n to T_{n+1} .

A sequence number, say x , is a number which can be decomposed into the form $2^{x_0} \cdot 3^{x_1} \cdot \dots \cdot p_{n-1}^{x_{n-1}}$, where $x_i = 0$ or 1 for each i , $0 \leq i \leq n$. Let $\text{seq}(x, n)$ be a (primitive recursive) predicate which expresses that x is a sequence number of the above form. We call n the length of x . The i th exponent of x , x_i , will be denoted $x(i)$. Let $\text{st}('A')$ express " A is a sentence", and let $\text{ls}('A')$ be the number of logical symbols in A . Then T_{n+1} is defined as follows.

$$\begin{aligned} T_{n+1}('A') \leftrightarrow & \\ \leftrightarrow \text{st}('A') \wedge \text{ls}('A') \leq n+1 & \\ \wedge \exists x [\text{seq}(x, 'A') \wedge \forall i (0 \leq i \leq 'A' \supset & \\ (\forall 'B'[i = ' \neg B' \supset (x(i) = 1 \equiv x('B') = 0)] & \\ \wedge \forall 'B' \forall 'C'[i = ' B \wedge C' & \\ \supset (x(i) = 1 \equiv x('B') = 1 \wedge x('C') = 1)] & \\ \wedge \forall ' \forall y B(y)'[i = ' \forall y B(y)' \supset (x(i) = 1 \equiv \forall y T_n('B(\bar{y}')))] & \\ \wedge \forall ' \exists y B(y)'[i = ' \exists y B(y)' \supset (x(i) = 1 \equiv \exists y T_n('B(\bar{y}')))] & \\ \wedge x('A') = 1]. & \end{aligned}$$

It is easily seen that

$$T_{n+1}(A(\bar{b}_1, \dots, \bar{b}_n)) \equiv A(b_1, \dots, b_n)$$

is **PA**-provable for every A is Φ_n , where all the free variables of A are among b_1, \dots, b_n .

Let $S: A_1, \dots, A_m \rightarrow B_1, \dots, B_l$ be a sequent such that all of $A_1, \dots, A_m, B_1, \dots, B_l$ are in Φ_n . Then $T_n('S')$ is defined to be

$$\exists i (1 \leq i \leq m \wedge \neg T_n('A_i')) \vee \exists i (1 \leq i \leq l \wedge T_n('B_i')).$$

Here of course m and l are primitive recursive functions of ' S ' and A_i and B_i are determined primitive recursively from ' S ' and i .

PROPOSITION 14.2. *PA cannot be formulated with finitely many axioms; in other words, mathematical induction cannot be expressed by finitely many formulas.*

PROOF (Feferman). First note that

$$\mathbf{PA} \vdash (\vdash_{CF} 'S' \rightarrow \vdash_{CF} 'S'), \quad (1)$$

by formalizing the cut-elimination theorem for **LK** in **PA**.

Next, suppose P is a cut-free proof of a sequent S , and all the formulas in S are in F_n . Then every formula in P is in F_n . Further, if P is in the language of **PA**, then we can prove in **PA** that every numerical instance of S is true; in other words:

$$\mathbf{PA} \vdash \vdash_{CF} 'S(b_1, \dots, b_m)' \rightarrow \forall x_1 \dots x_m T_n('S(\bar{x}_1, \dots, \bar{x}_m)'), \quad (2)$$

where all the free variables of S are among b_1, \dots, b_m . The proof of (2) is by induction on the number of sequents in P .

Now let Γ_0 be any finite set (or rather sequence) of axioms of $\mathbf{CA} \cup \mathbf{VJ}$ (Definition 9.5) and let n be the maximum number of logical symbols in any formula of Γ_0 . Letting S be $\Gamma_0 \rightarrow \bar{0} = \bar{1}$, we obtain from (2):

$$\mathbf{PA} \vdash \vdash_{CF} '\Gamma_0 \rightarrow \bar{0} = \bar{1}' \rightarrow T_n(' \Gamma_0 \rightarrow \bar{0} = \bar{1} '). \quad (3)$$

Further (of course):

$$\mathbf{PA} \vdash \neg T_n(' \Gamma_0 \rightarrow \bar{0} = \bar{1} ')$$

and hence, from (1) and (3):

$$\mathbf{PA} \vdash \neg \vdash_{CF} '\Gamma_0 \rightarrow \bar{0} = \bar{1}'.$$

This sentence, $\neg \vdash_{CF} '\Gamma_0 \rightarrow \bar{0} = \bar{1}'$, can be taken as expressing the consistency of Γ_0 , which, as we see, is provable in **PA**. Hence, by Gödel's second incompleteness theorem (Theorem 10.18), Γ_0 cannot be proof-theoretically equivalent to **PA**.

EXERCISE 14.3. Show that **ZF** (Zermelo-Fraenkel set theory) cannot be formulated with finitely many axioms; in other words, the axiom of replacement cannot be expressed by finitely many formulas.

