PROOF THEORY

GAISI TAKEUTI

PROOF THEORY

GAISI TAKEUTI

Professor of Mathematics
The University of Illinois
Urbana, Illinois, U.S.A.

Second edition

NORTH-HOLLAND
AMSTERDAM • NEW YORK • OXFORD • TOKYO

ISBN: 0 444 87943 9

First edition 1975
Second edition 1987

Published by:
ELSEVIER SCIENCE PUBLISHERS B.V.
P.O. Box 1991
1000 BZ Amsterdam
The Netherlands

Sole distributors for the U.S.A. and Canada:
ELSEVIER SCIENCE PUBLISHING COMPANY, INC.
52 Vanderbilt Avenue
New York, N.Y. 10017
U.S.A.

Library of Congress Cataloging-in-Publication Data

Takeuti, Gaisi, 1926–
Proof theory.

(Studies in logic and the foundations of mathematics; v. 81)
Based on a series of lectures given at the Symposium on Intuitionism and Proof Theory held at Buffalo, 1968.
Bibliography: p.
Includes index.
1. Proof theory. I. Title. II. Series.
QA9.54.T34 1987 511.3 86-4489
ISBN 0-444-87943-9 (U.S.)

PRINTED IN THE NETHERLANDS

PREFACE

This book is based on a series of lectures that I gave at the Symposium on Intuitionism and Proof Theory held at Buffalo in the summer of 1968. Lecture notes, distributed at the Buffalo symposium, were prepared with the help of Professor John Myhill and Akiko Kino. Mariko Yasugi assisted me in revising and extending the original notes. This revision was completed in the summer of 1971. At this point Jeffery Zucker read the first three chapters, made improvements, especially in Chapter 2, and my colleagues Wilson Zaring provided editorial assistance with the final draft of Chapters 4–6.

To all who contributed, including our departmental secretaries, who typed versions of the material for use in my classes. I express my deep appreciation.

Gaisi Takeuti

Urbana, March 1975

CONTENTS

INTRODUCTION

Mathematics is a collection of proofs. This is true no matter what standpoint one assumes about mathematics—platonism, anti-platonism, intuitionism, formalism, nominalism, etc. Therefore, in investigating "mathematics", a fruitful method is to formalize the proofs of mathematics and investigate the structure of these proofs. This is what proof theory is concerned with.

Proof theory was initiated by D. Hilbert in his attempt to prove the consistency of mathematics. Hilbert's approach was later developed by the brilliant work of G. Gentzen. This textbook is devoted to the proof theory inspired by Gentzen's work: so-called Gentzen-type proof theory.

Part I treats the proof theory of first order formal systems. Chapter 1 deals with the first order predicate calculus; Gentzen's cut-elimination theorem plays a major role here. There are many consequences of this theorem as for example the various interpolation theorems.

We prove the completeness of the classical predicate calculus, by the use of reduction trees (following Schütte), and then we prove the completeness of the intuitionistic predicate calculus, by adapting this method to Kripke semantics.

Chapter 2 deals with the theory of natural numbers; the main topics are Gödel's incompleteness theorem and Gentzen's consistency proof. Since the author believes that the true significance of Gentzen's consistency proof has not been well understood so far, a philosophical discussion is also presented in this chapter. The author believes that the Hilbert-Gentzen finitary standpoint, with "Gedankenexperimenten" involving finite (and concrete) operations on (sequences of) concretely given figures, is most important in the foundations of mathematics.

Part II concerns the finite order predicate calculi and infinitary languages. In Chapter 3, the semantics for finite order systems, and the cut-elimination theorem for them, due to Tait, Takahashi and Prawitz, are considered. Since the finite type calculus is not complete, and further, much of traditional mathematics can be formalized in it, we are anxious to see progress in investigating the significance of the cut-elimination theorem here. The significance of the systems with infinitary languages which are presented in Chapter 4 is that they are complete systems in which the cut-elimination theorem holds, while at the same time they are essentially second order systems. The situation is, however, quite uncertain for systems with heterogeneous quantifiers. Here we propose a basic system of heterogeneous quantifiers which seems reasonable and for which so-called "weak completeness" holds. It seems, however, that our system is far from complete. A system which is obtained from ours by a slight modification is closely related to the axiom of determinateness (AD). Therefore the problem of how to extend our system to a (sound and) complete system is related to the justification of the axiom of determinateness.

Let M be a transitive model of ZF + DC (the axiom of dependent choices) which contains $P(\omega)$. It has been shown that the following two statements are equivalent: (1) AD holds in M; and (2) the cut-elimination theorem holds for any M-definable determinate logic. This suggests an interesting direction for the study of infinitary languages.

Part III is devoted to consistency proofs for stronger systems on which the author has worked.

We have tried to avoid overlapping of material with other textbooks. Thus, for example, we do not present the material in K. Schütte's Beweistheorie, although much of it is Gentzen-type proof theory. Those who wish to learn other approaches to proof theory are advised to consult G. Kreisel's Survey of Proof Theory I and II, Journal of Symbolic Logic (1968), and Proceedings of the Second Scandinavian Logic Symposium, ed. J. E. Fenstad (North-Holland, Amsterdam, 1971), respectively. We have made special efforts to clarify our position on foundational issues. Indeed, it is our view that in the study of the foundations of mathematics (which is not restricted to consistency problems), it is philosophically important to study and clarify the structures of mathematical proofs.

Concerning the impact of foundational studies on mathematics itself, we remark that while set theory, for example, has already contributed essentially to the development of modern mathematics, it remains to be seen what influence proof theory will have on mathematics.

No attempt has been made to make the references comprehensive although some names are attached to the theorems. In addition to those given above, a few references are recommended in the course of the book.

PART I

FIRST ORDER SYSTEMS

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: $k_0, k_1, \ldots, k_j, \ldots$ ($j = 0, 1, 2, \ldots$).
   1.2) Function constants with i argument-places ($i = 1, 2, \ldots$): $f_0^i, f_1^i, \ldots, f_j^i, \ldots$ ($j = 0, 1, 2, \ldots$).
   1.3) Predicate constants with i argument-places ($i = 0, 1, 2, \ldots$): $R_0^i, R_1^i, \ldots, R_j^i, \ldots$ ($j = 0, 1, 2, \ldots$).
2) *Variables*:
   2.1) Free variables: $a_0, a_1, \ldots, a_j, \ldots$ ($j = 0, 1, 2, \ldots$).
   2.2) Bound variables: $x_0, x_1, \ldots, x_j, \ldots$ ($j = 0, 1, 2, \ldots$).
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 inelementary 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 $g, h, \ldots$ may be used as symbols for function constants, while $a, b, c, \ldots$ may be used for free variables and $x, y, z, \ldots$ 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 $t_1, \ldots, t_i$ are terms, then $f^i(t_1, \ldots, t_i)$ is a term.

4) Terms are only those expressions obtained by 1)–3). Terms are often denoted by $t, s, t_1, \ldots$.

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 $t_1, \ldots, t_i$ are terms, then $R^i(t_1, \ldots, t_i)$ 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, $A, B, C, \ldots, F, G, \ldots$ 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 $\tau_1, \dots, \tau_n$ 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 $\tau_1, \dots, \tau_n$, respectively, at each occurrence of $\tau_1, \dots, \tau_n$ (where these symbols are replaced simultaneously). Such an operation is called the *(simultaneous) replacement of* $(\tau_1, \dots, \tau_n)$ *by* $(\sigma_1, \dots, \sigma_n)$ *in* A. It is not required that $\tau_1, \dots, \tau_n$ actually occur in A.

PROPOSITION 1.5. (1) *If A contains none of $\tau_1, \dots, \tau_n$, then*

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

is A itself.

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

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

is identical with

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

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

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

then for each i $(1 \leqslant i \leqslant n)$ 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 $B(b_1, \ldots, b_n)$, and A as $B(t_1, \ldots, t_n)$. 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 $\Gamma, \Delta, \Pi, \Lambda, \Gamma_0, \Gamma_1, \ldots$ 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 $A_1, \ldots, A_m \to B_1, \ldots, B_n$ (where $m, n \geqslant 1$) means: if $A_1 \wedge \ldots \wedge A_m$, then $B_1 \vee \ldots \vee B_n$. For $m \geqslant 1$, $A_1, \ldots, A_m \to$ means that $A_1 \wedge \ldots \wedge A_m$ yields a contradiction. For $n \geqslant 1$, $\to B_1, \ldots, B_n$ means that $B_1 \vee \ldots \vee B_n$ holds. The empty sequent $\to$ 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*:

$$\text{left}: \frac{\Gamma \to \Delta}{D, \Gamma \to \Delta}; \qquad \text{right}: \frac{\Gamma \to \Delta}{\Gamma \to \Delta, D}.$$

D is called the weakening formula.

1.2) *Contraction*:

$$\text{left}: \frac{D, D, \Gamma \to \Delta}{D, \Gamma \to \Delta}; \qquad \text{right}: \frac{\Gamma \to \Delta, D, D}{\Gamma \to \Delta, D}.$$

1.3) *Exchange*:

$$\text{left}: \frac{\Gamma, C, D, \Pi \to \Delta}{\Gamma, D, C, \Pi \to \Delta}; \qquad \text{right}: \frac{\Gamma \to \Delta, C, D, \Lambda}{\Gamma \to \Delta, D, C, \Lambda}$$

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

1.4) *Cut*:

$$\frac{\Gamma \to \Delta, D \qquad D, \Pi \to \Lambda}{\Gamma, \Pi \to \Delta, \Lambda}.$$

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

2) Logical rules:

2.1) $\neg$: left: $\dfrac{\Gamma \to \Delta, D}{\neg D, \Gamma \to \Delta}$; $\neg$: right: $\dfrac{D, \Gamma \to \Delta}{\Gamma \to \Delta, \neg D}$.

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

2.2) $\wedge$: left: $\dfrac{C, \Gamma \to \Delta}{C \wedge D, \Gamma \to \Delta}$ and $\dfrac{D, \Gamma \to \Delta}{C \wedge D, \Gamma \to \Delta}$;

$\wedge$: right: $\dfrac{\Gamma \to \Delta, C \qquad \Gamma \to \Delta, D}{\Gamma \to \Delta, C \wedge D}$.

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

2.3) $\vee$: left: $\dfrac{C, \Gamma \to \Delta \quad D, \Gamma \to \Delta}{C \vee D, \Gamma \to \Delta}$;

$\vee$: right: $\dfrac{\Gamma \to \Delta, C}{\Gamma \to \Delta, C \vee D}$ and $\dfrac{\Gamma \to \Delta, D}{\Gamma \to \Delta, C \vee D}$.

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

2.4) $\supset$: left: $\dfrac{\Gamma \to \Delta, C \quad D, \Pi \to \Lambda}{C \supset D, \Gamma, \Pi \to \Delta, \Lambda}$;

$\supset$: right: $\dfrac{C, \Gamma \to \Delta, D}{\Gamma \to \Delta, C \supset D}$.

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) $\forall$: left: $\dfrac{F(t), \Gamma \to \Delta}{\forall x\, F(x), \Gamma \to \Delta}$, $\forall$: right: $\dfrac{\Gamma \to \Delta, F(a)}{\Gamma \to \Delta, \forall x\, F(x)}$,

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 $\forall$: right is called the *eigenvariable* of this inference.

Note that in $\forall$: right all occurrences of a in $F(a)$ are indicated. In $\forall$: 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) $\exists$: left: $\dfrac{F(a), \Gamma \to \Delta}{\exists x\, F(x), \Gamma \to \Delta}$, $\exists$: right: $\dfrac{\Gamma \to \Delta, F(t)}{\Gamma \to \Delta, \exists x\, F(x)}$,

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 $\exists$: left is called the eigenvariable of this inference.

Note that in $\exists$: left a is fully indicated, while in $\exists$: 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 $\forall$: right and $\exists$: left, is called the *eigenvariable condition* for these inferences.

A sequent of the form $A \to A$ 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 $\to A$ 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,