From de Jongh's theorem to intuitionistic logic of proofs

Sergei Artemov
City University of New York
Graduate Center
365 Fifth Avenue
New York, NY 10016, U.S.A.
SArtemov@gc.cuny.edu

Rosalie Iemhoff*
Institute for Discrete Mathematics and Geometry, Technical University Vienna
Wiedner Hauptstrasse 8-10
1040, Vienna, Austria
Iemhoff@logic.at

July, 2004

Abstract

The famous de Jongh's theorem of 1970 stated that the intuitionistic logic captured all the logical formulas which have all arithmetical instances derivable in the Heyting Arithmetic HA. In this note we extend de Jongh's arithmetical completeness property from IPC to the basic intuitionistic logic of proofs, which allows proof assertion statements of the sort *x is a proof of F*. The logic of proofs seems to provide an appropriate language of describing admissible rules in HA.

1 Introduction.

De Jongh's theorem [14] on the "maximality" of intuitionistic logic with respect to Heyting's Arithmetic HA has been a precursor of the whole series of arithmetical completeness theorems for various nonclassical logics, e.g. Solovay's arithmetical completeness theorem with respect to the classical Peano Arithmetic PA for the provability logic GL [20], Shavrukov and Berarducci arithmetical completeness theorem for the interpretability logic ILM [6, 18], arithmetical completeness of the logic of proofs LP [2, 3], etc.

In this paper we begin tackling the problem of building the intuitionistic logic of proofs, more precisely, a logic of proofs for HA. This problem has numerous motivations. Here are some of them

- The logic of proofs for HA provides a proper format for internalizing admissible rules in HA as proof terms and studying their functional and algebraic behavior.
- The future system of intuitionistic proof terms will be a nontrivial extension of the typed combinatory logic/λ-calculus and could serve as a source of new principles of reflexive character for the latter. Along with the intended provability interpretation these new principles have meaningful computational interpretation as well [4]. This considerably enhances the Curry-Howard isomorphism of constructive proofs and typed λ-terms which has a potential of influencing applications to functional programming.

*Supported by the Austrian Science Fund FWF under projects P16264 and P16539.

- The intuitionistic logic of proofs provides a more expressive version of the modal λ-calculus [7, 15, 16] which also has interesting applications.

There are two distinct parts of the problem of building the intuitionistic logic of proofs. Firstly, one has to answer the question about propositional logical principles that axiomatize HA-tautologies in the propositional language enriched by new atoms $u:F$ denoting *u is a proof of F* without any operations on proof terms, i.e. when u is a variable. The resulting *Basic Intuitionistic Logic of Proofs*, iBLP, reflects purely logical principles of the chosen format. Secondly, one has to pick appropriate natural systems of proof terms and study versions of the intuitionistic logic of proofs corresponding to there versions. In this paper we will concentrate on solving the first of the above problems and discuss the second one in section 4.

This paper combines technique and results by de Jongh [14], Smorynski [19], de Jongh and Visser work on a basis for admissible rules in IPC (circa 1991, cf. [11]), Artemov & Strassen [5] and Artemov [1], Ghilardi [8], Iemhoff [10, 12, 13].

2 Preliminaries.

The language of the basic logic of proofs consists of the usual language of propositional logic (with $\perp$) plus proof variables $u, v, w, \ldots$. Using u to stand for any proof variable and p for any propositional variable, the formulas are defined by the grammar

$$A \equiv_{def} p \mid A_1 \rightarrow A_2 \mid A_1 \wedge A_2 \mid A_1 \vee A_2 \mid u{:}A.$$

$\neg A$ is defined as $A \rightarrow \perp$. An *atom* is a propositional variable or a formula of the form $u:F$. A *literal* is an atom or the negation of an atom. Note that we can consider the language of the basic logic of proofs as a propositional language in which some propositional variables, $u:A$, are labelled by a formula in the language. When we write a formula in the context of IPC, e.g. in expressions $\nvdash_{\mathsf{IPC}} A$ or $\mathrel{|\!\sim}_{\mathsf{IPC}} A$, A should be interpreted as a propositional formula in the way just explained. Subformulas are defined as usual, with the extra clause that $u{:}A$ and subformulas of A are subformulas of $u{:}A$. We adhere to the convention that "u:" and "$\neg$" bind stronger than "$\wedge$", "$\vee$", which bind stronger than "$\rightarrow$".

Definition 1. A *proof predicate* is a primitive recursive formula $Prf(x, y)$ such that for every arithmetical sentence φ

$$\mathsf{HA} \vdash \varphi \quad \Leftrightarrow \quad \text{for some } n \in \omega \quad Prf(n, \ulcorner\varphi\urcorner) \text{ holds}^1.$$

Definition 2. An *arithmetical interpretation* * has the following parameters [1, 5].

1. a proof predicate $Prf(x, y)$,
2. a mapping of propositional variables p to sentences p^* of HA,
3. a mapping of proof variables u to natural numbers u^*.

The arithmetical interpretation F^* of a formula F is defined inductively

$$\perp^* := (0 = 1), \quad (A \rightarrow B)^* := A^* \rightarrow B^*, \quad (u{:}A)^* := Prf(u^*, \ulcorner A^* \urcorner)$$

Naturally, an arithmetical interpretation of the iBLP-language can be considered as a special case of the arithmetical substitution in the language of IPC.

[1] We omit bars over numerals for natural numbers $n, \ulcorner\varphi\urcorner$, etc.

2.1 Substitutions.

We will use two kind of substitutions. Substitutions of propositional formulas for propositional variables are denoted by σ or σ'. Substitutions of arithmetical formulas for propositional letters are denoted by τ or τ'. For a set of formulas Γ we write $\sigma\Gamma$ for $\{\sigma A \mid A \in \Gamma\}$. If formulas in the language of iBLP are involved, these substitutions consider them as formulas in propositional logic in the way explained above, i.e. such that expressions $u{:}A$ are treated as propositional variables. For example $\sigma(u{:}A)$ may be any propositional formula, and $\sigma(v{:}(u{:}p))$ bears no connection to $\sigma(u{:}p)$ or σp.

2.2 Admissible rules.

A *(propositional) admissible rule* of a logic L is a rule A/B, where A and B are propositional formulas, such that adding the rule to the logic does not lead to new theorems of L, i.e. for any substitution σ of formulas of L for propositional variables

$$\vdash_{\mathsf{L}} \sigma A \text{ implies } \vdash_{\mathsf{L}} \sigma B.$$

We write $A \mathrel{|\!\sim}_{\mathsf{L}} B$ if A/B is an admissible rule of L. The rule is called *derivable* if $\vdash_{\mathsf{L}} A \to B$ and *nonderivable* if $\nvdash_{\mathsf{L}} A \to B$. We say that a collection R of rules is admissible for L if all rules in R are admissible for L. R is derivable for L if all rules in R are derivable for L. We write $A \vdash^R_{\mathsf{L}} B$ if B is derivable from A in the logic consisting of L extended with the rules R, i.e. if there are $A = A_1, \ldots, A_n = B$ such that for all $i < n$, $A_i \vdash_{\mathsf{L}} A_{i+1}$ or there exists a σ such that $\sigma B_i/\sigma B_{i+1} = A_i/A_{i+1}$ and $B_i/B_{i+1} \in R$. A set R of admissible rules of L is a *basis for the admissible rules of* L if for every admissible rule $A \mathrel{|\!\sim}_{\mathsf{L}} B$ we have $A \vdash^R_{\mathsf{L}} B$.

Definition 3. The *basic intuitionistic logic of proofs*, iBLP, consists of the following axioms

$A1$	Theorems of IPC	
$A2$	$u{:}F \to F$	
$A3$	$u{:}F \vee \neg u{:}F$	
$A4$	$\bigwedge_{i=1}^n (u_i{:}F_i) \to G$	for F_i, G such that $(\bigwedge_{i=1}^n F_i) \mathrel{|\!\sim}_{\mathsf{HA}} G$
$R1$	Rule *Modus Ponens*	

Note that in A4 the F_i and G are considered as propositional formulas, see the remarks about this at section on substitutions.

As it follows from well-known results by Rybakov [17] and Visser [21], the predicate $F \mathrel{|\!\sim}_{\mathsf{HA}} G$ is decidable, hence axioms of iBLP constitute a decidable set of formulas.

Proposition 1. iBLP *is sound for* HA.

Proof. It suffices to show that for any arithmetical interpretation *, for all instances A of one of the axioms, A^* is provable in HA. We only treat the case that A is an instance of $A4$ and leave the other cases to the reader. Thus A is of the form $\bigwedge_{i=1}^n (u_i{:}F_i) \to G$ for some F_i and G such that $(\bigwedge_{i=1}^n F_i) \mathrel{|\!\sim}_{\mathsf{IPC}} G$. Whence A^* is

$$\bigwedge_{i=1}^n \mathit{Prf}(m_i, F_i^*) \to G^*,$$

where $u_i^* = m_i$. Since *Prf*, being a primitive recursive predicate, is decidable in HA, either $\mathsf{HA} \vdash \mathit{Prf}(m_i, F_i^*)$ for all $i \leq n$, or $\mathsf{HA} \vdash \neg\mathit{Prf}(m_i, F_i^*)$ for some $i \leq n$. In the last case it follows immediately that A^* is provable in HA, as in this case

$\mathsf{HA} \vdash \neg \bigwedge_{i=1}^{n} Prf(m_i, F_i^*)$. We consider the first case. As HA is sound this implies that $\mathsf{HA} \vdash F_i^*$, for all $i \leq n$. The fact that $\bigwedge_{i=1}^{n} F_i \mathrel{|\!\sim}_{\mathsf{HA}} G$ means that for all arithmetical substitutions τ, $\mathsf{HA} \vdash \bigwedge_{i=1}^{n} \tau F_i$ implies $\mathsf{HA} \vdash \tau G$. As explained above, in the context of propositional logic an arithmetical interpretation can be considered as an arithmetical substitution. As we have $\mathsf{HA} \vdash \bigwedge_{i=1}^{n} F_i^*$, this therefore implies that $\mathsf{HA} \vdash G^*$, and hence A^* is provable in HA also in this case. $\square$

In Section 3 we will show that iBLP is also complete for HA. First, we present a more transparent axiomatization of iBLP by giving a simple axiomatization of $A4$. This axiomatization is given in terms of so-called *Visser's* rules V_n that are defined as follows.

Definition 4. For A of the form $(A_0 \to A_{n+1} \vee A_{n+2})$, with $A_0 = \bigwedge_{i=1}^{n}(A_i \to B_i)$, we define

$$A^V = \bigvee_{i=1}^{n+2} (A_0 \to A_i).$$

Visser's rules V_n are defined as

$$V_n \qquad \bigwedge_{i=1}^{n}(A_i \to B_i) \to A_{n+1} \vee A_{n+2} \ / \ \Big(\bigwedge_{i=1}^{n}(A_i \to B_i) \to A_{n+1} \vee A_{n+2}\Big)^V.$$

We denote $\{V_n \mid n \in \omega\}$ by V.

Note that for such A of the form

$$\bigwedge_{i=1}^{n}(A_i \to B_i) \to A_{n+1} \vee A_{n+2}$$

it classically holds that $(A \to \bigvee_{i=1}^{n+2} A_i)$, whence also $A \to A^V$. This in contrast to IPC in which this is not derivable. As was first observed by D. de Jongh and A. Visser, the rules V are admissible for IPC (cf. [11]). Whence they are non-derivable admissible rules of IPC. Thus $A \mathrel{|\!\sim}_{\mathsf{IPC}} A^V$, while in general not $A \nvdash_{\mathsf{IPC}} A^V$. Some well-known admissible rules are instances of Visser's rules, e.g. Harrop's rule

$$\neg A \to B \vee C \mathrel{|\!\sim} (\neg A \to B) \vee (\neg A \to C).$$

Namely, $(\neg A \to B \vee C)^V = (\neg A \to B) \vee (\neg A \to C) \vee (\neg A \to A)$. Since $(\neg A \to A) \leftrightarrow \neg\neg A$, $(\neg A \to B \vee C)^V \leftrightarrow (\neg A \to B) \vee (\neg A \to C)$.

Visser's rules provide an alternative axiomatization for iBLP in the following way.

Theorem 1. *In the axiomatization of* iBLP *the axiom* $A4$ *can be replaced by the axiom*

$$\bigwedge_{i=1}^{n}(u_i : F_i) \to G \quad \textit{for } F_i, G \textit{ such that } (\bigwedge_{i=1}^{n} F_i) \vdash_{\mathsf{IPC}}^{V} G.$$

Proof. In [21] it is shown that the propositional admissible rules of HA are the same as the admissible rules of IPC. Whence $A4$ can be replaced by

$$\bigwedge_{i=1}^{n}(u_i : F_i) \to G \quad \text{for } F_i, G \text{ such that } (\bigwedge_{i=1}^{n} F_i) \mathrel{|\!\sim}_{\mathsf{IPC}} G.$$

In [10, 11] it was established that Visser's rules form a basis for the admissible rules of IPC, i.e. $\mathrel{|\!\sim}_{\mathsf{IPC}}$ is equivalent to $\vdash_{\mathsf{IPC}}^{V}$. This proves the theorem. $\square$

2.3 Kripke models and the extension property.

Kripke models for intuitionistic propositional logic are defined as usual. We assume our models to be rooted. We say that two Kripke models are *variants* of each other when they have the same set of nodes and partial order, and their valuations agree on all nodes except possibly the root. Given Kripke models $K_1, \ldots, K_n$, $(\Sigma K_i)'$ denotes the Kripke model which is the result of attaching one new node at which no propositional variables are forced, below all nodes in $K_1, \ldots, K_n$. $(\Sigma)'$ is called the *Smorynski operator*. A class of models $\mathcal{K}$ has the *extension property* if for every family of models $K_1, \ldots, K_n \in \mathcal{K}$,there is a variant of $(\sum_i K_i)'$ which belongs to $\mathcal{K}$. A formula has the extension property if its class of models has the extension property.

2.4 Projective formulas.

Definition 5. A formula A is called *projective* if there exists a substitution σ, a *projective unifier of* A, such that

$$\vdash_{\mathsf{IPC}} \sigma A \text{ and } \forall B \; (A \vdash_{\mathsf{IPC}} B \leftrightarrow \sigma B).$$

A *projective approximation* Π_A of A is a set of projective formulas in which no other variables occur than the ones that occur in A, and such that $B \vdash A$ for all $B \in \Pi_A$, and which is maximal as such, i.e. such that for every projective formula C such that $C \vdash A$, there exists a $B \in \Pi_A$ such that $C \vdash B$. In fact, in the definition of projective approximation from [9] there is also a complexity bound on the formulas in Π_A, but as we do not need it in the sequel, we have omitted it in the definition given here. The properties that we use of Π_A remain the same under this omission. Define

$$\bar{\Pi}_A \equiv_{def} \{B \mid B \text{ is projective and } B \vdash_{\mathsf{IPC}} A\}.$$

Note that for projective A with projective unifier σ, $\{B \mid A \vdash_{\mathsf{IPC}} B\} = \{B \mid \vdash_{\mathsf{IPC}} \sigma B\}$. Thus A axiomatizes the logic of formulas valid in IPC under σ.

Theorem 2 (Ghilardi [9])**.**

1. *A is projective if and only if A has the extension property.*
2. *Every consistent formula has a finite projective approximation.*
3. *For every σ such that $\vdash_{\mathsf{IPC}} \sigma A$, there is a $B \in \Pi_A$ such that $\vdash_{\mathsf{IPC}} \sigma B$.*

Theorem 3. *For each finite projective approximation Π_A of A, we have $A \vdash^V_{\mathsf{IPC}} \bigvee \Pi_A$.*

Proof. From the previous theorem it follows that $A \mathrel{|\!\sim}_{\mathsf{IPC}} \bigvee \Pi_A$. For suppose that for some substitution σ, $\vdash_{\mathsf{IPC}} \sigma A$. Then by the last part of the previous theorem it follows that there is a $B \in \Pi_A$ such that $\vdash_{\mathsf{IPC}} \sigma B$. Hence $\vdash_{\mathsf{IPC}} \sigma(\bigvee \Pi_A)$. This proves that $A \mathrel{|\!\sim}_{\mathsf{IPC}} \bigvee \Pi_A$. In [10] it has been shown that V is a basis for the admissible rules of IPC, that is, that $\mathrel{|\!\sim}_{\mathsf{IPC}}$ is equivalent to $\vdash^V_{\mathsf{IPC}}$. Therefore, $A \vdash^V_{\mathsf{IPC}} \bigvee \Pi_A$. $\square$

Projective formulas show special behavior with respect to admissibility: it is not difficult to see that for projective formulas A and for all B we have that $A \mathrel{|\!\sim} B$ if and only if $A \vdash B$. Together with the fact that $A \mathrel{|\!\sim} \bigvee \Pi_A$ this implies that for all A

$$A \mathrel{|\!\sim}_{\mathsf{IPC}} B \text{ if and only if } \Pi_A \vdash_{\mathsf{IPC}} B.$$

The direction from left to right follows from the fact that all formulas in Π_A are projective and imply A. The other direction follows from the fact that $A \mathrel{|\!\sim} \bigvee \Pi_A$.

Lemma 1. *If A is projective, B is an atom or the negation of an atom, and $A \wedge B$ is consistent, then $A \wedge B$ is projective.*

Proof. Show that $A \wedge B$ has the extension property. $\square$

2.5 Projective saturation.

In the completeness proof for iBLP we show that if $\Gamma \nvdash_{\mathsf{iBLP}} A$ then $\Gamma^* \nvdash_{\mathsf{HA}} A^*$ for some arithmetical interpretation *. In the proof we need to replace Γ by some set Θ with some extra properties as given in the lemma below. The main idea is that we have to make sure that a certain projective formula belongs to Θ.

Definition 6. For a given set X of iBLP-formulas we define

$$\begin{array}{lll} X_0 & \equiv_{def} & \{B \mid u:B \in X\} \\ X_1 & \equiv_{def} & X_0 \cup \{u:B \mid u:B \in X\} \cup \{\neg u:B \mid \neg u:B \in X\} \end{array}$$

An implication $(\bigwedge \Gamma \to A)$ is called *projectively saturated* if

Γ is consistent,

$\Gamma \cap \bar{\Pi}_{\Gamma_1}$ is nonempty,

$u:B \in \Gamma$ or $\neg u:B \in \Gamma$, for all $u:B$ that occur in Γ or A.

Lemma 2. *If $\Gamma \nvdash_{\mathsf{iBLP}} A$, then there exists a projectively saturated $(\bigwedge \Theta \to A)$ such that $\Theta \supseteq \Gamma$ and $\Theta \nvdash_{\mathsf{iBLP}} A$. If Γ is finite, we can take Θ finite.*

Proof. First construct $\Delta \supseteq \Gamma$ such that $\Delta \nvdash_{\mathsf{iBLP}} A$, and $u:B \in \Delta$ or $\neg u:B \in \Delta$, for all $u:B$ that occur in Δ or A. Δ can be obtained by standard saturation techniques. It is finite when Γ is finite. Let $B = \bigwedge \Delta_0$. As $\Delta_0 \vdash^{V}_{\mathsf{IPC}} \bigvee \Pi_{\Delta_0}$ by Theorem 3, we have $\Delta \vdash_{\mathsf{iBLP}} \bigvee \Pi_{\Delta_0}$ by the axioms of iBLP (Theorem 1). Therefore, there is a $C \in \Pi_{\Delta_0}$ such that $\Delta \wedge C \nvdash_{\mathsf{iBLP}} A$. For if not, $\Delta \wedge \bigvee \Pi_{\Delta_0} \vdash_{\mathsf{iBLP}} A$, and whence $\Delta \vdash_{\mathsf{iBLP}} A$. Let

$$B = C \wedge \bigwedge \{u:D, \neg v:E \mid u:D \in \Delta, \neg v:E \in \Delta\}$$

and $\Theta = \Delta \cup \{B\}$. Note that $\Theta \nvdash_{\mathsf{iBLP}} A$. Therefore, it remains to show that $(\bigwedge \Theta \to A)$ is projectively saturated, for which it suffices to show that

1. Θ is consistent,
2. $B \vdash_{\mathsf{IPC}} \Theta_1$ and B is projective,
3. $u:D \in \Theta$ or $\neg u:D \in \Theta$, for all $u:D$ that occur in Θ or A.

We leave verification of the first statement to the reader. For the last statement, consider a $u:D$ that occurs in Θ or A. Thus $u:D$ occurs in Δ or B or A, and thus in Δ or C, by the definition of Δ and of B. By the definition of $\bigvee \Pi_{\Delta_0}$, all variables that occur in C occur in Δ_0, whence in Δ. Thus $u:D$ occurs in Δ. The construction of Δ implies that whence $u:D \in \Delta$ or $\neg u:D \in \Delta$, which again implies the statement. For the second statement, note that the projectivity of B follows from Lemma 1. For $B \vdash_{\mathsf{IPC}} \Theta_1$, consider a $u:D \in \Theta$. As observed above, $u:D$ occurs in Δ, and whence $u:D \in \Delta$ by the consistency of Θ. Therefore, $B \vdash_{\mathsf{IPC}} u:D$. Similar reasoning applies to $\neg u:D \in \Theta$. $\square$

3 Completeness.

In the completeness proof for iBLP that we present in this section we will use de Jongh's theorem that states that the propositional logic of HA is IPC.

Theorem 4 (de Jongh's theorem [19])**.**
$\mathsf{IPC} \vdash A$ *if and only if* $\mathsf{HA} \vdash \tau A$ *for all substitutions* τ*.*

The main part of the completeness proof lies in the following lemma that shows that the existence of certain substitutions suffice to construct certain arithmetical interpretations.

Lemma 3. *If for some finite projectively saturated* $(\bigwedge \Gamma \to A)$*,* $\Gamma \nvdash_{\mathsf{iBLP}} A$ *and there is a substitution* σ *such that*

1. $\vdash_{\mathsf{IPC}} \sigma B \wedge \sigma(u\!:\!B)$ *for all* $u\!:\!B \in \Gamma$*,*
2. $\vdash_{\mathsf{IPC}} \neg\sigma(u\!:\!B)$ *for all* $\neg u\!:\!B \in \Gamma$*,*
3. $\sigma\Gamma \nvdash_{\mathsf{IPC}} \sigma A$*,*

then there is a arithmetical interpretation * *such that* $\Gamma^* \nvdash_{\mathsf{HA}} A^*$*.*

Proof. Let $\bigwedge \Gamma \to A$ be as in the lemma. Let $\circ$ denote composition of substitutions. By de Jongh's theorem (Theorem 4), using the fact that Γ is finite, there is a substitution τ' such that $\tau' \circ \sigma(\Gamma) \nvdash_{\mathsf{HA}} \tau' \circ \sigma(A)$. Let $\tau = \tau' \circ \sigma$. Thus $\tau\Gamma \nvdash_{\mathsf{HA}} \tau A$. Recall that σ, τ' and τ treat formulas $u\!:\!B$ as propositional variables. Note that

$$\forall u\!:\!B \in \Gamma\ \mathsf{HA} \vdash \tau B \wedge \tau(u\!:\!B) \text{ and } \forall \neg u\!:\!B \in \Gamma\ \mathsf{HA} \vdash \neg\tau(u\!:\!B). \tag{1}$$

We pick a Gödel numbering of the joint language of iBLP and HA that is injective, i.e. such that

$$\ulcorner A \urcorner = \ulcorner B \urcorner \leftrightarrow \ \textit{A and B coincide.}$$

We define a desired arithmetical interpretation * by a fixed point construction in a similar way as in [3]. First for a given proof predicate $\mathit{Prf}(x, y)$ we define an auxiliary translation $(\cdot)^+$ as follows:

$$\begin{array}{lcll} p^+ & = & \tau(p) & \text{for propositional variables } p \\ u^+ & = & \ulcorner u \urcorner & \text{for proof variables } u \\ (u\!:\!B)^+ & = & \mathit{Prf}(u^+, \ulcorner B^+ \urcorner) & \\ \multicolumn{4}{l}{(\cdot)^+ \text{ commutes with connectives}} \end{array}$$

Let $\mathit{PROOF}(x, y)$ denote a standard nondeterministic proof predicate

x is a code of a derivation in HA *which contains a formula having a code y.*

Without loss of generality we assume that $\mathit{PROOF}(\ulcorner u \urcorner, n)$ is false for any proof variable u and any $n \in \omega$. By the arithmetical fixed point argument we construct a formula $\mathit{Prf}(x, y)$ such that HA proves the following fixed point equation:

$$\begin{array}{lcl} \mathit{Prf}(x, y) & \leftrightarrow & \mathit{PROOF}(x, y) \vee \text{“}x = \ulcorner u \urcorner \text{ for some proof variable } u \text{ and} \\ & & y = \ulcorner B^+ \urcorner \text{ for some } \mathsf{iBLP}\text{-formula } B \text{ such that } u\!:\!B \in \Gamma\text{”} \end{array}$$

Consider the arithmetical interpretation $(\cdot)^*$ given by Prf as a proof predicate and by

$$\begin{array}{lcll} p^* & = & \tau(p) & \text{for propositional variables } p \\ u^* & = & \ulcorner u \urcorner & \text{for proof variables } u. \end{array}$$

The following claims imply that Prf is indeed a proof predicate and that $\Gamma^* \nvdash_{\mathsf{HA}} A^*$, and whence complete the proof of the theorem.

Claim 4. *For all B, $B^+ = B^*$. For all B that occur in Γ or A, $\mathsf{HA} \vdash B^* \leftrightarrow \tau B$. For all proof variables u, $u^+ = u^*$.*

Proof of the claim. The last statement holds by definition. For the first statement we use formula induction. If B is a propositional letter, $B^+ = \tau(B) = B^*$. If $B = u : C$, $B^+ = \mathit{Prf}(\ulcorner u \urcorner, \ulcorner B^+ \urcorner) = \mathit{Prf}(u^*, \ulcorner B^* \urcorner) = B^*$ because $\ulcorner u \urcorner = u^*$ and $B^+ = B^*$ by IH, whence $\ulcorner B^+ \urcorner = \ulcorner B^* \urcorner$. The steps corresponding to the connectives follow easily.

The second statement is also proved by formula induction. Consider a B that occurs in Γ or A. If B is a propositional letter it follows by definition. If $B = u : C$, either $u : C \in \Gamma$ or $\neg u : C \in \Gamma$, as $\Gamma \to A$ is projectively saturated. If $u : C \in \Gamma$, then $\mathsf{HA} \vdash \tau(u : C)$ by (1). By the fixed point equation above, $\mathsf{HA} \vdash \mathit{Prf}(u^+, \ulcorner C^+ \urcorner)$, whence $\mathsf{HA} \vdash (u : C)^+$. By the first statement of the claim this implies $\mathsf{HA} \vdash (u : C)^*$. Thus $\mathsf{HA} \vdash (u : C)^* \leftrightarrow \tau(u : C)$. The case that $\neg u : C \in \Gamma$ is similar. The steps corresponding to the connectives are easy.

Claim 5. $\mathsf{HA} \vdash \varphi$ *if and only if* $\mathit{Prf}(n, \ulcorner \varphi \urcorner)$ *for some* $n \in \omega$.

Proof of the claim. The direction from left to right is clear, as the standard proof predicate PROOF is contained in Prf. For the direction from right to left, we distinguish two cases: $\mathit{PROOF}(n, \ulcorner \varphi \urcorner)$ or $n = \ulcorner u \urcorner$ and $\ulcorner \varphi \urcorner = \ulcorner B^+ \urcorner$ for some proof variable u and some iBLP-formula B such that $u : B \in \Gamma$. In the first case, $\mathsf{HA} \vdash \varphi$ follows because PROOF is the standard proof predicate. In the second case, note that $u : B \in \Gamma$ implies $\mathsf{HA} \vdash \tau B$ by (1). Thus, by the previous claim and the fact that B occurs in Γ, $\mathsf{HA} \vdash B^+$. By assumption on the Gödel numbering, φ and B^+ coincide, which gives $\mathsf{HA} \vdash \varphi$. This finishes the proof of the lemma. $\square$

Theorem 5. *For finite Γ, $\Gamma \vdash_{\mathsf{iBLP}} A$ if and only if $\Gamma^* \vdash_{\mathsf{HA}} A^*$ for every arithmetical interpretation *.*

Proof. Soundness, the direction from left to right, is treated in Proposition 1. We prove completeness. Assume $\Gamma \nvdash_{\mathsf{iBLP}} A$. By Lemma 2, there is a finite $\Theta \supseteq \Gamma$ such that $\bigwedge \Theta \to A$ is projectively saturated and $\Theta \nvdash_{\mathsf{iBLP}} A$. We show that there is an arithmetical interpretation such that $\Theta^* \nvdash_{\mathsf{HA}} A^*$. This will prove that $\Gamma^* \nvdash_{\mathsf{HA}} A^*$. Let $B \in \Theta \cap \bar{\Pi}_{\Theta_1}$, which exists because Θ is saturated. Let σ be a projective unifier for B, i.e. a substitution such that

$$\vdash_{\mathsf{IPC}} \sigma B \text{ and } \forall D \ (B \vdash D \leftrightarrow \sigma D).$$

We show that σ fulfills the conditions of Lemma 3, i.e.

1. $\vdash_{\mathsf{IPC}} \sigma C \wedge \sigma(u : C)$ for all $u : C \in \Theta$,
2. $\vdash_{\mathsf{IPC}} \neg \sigma(u : C)$ for all $\neg u : C \in \Theta$,
3. $\sigma \Theta \nvdash_{\mathsf{IPC}} \sigma A$,

Recall (Section 2.4) that

$$\{D \mid B \vdash_{\mathsf{IPC}} D\} = \{D \mid \vdash_{\mathsf{IPC}} \sigma D\}.$$

For 3., note that since $\Theta \vdash_{\mathsf{IPC}} B$, we have $B \nvdash_{\mathsf{IPC}} \bigwedge \Theta \to A$, and thus $\nvdash_{\mathsf{IPC}} \sigma(\bigwedge \Theta \to A)$. For 1. and 2., consider $u : D \in \Theta$. Then $D \in \Theta_1$ and $u : D \in \Theta_1$. As $B \vdash_{\mathsf{IPC}} \Theta_1$, this gives $B \vdash_{\mathsf{IPC}} D \wedge u : D$, and thus $\vdash_{\mathsf{IPC}} \sigma D \wedge \sigma(u : D)$. If $\neg u : D \in \Theta$, then $B \vdash_{\mathsf{IPC}} \neg u : D$, so $\vdash_{\mathsf{IPC}} \sigma(\neg u : D)$, thus $\vdash_{\mathsf{IPC}} \neg \sigma(u : D)$. This shows that σ fulfills the conditions of Lemma 3, and whence there exists an arithmetical interpretation such that $\Theta^* \nvdash_{\mathsf{HA}} A^*$. $\square$

4 Discussion.

The next step in building intuitionistic logic of proofs iLP should be adding to iBLP operations on proofs. In order to get the internalization property

$$\frac{A_1, A_2, \ldots, A_n \vdash_{\mathsf{iLP}} B}{u_1{:}A_1, u_2{:}A_2, \ldots, u_n{:}A_n \vdash_{\mathsf{iLP}} t(u_1, u_2, \ldots, u_n){:}B}$$

we should add operations similar to *application* "$\circ$" and *proof checker* "!" (cf. [3]). Furthermore, by adding also the *choice* operation "+", we could gain a capacity to naturally capture the intuitionistic version of the modal logic S4 and hence the modal λ-calculus [7, 15, 16]. Note, that in iLP every admissible rule of HA will be represented by a proof term. Indeed, consider an admissible rule F/G. Then $!u{:}F \to G$ for some proof variable u not occurring in F, G is a theorem of iLP. By internalization, there should be a proof term g such that $\vdash_{\mathsf{iLP}} g : (!u : F \to G$. Using application we can conclude that $\vdash_{\mathsf{iLP}} u : !u : F \to (g \circ u) : G$. By the proof checker operation, $\vdash_{\mathsf{iLP}} u : F \to u : !u : F$, and hence $\vdash_{\mathsf{iLP}} u : F \to (g \circ u) : G)$. The latter shows that a proof term $g \circ u$ represents the rule F/G in iLP.

The explicit axiomatization of admissible rules by Visser's series $V_n = F_n/G_n$ established in [10, 11, 12] allows us to guess a more concise formulation of iLP in style of the classical logic of proofs LP.

Definition 7. The *intuitionistic logic of proofs*, iLP, consists of the following axioms and rules:

$A1$	Axioms of IPC	
$A2$	$u{:}F \to F$	
$A3$	$s{:}(F \to G) \to (t{:}F \to (s \cdot t){:}G$	*application*
$A4$	$t{:}F \to t{:}!t{:}F$	*proof checker*
$A5$	$s{:}F \to (s+t){:}F$,	
	$t{:}F \to (s+t){:}F$	*choice operation*
$A6$	$u{:}F \vee \neg u{:}F$	
$A7_n$	$t{:}F_n \to f_n(t){:}G_n$,	f_n is a functional symbol specific for V_n
$R1$	*Modus Ponens*	
$R2$	$c{:}A$,	c is a proof constant, $A \in A1 - A7_n$

This system is obviously sound with respect to the provability interpretation where operations $\cdot, !, +, f_n$ are interpreted the intended way. It is easy to see that iLP enjoys internalization property and contains proof terms for each admissible rule in IPC. We conjecture that this system is also arithmetically complete and believe, this fact could be established within the circle of ideas presented in this note and in [3].

References

[1] S. Artemov, "Logic of Proofs", *Annals of Pure and Applied Logic*, v. 67, pp. 29–59, 1994.

[2] S. Artemov, "Operational Modal Logic," *Tech. Rep. MSI 95-29*, Cornell University, December 1995.

[3] S. Artemov, "Explicit provability and constructive semantics", The *Bulletin for Symbolic Logic*, v. 7:1, pp. 1-36, 2001.

[4] S. Artemov, "Kolmogorov's and Gödel's approach to intuitionistic logic: current developments.", The *Russian Mathematical Surveys*, v. 59:2, 2004.

[5] S. Artemov and T. Strassen, "The Basic Logic of Proofs", in E. Boerger, G. Jaeger, H. Kleine Buening, S. Martini, M.M. Richter, eds. *Computer Science Logic 1992. Springer Lecture Notes in Computer Science*, v. 702, pp. 14-28, 1992.

[6] A. Berarducci, "The interpetability logic for Peano Arithmetic," Journal for Symbolic Logic, v. 55:3, pp. 1059-1089, 1990.

[7] G. Bierman and V. de Paiva, "Intuitionistic necessity revisited", *Proceedings of the Logic at Work Conference,* Amsterdam (December 1992), Second revision, June 1996 (http://theory.doc.ic.ac.uk/tfm/papers.html).

[8] S. Ghilardi, "Unification in intuitionistic logic," *The Journal of Symbolic Logic*, v. 64:2, pp. 859-880, 1999.

[9] S. Ghilardi, "Best solving modal equations," *Annals of Pure and Applied Logic*, v. 102, pp. 183-198, 2000.

[10] R. Iemhoff, "On the admissible rules of intuitionistic propositional logic," *The Journal of Symbolic Logic*, v. 66:1, pp. 281-294, 2001.

[11] R. Iemhoff, "Provability Logic and Admissible Rules," *Ph.D. Thesis, ILCC dissertations* 2001.

[12] R. Iemhoff, "Towards a proof system for admissibility," in *M. Baaz and A. Makowsky eds., Computer Science Logic '03, Lecture Notes in Computer Science 2803*, pp. 255-270, Springer, 2003.

[13] R. Iemhoff, "Intermediate logics and Visser's rules," Submitted, 2003.

[14] D.H.J. de Jongh, "The maximality of the intuitionistic predicate calculus with respect to Heyting's Arithmetic," *The Journal of Symbolic Logic*, v. 36, p. 606, 1970.

[15] S. Martini and A. Masini,"A computational interpretation of modal proofs", in Wansing, ed., *Proof Theory of Modal Logics*, (Workshop proceedings), Kluwer, 1994.

[16] F. Pfenning and H.C. Wong, "On a modal lambda-calculus for S4", *Electronic Notes in Computer Science* v. 1, 1995.

[17] 45) V. Rybakov, "A Criterion for Admissibility of Rules in the Modal System $S4$ and the Intuitionistic Logic," *Algebra and Logic*, v. 23:5, pp. 369-384 (Engl. Translation), 1984.

[18] V. Shavrukov, "The logic of relative interpretability over Peano Arithmetic", Technical Report, Steklov Mathematical Institute, Moscow, 1988

[19] C.A. Smorynski, "Applications of Kripke models," in Troelstra, ed.,*Mathematical Investigations of Intuitionistic Arithmetic and Analysis*, Springer Verlag, pp. 324-391, 1973

[20] R. Solovay, "Provability interpretations of modal logic", *Israel Journal of Mathematics*, v. 25, pp. 287-304, 1976.

[21] A. Visser, "Rules and Arithmetics", *Notre Dame Journal of Formal Logic*, v. 40:1, pp. 116-140, 1999.