Chapter 3

Provability and Refutability

We now turn our attention to the practical problems of proving theorems of first-order logic. If one has unlimited resources and patience, one can simply enumerate proofs until one finds a proof of the wff under consideration (provided, of course, that it actually is a theorem). As a practical matter, however, one usually wishes to find a proof as quickly and easily as possible, so various methods have been devised to facilitate efficient searches for proofs. We shall discuss some of these methods in this chapter, along with various results related to them.

A *refutation* of a wff **B** is a proof that **B** is contradictory; this amounts to a proof of $\sim$ **B**. Thus, one way to prove a wff **A** is to refute $\sim$ **A**. This method is proving a wff **A** is often called the indirect method, and it is surprisingly useful, so a number of the procedures we discuss below are refutation procedures rather than proof procedures. Since a refutation of $\sim$ **A** provides a proof of **A**, we shall sometimes speak of refutation procedures as proof procedures.

We say that we refute a set $\mathcal{S}$ of sentences when we drive a contradiction from $\mathcal{S}$. Naturally, such a refutation shows that some finite conjunction of members of $\mathcal{S}$ is contradictory.

§30. Natural Deduction

Proofs of theorems of $\mathcal{F}$ (which is known as a *Hilbert-style* system) are rarely written out in full, since they tend to be long, awkward, and unpleasant to read. In practice, one uses proofs from hypotheses and derived rules of

inference of $\mathcal{F}$. In this section we introduce a system $\mathcal{N}$ of *natural deduction*,[1] in which it is possible to give fairly natural and well structured proofs, and express the forms of arguments which arise in mathematical practice. Of course, the rules of inference of $\mathcal{N}$ are all derived rules of inference of $\mathcal{F}$, and this section may be regarded simply as a summary of those derived rules of inference of $\mathcal{F}$ which are most useful for writing our proofs.

Later in this chapter we discuss a variety of methods and logical tools for establishing the validity of wffs of first-order logic. Generally, proofs can be translated from one format into another (though real insight may be required to design algorithms to do this), and once one has found the essential ingredients of a proof, one may wish to express them in a proof which is reasonably comprehensible. The system $\mathcal{N}$ provides one standard for what such a proof should look like.

The exact choice of primitive connectives and quantifiers for this section does not matter very much, but it is natural to take at least $\sim$, $\vee$, $\wedge$, $\supset$, and f (falsehood) as primitive connectives, and both $\forall$ and $\exists$ as primitive quantifiers. f plays the role of a contradiction in indirect proofs.

Various definitions, such as *free for*, must be adjusted in trivial ways to take account of the fact that $\exists$ is now a primitive quantifier, and we leave this task to the reader. To avoid needless redundancy we shall use $\mathbf{M}$ and $\mathbf{N}$ as syntactical variables for wffs or for the "null formula" (empty disjunction). When $\mathbf{M}$ is null, $\mathbf{M} \vee \mathbf{A}$ and $\mathbf{A} \vee \mathbf{M}$ both stand for $\mathbf{A}$. A null formula standing alone may be regarded as an abbreviation for f. In this section we use $\mathcal{H}$ as a syntactical variable for a finite (possibly empty) *sequence* of wffs, and write $\mathcal{H}, \mathbf{A}$ for the sequence obtained by appending $\mathbf{A}$ to the sequence $\mathcal{H}$. As in §21, we may say that $\mathbf{x}$ is not free in $\mathcal{H}$ when we mean that $\mathbf{x}$ is not free in any wff of $\mathcal{H}$.

A *natural deduction proof* consists of a finite sequence of *lines* of the form $\mathcal{H} \vdash \mathbf{A}$. The members of the sequence $\mathcal{H}$ are called *hypotheses*, and the wff $\mathbf{A}$ is called the *assertion* of the line. Each line must be inferred from zero or more preceding lines by one of the following rules of inference.

Rules of Inference

Hypothesis Rule (Hyp). Infer $\mathcal{H} \vdash \mathbf{A}$ whenever $\mathbf{A}$ is a member of $\mathcal{H}$.

Rule for Expanding or Rearranging Hypotheses. From $\mathcal{H}_1 \vdash \mathbf{A}$ infer $\mathcal{H}_2 \vdash \mathbf{A}$, provided that every wff in $\mathcal{H}_1$ is also in $\mathcal{H}_2$.

[1] Natural deduction was introduced in [Gentzen, 1935]. Also see [Quine, 1950], [Prawitz, 1965], and references cited therein.

Deduction Rule (Ded). From $\mathcal{H}$, $\mathbf{A} \vdash \mathbf{B}$ infer $\mathcal{H} \vdash \mathbf{A} \supset \mathbf{B}$.

Rule P. From $\mathcal{H} \vdash \mathbf{A}_1, \ldots,$ and $\mathcal{H} \vdash \mathbf{A}_n$ infer $\mathcal{H} \vdash \mathbf{B}$, provided that $[[\mathbf{A}_1 \wedge \ldots \wedge \mathbf{A}_n] \supset \mathbf{B}]$ is tautologous.

Negation Rule (Neg.). From $\mathcal{H} \vdash \mathbf{A}$, infer $\mathcal{H} \vdash \mathbf{B}$, where $\mathbf{A}$ is $\sim \forall \mathbf{x}\mathbf{C}$, $\sim \exists \mathbf{x}\mathbf{C}$, $\forall \mathbf{x} \sim \mathbf{C}$, or $\exists \mathbf{x} \sim \mathbf{C}$, and $\mathbf{B}$ is $\exists \mathbf{x} \sim \mathbf{C}$, $\forall \mathbf{x} \sim \mathbf{C}$, $\sim \exists \mathbf{x}\mathbf{C}$, or $\sim \forall \mathbf{x}\mathbf{C}$, respectively.

Rule of Indirect Proof (IP). From $\mathcal{H}$, $\sim \mathbf{A} \vdash \mathsf{f}$ infer $\mathcal{H} \vdash \mathbf{A}$.

Rule of Cases (Cases). From $\mathcal{H} \vdash \mathbf{A} \vee \mathbf{B}$ and $\mathcal{H}$, $\mathbf{A} \vdash \mathbf{C}$ and $\mathcal{H}$, $\mathbf{B} \vdash \mathbf{C}$ infer $\mathcal{H} \vdash \mathbf{C}$.

Rule of Alphabetic Change of Bound Variables (α). From $\mathcal{H} \vdash \mathbf{A}$ infer $\mathcal{H} \vdash \mathbf{A}'$, where $\mathbf{A}'$ is obtained from $\mathbf{A}$ upon replacing an occurrence of $\forall \mathrm{x}\mathrm{C}$ $[\exists \mathbf{x}\mathbf{C}]$ in $\mathbf{A}$ by an occurrence of $\forall \mathbf{y}\mathsf{S}^{\mathbf{x}}_{\mathbf{y}}\mathbf{C}$ $[\exists \mathbf{y}\mathsf{S}^{\mathbf{x}}_{\mathbf{y}}\mathbf{C}]$, where $\mathbf{y}$ is not free in $\mathbf{C}$ and $\mathbf{y}$ is free for $\mathbf{x}$ in $\mathbf{C}$.

Universal Generalization ($\forall$G). From $\mathcal{H} \vdash \mathbf{M} \vee \mathbf{A} \vee \mathbf{N}$ infer $\mathcal{H} \vdash \mathbf{M} \vee \forall \mathbf{x}\mathbf{A} \vee \mathbf{N}$, provided that $\mathbf{x}$ is not free in $\mathcal{H}$, $\mathbf{M}$, or $\mathbf{N}$.

Existential Generalization ($\exists$G). Let $\mathbf{A}(\mathbf{x})$ be a wff and let $\mathbf{t}$ be a term which is free for $\mathbf{x}$ in $\mathbf{A}(\mathbf{x})$. ($\mathbf{t}$ may occur in $\mathbf{A}(\mathbf{x})$.) From $\mathcal{H} \vdash \mathbf{M} \vee \mathbf{A}(\mathbf{t}) \vee \mathbf{N}$ infer $\mathcal{H} \vdash \mathbf{M} \vee \exists \mathbf{x}\mathbf{A}(\mathbf{x}) \vee \mathbf{N}$.

Universal Instantiation ($\forall$I). From $\mathcal{H} \vdash \forall \mathbf{x}\mathbf{A}(\mathbf{x})$ infer $\mathcal{H} \vdash \mathbf{A}(\mathbf{t})$, provided that $\mathbf{t}$ is a term free for $\mathbf{x}$ in $\mathbf{A}(\mathbf{x})$.

Rule C. From $\mathcal{H} \vdash \exists \mathbf{x}\mathbf{B}(\mathbf{x})$ and $\mathcal{H}$, $\mathbf{B}(\mathbf{y}) \vdash \mathbf{A}$ infer $\mathcal{H} \vdash \mathbf{A}$, where $\mathbf{y}$ is an individual variable which is free for $\mathbf{x}$ in $\mathbf{B}(\mathbf{x})$ and which is not free in $\mathcal{H}$, $\exists \mathbf{x}\mathbf{B}(\mathbf{x})$ or in $\mathbf{A}$.

Note that the system $\mathcal{N}$ has no axioms. We remark that the Rule for Expanding or Rearranging Hypotheses is often used tacitly and without explicit mention in combination with other rules. Rule $\forall$G really has four forms:

from $\mathcal{H} \vdash \mathbf{A}$	infer $\mathcal{H} \vdash \forall \mathbf{x}\mathbf{A}$;
from $\mathcal{H} \vdash \mathbf{A} \vee \mathbf{C}$	infer $\mathcal{H} \vdash \forall \mathbf{x}\mathbf{A} \vee \mathbf{C}$;
from $\mathcal{H} \vdash \mathbf{B} \vee \mathbf{A}$	infer $\mathcal{H} \vdash \mathbf{B} \vee \forall \mathbf{x}\mathbf{A}$;
from $\mathcal{H} \vdash \mathbf{B} \vee \mathbf{A} \vee \mathbf{C}$	infer $\mathcal{H} \vdash \mathbf{B} \vee \forall \mathbf{x}\mathbf{A} \vee \mathbf{C}$.

(In each case, $\mathbf{x}$ must not be free in $\mathcal{H}$, $\mathbf{B}$, or $\mathbf{C}$.) Our use of the null formula simply enables us to compress these four statements into one. Rule P can actually be restricted to certain special cases of Rule P (such as certain rules of the system $\mathcal{G}$ of §31), but we shall not discuss that here. Naturally, if one wishes to prove theorems involving $=$, one should add to the rules above certain derived rules of inference of the system discussed in §26. Also, in some contexts it would be natural to include a rule permitting one to infer any previously proved theorem.

The soundness and completeness of $\mathcal{N}$ follow from the corresponding results for $\mathcal{F}$, though a careful proof must deal with the fact that $\exists$ is a primitive symbol of $\mathcal{N}$, but not of $\mathcal{F}$. We leave further consideration of these matters to the reader (Exercises X3003 and X3004).

If $\mathbf{A}(\mathbf{x})$ is a wff in which $\mathbf{x}$ occurs free, and one wishes to prove $\exists\mathbf{x}\mathbf{A}(\mathbf{x})$, a natural approach is to try to find a term $\mathbf{t}$ such that one can prove $\mathbf{A}(\mathbf{t})$, and then derive $\exists\mathbf{x}\mathbf{A}(\mathbf{x})$ by $\exists$G. For example, if $\mathbf{A}(\mathbf{x})$ is $[Qy \supset Q\mathbf{x}]$, one can prove $\mathbf{A}(y)$ (i.e., $[Qy \supset Qy]$), and from this infer $\exists\mathbf{x}\mathbf{A}(\mathbf{x})$ (i.e., $\exists\mathbf{x}[Qy \supset Q\mathbf{x}]$).

Sometimes this approach will not work, as in the case where $\mathbf{A}(\mathbf{x})$ is $[Q\mathbf{x} \supset \cdot Qa \wedge Qb]$. Nevertheless, in this case one can prove $\mathbf{A}(a) \vee \mathbf{A}(b)$ (i.e., $[Qa \supset \cdot Qa \wedge Qb] \vee [Qb \supset \cdot Qa \wedge Qb]$, which is tautologous), from which one can infer $\exists\mathbf{x}\mathbf{A}(\mathbf{x}) \vee \exists\mathbf{x}\mathbf{A}(\mathbf{x})$ and hence infer $\exists\mathbf{x}\mathbf{A}(\mathbf{x})$ by Rule P. Thus, a natural generalization of the approach to proving $\exists\mathbf{x}\mathbf{A}(\mathbf{x})$ mentioned above is to find terms $\mathbf{t}_1, \ldots, \mathbf{t}_n$ such that one can prove $\mathbf{A}(\mathbf{t}_1) \vee \ldots \vee \mathbf{A}(\mathbf{t}_n)$ and from this infer $\exists\mathbf{x}\mathbf{A}(\mathbf{x}) \vee \ldots \vee \exists\mathbf{x}\mathbf{A}(\mathbf{x})$, and hence $\exists\mathbf{x}\mathbf{A}(\mathbf{x})$.

However, there are cases when even this generalized approach does not quite work. Consider the problem of giving a direct natural deduction proof of $\exists x \forall y \cdot Px \supset Py$. One proof is:

$\vdash [Px \supset Py] \vee \cdot Py \supset Pz$	Rule P
$\vdash [Px \supset Py] \vee \forall z \cdot Py \supset Pz$	$\forall$G
$\vdash [Px \supset Py] \vee \exists x \forall z \cdot Px \supset Pz$	$\exists$G
$\vdash \forall y[Px \supset Py] \vee \exists x \forall z \cdot Px \supset Pz$	$\forall$G
$\vdash \exists x \forall y[Px \supset Py] \vee \exists x \forall z \cdot Px \supset Pz$	$\exists$G
$\vdash \exists x \forall y[Px \supset Py] \vee \exists x \forall y \cdot Px \supset Py$	α
$\vdash \exists x \forall y \cdot Px \supset Py$	Rule P

Note that in this proof we do not have terms $\mathbf{t}_1$ and $\mathbf{t}_2$ in which y is not free such that we prove $\forall y[P\mathbf{t}_1 \supset Py] \vee \forall y[P\mathbf{t}_2 \supset Py]$. Could there be such terms? Consider an interpretation $\mathcal{M} = \langle \mathcal{D}, \mathcal{J} \rangle$, where

$\mathcal{D} = \{a, b\}$;

$\mathcal{J}\mathbf{c} = a$ for all constants $\mathbf{c}$;

for each function symbol $\mathbf{f}^n$

$(\mathcal{J}\mathbf{f}^n)d_1 \ldots d_n = a$ for all $d_1, \ldots, d_n$ in $\mathcal{D}$;

$(\mathcal{J}\ P)a = \mathsf{T}$, and $(\mathcal{J}\ P)b = \mathsf{F}$.

Let $\varphi\mathbf{x} = a$ for all individual variables $\mathbf{x}$; then $\mathcal{V}_\varphi^{\mathcal{M}}\mathbf{t} = a$ for each term $\mathbf{t}$. Thus if y does not occur in a term $\mathbf{t}$, and ψ is the assignment which agrees with φ off y, while $\psi y = b$, then

$$\mathcal{V}_\psi[P\mathbf{t} \supset Py] = \mathsf{F}, \quad \text{so} \quad \mathcal{V}_\varphi^{\mathcal{M}}\forall y[P\mathbf{t} \supset Py] = \mathsf{F}.$$

Thus one cannot prove any disjunction of the form $\bigvee_{i=1}^n \forall y[P\mathbf{t}_i \supset Py]$, where the terms $\mathbf{t}_i$ do not contain y.

EXERCISES

Prove the following theorems in $\mathcal{N}$:

X3000. $\sim \forall \mathbf{x}\mathbf{A} \equiv \exists \mathbf{x} \sim \mathbf{A}$.

X3001. $\sim \exists \mathbf{x}\mathbf{A} \equiv \forall \mathbf{x} \sim \mathbf{A}$.

X3002. $\forall u \forall v \forall w[Puv \vee Pvw] \supset \exists x \forall y Pxy$. (*Hint:* recall the advice given near the end of §21 about proving theorems of the form $\mathbf{A} \supset \mathbf{B}$.)

X3003. Prove that the system $\mathcal{N}$ is sound in the sense of 2303.

X3004. Prove that the system $\mathcal{N}$ is complete in the sense of 2509.

X3005. Add rules of inference for $=$ to $\mathcal{N}$, and prove that the resulting system is sound and complete in the sense of 2609 and 2612.

X3006. Are any of the rules of inference of $\mathcal{N}$ dependent (non-independent) in the sense of §13?

X3007. Find a system $\mathcal{N}'$ which can be obtained from $\mathcal{N}$ by deleting certain rules of inference, and whose rules of inference are all independent. Prove the independence of these rules.

http://www.springer.com/978-1-4020-0763-7

An Introduction to Mathematical Logic and Type Theory
To Truth Through Proof
Andrews, P.B.
2002, XVIII, 390 p., Hardcover
ISBN: 978-1-4020-0763-7