Operational modal logic*

Sergei N. Artemov†

December, 1995

Abstract

Answers to two old questions are given in this paper.

1. Modal logic $\mathcal{S}4$, which was informally specified by Gödel in 1933 as a logic for provability, meets its exact provability interpretation.

2. Brouwer - Heyting - Kolmogorov realizing operations (1931-32) for intuitionistic logic $\mathcal{I}nt$ also get exact interpretation as corresponding propositional operations on proofs; both $\mathcal{S}4$ and $\mathcal{I}nt$ turn out to be complete with respect to this proof realization.

These results are based on operational reading of $\mathcal{S}4$, where a modality is split into three operations. The *logic of proofs* with these operations is shown to be arithmetically complete with respect to the intended provability semantics and sufficient to realize every operation on proofs admitting propositional specification in arithmetic.

1 Introduction

A provability reading of a modality $\Box F$ as

"F is provable"

was an intended informal semantics for the classical system $\mathcal{S}4$ of propositional modal logic in Gödel's paper [4]. Intuitionistic propositional logic $\mathcal{I}nt$ has also

* *Techical Report MSI 95-29, Cornell University.*

†Steklov Mathematical Institute, Russian Academy of Sciences, Vavilova str. 42, Moscow, 117966 RUSSIA, (email:sergei@artemov.mian.su). This paper had been accomplished during a visit to the Department of Mathematics, Cornell University, Ithaca, NY 14853, USA, in 1995 (email: artemov@math.cornell.edu).

been supplied with an informal *Brouwer-Heyting-Kolmogorov operational semantics* in [6], [8], cf.[10]. However, both $\mathcal{S}4$ and $\mathcal{I}nt$ have lacked exact descriptions of their intended semantics. The straightforward interpretation of $\Box F$ as

"*F is provable in Peano Arithmetic*"

leads to logics of formal provability incompatible with $\mathcal{S}4$. Also, Kleene realizability is known to capture more, than $\mathcal{I}nt$ is able to derive. It turns out that these questions can be resolved on the basis of operational reformulation of modal logic with realization of functions that appear as operations on proofs.

Nothing is wrong with the Provability Logic, as far as provability in Peano Arithmetic $\mathcal{PA}$ is concerned. However, traditional Provability Logic fails to provide an adequate model for the informal notion of provability. The arithmetical formula $Provable(\ulcorner F \urcorner)$, i.e.

"*there exists a proof x of F*"

is weaker than the intended "*F is provable*", since x may be nonstandard. Hence

$$Provable(\ulcorner F \urcorner) \rightarrow F$$

is stronger, than the intended

"*if F is provable, then F is true*"

As a result the formula $Provable(\ulcorner F \urcorner) \rightarrow F$ is not provable in arithmetic and the reflexivity formula

$$\Box F \rightarrow F$$

is not derivable in Provability Logic.

To deal with this phenomenon one has to incorporate into modal language a machinery to keep all proofs "real". Getting rid of quantifiers over proofs, we have to use Skolem type functions instead. Where should these functions come from?

The proof of the Second Gödel incompleteness theorem tells much more about provability properties than the plain modal language is able to express. Modal provability formulas forget some essential information: for example in the provability context the usual distributivity formula

$$\Box(F \rightarrow G) \rightarrow (\Box F \rightarrow \Box G)$$

is a modal version of

> "*there is a recursive operation m which for a given proof x of $F \rightarrow G$ and a given proof y of F produces a proof $m(x, y)$ of G.*"

A similar decoding can be done for the transitivity modal formula

$$\Box F \rightarrow \Box\Box F:$$

> *"there is a recursive operation c which for a given proof x of F returns a proof $c(x)$ of "x is a proof of F" ".*

We show that an additional operation on proofs is needed to provide a complete basis for the entire class of operations over proofs which can be specified in arithmetic by propositional conditions. Three basic operations on proofs can be naturally interpreted as Brouwer - Heyting - Kolmogorov realizing operations; $\mathcal{I}nt$ and $\mathcal{S}4$ are proved to be complete with respect to this sort of realizability.

We introduce the Logic of Proofs $\mathcal{LP}$ and show that

$$\mathcal{S}4 \vdash F \quad \Leftrightarrow \quad \textit{there is a realization } r \textit{ of } F \textit{ by proof terms such that } \mathcal{LP} \vdash F^r$$

and

$$\mathcal{LP} \vdash G \quad \Leftrightarrow \quad G^* \textit{is true for every proof interpretation } * .$$

In a certain sense, the logic of proofs is good old $\mathcal{S}4$, but presented in more rich operational language. This split of classical modalities into a finitely generated set of operations handles proper realizability and provability. It is expected to be useful in other applications of modal and provability logics as well.

We will not distinguish between a Δ_1-predicate and the arithmetical formula that represents it in Peano Arithmetic $\mathcal{PA}$. We also assume that the system of arithmetical terms includes so called ι-terms (cf. [7],[3]). So, for any arithmetical formula $\varphi(\vec{x}, y)$ such that $\mathcal{PA} \vdash \forall \vec{x} \exists ! y \varphi(\vec{x}, y)$, there exists a term $\iota y \varphi(\vec{x}, y)$ such that $\mathcal{PA} \vdash \forall \vec{x} \varphi(\vec{x}, \iota y \varphi(\vec{x}, y))$. In particular, we assume that there are arithmetical terms for all provably total recursive functions. *Closed recursive term* is a ι-term $\iota z \varphi(z)$ where formula $\varphi(z)$ contain no variables other than z. For any arithmetical formula φ by $\mu z \varphi$ we understand ι-term determined by the formula

$$\varphi(z) \wedge \forall v < z \neg \varphi(v),$$

while $\mu z \varphi \downarrow$ means

$$\exists z (\varphi(z) \wedge \forall v < z \neg \varphi(v)).$$

According to the rules for ι-terms for any arithmetical formula $A(x)$

$$A(\mu z \varphi(z)) \ = \ \exists z [\varphi(z) \wedge \forall w < z \neg \varphi(w) \wedge A(z)].$$

Note, that if A is provably Δ_1-formula and $\mu z \varphi(z)$ is a closed recursive term, then $A(\mu z \varphi(z))$ is again a provably Δ_1-formula.

Also let *Proof* (x, y) stand for the usual Gödel proof predicate

> *"x is a derivation code of a formula with a code y".*

2 Logic of operations on proofs

The language of $\mathcal{LP}$ contains

- boolean constants $\top, \bot$, sentence letters $S_1, \ldots, S_n, \ldots$
- proof letters $p_1, \ldots, p_n, \ldots$
- proof axiom constants $a_1, \ldots, a_n, \ldots$
- boolean connectives $\rightarrow, \ldots$
- functional symbols: monadic !, binary $+$ and $\times$
- operator symbol $[\![\ ]\!]\ (\ )$.

The sets Tm of terms and Fm of formulas are defined in a natural way. Any proof letter and axiom constant is in Tm; any sentence letter or boolean constant is in Fm; whenever $s, t \in Tm$ we have $!t, (s+t), (s \times t) \in Tm$; boolean connectives behave conventionally, and if $F \in Fm$ and $t \in Tm$, then $[\![t]\!]\ F \in Fm$. We will write $s \cdot t$ or even st instead of $(s \times t)$ and skip parentheses when convenient. Formulas $[\![t]\!]\ F$ are called *quasiatomic* formulas (q-atomic, for short). Without loss of generality we restrict ourselves to a finite fragment of the $\mathcal{LP}$-language, assuming that sets of sentence and proof letters, along with a set of axiom constants, have cardinality $\leq n$ for some unspecified natural number n.

2.1 Definition. System $\mathcal{LP}$. The axioms are all formulas of the form

A0. Tautologies in the language of $\mathcal{LP}$

A1. $[\![t]\!]\ F \rightarrow F$

A2. $[\![t]\!](F \rightarrow G) \ \rightarrow ([\![s]\!]\ F \ \rightarrow [\![ts]\!]\ G)$

A3. $[\![t]\!]\ F \ \rightarrow \ [\![!t]\!][\![t]\!]\ F$

A4. $[\![s]\!]\ F \vee \ [\![t]\!]\ F \ \rightarrow \ [\![s+t]\!]\ F$

A5. $[\![c]\!]A$, where c is an axiom constant, and A is an axiom A0 - A4.

Rule: *modus ponens.*

2.2 Comment. The intended understanding of $\mathcal{LP}$ is as a logic of operations on proofs, where $[\![t]\!]F$ stands for

"t is a code for a proof of F".

For the usual Gödel proof predicate $Proof(x, y)$ in $\mathcal{PA}$ there are primitive recursive functions from codes of proofs to codes of proofs which correspond to "$\times$" and

"!". So, "×" corresponds to a concatenation of proof sequences which realizes the *modus ponens* rule in arithmetic, and "!" is represented by a special case of a Gödel function appearing in the proof of Σ_1-completeness of arithmetic (cf. [11]). The usual proof predicate has a natural nondeterministic version $PROOF(x,y)$ called *standard nondeterministic proof predicate*

"*x is a code of a derivation containing a formula with a code y*".

$PROOF$ already has all three operations of the $\mathcal{LP}$-language:

- $u \otimes v$ is the code of the concatenation of u, v and a finite sequence of all formulas Y such that $X \rightarrow Y \in u$, $X \in v$
- $u \oplus v$ is just the concatenation of proof codes u and v
- $\Uparrow u$ for a given u calculates the first code of a proof which contains

  $$PROOF(u, \ulcorner\varphi_1\urcorner), \ldots, PROOF(u, \ulcorner\varphi_k\urcorner)$$

  for all $\varphi_1, \ldots, \varphi_k$ from a proof with the code u.

There exist natural extensions of the operations $\otimes$, $\oplus$ from numbers to ι-terms in such a way, that for any $f = \mu z F(z)$, $g = \mu u G(u)$ and for any formulas φ, ψ

$$\mathcal{PA} \vdash PROOF(f, \ulcorner\varphi \rightarrow \psi\urcorner) \wedge PROOF(g, \ulcorner\varphi\urcorner) \rightarrow PROOF(f \otimes g, \ulcorner\psi\urcorner)$$

$$\mathcal{PA} \vdash PROOF(f, \ulcorner\varphi\urcorner) \vee PROOF(g, \ulcorner\varphi\urcorner) \rightarrow PROOF(f \oplus g, \ulcorner\varphi\urcorner).$$

The operation $\Uparrow$ now consumes the Gödel number of a closed recursive term $\mu z F(z)$, and produces the first nondeterministic proof $\Uparrow(\ulcorner\mu z F(z)\urcorner)$ of all true formulas $PROOF(f, \ulcorner\varphi\urcorner)$ (a finite set). Since $PROOF(f, \ulcorner\varphi\urcorner)$ is a provably Δ_1-condition, then

$$\mathcal{PA} \vdash PROOF(f, \ulcorner\varphi\urcorner) \rightarrow PROOF(\Uparrow(\ulcorner f\urcorner), \ulcorner PROOF(f, \ulcorner\varphi\urcorner)\urcorner).$$

2.3 Definition. A *proof predicate* is a provably Δ_1-formula $Prf(x,y)$ such that for all φ

$$\mathcal{PA} \vdash \varphi \quad \Leftrightarrow \quad \text{for some } n \in \omega \ Prf(n, \ulcorner\varphi\urcorner) \text{ holds.}$$

For any proof predicate $Prf(x,y)$ under $Pr(y)$ we understand the corresponding *provability predicate*: $Pr(y)$ is $\exists x Prf(x,y)$.

2.4 Definition. A proof predicate is *normal* if

1. for every proof the set of corresponding theorems is finite and the function

$$T(k) = \textit{the code of the set } \{l \mid \mathit{Prf}(k,l)\}$$

is total recursive.

2. Prf is supplied with provably total recursive functions $m(x,y)$, $e(x,y)$ such that for all arithmetical formulas φ, ψ

$$\mathcal{PA} \vdash \forall x,y[\mathit{Prf}(x,\ulcorner\varphi \to \psi\urcorner) \to (\mathit{Prf}(y,\ulcorner\varphi\urcorner) \to \mathit{Prf}(m(x,y),\ulcorner\psi\urcorner)]$$

$$\mathcal{PA} \vdash \forall x,y[\mathit{Prf}(x,\ulcorner\varphi\urcorner) \vee \mathit{Prf}(y,\ulcorner\varphi\urcorner) \to \mathit{Prf}(e(x,y),\ulcorner\varphi\urcorner)].$$

Note, that PROOF is a normal proof predicate with $m(x,y) = x \otimes y$, $e(x,y) = x \oplus y$.

2.5 Lemma. *For any nomal proof predicate Prf there is a provably recursive function $c(x)$ such that for any closed recursive term f*

$$\mathcal{PA} \vdash \mathit{Prf}(f,\ulcorner\varphi\urcorner) \to \mathit{Prf}(c(\ulcorner f\urcorner),\ulcorner\mathit{Prf}(f,\ulcorner\varphi\urcorner)\urcorner)$$

Proof. The function c on an input $k \in \omega$ works as follows: c recovers the term f such that $k = \ulcorner f\urcorner$ and calculates $T(f)$. Then for every φ from $T(f)$ it computes $l = l_\varphi$ such that $\mathit{Prf}(l,\ulcorner\mathit{Prf}(f,\ulcorner\varphi\urcorner)\urcorner)$; such l exists by the Σ_1-completeness property of arithmetic, since $\mathit{Prf}(f,\ulcorner\varphi\urcorner)$ is a recursive formula. Finally, $c(k)$ is equal the e-sum of l_φ's for all φ's from $T(f)$.
◄

From now on we assume that a normal proof predicate is supplied also with a function $c(x)$, satisfying the conclusion of the previous lemma.

Remark. Obviously for any proof predicate Prf with the "summation" function $e(x,y)$ and any provable formula φ the set

$$P(\varphi) = \{n \in \omega \mid \mathit{Prf}(n,\ulcorner\varphi\urcorner)\}$$

is infinite recursive. Suppose $P(\varphi)$ is finite and consider

$$P' = \{e(n,l) \mid n \in P(\varphi),\ \textit{and } \exists\psi \mathit{Prf}(l,\ulcorner\psi\urcorner)\}.$$

By the normality property of the function e every theorem has a proof from P'. By the assumption about P however $P' \subseteq P$, i.e. P' is finite, which gives a clear decision procedure for $\mathcal{PA}$.

2.6 Definition. *Axiom specification (AS)* is a finite subset of A5. For any axiom specification AS by $\mathcal{LP}_{AS}$ we understand $\mathcal{LP}$ with AS instead of A5. Axiom specification AS is *well-founded* if for the following binary relation on axiom constants

$$a_1 \succ a_2 \quad \Leftrightarrow \quad \begin{array}{l} \textit{there exists a term } t \textit{ containing } a_2 \textit{ such that} \\ [\![a_1]\!]([\![t]\!]F \to F) \in AS \textit{ or } [\![a_1]\!]([\![t]\!]F \to [\![!t]\!][\![t]\!]F) \in AS, \end{array}$$

any chain $a_1 \succ a_2 \succ a_3 \succ \ldots$ is finite.

2.7 Definition. An *arithmetical AS-interpretation* $*$ of $\mathcal{LP}$-language has the following parameters:

1. an axiom specification AS
2. a normal proof predicate Prf
3. an evaluation of sentence letters by sentences of arithmetic, an evaluation of proof letters and axiom constants by closed provably recursive terms.

We assume that $\top^* = (0 = 0)$ and $\bot^* = (0 = 1)$, $*$ commute with boolean connectives, $(t \cdot s)^* = m(t^*, s^*)$, $(t + s)^* = e(t^*, s^*)$, $(!t)^* = c(\ulcorner t^* \urcorner)$,

$$([\![t]\!]F)^* \text{ is } Prf(t^*, \ulcorner F^* \urcorner),$$

and

$$\mathcal{PA} \vdash G^* \text{ for all } G \in AS.$$

2.8 Lemma. *If an axiom specification AS is well-founded, then for any normal proof predicate Prf any evaluation $*$ of proof letters can be extended to an AS-interpretation based on Prf.*

Proof. Consider the following evaluation of constants: those a's which do not occur among $c_1, \ldots, c_k$ in AS are evaluated by arbitrary natural numbers. Sort the remaining $c_1, \ldots, c_k$ in an order respecting the relation $\succ$; without loss of generality we assume that $c_i \succ c_j \;\Rightarrow\; i > j$. Constants $c_1, \ldots, c_k$ are evaluated according to a multiple arithmetical fixed point construction: there exist arithmetical formulas $\varphi_1, \ldots, \varphi_k$ such that

$$\varphi_i(z) \;\leftrightarrow\; z = \mu w[Prf(w, \ulcorner B_{i,1}{}^* \urcorner) \wedge \ldots \wedge Prf(w, \ulcorner B_{i,k_i}{}^* \urcorner)],$$

where $[\![c_i]\!]B_{i,1}, \ldots, [\![c_i]\!]B_{i,k_i}$ is the total list of formulas from AS which correspond to c_i and $*$ is extended to $c_1, \ldots, c_k$ by

$$c_i{}^* \;=\; \mu z \varphi_i(z).$$

We claim that $\mathcal{PA} \vdash \mu z\varphi_i(z)\downarrow$ and $\mathcal{PA} \vdash ([\![c_i]\!]B_{i,j})^*$ for all $i = 1,\ldots,k,\ j = 1,\ldots,k_i$.

By induction on i. Basis, i.e. $i = 1$. Then AS is $\{[\![c_1]\!]B_{1,1},\ldots,[\![c_1]\!]B_{1,k_1}\}$. We claim that $\mathcal{PA} \vdash {B_{1,j}}^*$ for all $j = 1,\ldots,k_1$. Consider the cases.

A0. Here $B_{1,j}$, therefore ${B_{1,j}}^*$ are tautologies, and $\mathcal{PA} \vdash {B_{1,j}}^*$.

A1. $B_{1,j}$ is $[\![t]\!]F \to F$. By the well-foundness of AS t contains none of c_i for $i = 1,\ldots,k$, thus t^* is a closed recursive term. Let n be the value of t^*. If $Prf(n,\ulcorner F^*\urcorner)$ is true, then $\mathcal{PA} \vdash F^*$, thus $\mathcal{PA} \vdash Prf(n,\ulcorner F^*\urcorner) \to F^*$. If $Prf(n,\ulcorner F^*\urcorner)$ is false, then $\mathcal{PA} \vdash \neg Prf(n,\ulcorner F^*\urcorner)$, and again $\mathcal{PA} \vdash Prf(n,\ulcorner F^*\urcorner) \to F^*$.

Cases A2 and A4 follow easily from the normality condition 2 by arguing in $\mathcal{PA}$.

A3. $B_{1,j}$ is $[\![t]\!]F \to [\![!t]\!][\![t]\!]F$. Here again, by the well-foundness of AS term t does not contain $c_1,\ldots,c_k$, thus t^* is a closed recursive term and we are done by 2.5.

Now since $\mathcal{PA} \vdash {B_{1,j}}^*$ there exists $n_j \in \omega$ such that $Prf(n_j,\ulcorner {B_{1,j}}^*\urcorner)$, thus $\mathcal{PA} \vdash Prf(n_j,\ulcorner {B_{1,j}}^*\urcorner)$ for all $j = 1,\ldots,k_1$. Put N to be the "sum" in sense of the function $e(x,y)$ of $n_1,\ldots,n_{k_1}$. Clearly

$$\mathcal{PA} \vdash Prf(N,\ulcorner {B_{1,1}}^*\urcorner) \wedge \ldots \wedge Prf(N,\ulcorner {B_{1,k_1}}^*\urcorner).$$

Let M be the least natural number such that

$$\mathcal{PA} \vdash Prf(M,\ulcorner {B_{1,1}}^*\urcorner) \wedge \ldots \wedge Prf(M,\ulcorner {B_{1,k_1}}^*\urcorner).$$

Then $\mathcal{PA} \vdash M = \mu z\varphi_1(z)$, since Prf is provably recursive, and $\mathcal{PA} \vdash ([\![c_1]\!]B_{1,j})^*$ for all $j = 1,\ldots,k_1$.

The induction step is similar to the basis. In the cases A1 and A3 by the well-foundness of AS term t does not contain constants c_j with $j > i$, and thus t^* is again a closed recursive term.

◀

2.9 Comment. We might restrict ourselves to well-founded AS only and stick to a particular procedure of recovering an evaluation of axiom constants from given AS, Prf and evaluations of sentence and proof letters, say as in lemma 2.8. This approach works as well; the completeness proof there may be obtained by a slight modification of the arithmetical fixed point construction from Section 6.

2.10 Theorem. *If $\mathcal{LP}_{AS} \vdash F$, then $\mathcal{PA} \vdash F^*$ under any AS-interpretation $*$.*

Proof. By induction on the length of derivations in $\mathcal{LP}$. Axioms A2, A4 are correct by the definition of a natural proof predicate. A0, A1 and A3 have just been checked within the proof of lemma 2.8. AS is correct by the definition of an AS-interpretation.
◀

2.11 Lemma. (Constructive necessitation)

$$\mathcal{LP} \vdash F \ \Rightarrow \ \textit{for some term } t \textit{ of axiom constants } \mathcal{LP} \vdash [\![t]\!]F.$$

Proof. By induction on a proof of F in $\mathcal{LP}$. If F is an axiom A0 – A4, then take $[\![c]\!]F$ from A5 with a fresh axiom constant c. If F is A5, then use A3. Let F be obtained from $E \to F$ and E by *modus ponens*. Then, by the induction hypothesis, $\mathcal{LP} \vdash [\![t]\!]E$ and $\mathcal{LP} \vdash [\![s]\!](E \to F)$ for some terms s and t. By A2, $\mathcal{LP} \vdash [\![st]\!]\ F$.
◀

2.12 Corollary.

$$\mathcal{LP} \vdash F \to G \ \Rightarrow \ \forall s\ \exists t \ \ \mathcal{LP} \vdash [\![s]\!]F \to [\![t]\!]G.$$

Indeed, if $\mathcal{LP} \vdash F \to G$, then, by the constructive necessitation, for some term u we have $\mathcal{LP} \vdash [\![u]\!](F \to G)$. By A2,

$$\mathcal{LP} \vdash [\![u]\!](F \to G) \ \to \ ([\![s]\!]\ F \to [\![us]\!]\ G)$$

and thus $\mathcal{LP} \vdash [\![s]\!]F \to [\![us]\!]G$.

2.13 Lemma.

$$\forall s,t\ \forall F,G\ \exists u\ \mathcal{LP} \vdash [\![s]\!]F \wedge [\![t]\!]G \to [\![u]\!](F \wedge G).$$

Proof. Pick an A5 axiom $[\![c]\!](F \to (G \to F \wedge G))$ with a fresh axiom constant c. By A2

$$\mathcal{LP} \vdash [\![c]\!](F \to (G \to F \wedge G)) \to ([\![s]\!]\ F \to [\![cs]\!](G \to F \wedge G)).$$

Then

$$\mathcal{LP} \vdash [\![s]\!]F \to [\![cs]\!](G \to F \wedge G).$$

Similarly,

$$\mathcal{LP} \vdash [\![cs]\!](G \to F \wedge G) \to ([\![t]\!]G \to [\![(cs)t]\!](F \wedge G)),$$

and we are done with $u = (cs)t$.

◀

2.14 Definition. By a *positive* δ-formula we understand a $\{\wedge, \vee\}$ combination of q-atomic formulas.

2.15 Lemma. (Lifting) *If D is a $\{\wedge, \vee\}$ combination of $[\![t_1]\!]Q_1, \ldots, [\![t_k]\!]Q_k$, then fore some term s*

$$\mathcal{LP} \vdash D \to [\![s]\!]D.$$

Proof. By induction on the length of formula D. The case D is q-atomic is covered by A3. Let now D be $F \wedge G$. By the induction hypothesis, for some terms s, t $\mathcal{LP}_{AS}$ proves both $F \to [\![s]\!]F$ and $G \to [\![t]\!]G$. By lemma 2.13 there exists u such that $\mathcal{LP} \vdash [\![s]\!]F \wedge [\![t]\!]G \to [\![u]\!](F \wedge G)$.

Let D be $F \vee G$. By the induction hypothesis, for some terms s, t $\mathcal{LP} \vdash (F \vee G) \to ([\![s]\!]F \vee [\![t]\!]G)$. By lemma 2.12 there are u, v such that

$$\mathcal{LP} \vdash [\![s]\!]F \to [\![u]\!](F \vee G) \quad \text{and} \quad \mathcal{LP} \vdash [\![t]\!]G \to [\![v]\!](F \vee G).$$

By A4, and according to the propositional logic

$$\mathcal{LP} \vdash [\![s]\!]F \vee [\![t]\!]G \;\to\; [\![u]\!](F \vee G) \vee [\![v]\!](F \vee G) \;\to\; [\![u+v]\!](F \vee G).$$

◀

2.16 Definition. A derivation $\mathcal{D}$ in some $\mathcal{LP}_{AS}$ is *plain* if

1. in all A1 axioms $[\![t]\!]F \to F$ and all AS axioms $[\![c]\!]([\![t]\!]F \to F)$ from $\mathcal{D}$ term t is a proof letter.

2. in all A3 axioms $[\![t]\!]F \to [\![!t]\!][\![t]\!]F$ and AS axioms $[\![c]\!]([\![t]\!]F \to [\![!t]\!][\![t]\!]F)$ term t is either a proof letter or an axiom constant.

For two plain derivations $\mathcal{D}$ and $\mathcal{D}'$ we say that $\mathcal{D}'$ is a *fresh extension* of $\mathcal{D}$ (notation $\mathcal{D}' \sqsupseteq \mathcal{D}$) if $\mathcal{D}'$ is an extension of $\mathcal{D}$ and every new AS axiom $[\![c]\!]B$ comes to $\mathcal{D}'$ with a fresh constant c.

By "$\mathcal{D} : F$", where $\mathcal{D}$ is a derivation and F is a formula we understand "$\mathcal{D}$ *contains* F".

2.17 Lemma. *Let $\mathcal{D}$, $\mathcal{D}'$ be plain derivations, F a formula and t an $\mathcal{LP}$-term.*

a) If $\mathcal{D} : F$ then there exist a term t of axiom constants only and $\mathcal{D}' \sqsupseteq \mathcal{D}$ such that $\mathcal{D}' : [\![t]\!]F$,

b) If $\mathcal{D} : F \to G$ then for any term s there exist a term t of axiom constants and s only and $\mathcal{D}' \sqsupseteq \mathcal{D}$ such that $\mathcal{D}' : [\![s]\!]F \to [\![t]\!]G$,

c) if F is a $\{\wedge, \vee\}$ combination of $[\![q_1]\!]Q_1, \dots, [\![q_k]\!]Q_k$, where q_i are proof letters, then

$$\forall \mathcal{D} \exists \mathcal{D}' \sqsupseteq \mathcal{D} \exists t \ \mathcal{D} : F \to [\![t]\!]F.$$

Proof is obtain by a straightforward inspection of the proofs of 2.11, 2.12 and 2.15.
◄

2.18 Corollary. *Under the conditions of lemma 2.15 there exists a well-founded axiom specification AS such that $\mathcal{LP}_{AS} \vdash D \to [\![s]\!]D$.*

3 Functional completeness

Now we establish a remarkable closure property of the basis $\times, +, !$. We prove that the logic of proofs describes *all* possible propositional operations on proofs. The basic operations $\times, !, +$ thus play for proofs a role similar to that boolean connectives play for classical logic.

Consider an arbitrary scheme of an operation of proofs specification in arithmetic:

$$\models \forall \vec{x} \in C \ \exists y \text{ ``}y \textit{ is a proof of } G(\vec{x})\text{''}.$$

(here $\models$ means "true in the standard model of arithmetic") or, equivalently,

$$\models \forall \vec{x}(C(\vec{x}) \ \to \ \exists y \text{ ``}y \textit{ is a proof of } G(\vec{x})\text{''}).$$

If C and G are arbitrary arithmetical conditions, one should expect hyperarithmetical operations on proofs to appear. However, if we restrict C and G by a propositional language, although already capable of expressing the proof – theorem relation, every operation on proofs reduces to superposition of $\times, !, +$.

3.1 Definition. The *specification language* $\mathcal{L}([\![\cdot]\!])$ is the operation-free fragment of $\mathcal{LP}$-language, i.e. proof variables are the only proof terms in $\mathcal{L}([\![\cdot]\!])$.

3.2 Definition. A *interpretation* $*$ of $\mathcal{L}([\![\cdot]\!])$ is defined as a interpretation of $\mathcal{LP}$-language (omitting clauses for functional symbols and axiom constants).

Now we can make $C(\vec{x})$ and $G(\vec{x})$ occurring in

$$\forall \vec{x}(C(\vec{x}) \ \rightarrow \ \exists y \text{ ``} y \textit{ is a proof of } G(\vec{x})\text{''}).$$

conditions in a propositional specification language $\mathcal{L}([\![\cdot]\!])$. Also, we express the existential quantifier $\exists y$ *"y is a proof of* $G(\vec{x})$*"* by the usual provability modality $\Box$, extending the definition of F^* by one more item: $(\Box F)^*$ is $Pr(\ulcorner F^* \urcorner)$.

Finally we restrict C to a "*proof positive*" condition, i.e. one where the outermost q-atomic subformulas are positive in C.

> Indeed, a condition of the sort
>
> $$\neg[\![x]\!] \ P \ \rightarrow \ \Box\neg[\![x]\!]P,$$
>
> although valid for any proof predicate, may hardly be accepted as an operation on proofs equally as good as $\times, !, +$, because it derives conclusions from *negative* information about proofs; here, from "*x IS NOT a proof*".

It seems that now we have found a balanced definition of an operation on proofs. The regular case

$$[\![x_1]\!]C_1 \wedge \ldots \wedge [\![x_n]\!]C_n \rightarrow G,$$

which comes from the straightforward formalization of the notion of an admissible inference rule

$$\frac{C_1, \ldots, C_n}{G}$$

is covered. Further shrinking of C to say conjunctions of q-atomic formulas would eliminate natural and useful nondeterministic proof predicates.

3.3 Definition. We may define now an *abstract propositional operation on proofs* as a formula

$$C \ \rightarrow \Box G,$$

valid under all arithmetical interpretations, where C, G are formulas in the specification language $\mathcal{L}([\![\cdot]\!])$ and C is proof positive.

3.4 Lemma. *$\mathcal{LP}$ operations $\times, !, +$ can be identified as abstract propositional operations on proofs.*

Proof. Formulas

$$[\![x_1]\!](F \rightarrow G) \wedge [\![x_2]\!]\ F \rightarrow \Box\ G$$

$$[\![x]\!]F \rightarrow \Box [\![x]\!]\ F$$

$$[\![x_1]\!]F \vee [\![x_2]\!]F \rightarrow \Box F$$

are valid under every arithmetical translation since Skolem functions for the existential quantifiers on proofs in $\Box$'s here can be realized by correspondingly $m(x,y),\ c(x),\ e(x,y)$.
◀

The following theorem demonstrates that $\mathcal{LP}$-terms suffice to realize any propositional operation on proofs.

3.5 Theorem. *For any abstract propositional operation on proofs*

$$C \rightarrow \Box G$$

there exist an $\mathcal{LP}$-term t and a well-founded axiom specification AS such that

$$\mathcal{LP}_{AS} \vdash C \rightarrow [\![t]\!]G.$$

Proof. The proof is based on paper [2], which gives a complete axiomatization $\mathcal{B}'$ of all valid formulas in the language $\mathcal{L}([\![\cdot]\!], \Box)$, and on [1] which axiomatizes the arithmetical validity in the language $\mathcal{L}([\![\cdot]\!])$. We consider the following conditions:

1. $C \rightarrow \Box G$ is arithmetically valid
2. $\mathcal{B}' \vdash C \rightarrow \Box G$
3. $\mathcal{LP}_{AS} \vdash C \rightarrow [\![t]\!]G$ for some term t and some well-founded AS.

(1) $\Rightarrow$ (2) is the lion share of the job, it follows immediately from the results of [2]. (2) $\Rightarrow$ (3) is the main lemma of the current section. It is proved below using Kripke models for $\mathcal{B}'$, the arithmetical completeness theorem from [1] and some lemmas from the previous sections.

Now we list some results from [1], [2] we need here.

We recall the logic $\mathcal{B}'$ in the language $\mathcal{L}([\![\cdot]\!], \Box)$. The axioms of $\mathcal{B}$ are boolean tautologies, $\Box(A \to B) \to (\Box A \to \Box B)$, $\Box(\Box A \to A) \to \Box A$, $\Box_p A \to A$, $\Box_p A \to \Box\Box_p A$ and $\neg\Box_p A \to \Box(\neg\Box_p A)$, where p is a proof variable, and A and B are formulas. Rules of $\mathcal{B}$: *modus ponens*, $F \vdash \Box F$, $\Box F \vdash F$. The system $\mathcal{B}'$ has as axioms all theorem of $\mathcal{B}$ and all formulas $\Box A \to A$, and *modus ponens* as its sole deduction rule.

System $\mathcal{P}$ is the $\Box$-free fragment of $\mathcal{B}'$ (or, equivalently, $\mathcal{B}$), and can be axiomatized by $\Box$-free axioms and rules of $\mathcal{B}$ (cf.[1]). It is easy to see that $\mathcal{P}$ is an (operation-free) fragment of $\mathcal{LP}$.

The Kripke models for $\mathcal{B}'$ are finite irreflexive tree-like orderings, the forcing relation $\models$ is defined in the usual way for booleans and $\Box$, and

1. $\forall x \in K\ x \models \Box_p A$ or $\forall x \in K\ x \models \neg\Box_p A$ for every q-atomic formula $\Box_p A$ (stability)
2. $x \models \Box_p A \ \Rightarrow\ x \models A$ for every q-atomic formula $\Box_p A$ (q-reflexivity)

Let $H(F) = \bigwedge\{\Box B \to B \mid \Box B$ is a subformula of $F\}$. We call a model F*-sound* if its root forces $H(F)$. For any $\mathcal{L}([\![\cdot]\!], \Box)$-formula F

$$\mathcal{B}' \vdash F \quad \Leftrightarrow \quad F \text{ holds at the root node of every } F\text{-sound model.}$$

Models for $\mathcal{P}$ are just singleton $\mathcal{B}'$ models.

Let $C \to \Box G$ be arithmetically valid.

3.6 Lemma. $\mathcal{B}' \vdash C \to \Box G$.

Proof. This is a corollary of the arithmetical completeness theorem for $\mathcal{B}'$ from [2].
◀

3.7 Lemma. $\mathcal{LP}_{AS} \vdash C \to G$ *with empty* AS .

Proof. Since $\mathcal{B}' \vdash C \to \Box G$, we have $\mathcal{B}' \vdash C \to G$. Formula $C \to G$ is $\Box$-free, thus $\mathcal{P} \vdash C \to G$ and $\mathcal{LP}_{AS} \vdash C \to G$ with AS being empty.

◀

3.8 Corollary. *If C, G are formulas in the language $\mathcal{L}(\llbracket\cdot\rrbracket)$ and C is a positive δ-formula, then there exists an $\mathcal{LP}$-term t and a well-founded axiom specification AS such that $\mathcal{LP}_{AS} \vdash C \to \llbracket t \rrbracket G$.*

Proof. By 3.7 $\mathcal{LP} \vdash C \to G$ with the empty axiom specification. By 2.17(c) there is AS there is such that $\mathcal{LP}_{AS} \vdash C \to \llbracket u \rrbracket G$ for some term u. By 2.17(b) for some new AS there exists t such that $\mathcal{LP}_{AS} \vdash \llbracket u \rrbracket C \to \llbracket t \rrbracket G$, thus $\mathcal{LP}_{AS} \vdash C \to \llbracket t \rrbracket G$.
◀

3.9 Lemma. *If $\mathcal{B}' \vdash C \to \Box G$, then there exists a δ-formula Q such that*

$$\mathcal{B}' \vdash C \to Q \quad \textit{and} \quad \mathcal{B}' \vdash Q \to \Box G.$$

Proof. The set of $\mathcal{P}$-models of the variables from C is finite; pick those, where C is true, say $a_1, \ldots, a_n$. Let $\sharp_1, \ldots, \sharp_n$ be truth assignments of atomic and q-atomic subformulas of C in $a_1, \ldots, a_n$ correspondingly. For any atomic and q-atomic subformula F of C and every $\sharp \in \{\sharp_1, \ldots, \sharp_n\}$ we define

$$F^\sharp = \begin{cases} F, & \text{if } \sharp \text{ is true on } F \\ \neg F, & \text{if } \sharp \text{ is false on } F. \end{cases}$$

For $i = 1, \ldots, n$, let

$$C_i \;=\; \bigwedge\{F^{\sharp_i} \mid F \;\text{ is an atomic or q-atomic subformula of } C\}.$$

Then $\mathcal{P} \vdash C \leftrightarrow (C_1 \vee \ldots \vee C_n)$. Indeed, if not, then $C \leftrightarrow (C_1 \vee \ldots \vee C_n)$ should be false in some model a of $\mathcal{P}$. If C is true in a, then $a = a_i$ for some $i = 1, \ldots, n$, and C_i is true in a. If C it false in a, then all C_i's are also false in a, since $\mathcal{P}$-model is totally determined by truth assignments of atomic and q-atomic subformulas.

Let C_i^- be the q-part of C_i, i.e.

$$C_i^- \;=\; \bigwedge\{F^{\sharp_i} \mid F \;\text{ is a q-atomic subformula of } C\},$$

and let $Q = C_1^- \vee \ldots \vee C_n^-$. Note, that Q is a positive δ-formula, since C is proof positive. $\mathcal{P} \vdash C \to Q$ is easy, since $\mathcal{P} \vdash C_i \to C_i^-$, $i = 1, \ldots, n$. So we have $\mathcal{B}' \vdash C \to Q$.

Suppose $\mathcal{B}' \not\vdash Q \to \Box G$. Then for some model K of $\mathcal{B}'$, Q is forced at the root node a of K, but $\neg G$ is forced at some node b above a. In this situation there exist $i = 1, \ldots, n$ such that $a \Vdash C_i^-$. Consider a new model K' with the frame $a_i \prec b$, and truth assignments at a_i as in the $\mathcal{P}$-model a_i, and in b according to the model K. We claim that K' is a $\mathcal{B}'$-countermodel for $C \to \Box G$, which is impossible according to the conditions of the lemma. Indeed, $b \not\Vdash G$, thus $a_i \not\Vdash \Box G$ and $a_i \Vdash \Box G \to G$. Also, $a_i \Vdash C$ by the choice of a_i. The condition of q-reflexivity is fulfilled at a_i and b since they are both nodes of legitimate $\mathcal{B}'$-models. The stability condition is also satisfied, since it holds for a pair a, b in K and truth assignments of q-atomic subformulas of C at a_i and a coincide.
◄

This completes the proof of the theorem 3.5.
◄

4 Realization of modal logic

Let F^o be the result of substituting $\Box$ for all occurrences of $[\![t]\!]$ in F, and $X^o = \{F^o \mid F \in X\}$ for any set X of $\mathcal{LP}$-formulas.

4.1 Lemma. $(\mathcal{LP})^o \subseteq \mathcal{S}4$.

Proof. This is a straightforward induction on a derivation in $\mathcal{LP}$.
◄

The goal of the current section is to establish the converse, namely $\mathcal{LP}$ suffices for realization of any $\mathcal{S}4$ theorem. By an *$\mathcal{LP}$-realization* $r = r(AS)$ of a modal formula F we mean

1. an assignment of $\mathcal{LP}$-terms to all occurrences of the modality in F,
2. a choice of an axiom specification AS;

F^r is the image of F under a realization r. A realization r is *normal* if all negative occurrences of $\Box$ are realized by proof letters.

4.2 Theorem. *If $\mathcal{S}4 \vdash F$, then $\mathcal{LP}_{AS} \vdash F^r$ for some well-founded axiom specification AS and some normal realization $r = r(AS)$.*

Proof. Consider a cut-free sequential formulation of $\mathcal{S}4$, with sequents $\Gamma \Rightarrow \Delta$, where Γ and Δ are multisets of modal formulas. Axioms are sequents of the form

$S \Rightarrow S$, where S is a sentence letter. Along with usual structural rules and rules introducing boolean connectives there are two proper modal rules

$$\frac{A, \Gamma \Rightarrow \Delta}{\Box A, \Gamma \Rightarrow \Delta}(\Box \Rightarrow) \qquad \text{and} \qquad \frac{\Box\Gamma \Rightarrow A}{\Box\Gamma \Rightarrow \Box A}(\Rightarrow \Box)$$

(A is a formula, Γ, Δ - multisets of formulas, $\Box\{A_1, \ldots, A_n\} = \{\Box A_1, \ldots, \Box A_n\}$).

If $\mathcal{S}4 \vdash F$, then there exists a cut-free derivation $\mathcal{T}$ of a sequent $\Rightarrow F$. It suffices now to construct a normal realization r and a plain $\mathcal{LP}$-derivation $\mathcal{D}$ which contains all $\mathcal{LP}$-formulas $\mathcal{LP}^- \vdash \bigwedge \Gamma^r \to \bigvee \Delta^r$ for any sequent $\Gamma \Rightarrow \Delta$ in $\mathcal{T}$. We write Γ instead of $\bigwedge \Gamma$ and Δ for $\bigvee \Delta$ whenever unambiguous.

Positive and negative occurrences of modality in a formula and a sequent are defined in the usual way.

1. An indicated occurrence of $\Box$ in $\Box F$ is positive.

2. A corresponding occurrence of $\Box$ in F and $G \to F$, $G \wedge F$, $G \vee F$, $\Box F$ and $(\Gamma \Rightarrow \Delta, F)$ has the same polarity.

3. A corresponding occurrence of $\Box$ in F and $\neg F$, $F \to G$ and $(F, \Gamma \Rightarrow \Delta)$ has opposite polarities.

Note that in a cut-free derivation $\mathcal{T}$, the rules respect polarities, all occurrences of $\Box$ introduced by $(\Rightarrow \Box)$ are positive, and all negative occurrences are introduced by $(\Box \Rightarrow)$ or by weakening.

Occurrences of $\Box$ are related if they occur in related formulas of premises and conclusions of rules; we extend this relationship by transitivity. The following example demonstrates how related boxes (painted black) proliferate through a contraction rule:

4.3 Example.

$$\frac{X(\Box Y), X(\blacksquare Y), \Gamma \Rightarrow \Delta}{X(\Box Y), \Gamma \Rightarrow \Delta} \quad \rightsquigarrow \quad \frac{X(\Box Y), X(\blacksquare Y), \Gamma \Rightarrow \Delta}{X(\blacksquare Y), \Gamma \Rightarrow \Delta}$$

$$\rightsquigarrow \quad \frac{X(\blacksquare Y), X(\blacksquare Y), \Gamma \Rightarrow \Delta}{X(\blacksquare Y), \Gamma \Rightarrow \Delta}.$$

All positive occurrences of $\Box$ in $\mathcal{T}$ are naturally split into disjoint *families* of related ones; we call a family *essential* if it contains at least one case of $(\Rightarrow \Box)$ rule.

Now the desired r will be constructed by stages A – C. We reserve a large enough set of proof letters as new *term variables*; so there are proof letters, axiom constants and term variables at our disposal as term generators. Eventually we will get rid of the term variables in the final realization r and in the corresponding proof of F^r in $\mathcal{LP}_{AS}$.

Stage A. Every negative family and nonessential positive family is realized by a fresh proof letter.

Stage B. Pick an essential family f, enumerate all the occurrences of rules $(\Rightarrow \Box)$, which introduce boxes of this family and let n_f be the total number of such rules for the family f. Realize all boxes of the family f by the term

$$(x_1 + \ldots + x_{n_f}),$$

where x_i's are fresh term variables.

Stage C. Proceed with the following process of

- assigning to a sequent $\Gamma \Rightarrow \Delta$ an $\mathcal{LP}$-term t (containing no term variables) and upgrading a plain derivation $\mathcal{D}$ in order to reach

$$\mathcal{D} : [\![t]\!](\Gamma \rightarrow \Delta),$$

- possibly substituting some $\mathcal{LP}$-term s for a term variable,

- moving downwards.

We start from the axiom nodes. Assign a fresh axiom constant a to each axiom $S \Rightarrow S$. Clearly $[\![a]\!](S \rightarrow S)$ is a proof of itself.
Weakening rule:

$$\frac{\Gamma \Rightarrow \Delta}{Y, \Gamma \Rightarrow \Delta}\ .$$

Let term t be assigned to $\Gamma \Rightarrow \Delta$. Pick a fresh axiom constant b, add

$$[\![b]\!]((\Gamma \rightarrow \Delta) \rightarrow (Y \wedge \Gamma \rightarrow \Delta))$$

to $\mathcal{D}$. Then, by A2 find a new $\mathcal{D}$ such that

$$\mathcal{D} : [\![bt]\!](Y \wedge \Gamma \rightarrow \Delta).$$

Weakening rule (succedent) is treated similarly.

Contraction rule:

$$\frac{Y, Y, \Gamma \Rightarrow \Delta}{Y, \Gamma \Rightarrow \Delta}\ .$$

Let term t be assigned to $Y, Y, \Gamma \Rightarrow \Delta$. Pick a fresh axiom constant b, add

$$[\![b]\!]((Y \wedge Y \wedge \Gamma \to \Delta) \to (Y \wedge \Gamma \to \Delta))$$

to $\mathcal{D}$. Then, by A2 find a new $\mathcal{D}$ such that

$$\mathcal{D} : [\![bt]\!](Y \wedge \Gamma \to \Delta).$$

Similar treatment should be given to all remaining structural rules and rules introducing boolean connectives.

Rule $(\Box \Rightarrow\ )$ has already looked like:

$$\frac{X, \Gamma \Rightarrow \Delta}{[\![p]\!]X, \Gamma \Rightarrow \Delta}$$

for some proof letter p. Let term t be assigned to the premise $X, \Gamma \Rightarrow \Delta$. Extend $\mathcal{D}$ by $[\![b]\!]([\![p]\!]X \to X)$ for a fresh axiom constant b. Since $\mathcal{D} : [\![t]\!](X \wedge \Gamma \to \Delta)$, it is now an easy exercise to construct t' and $\mathcal{D}' \sqsupseteq D$ such that

$$\mathcal{D}' : [\![t']\!](X \to (\Gamma \to \Delta)),$$

then $s(t', b)$ and $\mathcal{D}'' \sqsupseteq \mathcal{D}'$ such that

$$\mathcal{D}'' : [\![s(t', b)]\!]([\![p]\!]X \to (\Gamma \to \Delta)),$$

and finally $s'(t', b)$, $\mathcal{D}''' \sqsupseteq \mathcal{D}''$ such that

$$\mathcal{D}''' : [\![s'(t', b)]\!]([\![p]\!]X \wedge \Gamma \to \Delta).$$

Let an occurrence of the rule $(\ \Rightarrow \Box)$ have number i in the numbering of all rules $(\ \Rightarrow \Box)$ from a given family f. This rule already has a form

$$\frac{[\![q_1]\!]Y_1, \ldots, [\![q_k]\!]Y_k \Rightarrow Y}{[\![q_1]\!]Y_1, \ldots, [\![q_k]\!]Y_k \Rightarrow [\![u_1 + \ldots + u_{n_f}]\!]Y} \ ,$$

where $q_1, \ldots, q_k$ are proof letters, $u_1, \ldots, u_{n_f}$ are $\mathcal{LP}$-terms, and u_i is a term variable; assume the latter condition to be built-in an inductive hypothesis. Let term t be assigned to $[\![q_1]\!]Y_1, \ldots, [\![q_k]\!]Y_k \Rightarrow Y$, i.e.

$$\mathcal{D} : [\![t]\!]([\![q_1]\!]Y_1 \wedge \ldots \wedge [\![q_k]\!]Y_k \to Y).$$

By the lemma 2.17(c), there exists an $\mathcal{LP}$-term s of axiom constants and proof letters $q_1, \ldots, q_k$ and $\mathcal{D}' \sqsupseteq \mathcal{D}$ such that

$$\mathcal{D}' : [\![q_1]\!]Y_1 \wedge \ldots \wedge [\![q_k]\!]Y_k \to [\![s]\!]([\![q_1]\!]Y_1 \wedge \ldots \wedge [\![q_k]\!]Y_k).$$

By A2 we get $\mathcal{D}'' \sqsupseteq \mathcal{D}'$ such that

$$\mathcal{D}'' : [\![s]\!]([\![q_1]\!]Y_1 \wedge \ldots \wedge [\![q_k]\!]Y_k) \rightarrow [\![ts]\!]Y.$$

By A4 we construct $\mathcal{D}''' \sqsupseteq \mathcal{D}''$

$$\mathcal{D}''' : [\![ts]\!]Y \rightarrow [\![u_1 + \ldots + u_{i-1} + ts + u_{i+1} + \ldots + u_{n_f}]\!]Y.$$

Finally, $\mathcal{D}'''$ has a straightforward fresh extension $\mathcal{D}''''$ such that

$$\mathcal{D}'''' : \bigwedge_{i=1}^{k} [\![q_i]\!]Y_i \rightarrow [\![u_1 + \ldots + u_{i-1} + ts + u_{i+1} + \ldots + u_{n_f}]\!]Y.$$

By the lemma 2.17(a) there exist an $\mathcal{LP}$-term b of axiom constants only and $\mathcal{D}''''' \sqsupseteq \mathcal{D}''''$ such that

$$\mathcal{D}''''' : [\![b]\!](\bigwedge_{i=1}^{k} [\![q_i]\!]Y_i \rightarrow [\![u_1 + \ldots + u_{i-1} + ts + u_{i+1} + \ldots + u_{n_f}]\!]Y).$$

Finally, we substitute term ts for variable u_i everywhere in $\mathcal{T}$ and in $\mathcal{D}$; this remains possible since ts does not contain term variables. Also, $\mathcal{D}$ remains a plain derivation since this substitution does not effect proof letters and axiom constants.

By the end of stage C all the term variables are replaced by $\mathcal{LP}$-terms of proof letters and axiom constants, which determines the desired normal realization r. By the construction the $\mathcal{LP}$-proof $\mathcal{D}$ contains F^r.
◀

Combining 4.1 and 4.2 we get

4.4 Corollary.

$$\mathcal{S}4 \vdash F \quad \Leftrightarrow \quad \mathcal{LP} \vdash F^r \textit{ for some realization } r.$$

4.5 Comment. The realization algorithm above produces a normal realization. Gödel in [4] defined a translation *tr* of an intuitionistic formula, into an $\mathcal{S}4$-formula where *tr(F)* is obtained from F by prefixing every subformula of the latter by $\Box$. This Gödel translation is shown ([4], [9]) to provide an exact embedding of $\mathcal{I}nt$ into $\mathcal{S}4$: for any $\mathcal{I}nt$-formula F

$$\mathcal{I}nt \vdash F \quad \Leftrightarrow \quad \mathcal{S}4 \vdash tr(F).$$

The Brouwer - Heyting - Kolmogorov operations via Godel embedding of $\mathcal{I}nt$ into $\mathcal{S}4$ may now be regarded as $\mathcal{LP}$-terms under normal realization of $\mathcal{S}4$. The proof interpretation of $\mathcal{LP}$-terms makes this defitinition precise. Note, that by 4.2 the proof constructed for F^r in $\mathcal{LP}$ also produces a well-founded axiom specification AS for F^r.

4.6 Corollary. *For any $\mathcal{I}nt$-formula F*

$$\mathcal{I}nt \vdash F \quad \Leftrightarrow \quad \mathcal{LP} \vdash (tr(F))^r \textit{ for some realization } r.$$

By 2.10 and 4.2 we have

4.7 Theorem. (Arithmetical correctness of $\mathcal{S}4$)

$$\mathcal{S}4 \vdash F \quad \Rightarrow \quad \begin{array}{l} \textit{there exist a (well-founded) axiom specification } AS \\ \textit{and a (normal) realization } r(AS) \textit{ of } F \textit{ such that} \\ \qquad\qquad\qquad \mathcal{PA} \vdash (F^r)^* \\ \textit{for any } AS\textit{-interpretation } *. \end{array}$$

5 Canonical model

5.1 Definition. The *saturation algorithm* $\mathcal{A}$ starts from a $\mathcal{LP}$-formula F and an axiom specification AS such that

$$\mathcal{LP}_{AS} \not\vdash F,$$

and produces a pair of sets (Γ, Δ) of $\mathcal{LP}$-formulas by cycles of transformations 1-6 below. Each step 1 – 6, before performing "goto" command, does the following test: "*If $\Gamma \cap \Delta \neq \emptyset$, then backtrack to the nearest branching point and if no paths remain unexplored, then terminate with failure. If no transformations 1 – 6 can be applied, terminate with success*".

0. Put $\Delta_0 = \{\bot, F\}$ and $\Gamma_0 = \{\top\} \cup \{[\![c]\!]A \mid [\![c]\!]A \in AS\}$, goto 1.

1. For every formula $X \to Y \in \Gamma$ which has not been discharged by the rule 1 before nondeterministically put Y into Γ, if $Y \notin \Gamma$ or put X into Δ, if $X \notin \Delta$, and discharge the formula $X \to Y \in \Gamma$. This is a branching point, and $\mathcal{A}$ backtracks (if any) to one of these points. If a backtracking happens, then all the discharges occured during the backtracked period are canceled. Goto 2.

2. For all formulas $X \to Y \in \Delta$ put X into Γ, unless $X \in \Gamma$, and put Y into Δ, unless $Y \in \Delta$, goto 3.

3. For all $[\![t]\!]X \in \Gamma$ such that $X \notin \Gamma$ put X into Γ, goto 4.

4. For all pairs $[\![s]\!]X \in \Gamma$, $[\![t]\!](X \to Y) \in \Gamma$, put $[\![ts]\!]Y$ into Γ, if it has not been there before, goto 5.

5. For all $[\![t]\!]X \in \Gamma$ put $[\![!t]\!][\![t]\!]X$ into Γ, if it has not been there before, goto 6.

6. For all $[\![t]\!]X \in \Gamma$ and all s occurring in the current pair (Γ, Δ) put both $[\![t+s]\!]X$ and $[\![s+t]\!]X$ into Γ, if they have not been there before, goto 1.

It is clear, that saturation algorithm either terminates with failure or terminates with success or runs forever.

5.2 Lemma. *If $\mathcal{A}$ terminates with failure, then $\mathcal{LP}_{AS} \vdash F$.*

Proof. This is a fairly standard lemma. Consider a finite tree $\mathcal{T}$ of a failed saturation process. Every node of $\mathcal{T}$ is a pair (Γ, Δ) of finite sets of $\mathcal{LP}$-formulas. By an easy induction on the depth of a node in $\mathcal{T}$ we can prove that $\mathcal{LP}_{AS} \vdash \Gamma \to \Delta$. Thus $\mathcal{LP}_{AS} \vdash F$.
◀

Without loss of generality we may assume that $\mathcal{A}$ runs forever.

Let $|t|$ denote the length of t. Let also Sb denote the set of all subformulas of (Γ_0, Δ_0), and let N be maximum of the cardinality of Sb and the lengths of terms, occurring in Sb. Let

$$\widetilde{\Gamma} = \{X \mid [\![t]\!]X \in \Gamma \text{ for some } t\},$$

and $M(\Gamma) = \widetilde{\Gamma} \cap Sb$. A *cycle* is one turn of transformations 1 – 6 in an $\mathcal{A}$ run.

5.3 Lemma. *If none of 1, 2, 3 is active and no backtracking occurs during consecutive $2N$ cycles, then no more activities of 1, 2, 3 or backtrackings will ever occur.*

Proof. Assume the conditions of the lemma. Let

$$m_j = min\{|t| \mid [\![t]\!]F \text{ is put to } \Gamma \text{ at the cylcle } j\}.$$

(a) $m_{j+1} > m_j$. Indeed, consider the cycle $j+1$ and let $[\![t]\!]F$ appears in Γ during this cycle. Consider three cases: 4, 5 and 6.

If $[\![t]\!]F$ is introduced by 4, i.e. from $[\![u]\!](X \to F) \in \Gamma$ and $[\![v]\!]X \in \Gamma$ with $t = uv$, then at least one of these formulas appeared in Γ during the j's cycle; otherwise $[\![t]\!]F$ would appeared in Γ during the cycle j or earlier. Thus

$$|t| = |uv| > \max(|u|, |v|) \geq m_j.$$

If $[\![t]\!]F$ is introduced by 5, i.e. from $[\![u]\!]X \in \Gamma$, and $t = !u$, $F = [\![u]\!]X$, then $[\![u]\!]X$ appeared in Γ either during the cycle j or by the rule 4 of the cycle $j+1$. In both cases

$$|t| = |!u| > |u| \geq m_j.$$

Case 6 is similar to 5. Thus (a) is established.

Let j denote the number of 4-5-6 cycles which have passed after the beginning of the interval from the conditions of the lemma, and let Γ_j denote the set Γ immediately after the last rule of the cycle j was performed.

(b) If $j > N$ and $M(\Gamma_j) = M(\Gamma_{j+1})$, then $M(\Gamma_j) = M(\Gamma_k)$ for all $k > j$.

Indeed, suppose the opposite and pick the first $k > j$ such that $M(\Gamma_j) \neq M(\Gamma_k)$. Again, consider the first rule of 4, 5, 6, which changes $M(\Gamma_j)$ at the cycle k.

It cannot be 4: from $[\![s]\!]X \in \Gamma$ and $[\![t]\!](X \to Y) \in \Gamma$ put $[\![ts]\!]Y$ into Γ, because for this rule both X, $X \to Y$ are from Sb, thus $X,\ X \to Y \in M(\Gamma_{j+1}) = M(\Gamma_j)$, and Y is already in $M(\Gamma_{j+1})$.

It cannot be 5: from $[\![t]\!]X \in \Gamma$ put $[\![!t]\!][\![t]\!]X$ into Γ. Indeed, by (a) $|t| > N$ and the formula $[\![t]\!]X$ is too long to be in Sb.

It cannot be 6 either, since this rule does not change $M(\Gamma)$.

(c) If $j > N$ and $M(\Gamma_j) = M(\Gamma_{j+1})$, then no rules 1, 2 or 3 can apply at all after the cycle $j+1$.

Indeed, consider the first active rule of 1, 2, 3 after the cycle j from the assumption (c), i.e. $j > N$ and $M(\Gamma_j) = M(\Gamma_{j+1})$. Let it happen during the cycle $k > j+1$, note that by (b) $M(\Gamma_k) = M(\Gamma_{k-1}) = M(\Gamma_{k-2})$. This rule cannot be 1, since it applies to new formulas of the form $X \to Y$, and no such formulas appeared at the cycle $k-1$. It cannot be 2 either, since no changes of Δ happen at the cycle $k-1$. Suppose it is 3 that applies at the cycle k to $[\![t]\!]F$. Then $[\![t]\!]F$ appeared at the cycle $k-1$ by one of the rules 4, 5, 6.

If by 4, then $F \in M(\Gamma_k)$, thus $F \in M(\Gamma_{k-2})$ and $F \in \Gamma_{k-1}$ by the rule 3 during the cycle $k-1$. So, 3 does not apply to $[\![t]\!]F$.

If by 5, then $F = [\![s]\!]X$, $t = !s$, and $[\![s]\!]X \in \Gamma_{k-1}$. Again, 3 does not apply to $[\![t]\!]F$.

If by 6, then $[\![t]\!]F = [\![u+v]\!]F$ and one of $[\![u]\!]F$, $[\![v]\!]F$ is from Γ_{k-1}. Suppose $[\![u]\!]F \in \Gamma_{k-1}$. If $[\![u]\!]F \in \Gamma_{k-2}$, then $F \in \Gamma_{k-1}$ by the rule 3 at $k-1$, and 3 does not apply to $[\![t]\!]F$ at k. So, $[\![u]\!]F$ is introduced during the cycle $k-1$ by 4 or 5. It cannot be 4, because then $F \in M(\Gamma_{k-1}) = M(\Gamma_{k-2})$ and $F \in \Gamma_{k-1}$. It cannot by 5 either since then again $F \in \Gamma_{k-1}$. So (c) is established.

(d) Since $M(\Gamma_j)$ is monotone on j and $M(\Gamma_j) \subseteq Sb$ it takes not more then N cycles after the first N ones until we meet $M(\Gamma_j) = M(\Gamma_{j+1})$. After this moment no further backtracking is possible and $\mathcal{A}$ runs forever.

◀

5.4 Lemma. *If an interval of an $\mathcal{A}$-run without backtrackings is longer than $8N^2$ cycles, then no more backtrackings can happen during this run.*

Proof. Suppose the opposite, i.e. that $\mathcal{A}$ backtracks after an interval of more than $8N^2$ cycles without backtracking. By the previous lemma rules 1, 2, 3 cannot all stay passive during more than $2N$ consecutive cycles without backtracking. Each of 1, 2, 3 cannot be active more than N times, since their inputs are formulas from Sb. That gives us a bound $(3N-1)(2N+1)+1 = 6N^2+N < 8N^2$ after which no more backtrackings can happen.

◀

5.5 Lemma. *Each run of $\mathcal{A}$ makes not more than 2^N backtrackings.*

Proof. From what we have already learned about $\mathcal{A}$, no formulas $X \to Y$ other than from Sb can ever appear in Γ, not more than N binary choices to break $X \to Y$ by the rule 1, not more than 2^N variants.

◀

Thus, after finite amount of returns an infinite computational process will no longer backtrack; let (Γ, Δ) denote the limit of current Γ's and Δ's correspondingly. The following lemma summarizes our knowledge about the saturation process.

5.6 Lemma. (Stabilization lemma) *After j cycles with $j > N^2 \cdot 2^{N+3}$ no more backtrackings can occur, only rules 4, 5, 6 can be active, all newcomings are to Γ and have a form $[\![t]\!]X$ with a term t having length greater than $j - N^2 \cdot 2^{N+3}$.*

5.7 Corollary. *Δ is finite, Γ is recursive, a set $I(t) = \{B \mid [\![t]\!]B \in \Gamma\}$ is finite for every term t, a function from t to $I(t)$ is recursive.*

Proof. Δ is finite, since $\Delta \subseteq Sb$. To decide whether a k symbols long formula H is in Γ it suffices now to wait $i = k + N^2 \cdot 2^{N+3}$ cycles of $\mathcal{A}$ and to check $H \in \Gamma_i$ for a finite set Γ_i. The same argument applies to a function from t to $I(t)$.
◀

5.8 Lemma. *If algorithm $\mathcal{A}$ on a given formula F succeeds or runs forever, then $\mathcal{LP}_{AS} \nvdash F$.*

The proof is a standard canonical model argument. Complete (Γ, Δ) to a maximal consistent pair of sets, define $(\Gamma, \Delta) \models Q$ as $Q \in \Gamma$ for any atomic or q-atomic Q, prove that $(\Gamma, \Delta) \models H \;\Leftrightarrow\; H \in \Gamma$ and $(\Gamma, \Delta) \models \mathcal{LP}_{AS}$. Conclude, that $\mathcal{LP}_{AS} \nvdash F$, since $F \in \Gamma$. However, we'll get the claim of this lemma for free after the arithmetical competeness theorem 6.1 below.

5.9 Corollary. *$\mathcal{LP}_{AS}$ is decidable for any AS.*

6 Arithmetical completeness

6.1 Theorem. *For any $\mathcal{LP}$-formula F and any axiom specification AS*

$$\mathcal{LP}_{AS} \nvdash F \;\Rightarrow\; F^* \textit{is false for some } AS\textit{-interpretation } *.$$

Proof. Let $\mathcal{LP}_{AS} \nvdash F$. Run the saturation algorithm $\mathcal{A}$ on F, which by lemma 5.2 either succeeds or does not terminate. Without loss of generality we may assume the latter, and let Γ, Δ denote the limit of current Γ_j's and Δ_j's correspondingly. By 5.7 Γ is recursive and Δ is finite.

We define the desired interpretation $*$ on sentence letters S_i, proof letters p_j and axiom constants a_j first. Put

$$S_i{}^* = \begin{cases} i+1 = i+1, & \text{if } S_i \in \Gamma \\ i+1 = 0, & \text{if } S_i \notin \Gamma, \end{cases} \qquad p_j{}^* = \ulcorner p_j \urcorner, \qquad a_j{}^* = \ulcorner a_j \urcorner.$$

The remaining parts of $*$ are constructed by a multiple arithmetical fixed point equation. Let *(PROOF*, $\otimes$, $\oplus$, $!$) be a standard nondeterministic proof predicate from 2.2. For technical convenience and without loss of generality we assume that $PROOF(\ulcorner t \urcorner, k)$ is false for any $\mathcal{LP}$-term t and any $k \in \omega$.

In what follows $*$ is based on *Prf* as proof predicate,

$$\times^* = \mu z M(x,y,z), \quad +^* = \mu z E(x,y,z), \quad !^* = \mu z C(x,z).$$

Note, that $\ulcorner B^* \urcorner$ can be calculated in a primitive recursive way from

$$\ulcorner Prf(x,y) \urcorner,\ \ulcorner M(x,y,z) \urcorner,\ \ulcorner C(x,z) \urcorner, \ulcorner E(x,y,z) \urcorner$$

for any subformula B from $\Gamma \cup \Delta$.

By the arithmetical fixed point argument there exist arithmetical formulas $Prf(x,y)$, $M(x,y,z)$, $E(x,y,z)$, $C(x,z)$ such that $\mathcal{PA}$ proves the following *fixed point equation (FPE)*:

$$\begin{array}{lcl}
Prf(x,y) & \leftrightarrow & PROOF(x,y) \quad \vee \\
 & & \vee(\text{“}x = \ulcorner t \urcorner \textit{ for some } \mathcal{LP}\textit{-term } t\text{”} \wedge y = \ulcorner B^* \urcorner \wedge \text{“}[\![t]\!]B \in \Gamma\text{”}).
\end{array}$$

$$\begin{array}{lcl}
M(x,y,z) & \leftrightarrow & \textit{if } x = \ulcorner s \urcorner \textit{ and } y = \ulcorner t \urcorner \textit{ for some terms } s,t, \textit{ then } z = \ulcorner st \urcorner, \\
 & & \\
 & & \textit{if } x = \ulcorner s \urcorner \textit{ and } y \neq \ulcorner t \urcorner \textit{ for any term } t, \textit{ then recover } I(s), \\
 & & \textit{put } z = \mu w(\bigwedge\{PROOF(w, \ulcorner B^* \urcorner) \mid B \in I(s)\}) \otimes y, \\
 & & \\
 & & \textit{if } y = \ulcorner t \urcorner \textit{ and } x \neq \ulcorner s \urcorner \textit{ for any term } s, \textit{ then recover } I(t), \\
 & & \textit{put } z = x \otimes \mu w(\bigwedge\{PROOF(w, \ulcorner B^* \urcorner) \mid B \in I(t)\}), \\
 & & \\
 & & z = x \otimes y, \textit{ else.}
\end{array}$$

$$\begin{array}{lcl}
C(x,z) & \leftrightarrow & \textit{if } x = \ulcorner (\overline{\ulcorner t \urcorner}) \urcorner, \textit{ then } z = \ulcorner !t \urcorner, \\
 & & z = \Uparrow x, \textit{ else.}
\end{array}$$

$$\begin{array}{lcl}
E(x,y,z) & \leftrightarrow & \textit{if } x = \ulcorner s \urcorner,\ y = \ulcorner t \urcorner \textit{ for some terms } s,t, \textit{ then } z = \ulcorner s + t \urcorner, \\
 & & \\
 & & \textit{if } x = \ulcorner s \urcorner \textit{ and } y \neq \ulcorner t \urcorner \textit{ for any term } t, \textit{ then recover } I(s), \\
 & & \textit{put } z = \mu w(\bigwedge\{PROOF(w, \ulcorner B^* \urcorner) \mid B \in I(s)\}) \oplus y, \\
 & & \\
 & & \textit{if } y = \ulcorner t \urcorner \textit{ and } x \neq \ulcorner s \urcorner \textit{ for any term } s, \textit{ then recover } I(t), \\
 & & \textit{put } z = x \oplus \mu w(\bigwedge\{PROOF(w, \ulcorner B^* \urcorner) \mid B \in I(t)\}), \\
 & & \\
 & & z = x \oplus y, \textit{ else.}
\end{array}$$

By *FPE* it is immediate that *Prf* is a provably Δ_1-formula and if $\mathcal{PA} \vdash \psi$, then $Prf(k, \ulcorner \psi \urcorner)$ for some $k \in \omega$.

6.2 Lemma. $\mathcal{PA} \vdash t^* = \ulcorner t \urcorner$ *for any term* t.

Indeed, according to *FPE*

$$(st)^* = m(s^*, t^*) = m(\ulcorner s \urcorner, \ulcorner t \urcorner) = \ulcorner st \urcorner.$$

The same holds for $(s+t)^*$ and $!t^*$; in the latter case we accept an arithmetical numeral $\overline{\ulcorner t \urcorner}$ for $\ulcorner t \urcorner$ as a legitimate ι-term.

6.3 Corollary. $*$ *is injective on formulas and terms from* $\Gamma \cup \Delta$.

6.4 Corollary. X^* *is provably* Δ_1 *for any* X*, occurring as a subformula in* $\Gamma \cup \Delta$.

Indeed, if X is atomic, then X is Δ_1 by the definition of $*$. If X is $[\![t]\!]Y$, then

$$([\![t]\!]Y)^* \quad = \quad \mathit{Prf}(t^*, \ulcorner Y^* \urcorner),$$

and since

$$\mathcal{PA} \vdash \mathit{Prf}(t^*, \ulcorner Y^* \urcorner) \leftrightarrow \mathit{Prf}(\ulcorner t \urcorner, \ulcorner Y^* \urcorner)$$

and $\mathit{Prf}(\ulcorner t \urcorner, \ulcorner Y^* \urcorner)$ is provably recursive, then $([\![t]\!]Y)^*$ surely is. Boolean connectives preserve Δ_1.

6.5 Lemma. *If* $X \in \Gamma$*, then* $\mathcal{PA} \vdash X^*$*, if* $X \in \Delta$*, then* $\mathcal{PA} \vdash \neg X^*$.

Proof. This is a standard boolean saturation lemma proven by the induction on X. Basis, i.e. X is atomic or q-atomic. If $[\![t]\!]Y \in \Gamma$, then $\mathcal{PA} \vdash$ "$[\![t]\!]Y \in \Gamma$" and $\mathcal{PA} \vdash ([\![t]\!]Y)^*$ by *FPE*. If $[\![t]\!]Y \in \Delta$, then $\mathcal{PA} \vdash ([\![t]\!]Y)^*$ is false by *FPE* since $*$ is injective on formulas and terms from $\Gamma \cup \Delta$. The induction steps corresponding to boolean connectives are trivial because (Γ, Δ) is a saturated pair.
◀

6.6 Lemma. $\mathcal{PA} \vdash \varphi \quad \Leftrightarrow \quad \mathit{Prf}(n, \ulcorner \varphi \urcorner)$ *for some* $n \in \omega$.

Proof. It remains to establish $(\Leftarrow)$. From *FPE* it is clear that

$\mathit{Prf}(n, \ulcorner \psi \urcorner) \;\Rightarrow\;$ "$\mathit{PROOF}(n, \ulcorner \psi \urcorner)$ or $\psi = B^*$ for some B such that $[\![t]\!]B \in \Gamma$".

In the latter case $B \in \Gamma$ by the saturation property of Γ, and $\mathcal{PA} \vdash B^*$ by 6.5.
◀

6.7 Lemma. *$\mu z M(x,y,z)$ and $\mu z E(x,y,z)$ are provably total.*

Proof. From FPE by a straightforward formalization of the proofs of 6.5 and 6.6 in $\mathcal{PA}$.
◀

6.8 Lemma. *Normality conditions for Prf are fulfilled.*

Proof. Both normality conditions follow easily from the normality of $PROOF$, FPE and the saturation properties of Γ and 5.7.
◀

So, Prf is a normal proof predicate. Now, by lemma 6.5 $\mathcal{PA} \vdash \neg F^*$, since $F \in \Delta$.
◀

6.9 Definition. For an axiom specification AS an $\mathcal{LP}$-formula F is *arithmetically AS-valid* if $\mathcal{PA} \vdash F^*$ for any AS-interpretation $*$.

6.10 Corollary. (Arithmetical completeness of $\mathcal{LP}$)

$\mathcal{LP} \vdash F \quad \Leftrightarrow \quad$ *F is arithmetically AS-valid for some axiom specification AS.*

6.11 Corollary. (Arithmetical completeness of $\mathcal{S}4$)

$\mathcal{S}4 \vdash F \quad \Leftrightarrow \quad$ *F^r is arithmetically AS-valid for some realization r and some axiom specification AS.*

6.12 Corollary. (Arithmetical completeness of $\mathcal{I}nt$)

$\mathcal{I}nt \vdash F \quad \Leftrightarrow \quad$ *$[tr(F)]^r$ is arithmetically AS-valid for some realization r and some axiom specification AS.*

6.13 Remark. 6.10, 6.11 and 6.12 remain valid under a reading of "F is arithmetically AS-valid" as "F^* is valid in the standard model of arithmetic for any AS-interpretation $*$."

Acknowledgements.

The research described in this publication was supported in part by the Russian Foundation for Basic Research, grant No. 93-011-16015; the International Science Foundation, grant No. NFQ300, and by INTAS grant No. 94-2412.

This work has benefited from many interactions over the past several years with a number of mathematicians, logicians and computer scientists: L. Beklemishev, J. van Benthem, G. Boolos, D. van Dalen, E. Engeler, J.-Y. Girard, G. Jäger, D. de Jongh, F. Montagna, A. Nerode, E. Nogina, D. Roorda, T. Strassen, A. Troelstra, A. Visser.

I am indebted to Tanya Sidon for a careful reading of this paper which led to valuable improvements.

References

[1] S. Artëmov and T. Strassen, "The Basic Logic of Proofs," *Lecture Notes in Computer Science* , v. 702 (1993), pp. 14-28.

[2] S. Artëmov, "Logic of Proofs," *Annals of Pure and Applied Logic*, v. 67 (1994), pp. 29-59.

[3] D. van Dalen, *Logic and Structure*, Springer-Verlag, 1994.

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

[5] D. Guaspari and R.M. Solovay, "Rosser sentences," *Annals of Mathematical Logic*, v. 16 (1979), pp. 81-99.

[6] A. Heyting, "Die intuitionistische Grundlegung der Mathematik", *Erkenntnis*, Bd. 2 (1931), S. 106-115.

[7] D. Hilbert and P. Bernays, *Grundlagen der Mathematik*, Springer, 1934-1939.

[8] A. Kolmogoroff, "Zur Deutung der intuitionistischen Logik," *Math. Ztschr.*, Bd. 35 (1932), S.58-65.

[9] J.C.C. McKinsey and A. Tarski, "Some theorems about the sentential calculi of Lewis and Heyting", Journ.Symb. Logic, v. 13 (1948), pp. 1-15.

[10] A.S. Troelstra and D. van Dalen, *Constructivism in Marthematics. An Introduction*, v. 1, Amsterdam; North Holland, 1988.

[11] C. Smorynski, "The incompleteness theorems", in *Handbook of mathematical logic*, Amsterdam; North Holland, 1977, pp. 821-865.