The Basic 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*
University Utrecht
Dept. of Philosophy
Heidelberglaan 6-8
Utrecht, the Netherlands
Rosalie.Iemhoff@phil.uu.nl

August 4, 2006

Abstract

The language of the basic logic of proofs extends the usual propositional language by forming sentences of the sort *x is a proof of F* for any sentence F. In this paper a complete axiomatization for the basic logic of proofs in Heyting Arithmetic HA was found.

1 Introduction.

The classical logic of proofs LP inspired by the works by Kolmogorov [24] and Gödel [16, 17] was found in [3, 4] (see also surveys [6, 8, 12]). LP is a natural extension of the classical propositional logic in a language of proof-carrying formulas. LP axiomatizes all valid logical principles concerning propositions and proofs with a fixed sufficiently rich set of operations. Operations on proofs in LP suffice to recover explicit provability content in the classical modal logic by realizing modalities by appropriate proof terms. This helped to settle an old question discussed by Gödel in 1933/38 concerning the intended provability semantics of the classical modal logic S4 and intuitionistic logic IPC ([4]).

The logic of proofs LP naturally extends both the classical modal logic and typed combinatory logic (hence the typed λ-calculus) [5]. This connection to modal logic led to applications of LP in the logics of knowledge, where the proof-carrying language of LP helped to capture the notions of "evidence" and "knowing for a reason" ([7, 9, 13]).

Another line of applications of the logic of proofs comes from the fact that LP considerably extends the typed λ-calculus by providing the latter with reflexive capabilities, which model reflection in typed theories and typed functional programming [1, 6, 25]. In this connection finding the intuitionistic logic of proofs, more precisely, the logic of proofs for HA is an important task, since this logic could serve as a source of new operations for the reflexive λ-calculi. The logic of proofs provides a proper

*Supported by the Austrian Science Fund FWF under projects P16264, P16539 and P17503.

format for reasoning about admissible rules in HA and studying their functional and algebraic behavior. The intuitionistic logic of proofs provides a more expressive version of the modal λ-calculus [11, 26, 27] which has interesting applications.

The problem of building the intuitionistic logic of proofs has two distinct parts. Firstly, one has to answer the question about the propositional logical principles that axiomatize HA-tautologies in the propositional language enriched by atoms *u is a proof of F* without operations on proof terms, i.e. when u is a variable. The resulting basic logic of proofs will reflect purely logical principles of the chosen format. Secondly, one has to pick a system of operations on proofs and study the corresponding intuitionistic logic of proofs. In this paper we will concentrate on solving the first of the above problems and discuss the second one in section 4.

We introduce the *Basic Intuitionistic Logic of Proofs*, iBLP, and establish its completeness with respect to the semantics of proofs in HA. The paper essentially uses technique and results by de Jongh [23], Smorynski [28], de Jongh and Visser's work on a basis for admissible rules in IPC (circa 1991, cf. [19]), Artemov & Strassen [10] and Artemov [2], Ghilardi [14], Iemhoff [18, 20, 21].

Finally, let us remark that besides the reasons mentioned above, the completeness proof presented in this paper is also interesting because it is the first result in this area for constructive theories. For example, the corresponding problem for the provability logic of Heyting Arithmetic is still open [8].

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 or $\perp$, 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 $\perp$ 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 [2, 10].

1. a proof predicate $Prf(x, y)$;

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

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

$$\bot^* := (0 = 1), \qquad (u{:}A)^* := \mathit{Prf}(u^*, \ulcorner A^* \urcorner),$$

and $(\cdot)^*$ commutes with the connectives. Naturally, an arithmetical interpretation of the iBLP-language can be considered as a special case of the arithmetical substitution in the language of IPC.

2.1 Substitutions.

We will use two kinds of substitutions. Substitutions of propositional formulas for propositional variables are denoted by σ or σ'. Substitutions of arithmetical formulas for propositional variables 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 $A \vdash_{\mathsf{L}}^{R} B$ 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 $i < n$, either there are $j_1, \ldots, j_m \leq i$ such that $A_{j_1}, \ldots, A_{j_m} \vdash_{\mathsf{L}} A_{i+1}$ 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 $A \vdash_{\mathsf{L}}^{R} B$.

2.2.1 The Visser Rules.

Definition 3. 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

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

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 $A \to A^V$. On the other hand, this formula is not derivable in IPC. As was first observed by D. de Jongh and A. Visser, the rules V are admissible for IPC (cf. [19]). 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 $(\neg A \to A) \leftrightarrow \neg\neg A$, $(\neg A \to B \vee C)^V \leftrightarrow (\neg A \to B) \vee (\neg A \to C)$.

The interest of the Visser rules lies in the fact that they form a basis for the admissible rules of IPC and HA.

Theorem 1. [18, 19] *The Visser rules form a basis for the admissible rules of* IPC.

Theorem 2. [29] *The propositional admissible rules of* HA *are the same as the admissible rules of* IPC.

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 $K_1, \dots, K_n$, $(\Sigma K_i)'$ denotes the Kripke model which is the result of attaching one new node at which no propositional variables are forced, below all nodes in $K_1, \dots, K_n$. $(\Sigma)'$ is called the *Smorynski operator*. A class of models $\mathcal{K}$ has the *extension property* if for every family of models $K_1, \dots, K_n \in \mathcal{K}$, 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 4. 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 [15] 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

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

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 3. (Ghilardi [15])**.**

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 $B \in \overline{\Pi}_A$ such that $\vdash_{\mathsf{IPC}} \sigma B$.*

Theorem 4. *For each finite projective approximation Π_A of A, we have $A \mathrel{|\!\!\sim}_{\mathsf{IPC}} \bigvee \Pi_A$. Thus also $A \mathrel{|\!\!\sim}_{\mathsf{HA}} \bigvee \Pi_A$ by Theorem 2.*

Proof. 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 $B \in \overline{\Pi}_A$ such that $\vdash_{\mathsf{IPC}} \sigma B$. As Π_A is a projective approximation it follows that $B \vdash C$ for some $C \in \Pi_A$. Hence $\vdash \sigma C$, and thus $\vdash_{\mathsf{IPC}} \sigma(\bigvee \Pi_A)$. This proves that $A \mathrel{|\!\!\sim}_{\mathsf{IPC}} \bigvee \Pi_A$. □

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

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

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 then for all atoms p, if $(A \wedge \neg p)$ is consistent then $(A \wedge \neg p)$ is projective.*

Proof. Show that $(A \wedge \neg p)$ has the extension property. □

3 The Basic Logic of Proofs.

Definition 5. The *basic intuitionistic logic of proofs*, iBLP, consists of the following axioms

$A1$	Axioms 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 $\left(\bigwedge_{i=1}^n (F_i \wedge u_i{:}F_i)\right) \mathrel{|\!\!\sim}_{\mathsf{HA}} G$

and the rule Modus Ponens.

Note that in A4 the $u_i\!:\!F_i$, F_i and G are considered as propositional formulas, see the remarks about this in the section on substitutions.

As it follows from well-known results by Rybakov and Visser that the predicate $F \mathrel{|\!\sim}_{\mathsf{HA}} G$ is decidable, the 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 when 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 u_i, F_i and G such that $\big(\bigwedge_{i=1}^n (F_i \wedge u : F_i)\big) \mathrel{|\!\sim}_{\mathsf{HA}} G$. Whence A^* is

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

where $u_i^* = m_i$. Since Prf, being a primitive recursive predicate, is decidable in HA, either $\mathsf{HA} \vdash Prf(m_i, F_i^*)$ for all $i \leq n$, or $\mathsf{HA} \vdash \neg Prf(m_i, F_i^*)$ 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 $\mathsf{HA} \vdash Prf(m_i, F_i^*) \wedge F_i^*$, for all $i \leq n$. The fact that $\big(\bigwedge_{i=1}^n (u_i\!:\!F_i \wedge F_i)\big) \mathrel{|\!\sim}_{\mathsf{HA}} G$ means that for all arithmetical substitutions τ, $\mathsf{HA} \vdash \bigwedge_{i=1}^n \tau(u_i : F_i) \wedge \tau(F_i)$ 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 $\mathsf{HA} \vdash \bigwedge_{i=1}^n (u_i\!:\!F_i)^* \wedge F_i^*$, this therefore implies that $\mathsf{HA} \vdash G^*$, and hence A^* is provable in HA also in this case. □

In Section 4 we will show that iBLP is complete for HA. First, we present a more transparent axiomatization of iBLP by providing the following replacement for $A4$.

Theorem 5. *In the axiomatization of* iBLP *the axiom* $A4$ *can be replaced by the axiom*

$$\bigwedge_{i=1}^n (u_i\!:\!F_i) \to G \quad \textit{for } F_i, G \textit{ such that } \big(\bigwedge_{i=1}^n (F_i \wedge u_i\!:\!F_i)\big) \vdash^V_{\mathsf{IPC}} G.$$

Proof. By Theorem 2, $\mathrel{|\!\sim}_{\mathsf{IPC}} = \mathrel{|\!\sim}_{\mathsf{HA}}$. Whence $A4$ can be replaced by

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

By Theorem 1, $\mathrel{|\!\sim}_{\mathsf{IPC}} = \vdash^V_{\mathsf{IPC}}$. This proves the theorem. □

4 Completeness.

In this section we prove the arithmetical completeness theorem for iBLP:

Theorem 6. *For finite* Γ, $\Gamma \vdash_{\mathsf{iBLP}} A$ *if and only if* $\Gamma^* \vdash_{\mathsf{HA}} A^*$ *for every arithmetical interpretation* *.

The soundness part has already been proved in Proposition 1. The proof of the completeness is the difficult part. We first present a sketch of this proof to explain the main idea, before we dive into the technicalities in the following sections.

4.1 Proof sketch

Suppose $\Gamma \nvdash_{\mathsf{iBLP}} A$. We have to find an arithmetical interpretation * such that $\Gamma^* \nvdash_{\mathsf{HA}} A^*$. First note that when neither Γ nor A contains labelled atoms, that is atoms of the form $u : B$, then the theorem follows immediately from de Jongh's theorem.

Theorem 7. (de Jongh's theorem [28])**.**
$\mathsf{IPC} \vdash A$ *if and only if* $\mathsf{HA} \vdash \tau A$ *for all substitutions* τ*.*

Indeed, since $\Gamma \nvdash_{\mathsf{iBLP}} A$, $\mathsf{IPC} \nvdash \bigwedge \Gamma \to A$. Let τ' be a substitution such that $\mathsf{HA} \nvdash \tau'(\bigwedge \Gamma \to A)$. Then define a substitution τ as τ' on the atoms that occur in Γ or A and as $\bot$ on the atoms (labelled as well as not labelled) that do not occur in Γ or A. This substitution leads to an arithmetical interpretation in the following way. We pick a Gödel numbering of the joint language of iBLP and HA that is injective, i.e. such that

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

And then we can construct a proof predicate $\mathit{Prf}(x, y)$ such that $\mathit{Prf}(n, m)$ holds if and only if

"n is a code of a derivation in HA which contains a formula having code m",

and such that

$$\mathit{Prf}(\ulcorner u \urcorner, n) \text{ is false for every } n \text{ and every label } u.$$

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

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

Since under this interpretation $\tau(u\!:\!B) = \bot = (u\!:\!B)^*$, it follows that $\mathsf{HA} \vdash \tau(B) \leftrightarrow B^*$. Whence that $\Gamma^* \nvdash_{\mathsf{HA}} A^*$. So this shows that Theorem 6 holds when neither Γ nor A contain labelled atoms.

What is the problem when we do not have this restriction on Γ and A? First observe that as $\mathit{Prf}(u^*, B^*)$ or $\neg \mathit{Prf}(u^*, B^*)$ is provable in HA, and we wish $\Gamma^* \nvdash_{\mathsf{HA}} A^*$, we should have $\mathsf{HA} \vdash \mathit{Prf}(u^*, B^*)$ for all $u\!:\!B \in \Gamma$, and whence also $\mathsf{HA} \vdash B^*$. For if not, $\Gamma^* \vdash_{\mathsf{HA}} \bot$. As we will see, we need that $\tau(u\!:\!B)$ and τB will become equivalent to $(u\!:\!B)^*$ and B^*. Hence HA should prove $\tau(u\!:\!B)$ and τB for all $u\!:\!B \in \Gamma$. Such a thing however is not guaranteed by the proof of de Jongh's theorem. Nor does it follow from the proof of the theorem as given in [28]. That nevertheless such a τ exists is shown in the following way.

Given $\Gamma \nvdash_{\mathsf{IPC}} A$ we extend Γ to Θ such that $\Theta \nvdash_{\mathsf{iBLP}} A$, and $u : B \in \Theta$ or $\neg u : B \in \Theta$ for all $u : B$ that occur in Γ or A. But we will require more of Θ: we will construct it in such a way that it also contains a projective formula B that implies

$$\bigwedge \{C, u : C \mid u : C \in \Theta\} \wedge \bigwedge \{\neg u : C \mid \neg u : C \in \Theta\}.$$

We call such $(\bigwedge \Theta \to A)$ projectively saturated, the precise definition follows below. Then we show that the existence of a projective unifier σ of B implies the following lemma.

Lemma 4. *For every finite projectively saturated* $\bigwedge \Gamma \to A$ *such that* $\Gamma \nvdash_{\mathsf{iBLP}} A$ *there exists 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 the following lemma completes the proof of the theorem.

Lemma 3. *If* Γ*,* A*,* σ *are as in Lemma 4, then there is a arithmetical interpretation* * *such that* $\Gamma^* \nvdash_{\mathsf{HA}} A^*$.

Thus the completeness proof (Theorem 6) consists of the proofs of the two main lemma's: Lemma 4, which shows that such a σ exists, and Lemma 3, which constructs the desired arithmetical interpretation on the basis of such a σ.

4.2 Projective saturation.

In this section we give the definition of projective saturation and prove that for every $\Gamma \nvdash_{\mathsf{iBLP}} A$ there is a $\Theta \supseteq \Gamma$ such that $\bigwedge \Theta \to A$ is projectively saturated.

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

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

$\overline{\Pi}_\Gamma$ denotes $\overline{\Pi}_{(\bigwedge \Gamma)}$, similarly for Π_Γ. An implication $(\bigwedge \Gamma \to A)$ is called *projectively saturated* if

$\Gamma \nvdash_{\mathsf{iBLP}} A$;

$\Gamma \cap \overline{\Pi}_{\Gamma_1}$ 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* $\Gamma \nvdash_{iBLP} A$*, then there exists a projectively saturated* $(\bigwedge \Theta \to A)$ *such that* $\Theta \supseteq \Gamma$*. 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, and $u\!:\!B \in \Delta$ implies $B \in \Delta$. Δ can be obtained by standard saturation techniques. It is finite when Γ is finite. Let Π_{Δ_0} be a finite projective approximation of $\bigwedge \Delta_0$ (Section 2.4). Recall that all atoms occurring in Π_{Δ_0} occur in Δ_0 too, and note that $\Delta_0 \subseteq \Delta$. Since $\Delta_0 \mathrel{|\!\!\sim}_{\mathsf{HA}} \bigvee \Pi_{\Delta_0}$, by Theorem 4, we have $\Delta_0 \vdash_{\mathsf{iBLP}} \bigvee \Pi_{\Delta_0}$, by axiom $A4$ of iBLP. Hence also $\Delta \vdash_{\mathsf{iBLP}} \bigvee \Pi_{\Delta_0}$. 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 $\Delta \vdash_{\mathsf{iBLP}} A$. Note that $C \vdash_{\mathsf{IPC}} \bigwedge \Delta_0$ by the definition of Π_{Δ_0}. Let

$$B = C \wedge \{\neg u\!:\!D \mid \neg u\!:\!D \in \Delta\}$$

and $\Theta = \Delta \cup \{B\}$. We show that $(\bigwedge \Theta \to A)$ is projectively saturated, that is,

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

The first statement is immediate. For the second 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, by the definition of Δ and of C. The construction of Δ implies that whence $u{:}D \in \Delta$ or $\neg u{:}D \in \Delta$, which implies the statement. For the last statement, first observe that $\Theta_1 = \Delta_1$. The projectivity of B follows from the projectivity of C by Lemma 1. For $B \vdash_{\mathsf{IPC}} \Theta_1$, consider $u{:}D \in \Theta$. Thus $u{:}D \in \Delta$, and thus $D, u{:}D \in \Delta_0$. Hence $C \vdash_{\mathsf{IPC}} D \wedge u{:}D$, as $C \vdash_{\mathsf{IPC}} \bigwedge \Delta_0$. Hence $B \vdash_{\mathsf{IPC}} D \wedge u{:}D$. That $B \vdash_{\mathsf{IPC}} \neg u{:}D$ for $\neg u{:}D \in \Theta$ follows from the definition of B and $\Theta_1 = \Delta_1$. □

4.3 Main lemma's.

The main part of the completeness proof lies in the following lemma that shows that the existence of certain substitutions suffices 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 7), 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

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

and such that for all φ, if $\mathsf{HA} \vdash \varphi$, then there exists at least one n that codes a proof of φ and is not equal to $\ulcorner u \urcorner$ for any proof variable u. We define a desired arithmetical interpretation * by a fixed point construction in a similar way as in [4]. First for a given proof predicate $\mathit{Prf}(x, y)$ we define an auxiliary translation $(\cdot)^+$ as follows:

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

Let $PROOF(x, y)$ 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 $PROOF(\ulcorner u \urcorner, n)$ is false for any proof variable u and any $n \in \omega$. By the arithmetical fixed point argument we construct a formula $Prf(x, y)$ such that HA proves the following fixed point equation:

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

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

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

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 $B = u : C$, $B^+ = Prf(\ulcorner u \urcorner, \ulcorner B^+ \urcorner) = Prf(u^*, \ulcorner B^* \urcorner) = B^*$ 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, $\mathsf{HA} \vdash Prf(u^+, \ulcorner C^+ \urcorner)$, whence $\mathsf{HA} \vdash (u{:}C)^+$. By the first statement of the claim this implies $\mathsf{HA} \vdash (u{:}C)^*$. Thus $\mathsf{HA} \vdash (u{:}C)^* \leftrightarrow \tau(u{:}C)$. If $\neg u{:}C \in \Gamma$, then $\mathsf{HA} \vdash \neg\tau(u{:}C)$ by (1). Since by the definition of $PROOF(x, y)$, we have that $PROOF(\ulcorner u \urcorner, \ulcorner C^+ \urcorner)$ is false, it follows that also $Prf(\ulcorner u \urcorner, \ulcorner C^+ \urcorner)$ is false. Hence $\mathsf{HA} \vdash \neg Prf(u^*, C^*)$ by IH, which shows that $\neg(u{:}C)^*$ and $\tau(u{:}C)$ are equivalent in HA.

The steps corresponding to the connectives are easy.

Claim 5. $\mathsf{HA} \vdash \varphi$ *if and only if $Prf(n, \ulcorner \varphi \urcorner)$ 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: $PROOF(n, \ulcorner \varphi \urcorner)$ 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. □

Lemma 4. *For every finite projectively saturated* $\bigwedge\Gamma \to A$ *such that* $\Gamma \nvdash_{\mathsf{iBLP}} A$ *there exists 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. $\sigma\Gamma \nvdash_{\mathsf{IPC}} \sigma A$.

Proof. Let $B \in \Gamma \cap \overline{\Pi}_{\Gamma_1}$, which exists because $\bigwedge\Gamma \to A$ is projectively saturated. Thus B is projective and $B \vdash_{\mathsf{IPC}} \bigwedge\Gamma_1$. 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 the lemma, i.e.

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

Recall (Section 2.4) that

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

To show 1., consider $u\!:\!D \in \Gamma$. Then $D \in \Gamma_0 \subseteq \Gamma_1$ and $u\!:\!D \in \Gamma_1$. As $B \vdash_{\mathsf{IPC}} \bigwedge\Gamma_1$, this gives $B \vdash_{\mathsf{IPC}} D \wedge u\!:\!D$, and thus $\vdash_{\mathsf{IPC}} \sigma D \wedge \sigma(u\!:\!D)$. For 2. the reasoning is the same. For 3., note that since $\Gamma \vdash_{\mathsf{IPC}} B$ and $\Gamma \nvdash_{\mathsf{iBLP}} A$, we have $B \nvdash_{\mathsf{IPC}} \bigwedge\Gamma \to A$, and thus $\nvdash_{\mathsf{IPC}} \sigma(\bigwedge\Gamma \to A)$. □

4.4 Completeness proof.

Here we finish the proof of Theorem 6. 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. Hence $\Theta \nvdash_{\mathsf{iBLP}} A$. We show that there is an arithmetical interpretation such that $\Theta^* \nvdash_{\mathsf{HA}} A^*$. By Lemma 4 there exists a substitution σ which fulfills the conditions of Lemma 3 (reading Θ for Γ). Whence there exists an arithmetical interpretation $*$ such that $\Theta^* \nvdash_{\mathsf{HA}} A^*$ by Lemma 3. Whence $\Gamma^* \nvdash_{\mathsf{HA}} A^*$, and we are done.

4.5 Extension of the results

The above results on Heyting Arithmetic can be extended to certain other arithmetical theories T in the following way. Let $\mathsf{iBLP}(T)$ stand for the logic that is the result of replacing HA by T in iBLP. Then for T such that

1. T allows for the definition of proof predicates with the appropriate properties,
2. $\mathrel{|\!\sim}_T\ =\ \mathrel{|\!\sim}_{\mathsf{IPC}}$,

3. $\mathsf{iBLP}(T)$ is sound for T,

we can almost copy the completeness proof for HA. Namely, for such T it is not difficult to see that Theorem 7 and the Lemmas's 2, 3 and 4 carry through when replacing HA by T. That for such T Theorem 7 (De Jongh's theorem) holds follows from property (2.). Thus we can prove, in a similar way as for HA, that for such T the logic $\mathsf{iBLP}(T)$ is the basic logic of proofs of T, i.e.

Theorem 8. *For T as above, for finite Γ, $\Gamma \vdash_{\mathsf{iBLP}(T)} A$ if and only if $\Gamma^* \vdash_T A^*$ for every arithmetical interpretation *.*

5 Discussion.

The next step in building intuitionistic logic of proofs iLP should be adding to iBLP operation on proofs. There are some natural choices for sets of operations. 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 could consider adding operations similar to *application* "$\circ$" and *proof checker* "!" (cf. [4]). Furthermore, by adding also the *choice* operation "+", we will gain a capacity to naturally capture the intuitionistic version of the modal logic $\mathsf{S4}$ and hence the modal λ-calculus [11, 26, 27]. 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 an axiom of iBLP, hence a theorem of iLP. By internalization, there should be a (ground) proof term g such that $\vdash_{\mathsf{iLP}} g{:}(u{:}F \to G)$. Using application we can conclude that $\vdash_{\mathsf{iLP}} v{:}u{:}F \to (g \cdot v){:}G$. Substituting $!u$ for v we get $\vdash_{\mathsf{iLP}} !u{:}u{:}F \to (g{\cdot}!u){:}G)$. By the proof checker operation, $\vdash_{\mathsf{iLP}} u{:}F \to !u{:}u{:}F$, and hence $\vdash_{\mathsf{iLP}} u{:}F \to (g{\cdot}!u){:}G)$. The latter shows that a proof term $g{\circ}!u$ represents in iLP the rule F/G.

This observation allows us to guess a concise formulation of iLP

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

$A1-4$	Axioms of iBLP	
$A5$	$s{:}(F \to G) \to (t{:}F \to (s{\cdot}t){:}G$	*application*
$A6$	$t{:}F \to t{:}!t{:}F$	*proof checker*
$A7$	$s{:}F \to (s+t){:}F$,	
	$t{:}F \to (s+t){:}F$	*choice operation*
$R1$	*Modus Ponens*	
$R2$	$c{:}A$,	c is a proof constant, $A \in A1 - A7$

The explicit axiomatization of admissible rules by Visser's series $V_n = F_n/G_n$ established in [18, 19, 20, 30] allows us to guess an alternative formulation of iLP, which is more in the style of the classical logic of proofs LP.

Definition 8. The *intuitionistic logic of proofs*, iLP, consists of the following axioms and rules:

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

These systems are obviously sound with respect to the provability interpretation where operations $\cdot, !, +, f_n$ are interpreted the intended way. It is easy to see that both formulations enjoy the internalization property and contain proof terms for each admissible rule in IPC. We conjecture that these systems are arithmetically complete in there languages and believe this fact could be established within the circle of ideas presented in this note and in [4].

References

[1] J. Alt and S. Artemov, "Reflexive lambda-calculus", In *Springer Lecture Notes in Computer Science*, v. 2183, Proceedings of the Dagstuhl-Seminar on Proof Theory in Computer Science, pp. 22–37, 2001.

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

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

[4] S. Artemov, "Explicit provability and constructive semantics", The *Bulletin for Symbolic Logic*, v.7, No. 1, pp. 1–36, 2001.

[5] S. Artemov. Unified semantics for modality and λ-terms via proof polynomials. In K. Vermeulen and A. Copestake, editors, *Algebras, Diagrams and Decisions in Language, Logic and Computation*, pages 89–119. CSLI Publications, Stanford University, 2002.

[6] S. Artemov. Kolmogorov and Gödel's approach to intuitionistic logic: current developments. *Russian Mathematical Surveys*, 59(2):203–229, 2004.

[7] Artemov, S., *Justified Common Knowledge*, Theoretical Computer Science, v. 357 (2006), pp. 4–22.

[8] S. Artemov and L. Beklemishev. Provability logic. In D. Gabbay and F. Guenthner, editors, *Handbook of Philosophical Logic, 2nd ed.*, volume 13, pages 229–403. Kluwer, Dordrecht, 2004.

[9] Artemov, S. and E. Nogina, *Introducing justification into epistemic logic*, Journal of Logic and Computation **15** (2005), pp. 1059–1073.

[10] S. Artemov and T. Strassen, "The Basic Logic of Proofs", *Springer Lecture Notes in Computer Science* , v.702, pp.14–28, 1992.

[11] 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).

[12] D. de Jongh and G. Japaridze. The Logic of Provability. Ed. S. Buss, *Handbook of Proof Theory.* Studies in Logic and the Foundations of Mathematics, Vol.137., Elsevier, pp. 475-546, 1998.

[13] M. C. Fitting. The logic of proofs, semantically. *Annals of Pure and Applied Logic*, 132(1):1–25, 2005.

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

[15] S. Ghilardi, "Best solving modal equations," *Annals of Pure and Applied Logic*, v.102, 2000.

[16] K. Gödel. Eine Interpretation des intuitionistischen Aussagenkalkuls. *Ergebnisse Math. Colloq.*, Bd. 4 (1933), S. 39-40.

[17] K. Gödel. Vortrag bei Zilsel (1938). In S. Feferman, ed. *Kurt Gödel Collected Works. Volume III*, pp. 86-113, Oxford University Press, 1995.

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

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

[20] 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.

[21] R. Iemhoff, "Intermediate logics and Visser's rules," *Notre Dame Journal of Formal Logic*, vol. 46 (1) (2005), pp. 65-81.

[22] R. Iemhoff, "Preservativity logic (An analogue of interpretability logic for constructive theories)," *Mathematical Logic Quarterly*, vol. 49 (3) (2003), pp. 1-21.

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

[24] A. Kolmogoroff. Zur Deutung der intuitionistischen logik. *Mathematische Zeitschrift*, 35:58–65, 1932. In German. English translation in V.M. Tikhomirov, editor, *Selected works of A.N. Kolmogorov. Volume I: Mathematics and Mechanics*, pages 151–158. Kluwer, Dordrecht 1991.

[25] N. Krupski, "Typing in reflective combinatory logic," *Annals of Pure and Applied Logic*, vol. 141, pp. 243-256, 2006.

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

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

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

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

[30] A. Visser, "Substitutions of Σ-sentences: explorations between intuitionistic propositional logic and intuitionistic arithmetic", *Annals of Pure and Applied Logic*, v. 114 (1-3), pp. 227-271, 2002.