Applications of Proof Theory to Isabelle

Lawrence C Paulson
Computer Laboratory
University of Cambridge

August 13, 1996

Abstract

Isabelle [3, 4] is a generic theorem prover. It suppports interactive proof in several formal systems, including first-order logic (intuitionistic and classical), higher-order logic, Martin-Löf type theory, and Zermelo-Fraenkel set theory. New logics can be introduced by specifying their syntax and rules of inference. Both natural deduction and sequent calculi are allowed.

Isabelle's approach is to represent the various formal systems, or object-logics, within a single meta-logic. The meta-logic is a fragment of higher-order logic, formulated in natural deduction. The proof theory of meta-logic is the main tool for proving that an object-logic is correctly formalized in Isabelle.

Contents

1 A fragment of higher-order logic

Higher-order logic, which was developed by Alonzo Church, is used to represent logics within Isabelle. In fact only a fragment of this logic is required for this purpose. It is called $\mathcal{M}$ below (for "meta-logic").

1.1 Syntax of the meta-logic $\mathcal{M}$

The *types*[1] consist of basic types and function types of the form $\sigma \to \tau$. Let the Greek letters σ, τ, and υ stand for types.

The *terms* are those of the typed λ-calculus — constants, variables, abstractions, combinations — with the usual type constraints. Let a, b, and c stand for terms, using f, g, and h for terms of function type. Typical bound variables will be x, y, and z. Write $a : \sigma$ to mean 'a has type σ.'

The basic types and constants depend on the logic being represented. But they always include the type of propositions, *prop*, and the logical constants of $\mathcal{M}$. A *formula* is a term of type *prop*. Let ϕ, ψ, and θ stand for formulae. The implication $\phi \Rightarrow \psi$ means 'ϕ implies ψ.' The universally quantified formula $\bigwedge x.\phi$ means 'for all x, ϕ is true,' where x ranges over some type σ. The equality $a \equiv b$ means 'a equals b.'

The symbols $\Rightarrow$, $\bigwedge$, and $\equiv$ have been chosen to differ from symbols of *object*-logics: those to be represented in $\mathcal{M}$. In an object-logic presented below the corresponding symbols are $\supset$, $\forall$, and $=$. The words 'meta-implication,' 'meta-equality,' 'meta-formula,' 'meta-theorem,' 'meta-rule,' etc., refer to expressions of $\mathcal{M}$.

Quantification involves λ-abstraction. For every type σ, there is a constant $\bigwedge_\sigma$ of type $(\sigma \to \mathit{prop}) \to \mathit{prop}$. The formula $\bigwedge x.\phi$, where x has type σ, abbreviates $\bigwedge_\sigma(\lambda x.\phi)$. Using λ-conversions every quantification can be put into the form $\bigwedge_\sigma(f)$, more readably $\bigwedge x.f(x)$, where f is a term of type $\sigma \to \mathit{prop}$. Abstraction also expresses quantifiers in object-logics, as we shall see in Section 3.

1.2 Syntactic conventions

The application of a to the successive arguments $b_1, \ldots, b_m$ is written $a(b_1, \ldots, b_m)$:

$$a(b_1, \ldots, b_m) \quad \text{abbreviates} \quad (\cdots(ab_1)\cdots b_m)$$

In the absence of parentheses, implication ($\Rightarrow$) groups to the right. Let Φ, Ψ, and Θ stand for lists of formulae. Implication can also be written for such lists: if Φ is the list $[\phi_1, \ldots, \phi_m]$, then

$$\left.\begin{array}{r} \phi_1 \Rightarrow \cdots \Rightarrow \phi_m \Rightarrow \psi \\ [\phi_1, \ldots, \phi_m] \Rightarrow \psi \\ \Phi \Rightarrow \psi \end{array}\right\} \quad \text{each abbreviate} \quad \phi_1 \Rightarrow (\cdots \Rightarrow (\phi_m \Rightarrow \psi)\cdots)$$

One λ or quantifier does the work of many:

$$\left.\begin{array}{r} \lambda x_1 \ldots x_m \,.\, a \\ \bigwedge x_1 \ldots x_m \,.\, \phi \end{array}\right\} \quad \text{abbreviates} \quad \left\{\begin{array}{l} \lambda x_1 \ldots . \lambda x_m . a \\ \bigwedge x_1 \ldots . \bigwedge x_m . \phi \end{array}\right.$$

[1] Sometimes called *arities*, following Martin-Löf, to avoid confusion with ML types or object-level types.

The scope of a λ or quantifier extends far to the right:

$$\left.\begin{array}{c}\lambda x\,.\,f(x,g(x)) \\ \bigwedge x\,.\,\phi \Rightarrow b \equiv c\end{array}\right\} \quad \text{abbreviates} \quad \left\{\begin{array}{c}\lambda x\,.\,(f(x,g(x))) \\ \bigwedge x\,.\,(\phi \Rightarrow (b \equiv c))\end{array}\right.$$

A *substitution* has the form $[a_1/x_1, \ldots, a_k/x_k]$, where $x_1, \ldots, x_k$ are distinct variables and $a_1, \ldots, a_k$ are terms. If b is an expression and s is the substitution above then bs is the expression that results from simultaneously replacing every free occurrence of x_i by a_i in b, for $i = 1, \ldots, k$ (of course a_i must have the same type as x_i). Substitution must be carefully defined to avoid capture of free variables.

Substitutions are not part of $\mathcal{M}$ itself. The term $f(a)$ indicates function application, not substitution. The β-reduction law, namely $((\lambda x.b)(a)) \equiv b[a/x]$, expresses substitution at the object-level.

1.3 Semantics of the meta-logic

Higher-order logic is a language for writing formal mathematics. It can be justified on intuitive grounds, or else we can demonstrate its consistency by constructing a standard model in set theory.

Every type denotes a non-empty set. Given sets for each basic type, the interpretation of $\sigma \to \tau$ is the set of functions from σ to τ. A closed term of type σ denotes a value of the corresponding set. Given a value for each constant, λ-abstractions denote functions.

The type *prop* denotes a set of truth values. Classical logic uses $\{\mathrm{T}, \mathrm{F}\}$, but intuitionistic interpretations are possible. The logical constants ($\bigwedge_\sigma$, $\Rightarrow$, and $\equiv_\sigma$) denote appropriate truth-valued functions.

1.4 Inference rules

The constant symbols include, for every type σ,

$$\begin{array}{rcl} \Rightarrow & : & \mathit{prop} \to (\mathit{prop} \to \mathit{prop}) \\ \bigwedge_\sigma & : & (\sigma \to \mathit{prop}) \to \mathit{prop} \\ \equiv_\sigma & : & \sigma \to (\sigma \to \mathit{prop}) \end{array}$$

The *implication* rules are $\Rightarrow$-introduction and $\Rightarrow$-elimination:

$$\frac{\begin{array}{c}[\phi] \\ \psi\end{array}}{\phi \Rightarrow \psi} \qquad \frac{\phi \Rightarrow \psi \qquad \phi}{\psi}$$

These are natural deduction rules; $\Rightarrow$-introduction discharges the assumption ϕ. In most other rules, the conclusion depends on all assumptions of the premises.

The *universal quantification* rules are $\bigwedge$-introduction and $\bigwedge$-elimination:

$$\frac{\phi}{\bigwedge x.\phi} \qquad \frac{\bigwedge x.\phi}{\phi[b/x]}$$

These are also called *generalization* and *specialization*. The generalization rule is subject to the eigenvariable condition that x is not free in the assumptions.

The *equality* rules are reflexivity, symmetry, and transitivity:

$$a \equiv a \qquad \frac{a \equiv b}{b \equiv a} \qquad \frac{a \equiv b \qquad b \equiv c}{a \equiv c}$$

The λ-conversions are α-conversion (bound variable renaming), β-conversion, and extensionality:

$$(\lambda x.a) \equiv (\lambda y.a[y/x]) \qquad ((\lambda x.a)(b)) \equiv a[b/x] \qquad \frac{f(x) \equiv g(x)}{f \equiv g}$$

The α-conversion axiom holds provided y is not free in a. Extensionality holds provided x is not free in the assumptions, f, or g. Extensionality is equivalent to η-conversion, namely $(\lambda x.f(x)) \equiv f$ where x is not free in f (see Hindley and Seldin [2, pages 72–74]).

The *abstraction* and *combination* rules are

$$\frac{a \equiv b}{(\lambda x.a) \equiv (\lambda x.b)} \qquad \frac{f \equiv g \qquad a \equiv b}{f(a) \equiv g(b)}$$

Abstraction holds provided x is not free in the assumptions.

Logical equivalence means equality of truth values:

$$\frac{\begin{array}{cc}[\phi] & [\psi] \\ \psi & \phi\end{array}}{\phi \equiv \psi} \qquad \frac{\phi \equiv \psi \qquad \phi}{\psi}$$

The typed λ-calculus satisfies the strong normalization and Church-Rosser properties [2]. Thus repeatedly applying β and η-reductions always terminates. The reductions can take place in any order; the resulting normal form will be the same up to α-conversion. To summarize:

Theorem 1 *Every term can be reduced to a normal form that is unique up to α-conversion.*

Remark. Because of normal forms, equality is decidable in the typed λ-calculus — but not in higher-order logic. The normal form does not take account of the logical rules. No effective procedure can reduce every theorem to some unique true formula.

There is also a normalization procedure for HOL proofs. This plays a crucial role in demonstrating that an object-logic is faithfully expressed.

2 Representing intuitionistic propositional logic

To represent an object-logic in Isabelle we extend the meta-logic with types, constants, and axioms. A simple example is intuitionistic propositional logic (IPL).

To represent the syntax of IPL, introduce the basic type *form* for denotations of formulae. Introduce the constant symbols

$$\begin{array}{rcl} \bot & : & form \\ \&, \vee, \supset & : & form \to (form \to form) \\ \mathrm{true} & : & form \to prop \end{array}$$

Variables of type *form* include A, B, and C.

Object-sentences are enclosed in double brackets $[\![]\!]$. The meta-formula $[\![A]\!]$ abbreviates $\mathrm{true}(A)$ and means that A is true. Keeping the types *form* and *prop* distinct avoids presuming that truth-values of the object-logic are identical to those of the meta-logic. To avoid confusing these logics, let us use distinctive terminology. There is a meta-rule called

$\Rightarrow$-elimination. The similar object-rule is called the $\supset$E rule, while the corresponding meta-axiom is called the $\supset$E axiom.

The natural deduction rules (Figure 1) of intuitionistic logic are represented by meta-level axioms (Figure 2). The resulting extension of $\mathcal{M}$ is called $\mathcal{M}_{\text{IPL}}$. The outer quantifiers of meta-axioms will often be dropped.

The new symbols have the usual interpretations. Let the type *form* denote a set of truth values such that &, $\vee$, $\supset$, and $\bot$ have their intuitionistic meanings [1, Chapter 5]. The axioms are true under this semantics: for example, if A is true and B is true then $A \,\&\, B$ is true. Meta-implication ($\Rightarrow$) expresses the discharge of assumptions. The $\supset$I axiom says that if the truth of A implies the truth of B, then the formula $A \supset B$ is true.

The resemblance between the meta-level axioms and the rules should be regarded as a happy coincidence. An axiom formalizes not the syntax of a rule but its semantic justification. The resemblance diminishes in first-order logic (Section 3).

An obvious question is whether the object-logic is faithfully represented. The definition below is oriented towards natural deduction: it concerns entailments rather than theorems.

Definition 1 Let L be a logic and A_1, ..., A_m, B be formulae of L. Let $\mathcal{M}_L$ be a meta-logic obtained from $\mathcal{M}$ by adding types, constants, and axioms. Suppose that $[\![-]\!]$ is a function mapping each formula A of L to a meta-formula $[\![A]\!]$ of $\mathcal{M}_L$. Then say

- $\mathcal{M}_L$ is *sound for* L if, for every $\mathcal{M}_L$-proof of $[\![B]\!]$ from $[\![A_1]\!], \ldots, [\![A_m]\!]$, there is an L-proof of B from $A_1, \ldots, A_m$.
- $\mathcal{M}_L$ is *complete for* L if, for every L-proof of B from $A_1, \ldots, A_m$, there is an $\mathcal{M}_L$-proof of $[\![B]\!]$ from $[\![A_1]\!], \ldots, [\![A_m]\!]$.
- $\mathcal{M}_L$ is *faithful for* L if $\mathcal{M}_L$ is sound and complete for L.

Informally, $\mathcal{M}_{\text{IPL}}$ is sound for IPL because the additional axioms are true and the rules of $\mathcal{M}$ are sound. A better argument is by induction on normal proofs in $\mathcal{M}$. Here is a summary of the proof-theoretic concepts of Prawitz [5, 6]. For simplicity, let us ignore equality rules, identifying terms that are equivalent up to λ-conversions.

A *branch* in a proof traces the construction and destruction of a formula. Each branch is obtained by repeatedly walking downwards from a premise of a rule to its conclusion, but terminates at the second premise of $\Rightarrow$-elimination. Thus in

$$\frac{\phi \Rightarrow \psi \qquad \phi}{\psi}$$

a branch may connect $\phi \Rightarrow \psi$ with ψ but not ϕ with ψ since these formulae may be syntactically unrelated. (This discussion is for $\mathcal{M}$. For logics having other connectives, most elimination rules are special cases.)

Every proof in $\mathcal{M}$ can be *normalized* such that, in every branch, no elimination rule immediately follows an introduction rule. In a normal proof, every branch begins with an assumption or axiom, then has a series of eliminations, then a series of introductions. During the eliminations the formulae shrink to a minimum; during the introductions they grow again.

Observe that $[\![B]\!]$ is an atomic $\mathcal{M}_{\text{IPL}}$-formula. A normal proof can be put into *expanded* normal form, where every minimum formula is atomic [6, page 254]. For example, if a

	introduction (I)	*elimination* (E)
Conjunction	$\dfrac{A \qquad B}{A \,\&\, B}$	$\dfrac{A \,\&\, B}{A}$ $\qquad$ $\dfrac{A \,\&\, B}{B}$
Disjunction	$\dfrac{A}{A \vee B}$ $\qquad$ $\dfrac{B}{A \vee B}$	$\dfrac{A \vee B \qquad \overset{[A]}{C} \qquad \overset{[B]}{C}}{C}$
Implication	$\dfrac{\overset{[A]}{B}}{A \supset B}$	$\dfrac{A \supset B \qquad A}{B}$
Contradiction		$\dfrac{\bot}{A}$

Figure 1: The rules of intuitionistic propositional logic

$$\bigwedge AB \,.\, [\![A]\!] \Rightarrow ([\![B]\!] \Rightarrow [\![A \,\&\, B]\!]) \tag{\&I}$$

$$\bigwedge AB \,.\, [\![A \,\&\, B]\!] \Rightarrow [\![A]\!] \qquad \bigwedge AB \,.\, [\![A \,\&\, B]\!] \Rightarrow [\![B]\!] \tag{\&E}$$

$$\bigwedge AB \,.\, [\![A]\!] \Rightarrow [\![A \vee B]\!] \qquad \bigwedge AB \,.\, [\![B]\!] \Rightarrow [\![A \vee B]\!] \tag{$\vee$I}$$

$$\bigwedge ABC \,.\, [\![A \vee B]\!] \Rightarrow ([\![A]\!] \Rightarrow [\![C]\!]) \Rightarrow ([\![B]\!] \Rightarrow [\![C]\!]) \Rightarrow [\![C]\!] \tag{$\vee$E}$$

$$\bigwedge AB \,.\, ([\![A]\!] \Rightarrow [\![B]\!]) \Rightarrow [\![A \supset B]\!] \tag{$\supset$ I}$$

$$\bigwedge AB \,.\, [\![A \supset B]\!] \Rightarrow [\![A]\!] \Rightarrow [\![B]\!] \tag{$\supset$ E}$$

$$\bigwedge A \,.\, [\![\bot]\!] \Rightarrow [\![A]\!] \tag{$\bot$E}$$

Figure 2: Meta-level axioms for intuitionistic propositional logic

$$\dfrac{\dfrac{\dfrac{\bigwedge AB\,.\,[\![A]\!] \Rightarrow ([\![B]\!] \Rightarrow [\![A \,\&\, B]\!])}{\bigwedge B\,.\,[\![C]\!] \Rightarrow ([\![B]\!] \Rightarrow [\![C \,\&\, B]\!])} \quad \vdots}{[\![C]\!] \Rightarrow ([\![D]\!] \Rightarrow [\![C \,\&\, D]\!])} \quad [\![C]\!]}{[\![D]\!] \Rightarrow [\![C \,\&\, D]\!]} \quad \vdots \; [\![D]\!]}{[\![C \,\&\, D]\!]}$$

Figure 3: The meta-proof formalizing a &I inference

$$\dfrac{\dfrac{\dfrac{\bigwedge AB\,.\,([\![A]\!] \Rightarrow [\![B]\!]) \Rightarrow [\![A \supset B]\!]}{\bigwedge B\,.\,([\![C]\!] \Rightarrow [\![B]\!]) \Rightarrow [\![C \supset B]\!]}}{([\![C]\!] \Rightarrow [\![D]\!]) \Rightarrow [\![C \supset D]\!]} \quad \dfrac{[\,[\![C]\!]\,]}{\vdots \; [\![D]\!]}}{[\![C]\!] \Rightarrow [\![D]\!]}}{[\![C \supset D]\!]}$$

Figure 4: The meta-proof formalizing an $\supset$I inference

minimum formula is $\phi \Rightarrow \psi$, then the following can be spliced into the proof, reducing the minimum formula to ψ:

$$\dfrac{\dfrac{\phi \Rightarrow \psi \qquad [\phi]}{\psi}}{\phi \Rightarrow \psi}$$

Completeness holds because to each object-level inference there corresponds a meta-proof involving an $\mathcal{M}_{\mathrm{IPL}}$ axiom. Soundness holds because to each occurrence of an $\mathcal{M}_{\mathrm{IPL}}$ axiom in a meta-proof there corresponds an object-level inference. Figures 3 and 4 illustrate the correspondence.

Theorem 2 *$\mathcal{M}_{\mathrm{IPL}}$ is sound for* IPL.

Proof: By induction on the size of the expanded normal proof in $\mathcal{M}_{\mathrm{IPL}}$ of $[\![B]\!]$ from $[\![A_1]\!], \ldots, [\![A_m]\!]$, construct an IPL proof of B from $A_1, \ldots, A_m$.

Since $[\![B]\!]$ is atomic, the branch terminating with $[\![B]\!]$ cannot contain introduction rules, and thus cannot discharge assumptions. The branch must consist entirely of elimination rules. If it is just $[\![B]\!]$ then B is an assumption, one of $A_1, \ldots, A_m$. Otherwise the branch contains elimination rules, so its first formula cannot be atomic. It must consist of an axiom followed by elimination rules. There is one case for each axiom.

For the &I axiom, B is $C \,\&\, D$ for some formulae C and D. The meta-proof must have the structure of Figure 3. It has two $\bigwedge$-eliminations involving C and D, and two $\Rightarrow$-eliminations, involving proofs of $[\![C]\!]$ and $[\![D]\!]$ from $[\![A_1]\!], \ldots, [\![A_m]\!]$. By the induction hypothesis, construct IPL proofs of C and D from $A_1, \ldots, A_m$. Applying &I gives an IPL proof of $C \,\&\, D$.

For the $\supset$I axiom, B is $C \supset D$. The meta-proof must have the structure of Figure 4. It contains a proof of $[\![C]\!] \Rightarrow [\![D]\!]$ from $[\![A_1]\!], \ldots, [\![A_m]\!]$. By expanded normal form this consists of a proof of $[\![D]\!]$ from $[\![A_1]\!], \ldots, [\![A_m]\!], [\![C]\!]$, followed by $\Rightarrow$-introduction, discharging the assumption $[\![C]\!]$. By the induction hypothesis, construct an IPL proof of D from $A_1, \ldots, A_m, C$, and $\supset$I gives an IPL proof of $C \supset D$ from $A_1, \ldots, A_m$.

The cases for the other axioms are similar. $\Box$

Theorem 3 $\mathcal{M}_{\rm IPL}$ *is complete for* IPL.
Proof: By induction on the size of the IPL proof of B from $A_1, \ldots, A_m$, construct a proof of $[\![B]\!]$ from $[\![A_1]\!], \ldots, [\![A_m]\!]$ in $\mathcal{M}_{\rm IPL}$.

Suppose the last inference of the IPL proof is $\supset$I, and the conclusion is $C \supset D$. Then the rule is applied to an IPL proof of D from $A_1, \ldots, A_m, C$. By the induction hypothesis, construct an $\mathcal{M}_{\rm IPL}$-proof of $[\![D]\!]$ from $[\![A_1]\!], \ldots, [\![A_m]\!], [\![C]\!]$. Now it is easy to construct a meta-proof like that in Figure 4.

The cases for the other axioms are similar. □

3 Quantification

Many logical constants introduce bound variables: universal and existential quantifiers ($\forall$ and $\exists$), description operators (λ, ι and ϵ), general product and sum (Π and Σ), union and intersection of families (as in $\bigcup_{i\in I} A_i$), and so on. Isabelle implements logics comprising most of these.

Adding quantifiers to the previous object-logic gives intuitionistic first-order logic (IFOL). Formally, extend $\mathcal{M}_{\rm IPL}$ to become $\mathcal{M}_{\rm IFOL}$. Add the type *term* for denotations of terms. The quantifiers are the constant symbols

$$\forall, \exists \quad : \quad (\mathit{term} \to \mathit{form}) \to \mathit{form}$$

If A, $A(x)$, and $A(x,y)$ each have type *form* then the three variables named A must have different types, and so are different variables. Rather than declaring a fixed list of variables with their types, let the context determine the types — avoiding things like $A \,\&\, A(x)$. For emphasis, F, G, and H will stand for formula-valued functions.

Write $\forall x.A$ for $\forall(\lambda x.A)$ and $\exists x.A$ for $\exists(\lambda x.A)$. By λ-conversion every quantified formula is equivalent to one of the form $\forall(F)$ or $\exists(F)$, where F has type $\mathit{term} \to \mathit{form}$.

The rules (Figure 5) and their meta-level axioms (Figure 6) do not have the close resemblance that we saw for propositional logic. The eigenvariable conditions of $\forall$I and $\exists$E are not formalized literally. Note that the two conditions differ in form but not in effect. Both ensure that x serves only to specify a truth-valued function, through its occurrences in A.

In the axioms, F denotes not the text of the quantification but its meaning: a truth-valued function. The axiom $\forall$I states that if F is an everywhere-true function then $\forall x.F(x)$ is true. Similarly, B denotes not the text of a formula but a truth-value. The $\exists$E axiom states that if $\exists x.F(x)$ is true and $F(x)$ implies B for all x, then B is true. The axioms reflect the meanings of the corresponding rules.

Although the justification of each axiom is semantic, they behave as expected in syntax. Substitution for the variables F and B avoids capture of the variable x. In particular, B may not be replaced by a formula containing x. Assumptions also obey the eigenvariable conditions, as we shall see below.

The demonstration that these axioms faithfully represent first-order logic is similar to that for propositional logic (Section 2).

Theorem 4 $\mathcal{M}_{\rm IFOL}$ *is sound for* IFOL.
Proof: By induction over the expanded normal proof in $\mathcal{M}_{\rm IFOL}$ of $[\![B]\!]$ from $[\![A_1]\!], \ldots, [\![A_m]\!]$, construct an IFOL proof of B from $A_1, \ldots, A_m$. The branch terminating with $[\![B]\!]$, unless it is trivial, consists of an axiom followed by elimination rules.

	introduction (I)	*elimination* (E)
Universal quantifier	$\dfrac{A}{\forall x.A}*$	$\dfrac{\forall x.A}{A[t/x]}$
Existential quantifier	$\dfrac{A[t/x]}{\exists x.A}$	$\dfrac{\exists x.A \qquad \begin{matrix}[A]\\ B\end{matrix}}{B}*$

**Eigenvariable conditions*:
$\forall$I: provided x not free in the assumptions
$\exists$E: provided x not free in B or in any assumption save A

Figure 5: Quantifier rules

$$\bigwedge F\,.\,(\bigwedge x\,.\,[\![F(x)]\!]) \Rightarrow [\![\forall x.F(x)]\!] \tag{$\forall$I}$$

$$\bigwedge Fy\,.\,[\![\forall x.F(x)]\!] \Rightarrow [\![F(y)]\!] \tag{$\forall$E}$$

$$\bigwedge Fy\,.\,[\![F(y)]\!] \Rightarrow [\![\exists x.F(x)]\!] \tag{$\exists$I}$$

$$\bigwedge FB\,.\,[\![\exists x.F(x)]\!] \Rightarrow (\bigwedge x\,.\,[\![F(x)]\!] \Rightarrow [\![B]\!]) \Rightarrow [\![B]\!] \tag{$\exists$E}$$

Figure 6: Meta-level axioms for the quantifier rules

$$\dfrac{\dfrac{\dfrac{\bigwedge Fy\,.\,[\![F(y)]\!] \Rightarrow [\![\exists x.F(x)]\!]}{\bigwedge y\,.\,[\![G(y)]\!] \Rightarrow [\![\exists x.G(x)]\!]}}{[\![G(u)]\!] \Rightarrow [\![\exists x.G(x)]\!]} \qquad \begin{matrix}\vdots\\ [\![G(u)]\!]\end{matrix}}{[\![\exists x.G(x)]\!]}$$

Figure 7: The meta-proof formalizing an $\exists$I inference

$$\dfrac{\dfrac{\dfrac{\dfrac{\bigwedge FB\,.\,[\![\exists x.F(x)]\!] \Rightarrow (\bigwedge x\,.\,[\![F(x)]\!] \Rightarrow [\![B]\!]) \Rightarrow [\![B]\!]}{\bigwedge B\,.\,[\![\exists x.G(x)]\!] \Rightarrow (\bigwedge x\,.\,[\![G(x)]\!] \Rightarrow [\![B]\!]) \Rightarrow [\![B]\!]}}{[\![\exists x.G(x)]\!] \Rightarrow (\bigwedge x\,.\,[\![G(x)]\!] \Rightarrow [\![C]\!]) \Rightarrow [\![C]\!]} \qquad \begin{matrix}\vdots\\ [\![\exists x.G(x)]\!]\end{matrix}}{(\bigwedge x\,.\,[\![G(x)]\!] \Rightarrow [\![C]\!]) \Rightarrow [\![C]\!]} \qquad \dfrac{\begin{matrix}[\,[\![G(y)]\!]\,]\\ \vdots\\ [\![C]\!]\end{matrix}}{[\![G(y)]\!] \Rightarrow [\![C]\!]}}{[\![C]\!]} \qquad \dfrac{}{\bigwedge y\,.\,[\![G(y)]\!] \Rightarrow [\![C]\!]}$$

Figure 8: The meta-proof formalizing an $\exists$E inference

For the $\exists$I axiom, B is $\exists x.G(x)$. The normalized proof must have the form shown in Figure 7. Two $\bigwedge$-eliminations introduce G and u; then $\Rightarrow$-elimination is applied to a proof of $[\![G(u)]\!]$ from $[\![A_1]\!], \ldots, [\![A_m]\!]$. By the induction hypothesis construct an IFOL proof of $G(u)$ from $A_1, \ldots, A_m$, and use the $\exists$I rule to prove $\exists x.G(x)$. The $\mathcal{M}_{\rm IFOL}$ proof is shown without β-conversions, identifying terms that have the same normal form. If G is $\lambda x.A$ then $G(u) \equiv A[u/x]$, and $[\![\exists x.G(x)]\!] \equiv [\![\exists x.A]\!]$.

For $\exists$E, the proof (Figure 8) contains a proof of $\bigwedge y\,.\,[\![G(y)]\!] \Rightarrow [\![C]\!]$ from $[\![A_1]\!]$, ..., $[\![A_m]\!]$. Assuming expanded normal form, it consists of a proof of $[\![C]\!]$ followed by $\Rightarrow$-introduction, discharging $[\![G(y)]\!]$, followed by $\bigwedge$-introduction. (The bound variable y can be chosen so that it is not free in $[\![A_1]\!], \ldots, [\![A_m]\!]$.) By the induction hypothesis, there are IFOL proofs of C from $A_1, \ldots, A_m, G(y)$ and of $\exists x.G(x)$ from $A_1, \ldots, A_m$. The $\exists$E rule gives an IFOL proof of C from $A_1, \ldots, A_m$.

The cases for the other axioms are similar. $\Box$

Theorem 5 *$\mathcal{M}_{\rm IFOL}$ is complete for* IFOL.
Proof: By induction over the IFOL proof of B from $A_1, \ldots, A_m$, construct a proof of $[\![B]\!]$ from $[\![A_1]\!], \ldots, [\![A_m]\!]$ in $\mathcal{M}_{\rm IFOL}$.

The hardest case is when the last inference is $\exists$E. Then the rule is applied to an IFOL proof of $\exists x.A$, and to a proof of B from A. By the axiom for $\exists$E, it is enough to prove the theorems $[\![\exists x.A]\!]$ and $\bigwedge x\,.\,[\![A]\!] \Rightarrow [\![B]\!]$. By the induction hypothesis, there is an $\mathcal{M}_{\rm IFOL}$-proof of $[\![\exists x.A]\!]$, and also a proof of $[\![B]\!]$ from $[\![A]\!]$. The meta-proof resembles that in Figure 8, where G is $\lambda x.A$. Again, terms having the same normal form are identified. $\Box$

Remark. Perhaps the type names *term* and *form* are overly syntactic; *term* denotes a set of individuals while *form* denotes a set of truth-values. The meaning of $A \supset B$ should depend on the meanings of A and B, not on their syntactic structure.

Still, types play an important syntactic role. An expression of type *term* represents an IFOL term, and similarly *form* represents formulae. By assigning a type to each syntactic category of the object-logic, type-checking in $\mathcal{M}$ enforces syntactic constraints.

References

[1] Michael Dummett. *Elements of Intuitionism*. Oxford University Press, 1977.

[2] J. Roger Hindley and Jonathon P. Seldin. *Introduction to Combinators and λ-Calculus*. Cambridge University Press, 1986.

[3] Lawrence C. Paulson. The foundation of a generic theorem prover. *Journal of Automated Reasoning*, 5(3):363–397, 1989.

[4] Lawrence C. Paulson. Isabelle: The next 700 theorem provers. In P. Odifreddi, editor, *Logic and Computer Science*, pages 361–386. Academic Press, 1990.

[5] Dag Prawitz. *Natural Deduction: A Proof-theoretical Study*. Almquist and Wiksell, 1965.

[6] Dag Prawitz. Ideas and results in proof theory. In J. E. Fenstad, editor, *Second Scandinavian Logic Symposium*, pages 235–308. North-Holland, 1971.