Operations on proofs that can be specified by means of modal logic

Sergei N. Artemov *

Abstract

Explicit modal logic was first sketched by Gödel in [16] as the logic with the atoms "*t is a proof of F*". The complete axiomatization of the Logic of Proofs $\mathcal{LP}$ was found in [4] (see also [6],[7],[18]). In this paper we establish a sort of a functional completeness property of *proof polynomials* which constitute the system of proof terms in $\mathcal{LP}$. Proof polynomials are built from variables and constants by three operations on proofs: "$\cdot$" (application), "!" (proof checker), and "+" (choice). Here constants stand for canonical proofs of "simple facts", namely instances of propositional axioms and axioms of $\mathcal{LP}$ in a given proof system. We show that every operation on proofs that (i) can be specified in a propositional modal language and (ii) is invariant with respect to the choice of a proof system is realized by a proof polynomial.

Introduction

The intended meaning of the intuitionistic logic was informally explained first in terms of operations on proofs due to Brouwer, Heyting and Kolmogorov (cf. [43],[44],[12]). This interpretation is widely known as the *BHK* semantics of intuitionistic logic. However, despite some similarities in the informal description of the functions assigned to the intuitionistic connective, the Heyting semantics and the Kolmogorov semantics have fundamentally different objectives. The Heyting semantics explaines intuitionistic logic in terms of an undefined notion of intuitionistic proof. The Kolmogorov interpretation of $\mathcal{I}nt$ as a calculus of problems [21], along with the related papers by Gödel [15],[16] intended to interpret $\mathcal{I}nt$ on the basis of classical proofs, thus providing an independent definition of intuitionistic logic within the classical mathematics. We call this sort of interpretation of $\mathcal{I}nt$ *classical BHK semantics*.

Classical realizabilities: Kleene realizability [19], function realizability [20], modified realizability [24], Medvedev's calculus of finite problems [31] and its variants, give conditions necessary but not sufficient for $\mathcal{I}nt$(cf.[12],[45],[46],[47]). Each of them realizes some formulas

*Department of Mathematics, Cornell University, `email:artemov@math.cornell.edu` and Moscow University, Russia.

not derivable in $\mathcal{I}nt$. A formalization of the *BHK* semantics suggested by Kreisel in [23] turned out to be based on an inconsistent theory (cf. [48], [37]). For more discussion on realizability semntics for $\mathcal{I}nt$ see [45].

In 1933 Gödel ([15]) defined $\mathcal{I}nt$ on the basis of the notion of *proof* in a classical mathematical system, reminiscent to the one from the classical *BHK* semantics. Namely, Gödel introduced the *logic of provability* (coinciding with the modal logic $\mathcal{S}4$) and constructed an embedding of $\mathcal{I}nt$ into $\mathcal{S}4$. In [15] no formal provability semantics for $\mathcal{S}4$ was suggested. Moreover, Gödel noticed that the straightforward interpretation of $\Box F$ as the arithmetical formula $Provable(F)$

"there exists a number x which is the code of a proof of F".

was incompatible with $\mathcal{S}4$ (cf.[9],[10]).

> Let us consider, for example, the first order arithmetic $\mathcal{PA}$. If $\perp$ is the boolean constant *false*, then the $\mathcal{S}4$-axiom $\Box\perp\rightarrow\perp$ becomes a statement *Consis* $\mathcal{PA}$, expressing the consistency of $\mathcal{PA}$. By necessitation, $\mathcal{S}4$ derives $\Box(\Box\perp\rightarrow\perp)$. The latter formula expresses the assertion that *Consis* $\mathcal{PA}$ is provable in $\mathcal{PA}$, which contradicts the second Gödel incompleteness theorem.

The issue of a provability model for $\mathcal{S}4$ was studied by Gödel [16], Lemmon [28], Myhill [35],[36], Kripke [25], Montague [34], Mints [33], Kuznetsov & Muravitskii [27], Goldblatt [17], Boolos [9],[10] Shapiro [38],[39], Buss [11], Artemov [1], and many others. However, the problem of a formal provability semantics for $\mathcal{S}4$ has remained open.

A principal difficulty here is caused by the existential quantifier over proofs in $Provable(F)$. Indeed, the interpretation of the formula $\Box(\Box F\rightarrow F)$ is

'it is provable that "$Provable(F)$ implies F" '

Provability in $\mathcal{PA}$ can be characterized as "true in all models of $\mathcal{PA}$", including the nonstandard ones. In a given model of $\mathcal{PA}$ an element that instantiates the variable x from the existential quantifier for the code of a proof of F in $Provable(F)$ may be nonstandard. In such a case $Provable(F)$ is true in this model, but there is no "real" $\mathcal{PA}$-derivation behind such an x. So, $\mathcal{PA}$ is not able to conclude that F is true from $Provable(F)$ is true since the latter formula does not necessarily deliver a proof of F.

This consideration suggests replacing the provability formula $Provable(F)$ by the formula for proofs *Proof(t,F)* and the existential quantifier on proofs in the former by Skolem style operations on proofs in the latter. Such a conversion would help to avoid evaluation of proofs by nonstandard numbers.

The problem of finding the logic which accommodates the atoms *t is a proof of* F (the logic of proofs) has met considerable technical difficulties. The usual Skolem methods of converting quantifiers into functions do not apply here, since there are no universal laws of commutation of the provability operator with the quantifiers. In order to find the logic of proofs one has to address the issue of an appropriate set of proof terms t first. In particular, we have to figure out what operations on proofs are needed to express all logical laws of provability. Some of these operations come from the proof of Gödel's second incompleteness theorem. Within that proof it was established that

$$\mathcal{PA} \vdash Provable(F \rightarrow G) \wedge Provable(F) \ \rightarrow \ Provable(G).$$

This formula is a "forgetful" version of the following theorem.

For some computable function $m(x, y)$

$$\mathcal{PA} \vdash Proof(s, F \rightarrow G) \wedge Proof(t, F) \ \rightarrow \ Proof(m(s, t), G).$$

A similar decoding can be done for another lemma from Gödel's second incompleteness theorem $\mathcal{PA} \vdash Provable(F) \rightarrow Provable(Provable(F))$.

For some computable function $c(x)$

$$\mathcal{PA} \vdash Proof(t, F) \rightarrow Proof(c(t), Proof(t, F)).$$

In his Lecture at Zilsel's, 1938, (published in 1995 in [16], see also [37]) Gödel sketched a constructive version of $\mathcal{S}4$ with the basic propositions "t is a proof of F" and operations similar to $m(x, y)$ and $c(x)$. This Gödel's suggestion in principle suffices to justify the reflexivity principle along with the necessitation rule. However, the questions about a complete set of terms and axioms for the logic of proofs, as well as the question about its ability to realize the entire $\mathcal{S}4$ have remained unanswered. It turned out that Gödel's sketch of 1938 lacks the operation "+", without which a realization of $\mathcal{S}4$ cannot be completed.

The complete axiomatization of the logic of proofs $\mathcal{LP}$ was found by the author independently of Gödel's paper [16], which was published as late as 1995. The first presentations of $\mathcal{LP}$ took place at the author's talks at the conferences in Münster and Amsterdam in 1994. Preliminary versions of $\mathcal{LP}$ appeared in Technical Reports [4], [5], [7], cf. also the survey [18]. In these papers the axiom systems for $\mathcal{LP}$ in Hilbert, Gentzen and natural deduction format were found, soundness and completeness with respect to the standard provability semantics were established. It was also discovered that given $\mathcal{S}4$-derivation of a modal formula F one can reveal its explicit provability meaning by assigning proof terms to the modalities in such a way that the resulting formula F^r in the $\mathcal{LP}$ format is derivable in $\mathcal{LP}$. This yields a positive solution to the problem of finding the intended provability semantics for the modal logic $\mathcal{S}4$. Since $\mathcal{I}nt$ is embedded into $\mathcal{S}4$, for example, by the Gödel translation (cf. [15], [44], [12]), the above realization of $\mathcal{S}4$ in $\mathcal{LP}$ simultaneously provides an adequate realization of $\mathcal{I}nt$ in

$\mathcal{LP}$. Therefore, $\mathcal{LP}$ may be regarded as the natural formalization of the classical Brouwer-Heyting-Kolmogorov semantics for the intuitionistic logic. Intuitionistic logic $\mathcal{I}nt$ turned out to be complete with respect to this semantics (this was implicitly conjectured by Kolmogorov in 1932).

In $\mathcal{LP}$ the notion *term t is a proof of F* and *term t has type F* are subsumed by the basic $\mathcal{LP}$ proposition $t{:}F$. Under these interpretations $\mathcal{LP}$ naturally encompasses combinatory logic and λ-calculi corresponding to intuitionistic and modal logics. In addition, $\mathcal{LP}$ is strictly more expressive because it admits arbitrary combinations of ":" and propositional connectives. By treating ":" uniformly, $\mathcal{LP}$ unifies the semantics of modality, combinatory, and λ-terms. All these objects are realized as proof terms in $\mathcal{LP}$.

Gabbay's Labelled Deductive Systems ([14]) may serve as a natural framework for $\mathcal{LP}$. Intuitionistic Type Theory by Martin-Löf [29], [30] also makes use of the format $t{:}F$ with its informal provability reading. $\mathcal{LP}$ may also be regarded as a basic epistemic logic with explicit justifications; a problem of finding such systems was raised by van Benthem in [8].

In this paper we establish some sort of the functional completeness property of the system of $\mathcal{LP}$ proof terms (called *proof polynomials*). We show that every operation on proofs that (i) can be specified in a propositional modal language and (ii) is invariant with respect to the choice of a proof system is realized by a proof polynomial[1]. This theorem justifies the choice of the set of proof terms for $\mathcal{LP}$ and thus $\mathcal{LP}$ itself. Along with the completeness theorem for $\mathcal{LP}$ and the theorem about the realization of $\mathcal{S}4$ in $\mathcal{LP}$ ([4], [7]) this demonstrates that $\mathcal{LP}$ is indeed the logic of proofs in the format with "t is a proof of F" and $\mathcal{S}4$ is indeed the modal logic of explicit provability. In other words, given the intended provability semantics of $t:F$ and $\Box F$ there are no operations on proofs other than proof polynomials, no logical principles of proofs other than derivable in $\mathcal{LP}$ and no principles of provability other than derivable in $\mathcal{S}4$.

1 Logic of Proofs

1.1 Definition. The language of Logic of Proofs ($\mathcal{LP}$) contains

the usual language of classical propositional logic
proof variables $x_0, \ldots, x_n, \ldots$, proof constants $a_0, \ldots, a_n, \ldots$
function symbols: monadic !, binary $\cdot$ and $+$
operator symbol of the type "*term : formula*".

We will use $a, b, c, \ldots$ for proof constants, $u, v, w, x, y, z, \ldots$ for proof variables, i, j, k, l, m, n for natural numbers. Terms are defined by the grammar

$$p ::= x_i \mid a_i \mid\ !p \mid p_1 \cdot p_2 \mid p_1 + p_2$$

[1] The first version of this theorem appeared in the technical report [4].

We call these terms *proof polynomials* and denote them by $p, r, s, t \ldots$. By analogy we refer to constants as coefficients. Constants correspond to proofs of a finite fixed set of propositional schemas. We will also omit $\cdot$ whenever it is safe. We also assume that $(a \cdot b \cdot c)$, $(a \cdot b \cdot c \cdot d)$, *etc.* should be read as $((a \cdot b) \cdot c)$, $(((a \cdot b) \cdot c) \cdot d)$, *etc.*

Using t to stand for any term and S for any propositional letter, the formulas are defined by the grammar

$$\sigma ::= S \mid \sigma_1 \to \sigma_2 \mid \sigma_1 \wedge \sigma_2 \mid \sigma_1 \vee \sigma_2 \mid \neg \sigma \mid t{:}\sigma$$

We will use $A, B, C, F, G, H, X, Y, Z$ for the formulas in this language, and $\Gamma, \Delta, \ldots$ for the finite sets (also finite multisets, or finite lists) of formulas unless otherwise explicitly stated. We will also use $\vec{x}, \vec{y}, \vec{z}, \ldots$ and $\vec{p}, \vec{r}, \vec{s}, \ldots$ for vectors of proof variables and proof polynomials respectively. If $\vec{s} = (s_1, \ldots, s_n)$ and $\Gamma = (F_1, \ldots, F_n)$, then $\vec{s}{:}\Gamma$ denotes $(s_1 : F_1, \ldots, s_n : F_n)$, $\bigvee \Gamma = F_1 \vee \ldots \vee F_n$, $\bigwedge \Gamma = F_1 \wedge \ldots \wedge F_n$. We assume the following precedences from highest to lowest: $!, \cdot, +, :, \neg, \wedge, \vee, \to$. We will use the symbol $=$ in different situations, both formal and informal. Symbol $\equiv$ denotes syntactical identity, $\ulcorner E \urcorner$ is the Gödel number of E.

The intended semantics for $p : F$ is "p is a proof of F", which will be formalized in the next section. Note that proof systems which provide a formal semantics for $p : F$ are *multi-conclusion* ones, i.e. p may be a proof of several different F's (see Comment 1.7).

1.2 Definition. The system $\mathcal{LP}_0$. Axioms:

A0. Finite set of axiom schemes of classical propositional logic in the language of $\mathcal{LP}$	
A1. $t{:}F \to F$	*"verification"*
A2. $t{:}(F \to G) \to (s{:}F \to (t{\cdot}s){:}G)$	*"application"*
A3. $t{:}F \to\ !t{:}(t{:}F)$	*"proof checker"*
A4. $s{:}F \to (s{+}t){:}F, \quad t{:}F \to (s{+}t){:}F$	*"choice"*

Rule of inference:

R1. $$\frac{F \to G \qquad F}{G}$$ *"modus ponens".*

The system $\mathcal{LP}$ is $\mathcal{LP}_0$ plus the rule

R2. $$\frac{}{c{:}\mathbf{A}}\,,$$
if $\mathbf{A}$ *is an axiom A0 – A4, and c a proof constant* *"axiom necessitation".*

A *Constant Specification* ($\mathcal{CS}$) is a finite set of formulas $c_1 : A_1, \ldots, c_n : A_n$ such that c_i is a constant, and F_i an axiom *A0 – A4*. Each derivation in $\mathcal{LP}$ naturally generates the $\mathcal{CS}$ consisting of all formulas introduced in this derivation by the *necessitation* rule.

1.3 Comment. Proof constants in $\mathcal{LP}$ stand for proofs of "simple facts", namely propositional axioms and axioms *A1 – A4*. In a way the proof constants resemble atomic constant terms (*combinators*) of typed combinatory logic (cf. [44]). A constant c_1 specified as $c_1 : (A \to (B \to A))$ can be identified with the combinator $\mathbf{k}^{A,B}$ of the type $A \to (B \to A)$. A constant c_2 such that $c_2 : [(A \to (B \to C)) \to ((A \to B) \to (A \to C))]$ corresponds to the combinator $\mathbf{s}^{A,B,C}$ of the type $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$. The proof variables may be regarded as term variables of combinatory logic, the operation "$\cdot$" as the application of terms. In general an $\mathcal{LP}$-formula $t : F$ can be read as a combinatory term t of the type F. Typed combinatory logic $\mathbf{CL}_{\to}$ thus corresponds to a fragment of $\mathcal{LP}$ consisting only of formulas of the sort $t : F$ where t contains no operations other than "$\cdot$" and F is a formula built from the propositional letters by "$\to$" only.

There is no restriction on the choice of a constant c in *R2* within a given derivation. In particular, *R2* allows to introduce a formula $c : A(c)$, or to specify a constant several times as a proof of different axioms from *A0 – A4*. One might restrict $\mathcal{LP}$ to injective constant specifications, i.e. only allowing each constant to serve as a proof of a single axiom $\mathbf{A}$ within a given derivation (although allowing constructions $c : \mathbf{A}(c)$, as before). Such a restriction would not change the ability of $\mathcal{LP}$ to emulate classical modal logic, or the functional and arithmetical completeness theorems for $\mathcal{LP}$ (below), though it will provoke an excessive renaming of the constants.

Both $\mathcal{LP}_0$ and $\mathcal{LP}$ enjoy the deduction theorem

$$\Gamma, A \vdash B \quad \Rightarrow \quad \Gamma \vdash A \to B,$$

and the substitution lemma: *If* $\Gamma(x, P) \vdash B(x, P)$ *for a propositional variable* P *and a proof variable* x*, then for any proof polynomial* t *and any formula* F

$$\Gamma(x/t, P/F) \vdash B(x/t, P/F).$$

For a given constant specification $\mathcal{CS}$ under $\mathcal{LP}(\mathcal{CS})$ we mean $\mathcal{LP}_0$ plus $\mathcal{CS}$. Obviously, the following three statements are equivalent

- *"F is derivable in $\mathcal{LP}$ with a constant specification $\mathcal{CS}$"*,
- $\mathcal{LP}(\mathcal{CS}) \vdash F$
- $\mathcal{LP}_0 \vdash \bigwedge \mathcal{CS} \to F$.

1.4 Proposition. (Lifting lemma) *Given a derivation* $\mathcal{D}$ *of the type*

$$\vec{s} : \Gamma, \Delta \vdash_{\mathcal{LP}} F,$$

one can construct a proof polynomial $t(\vec{x},\vec{y})$ *such that*

$$\vec{s}\!:\!\Gamma, \vec{y}\!:\!\Delta \vdash_{\mathcal{LP}} t(\vec{s},\vec{y})\!:\!F.$$

Proof. By induction on the derivation $\vec{s}\!:\!\Gamma, \Delta \vdash F$. If $F = s_i\!:\!G_i \in \vec{s}\!:\!\Gamma$, then put $t :=!s_i$ and use *A3*. If $F = D_j \in \Delta$, then put $t := y_j$. If F is an axiom *A0* – *A4*, then pick a fresh proof constant c and put $t := c$; by *R2*, $F \vdash c\!:\!F$. Let F be introduced by *modus ponens* from $G \rightarrow F$ and G. Then, by the induction hypothesis, there are proof polynomials $u(\vec{s},\vec{y})$ and $v(\vec{s},\vec{y})$ such that $u\!:\!(G \rightarrow F)$ and $v\!:\!G$ are both derivable in $\mathcal{LP}$ from $\vec{s}\!:\!\Gamma, \vec{y}\!:\!\Delta$. By *A2*, $\vec{s}\!:\!\Gamma, \vec{y}\!:\!\Delta \vdash (uv)\!:\!F$, and we put $t := uv$. If F is introduced by *R2*, then $F = c\!:\!A$ for some axiom A. Use the same *R2* followed by *A3*: $c\!:\!A \rightarrow !c\!:\!c\!:\!A$, to get $\vec{s}\!:\!\Gamma, \vec{y}\!:\!\Delta \vdash !c\!:\!F$, and put $t :=!c$.
◀

Note that if $\Delta \vdash_{\mathcal{LP}_0} F$, then one can construct $t(\vec{y})$ which is a product of proof constants and variables from $\vec{y}$ such that $\vec{y}\!:\!\Delta \vdash_{\mathcal{LP}_0} t(\vec{y})\!:\!F$. It is easy to see from the proof that the lifting polynomial $t(\vec{x},\vec{y})$ is nothing but a blueprint of $\mathcal{D}$. Thus $\mathcal{LP}$ accommodates its own proofs as terms. The necessitation rule

$$\vdash F \quad \Rightarrow \ \vdash p\!:\!F \quad \textit{for some proof polynomial } p$$

is a special case of Lifting. Note that here p is a blueprint of a proof of F implicitly mentioned in "$\vdash F$". In particular, p is a ground polynomial, i.e. it does not contain variables.

Logic of Proofs may be regarded as an explicit version of the modal logic $\mathcal{S}4$. Not only the forgetful projection of every theorem of $\mathcal{LP}$ is provable in $\mathcal{S}4$, but every theorem F of $\mathcal{S}4$ admits an instantiation of the modalities by proof polynomials such that the resulting formula F^r is derivable in $\mathcal{LP}$ (cf. [4], [7]). The following examples show how the realization of $\mathcal{S}4$ in $\mathcal{LP}$ works.

1.5 Example. $\mathcal{S}4 \vdash (\Box A \wedge \Box B) \rightarrow \Box(A \wedge B)$

In $\mathcal{LP}$ the corresponding derivation is

1. $c\!:\!(A \rightarrow (B \rightarrow A \wedge B))$, by *R2*,
2. $x\!:\!A \rightarrow (c \cdot x)\!:\!(B \rightarrow A \wedge B)$, from 1, by *A2*,
3. $x\!:\!A \rightarrow (y\!:\!B \rightarrow (c \cdot x \cdot y)\!:\!(A \wedge B))$, from 2, by *A2* and propositional logic,
4. $x\!:\!A \wedge y\!:\!B \rightarrow (c \cdot x \cdot y)\!:\!(A \wedge B))$, from 3, by propositional logic.

1.6 Example. $\mathcal{S}4 \vdash (\Box A \vee \Box B) \rightarrow \Box(A \vee B)$.

In $\mathcal{LP}$ the corresponding derivation is

1. $a:(A \rightarrow A \vee B)$, $\quad b:(B \rightarrow A \vee B)$, by *R2*,
3. $x:A \rightarrow (a\cdot x):(A \vee B)$, $\quad y:B \rightarrow (b\cdot y):(A \vee B)$, from 1, by *A2*,
4. $(a\cdot x):(A \vee B) \rightarrow (a\cdot x+b\cdot y):(A \vee B)$, $\quad (b\cdot y):(A \vee B) \rightarrow (a\cdot x+b\cdot y):(A \vee B)$, by *A4*,
5. $(x:A \vee y:B) \rightarrow (a\cdot x+b\cdot y):(A \vee B)$, from 3, by propositional logic.

1.7 Comment. Operations "$\cdot$" and "!" are present for uni-conclusion as well as multi-conclusion proof systems. In turn, "+" is an operation for multi-conclusion proof systems only. Indeed, by *A4* we have $s:F \wedge t:G \rightarrow \; (s+t):F \wedge (s+t):G$, thus $s+t$ proves different formulas. The differences between uni-conclusion and multi-conclusion proof systems are mostly cosmetic. Usual proof systems (Hilbert or Gentzen style) may be considered as uni-conclusion, e.g. a proof derives only the end formula (sequent) of a proof tree. On the other hand, the same systems may be regarded as multi-conclusion by assuming that a proof derives all formulas assigned to the nodes of the proof tree. The logic of strictly uni-conclusion proof systems was studied in [2], [3] and in [26], where it meets a complete axiomatization (system $\mathcal{FLP}$). $\mathcal{FLP}$ is not compatible with any modal logic (cf. [7]). Therefore, provability as a modal operator corresponds to multi-conclusion proof systems.

No single operator "$t:$" in $\mathcal{LP}$ is a normal modality since none of them satisfies the property $t:(P \rightarrow Q) \rightarrow (t:P \rightarrow t:Q)$. This makes $\mathcal{LP}$ essentially different from numerous polymodal logics, e.g. the dynamic logic of programs ([22]), where the modality is upgraded by some additional features. In turn, in the Logic of Proofs the modality is decomposed into a family of proof polynomials.

2 Standard provability interpretation of $\mathcal{LP}$

The Logic of Proofs is meant to play for a notion of proof a role similar to that played by the boolean propositional logic for the notion of statement. It is shown in [4], [7] that $\mathcal{LP}$ enjoys the soundness/completeness property:

$$\mathcal{LP} \vdash F \qquad \Leftrightarrow \qquad F \textit{ is true under any interpretation }.$$

Any system of proofs with a proof checker operation capable of internalizing its own proofs as terms (cf. [41]) may be in the scope of $\mathcal{LP}$. In particular, any proof system for the first order Peano Arithmetic $\mathcal{PA}$ (cf. [9], [10], [32], [42]) provides a model for $\mathcal{LP}$ with Gödel numbers of proofs being a instrument of internalizing proofs as terms. The soundness ($\Rightarrow$) does not necessarily refer to the arithmetical models. However, $\mathcal{PA}$ is convenient for establishing the completeness ($\Leftarrow$) of $\mathcal{LP}$: given $\mathcal{LP} \not\vdash F$ one can always find a proof system for $\mathcal{PA}$ along with an evaluation of variables in F which makes F false.

Within this paper under Δ_1 and Σ_1 we mean the corresponding classes of arithmetical predicates. We will use φ, ψ to denote arithmetical formulas, f, g, h to denote arithmetical terms, i, j, k, l, n to denote natural numbers unless stated otherwise. We will use the letters u, v, w, x, y, z to denote individual variables in arithmetic and hope that a reader is able to distinguish them from the proof variables. If n is a natural number, then $\overline{n}$ will denote a numeral corresponding to n, i.e. a standard arithmetical term $0'''^{\cdots}$ where $'$ is a successor functional symbol and the number of $'$'s equals n. We will use the simplified notation n for a numeral $\overline{n}$ when it is safe.

2.1 Definition. We assume that $\mathcal{PA}$ contains terms for all primitive recursive functions (cf. [42]), called *primitive recursive terms.* Formulas of the form $f(\vec{x}) = 0$ where $f(\vec{x})$ is a primitive recursive term are *standard primitive recursive formulas. A standard Σ_1 formula* is a formula $\exists x \varphi(x, \vec{y})$ where $\varphi(x, \vec{y})$ is a standard primitive recursive formula. An arithmetical formula φ is *provably* Σ_1 if it is provably equivalent in $\mathcal{PA}$ to a standard Σ_1 formula; φ is *provably* Δ_1 iff both φ and $\neg\varphi$ are provably Σ_1.

2.2 Definition. A *proof predicate* is a provably Δ_1-formula $Prf(x, y)$ such that for every arithmetical sentence φ

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

A proof predicate *Prf(x,y)* is *normal* if the following conditions are fulfilled:

1) (*finiteness of proofs*) For every proof k the set $T(k) = \{l \mid Prf(k, l)\}$ is finite. The function from k to the canonical number of $T(k)$ is computable.

2) (*conjoinability of proofs*) For any natural numbers k and l there is a natural number n such that

$$T(k) \cup T(l) \subseteq T(n).$$

2.3 Comment. Every multi-conclusion normal proof predicate can be transformed into a uni-conclusion one by changing from

$$\text{“}p \text{ proves } F_1, \ldots, F_n\text{”} \qquad \text{to} \qquad \text{“}(p, i) \text{ proves } F_i,\ i = 1, \ldots n\text{”}.$$

In turn, every uni-conclusion proof predicate may be regarded as normal multi-conclusion by reading

$$\text{“}p \text{ proves } F_1 \wedge \ldots \wedge F_n\text{”} \qquad \text{as} \qquad \text{“}p \text{ proves each of } F_i,\ i = 1, \ldots n\text{”}.$$

2.4 Proposition. *For every normal proof predicate* Prf *there are computable functions* $m(x,y)$, $a(x,y)$, $c(x)$ *such that for all arithmetical formulas* φ,ψ *and all natural numbers* k,n *the following formulas are valid:*

$$Prf(k,\ulcorner\varphi\to\psi\urcorner)\wedge Prf(n,\ulcorner\varphi\urcorner)\to Prf(m(k,n),\ulcorner\psi\urcorner)$$

$$Prf(k,\ulcorner\varphi\urcorner)\to Prf(a(k,n),\ulcorner\varphi\urcorner),\qquad Prf(n,\ulcorner\varphi\urcorner)\to Prf(a(k,n),\ulcorner\varphi\urcorner)$$

$$Prf(k,\ulcorner\varphi\urcorner)\to Prf(c(k),\ulcorner Prf(k,\ulcorner\varphi\urcorner)\urcorner).$$

Proof. The following function can be taken as m:

> *Given* k,n *put* $m(k,n)=\mu z$"$Prf(z,\ulcorner\psi\urcorner)$ *for all* ψ *such that there are* $\ulcorner\varphi\to\psi\urcorner\in T(k)$ *and* $\ulcorner\varphi\urcorner\in T(n)$" .

Likewise, for a one could take

> *Given* k,n *put* $a(k,n)=\mu z$ "$T(k)\cup T(n)\subseteq T(z)$".

Finally, c may be put

> *Given* k *put* $c(k)=\mu z$"$Prf(z,\ulcorner Prf(k,\ulcorner\varphi\urcorner)\urcorner)$ *for all* $\ulcorner\varphi\urcorner\in T(k)$". *Such* z *always exists. Indeed,* $Prf(k,\ulcorner\varphi\urcorner)$ *are true* Δ_1 *formulas for every* $\ulcorner\varphi\urcorner\in T(k)$, *therefore they all are provable in* $\mathcal{PA}$. *Use conjoinability to find a uniform proof of all of them.*

◄

Note, that the natural arithmetical proof predicate *PROOF(x,y)*

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

is an example of a normal proof predicate.

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

- a normal proof predicate Prf with the functions $m(x,y)$, $a(x,y)$, $c(x)$ as in Proposition 2.4,
- an evaluation of propositional letters by sentences of arithmetic, and
- an evaluation of proof variables and proof constants by natural numbers.

Let $*$ commute with boolean connectives,

$$(t\cdot s)^* = m(t^*, s^*), \quad (t+s)^* = a(t^*, s^*), \quad (!t)^* = c(t^*),$$

$$(t\!:\!F)^* = Prf(t^*, \ulcorner F^* \urcorner).$$

Under an interpretation $*$ a proof polynomial t becomes a natural number t^*, an $\mathcal{LP}$-formula F becomes an arithmetical sentence F^*. A formula $(t\!:\!F)^*$ is always provably Δ_1. Note, that $\mathcal{PA}$ (as well as any theory containing certain finite set of arithmetical axioms, e.g. Robinson's arithmetic) is able to derive any true Δ_1 formula, and thus to derive a negation of any false Δ_1 formula (cf. [32]). For a set X of $\mathcal{LP}$-formulas under X^* we mean the set of all F^*'s such that $F \in X$. Given a constant specification $\mathcal{CS}$, an arithmetical interpretation $*$ is a $\mathcal{CS}$*-interpretation* if all formulas from $\mathcal{CS}^*$ are true (equivalently, are provable in $\mathcal{PA}$). An $\mathcal{LP}$-formula F is *valid* (with respect to the arithmetical semantics) if the arithmetical formula F^* is true under all interpretations $*$. F is $\mathcal{CS}$*-valid* if F^* is true under all $\mathcal{CS}$-interpretations $*$.

In Section 3 we will need the definition of $*$ to be extended to the language with $\Box$. Then we assume that $(\Box F)^* = \exists y Prf(y, \ulcorner F^* \urcorner)$.

2.6 Proposition. (Arithmetical soundness of $\mathcal{LP}_0$)

1. *If* $\mathcal{LP}_0 \vdash F$ *then* F *is valid.*
2. *If* $\mathcal{LP}_0 \vdash F$ *then* $\mathcal{PA} \vdash F^*$ *for any interpretation* $*$.

Proof. A straightforward induction on the derivation in $\mathcal{LP}_0$. Let us check 2. for the axiom $t : F \rightarrow F$. Under an interpretation $*$ $(t\!:\!F \rightarrow F)^* \equiv Prf(t^*, \ulcorner F^* \urcorner) \rightarrow F^*$. Consider two possibilities. Either $Prf(t^*, \ulcorner F^* \urcorner)$ is true, in which case t^* is indeed a proof of F^*, thus $\mathcal{PA} \vdash F^*$ and $\mathcal{PA} \vdash (t\!:\!F \rightarrow F)^*$. Otherwise $Prf(t^*, \ulcorner F^* \urcorner)$ is false, in which case being a false Δ_1 formula it is refutable in $\mathcal{PA}$, i.e. $\mathcal{PA} \vdash \neg Prf(t^*, \ulcorner F^* \urcorner)$ and again $\mathcal{PA} \vdash (t\!:\!F \rightarrow F)^*$.
◀

2.7 Corollary. (Arithmetical soundness of $\mathcal{LP}$)

1. *If* $\mathcal{LP}(\mathcal{CS}) \vdash F$ *then* F *is* $\mathcal{CS}$*-valid.*
2. *If* $\mathcal{LP}(\mathcal{CS}) \vdash F$ *then* $\mathcal{PA} \vdash F^*$ *for any* $\mathcal{CS}$*-interpretation* $*$.

3 Functional completeness of proof polynomials

In this section we show some sort of functional completeness for the system of proof polynomials in $\mathcal{LP}$. This provides one more justification of the choice of the basic set of operations $\cdot, !, +$ on proofs and eventually of $\mathcal{LP}$ itself, since no closed subsystem of the set of proof polynomials enjoies this functional completness property.

Operations on proofs invariant with respect to the choice of a proof system naturally arise from the notion of admissible rule in a formal system, e.g. arithmetic.

3.1 Definition. Let $\mathcal{L}$ be a logical language (propositional, first order, modal, etc.) with a class of its arithmetical interpretations such that for any interpretation $*$ and any formula F from $\mathcal{L}$ an arithmetical formula F^* is defined. An *admissible rule in $\mathcal{PA}$ over $\mathcal{L}$* is a figure

$$\frac{\vdash C_1, \ldots, \vdash C_n}{\vdash G} \qquad (1)$$

where $C_1, \ldots, C_n, G$ are $\mathcal{L}$-formulas such that for every interpretation $*$, G^* is provable in $\mathcal{PA}$ whenever ${C_1}^*, \ldots, {C_n}^*$ are. An *admissible multi-rule in $\mathcal{PA}$* is a figure

$$\frac{\vdash C_1^1, \ldots, \vdash C_1^{k_1} \quad or \quad \ldots \quad or \quad \vdash C_n^1, \ldots, \vdash C_n^{k_n}}{\vdash G}, \qquad (2)$$

such that for every interpretation $*$ G^* is derivable in $\mathcal{PA}$ whenever for some i, $0 \leq i \leq n$, all $(C_i^1)^*, \ldots, (C_i^{k_i})^*$ are derivable in $\mathcal{PA}$.

Using the modality $\Box$ to denote the provability in $\mathcal{PA}$ one can present and admissible rule (1) as the modal formula

$$\Box C_1 \wedge \Box C_2 \wedge \ldots \wedge \Box C_n \rightarrow \Box G$$

and an admissible multi-rule (2) as the modal formula

$$\bigvee_i \bigwedge_j \Box C_i^j \rightarrow \Box G$$

both true in arithmetic under every interpretation. As one can see, the admissible multi-rules rather then the admissible rules correspond the expressive power of the modal provability language.

In order to maintain a better control over the proof variables we will use the language of the explicit modal logic $\mathcal{LP}$ to describe the proof arguments of the admissible multi-rules. Indeed, every admissible multi-rule may be regarded as an implicit specification of a proof y of G as a function of proofs x_i^j's of C_i^j's.

3.2 Definition. Let C_i^j's and G be formulas in the language of $\mathcal{LP}$, An *abstract operation on proofs* is a formula

$$\bigvee_i \bigwedge_j x_i^j : C_i^j \rightarrow \Box G, \qquad (3)$$

that is valid under all arithmetical interpretations.

Since $(\Box G)^* = \exists y Prf(y, \ulcorner G^* \urcorner)$, formula (3) is a straight formalization of (2) where the existential quantifier over proofs in $(\Box G)^*$ is an implicit specification of a proof y of G^* as a function of x_i^j's.

3.3 Example. Some examples of abstract operations on proofs:

i) $x:(F \rightarrow G) \wedge y:F \rightarrow \Box G$,
ii) $x:F \rightarrow \Box x:F$,
iii) $x:F \wedge y:G \rightarrow \Box(F \wedge G)$,
iv) $x:F \vee y:G \rightarrow \Box(F \vee G)$.

For each of these examples there is a proof polynomial p realizing the operator $\Box$ in such a way that instantiating p inside $\Box$ gives a formula derivable in $\mathcal{LP}$:

i) $\mathcal{LP} \vdash x:(F \rightarrow G) \wedge y:F \rightarrow (x \cdot y):G$,
ii) $\mathcal{LP} \vdash x:F \rightarrow !x:x:F$,
iii) $\mathcal{LP} \vdash x:F \wedge y:G \rightarrow t(x,y):(F \wedge G)$, (Example 1.5)
iv) $\mathcal{LP} \vdash x:F \vee y:G \rightarrow (ax+by):(F \vee G)$. (Example 1.6)

The following theorem demonstrates that proof existence in any abstract operation on proofs can be instantiated with a specific proof polynomial.

3.4 Theorem. *For any abstract operation on proofs*

$$\bigvee_i \bigwedge_j x_i^j : C_i^j \rightarrow \Box G$$

one can construct a proof polynomial $p(\vec{x})$ *such that*

$$\mathcal{LP} \vdash \bigvee_i \bigwedge_j x_i^j : C_i^j \rightarrow p(\vec{x}):G.$$

Proof. Let (2) be an abstract operation on proofs, and let us denote

$$\bigvee_i \bigwedge_j x_i^j : C_i^j$$

by C. Since $\Box G \to G$ is valid, the formula $C \to G$ is also valid. By the completeness theorem for $\mathcal{LP}$ ([4],[7],[18]), $\mathcal{LP} \vdash C \to G$. By Lifting Lemma 1.4 one can construct a ground proof polynomial t such that $\mathcal{LP} \vdash t{:}(C \to G)$. By *A2*, given a fresh variable y

$$\mathcal{LP} \vdash y{:}C \to (t \cdot y){:}G. \qquad (4)$$

3.5 Lemma. *For any formulas A, B one can construct a proof polynomial $u(x,y)$ such that*

$$\mathcal{LP} \vdash x{:}A \wedge y{:}B \to u(x,y){:}(x{:}A \wedge y{:}B).$$

Proof. Indeed, $\mathcal{LP} \vdash x:A \to !x:x:A$ and $\mathcal{LP} \vdash y:B \to !y:y:B$, by *A3*. By 1.5, one can construct a proof polynomial t such that

$$\mathcal{LP} \vdash !x{:}x{:}A \wedge !y{:}y{:}B \to t(!x,!y){:}(x{:}A \wedge y{:}B),$$

thus

$$\mathcal{LP} \vdash x{:}A \wedge y{:}B \to t(!x,!y){:}(x{:}A \wedge y{:}B).$$

◀

3.6 Lemma. *For all formulas A, B there exists a proof polynomial $v(x,y)$ such that*

$$\mathcal{LP} \vdash x{:}A \vee y{:}B \to v(x,y){:}(x{:}A \vee y{:}B).$$

Proof. Again, $\mathcal{LP} \vdash x{:}A \to !x{:}x{:}A$ and $\mathcal{LP} \vdash y{:}B \to !y{:}y{:}B$, therefore

$$\mathcal{LP} \vdash x{:}A \vee y{:}B \to !x{:}x{:}A \vee !y{:}y{:}B.$$

Consider the Constant Specification consisting of two formulas $a:(x:A \to x:A \vee y:B)$ and $b{:}(y{:}B \to x{:}A \vee y{:}B)$. By *A2*

$$\mathcal{LP} \vdash !x{:}x{:}A \to (a!x){:}(x{:}A \vee y{:}B),$$

$$\mathcal{LP} \vdash !y{:}y{:}B \to (b!y){:}(x{:}A \vee y{:}B).$$

By *A4*,

$$\mathcal{LP} \vdash (a!x){:}(x{:}A \vee y{:}B) \vee (b!y){:}(x{:}A \vee y{:}B) \to (a!x + b!y){:}(x{:}A \vee y{:}B),$$

therefore

$$\mathcal{LP} \vdash !x{:}x{:}A \vee !y{:}y{:}B \to (a!x + b!y){:}(x{:}A \vee y{:}B)$$

and

$$\mathcal{LP} \vdash x\!:\!A \vee y\!:\!B \to (a!x + b!y)\!:\!(x\!:\!A \vee y\!:\!B).$$

◀

3.7 Lemma. *One can construct a proof polynomial $s(\vec{x})$ such that*

$$\mathcal{LP} \vdash C \to s(\vec{x})\!:\!C.$$

Proof. A straightforward induction on the number of the outer conjunctions and disjunctions in the formula

$$C = \bigvee_i \bigwedge_j x_i^j\!:\!C_i^j.$$

The base case $C = x\!:\!B$. Let $s(x)$ be $!x$. By *A3*, $\mathcal{LP} \vdash x\!:\!B \to !x\!:\!x\!:\!B$, thus $\mathcal{LP} \vdash C \to s(x)\!:\!C$.

There are two cases in the induction step. If C is $x : A \wedge y : B$, then use 3.5. If C is $x\!:\!A \vee y\!:\!B$, then use 3.6.

◀

From (4), by substituting $s(\vec{x})$ for y, we get

$$\mathcal{LP} \vdash s(\vec{x})\!:\!C \to (t \cdot s(\vec{x}))\!:\!G,$$

and thus, from 3.7, we get the desired $\mathcal{LP} \vdash C \to (t \cdot s(\vec{x}))\!:\!G$. This concludes the proof of 3.4.

◀

3.8 Comment. Whereas the realization of admissible multi-rules (2) requires all three proof connectives $\cdot, !, +$, the realization of the plain admissible rules of the form (1) does not require "+".

3.9 Comment. Modulo to renaming of the operations $\cdot, !, +$ no proper subset $\mathcal{F}$ of the set of all proof polynomials closed under substitution is able to realize all abstract operations on proofs in the style of Theorem 3.4. Indeed, examples 3.3(i) and 3.3(ii) specify some operations similar to "application" and "proof checker" respectively. By 3.3(iv), there is a proof polynomial $t(x,y)$ in $\mathcal{F}$ such that $\mathcal{LP} \vdash x : F \vee y : F \to t(x,y) : (F \vee F)$. On the other hand, for some proof polynomial p from $\mathcal{F}$ $\mathcal{LP} \vdash p\!:\!(F \vee F \to F)$. By 3.3(i), there should be a proof polynomial $q(x,y)$ from $\mathcal{F}$, which is the result of the "application" of p to $t(x,y)$ such that $\mathcal{LP} \vdash t(x,y)\!:\!(F \vee F) \to q(x,y)\!:\!F$. Therefore $\mathcal{LP} \vdash x\!:\!F \vee y\!:\!F \to q(x,y)\!:\!F$, and thus $q(x,y)$ is an operation in $\mathcal{F}$ similar to "+".

4 Acknowledgements

I am indebted to Albert Visser who asked the question about the justification of the choice of the basic set of operations on proofs during one of the first presentations of $\mathcal{LP}$ in Amsterdam in 1994. The functional completness of proof polynomials (Theorem 3.4) may be regarded as some sort of an answer to that natural question.

The research described in this paper was supported in part by ARO under the MURI program "Integrated Approach to Intelligent Systems", grant DAAH04-96-1-0341, by DARPA under program LPE, project 34145, and by the Russian Foundation for Basic Research, grant 96-01-01395.

References

[1] S. Artemov. "Kolmogorov logic of problems and a provability interpretation of intuitionistic logic", *Theoretical Aspects of Reasoning about Knowledge - III Proceedings*, Morgan Kaufman Pbl., pp. 257-272, 1990

[2] S. Artemov and T. Strassen, "Functionality in the Basic Logic of Proofs", *Tech.Rep. IAM 92-004, Department for Computer Science*, University of Bern, Switzerland, 1993.

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

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

[5] S. Artemov, "Proof realizations of typed λ-calculi," *Tech. Rep. MSI 97-2*, Cornell University, May 1997.

[6] S. Artemov, "Unified Semantics for Modality and λ-terms via Proof Polynomials," to appear in *Logic, Language and Computation'97, CSLI Publications*, Stanford University, 1998 (?).

[7] S. Artemov, "Explicit provability: the intended semantics for intuitionistic and modal logic" *Tech. Rep. CFIS 98-10*, Cornell University, September 1998.

[8] J. van Benthem. "Reflections on epistemic logic", *Logique & Analyse*, 133-134, pp. 5-14, 1991

[9] G. Boolos, *The Unprovability of Consistency: An Essay in Modal Logic*, Cambridge University Press, 1979

[10] G. Boolos, *The Logic of Provability*, Cambridge University Press, 1993

[11] S. Buss, "The Modal Logic of Pure Provability", *Notre Dame Journal of Formal Logic*, v. 31, No. 2, 1990

[12] A. Chagrov and M. Zakharyaschev, *Modal Logic*, Oxford Science Publications, 1997.

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

[14] D.M. Gabbay, *Labelled Deductive Systems*, Oxford University Press, 1994.

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

[16] K. Gödel, "Vortrag bei Zilsel" (1938), in S. Feferman, ed. *Kurt Gödel Collected Works. Volume III*, Oxford University Press, 1995

[17] R. Goldblatt, "Arithmetical necessity, provability and intuitionistic logic", *Theoria*, 44, pp. 38-46, 1978.

[18] G. Japaridze and D. de Jongh, "The Logic of Provability", in *S.R. Buss, ed., Handbook of Proof Theory*, Elsevier Science BV, pp. 475-546, 1998

[19] S. Kleene. "On the interpretation of intuitionistic number theory", *Journal of Symbolic Logic*, v. 10, pp. 109-124, 1945

[20] S. Kleene. "Classical extensions of intuitionistic mathematics", In *Y. Bar-Hillel, ed. Logic, Methodology and Philosophy of Science 2*, North Holland, pp. 31-44, 1965

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

[22] D. Kozen and J. Tiuryn, "Logic of Programs", in *Handbook of Theoretical Computer Science. Volume B, Formal Models and Semantics*, The MIT Press/Elsevier, pp. 789-840, 1990

[23] G. Kreisel, "Foundations of intuitionistic logic", in E.Nagel, P.Suppes and A.Tarski, eds., *Logic, Methodology and Philosophy of Science. Proceedings of the 1960 International Congress*, Stanford University Press, Stanford, pp. 198-210, 1962.

[24] G. Kreisel, "On weak completeness of intuitionistic predicate logic", *Journal of Symbolic Logic*, v. 27, pp. 139-158, 1962.

[25] S. Kripke, "Semantical considerations on modal logic", *Acta Philosophica Fennica*, 16, pp. 83-94, 1963.

[26] V.N. Krupski, “Operational Logic of Proofs with Functionality Condition on Proof Predicate”, Lecture Notes in Computer Science, v. 1234, *Logical Foundations of Computer Science' 97, Yaroslavl'*, pp. 167-177, 1997

[27] A.V. Kuznetsov and A.Yu. Muravitsky, “The logic of provability”, Abstracts of the *4-th All-Union Conference on Mathematical Logic*, p. 73, (Russian), 1976.

[28] E. Lemmon, “New Foundations for Lewis's modal systems”, *Journal of Symbolic Logic*, 22, pp. 176-186, 1957.

[29] P. Martin-Löf. “Constructive mathematics and computer programming”, in *Logic, Methodology and Philosophy of Science VI*, North-Holland, pp. 153-175, 1982.

[30] P. Martin-Löf. *Intuitionistic Type Theory*, Studies in Proof Theory, Bibliopolis, Naples, 1984.

[31] Yu. Medvedev, “Finite problems”, *Soviet Mathematics Doklady*, v. 3. pp. 227-230, 1962.

[32] E. Mendelson, *Introduction to mathematical logic. Third edition.*, Wadsworth, 1987.

[33] G. Mints. “Lewis' systems and system T (1965-1973)”. In *Selected papers in proof theory*, Bibliopolis, Napoli, 1992.

[34] R. Montague. “Syntactical treatments of modality with corollaries on reflection principles and finite axiomatizability”, *Acta Philosophica Fennica*, 16, pp. 153-168, 1963.

[35] J. Myhill, “Some Remarks on the Notion of Proof”, *Journal of Philosophy*, 57, pp. 461-471, 1960

[36] J. Myhill, “Intensional Set Theory”, In: S. Shapiro, ed., *Intensional Mathematics*, North-Holland, pp. 47-61, 1985.

[37] C. Parsons and W. Sieg. “Introductory note to *1938*a*”. In: S. Feferman, ed. *Kurt Gödel Collected Works. Volume III*, Oxford University Press, pp. 62-85, 1995.

[38] S. Shapiro. “Intensional Mathematics and Constructive Mathematics”. In: S. Shapiro, ed., *Intensional Mathematics*, North-Holland, pp. 1-10, 1985.

[39] S. Shapiro. "Epistemic and Intuitionistic Arithmetic”. In: S. Shapiro, ed., "Intensional mathematics”, North-Holland, pp. 11-46, 1985.

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

[41] R. Smullyan, *Diagonalization and Self-Reference*, Oxford University Press, 1994

[42] G. Takeuti, *Proof Theory*, North-Holland, 1975

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

[44] A.S. Troelstra and H. Schwichtenberg, *Basic Proof Theory*, Cambridge University Press, 1996.

[45] A.S. Troelstra "Realizability". In *S. Buss, ed., Handbook of Proof Theory*, Elsevier, pp. 407-474, 1998.

[46] V.A. Uspensky, "Kolmogorov and mathematical logic", *Journal of Symbolic Logic*, 57, No.2, 1992.

[47] V.A. Uspensky and V.E. Plisko "Intuitionistic Logic", In S.M. Nikol'ski, ed. *A.N. Kolmogorov, Collected works. Mathematics and Mechanics*, pp. 394-404, 1985 (in Russian).

[48] S. Weinstein, "The intended interpretation of intuitionistic logic", *Journal of Philosophical Logic*, 12, pp. 261-270 1983.