KOLMOGOROV'S LOGIC OF PROBLEMS AND A PROVABILITY INTERPRETATION OF INTUITIONISTIC LOGIC

S.Artemov
Steklov Mathematical Institute,
Vavilov str.,42, Moscow GSP-1,
117966, USSR.

ABSTRACT

In 1932 A.N.Kolmogorov suggested an interpretation of intuitionistic logic **Int** as a "logic of problems". Then K.Gödel in 1933 offered a "provability" understanding of problems, thus, providing an abstract "provability" interpretation for **Int** via a modal logic **S4**. Later papers by J.C.C.McKinsey & A.Tarski, A.Grzegorczyk, R.Solovay, A.V.Kuznetsov & A.Yu.Muravitskii, R.Goldblatt, G.Boolos imply that this provability interpretation of **Int** is complete if one decodes Gödel modality $\Box$ for an "abstract provability" in the following way: $\Box Q = Q \wedge Pr[Q]$, where $Pr[Q]$ is the standard provability predicate for Peano arithmetic. The paper shows that the definition of $\Box Q$ as $Q \wedge Pr[Q]$ is (in a certain sense) the only possible one. The Uniform Completeness Theorem for provability logics is extended to **Int** and other logics having Gödelian provability interpretation. The first order logics having provability interpretation are considered.

1 INTRODUCTION

A.N.Kolmogorov in [Kol] suggested an informal interpretation of sentences of intuitionistic logic **Int** as statements about the possibility of solving certain general problems; propositional variables were supposed to denote "problems", logical connectives were given a natural interpretation as operators over "problems": a formula $A \wedge B$ denotes a problem "to solve both A and B", a formula $A \vee B$ denotes "to solve either A or B", an implication $A \rightarrow B$ is interpreted as a problem "to reduce a solution of B to any solution of A", $\neg A$ is $A \rightarrow \perp$ that means a problem "to demonstrate an unsolvability of A". Kolmogorov hadn't given a precise definition of "problems", just appealing to the common sense of a working mathematician but had conjectured that his interpretation of **Int** was complete.

In [Göd] K.Gödel offered an interpretation of **Int** close to that in [Kol], where intuitionistic propositions were treated as assertions about provability. More precisely, in [Göd] there was defined a translation tr(F) of an intuitionistic formula, F obtained by prefixing a new operator $\Box$ that stands for an abstract "provability" to each subformula of F.

We call the logical language with the modality $\Box$ the $\Box$-language and a modal formula in $\Box$-language a $\Box$-formula. In [Göd] some properties of $\Box$ were accepted as axioms and rules of a modal logic S4. A possible axiom system for S4 includes

all the tautologies (in a propositional $\Box$-language),
$\Box P \wedge \Box(P \to Q) \to \Box Q$, $\Box P \to P$,
$\Box P \to \Box\Box P$

for all sentences P,Q. The rules of inference of S4 are *modus ponens* $P, P \to Q \vdash Q$ and *necessitation* $P \vdash \Box P$.

We look at logics as sets of formulae and therefore for each logic L and each formula F, $L \vdash F \iff F \in L$.

Theorem 1.(K.Gödel [Göd], J.C.C.McKinsey & A.Tarski [McK&Tar])
For each propositional formula F

$$F \in \mathbf{Int} \iff tr(F) \in S4. \qquad (*)$$

Later in [Grz] A.Grzegorczyk introduced a new modal logic **Grz** (a proper extension of S4):

$$\mathbf{Grz} = S4 + \Box(\Box(A \to \Box A) \to A) \to A$$

and showed that for **Grz** the property (*) was also valid.

Theorem 2. (A.Grzegorczyk [Grz]) *For each propositional $\Box$-formula* F

$$F \in \mathbf{Int} \iff tr(F) \in \mathbf{Grz}.$$

2 THE ARITHMETICAL PROVABILITY PREDICATE AS A MODALITY

In [Göd] K.Gödel considered also another interpretation of a modality as an arithmetical provability predicate Pr(x); we denote this modal operator by Δ, Δ-language is the logical language with Δ; a Δ-formula is a formula in Δ-language. A complete axiomatization of Δ was given in [Sol] where R.Solovay introduced a decidable propositional Δ-logic S, that describes all valid laws of provability Δ, and its sublogic GL, that stands for all laws of provability Δ, which can be demonstrated by means of Peano Arithmetic PA.

The logic GL can be axiomatized by the axioms:
tautologies (in a Δ-language), $\Delta P \wedge \Delta(P \to Q) \to \Delta Q$,
$\Delta(\Delta P \to P) \to \Delta P$,

for all sentences P,Q and rules *modus ponens, necessitation.*

Logic S can be defined as $GL + \Delta P \to P$ but without a necessitation rule.

A *realization* is a function that assigns to each sentence letter a sentence of the language of PA. The *translation* fA of a propositional Δ-formula A under a realization f is defined inductively: $f\bot=\bot$, $fp=f(p)$ (for each sentence letter p), $f(A\to B)=fA\to fB$, $f\Delta A=Pr[fA]$. We have taken the propositional constant $\bot$ (falsity) to be among the primitive logical symbols of PA; we understand Pr[F] as the result of substituting the numeral for the Gödel number of F for the free variable x in Pr(x), and therefore the translation of any modal formula under any realization is a sentence of the language of PA.

The following theorem shows that the logic S is exactly the collection of all valid principles of modal logic of provability Δ and that the logic GL is the set of those principles of this logic which are provable in PA.

Theorem 3. (R.Solovay [Sol]) *For each Δ-formula* Q

$Q\in S \iff$ fQ *is true in the standard model of* PA *for each realization* f,

$Q\in GL \iff$ *for each realization* f $PA\vdash fQ$.

The theorem implies also that

$$GL\vdash Q \iff S\vdash \Delta Q.$$

Several papers independently give a uniform version of the second part of the Solovay Completeness Theorem.

Theorem 4. (F.Montagna [Mon79], S.Artemov [Art79], A.Visser [Vis81], G.Boolos [Boo82]) *There exists a realization* f *such that for each Δ-formula* Q

$$Q\notin GL \iff PA\nvdash fQ.$$

The first part of the Solovay Theorem does not admit uniformization: for each realization f for a propositional variable p either fp or $\neg fp$ is true in the standard model of arithmetic, but neither p, nor $\neg p$ belongs to the logic S.

In [Art79],[Art80],[Vis84],[Art86a] a general notion of a logic of formal provability was developed. Let $\alpha(t)$ be a *r.e.* formula that binumerates some axiom system of an extension of PA (i.e. a theory in the language of PA containing PA). Following [Fef], we can call such a formula $\alpha(t)$ a *numeration*. We denote by $|\alpha|$ the set of axioms that is numerically expressed by the formula α

$$|\alpha|=\{F \mid F \text{ is an arithmetic sentence and } \alpha(\ulcorner F\urcorner) \text{ is true}\}$$

and by $\|\alpha\|$ the extension of PA determined by the set of axioms $|\alpha|$. Let $Pr_\alpha(x)$ signify a standard arithmetical formula of provability based on α as a formula for Gödel numbers of axioms ([Fef]). For each numeration α and each realization f we set $f_\alpha(p)=fp$ for each propositional letter p. Let f_α commutes with the Boolean connectives and

$$f_\alpha(\Delta Q)=Pr_\alpha[f_\alpha Q].$$

Let U be a theory and α a numeration. We define

$$L_\alpha(U)=\{Q \mid Q \text{ is a } \Delta\text{-formula and } U\vdash f_\alpha Q \text{ for each realization } \alpha\}.$$

The modal logics $L_\alpha(U)$ describe the laws of the provability Pr_α that can be justified by means of the theory U.

We say that a logic l is *logic of formal provability* if $l=L_\alpha(U)$ for some numeration α and extension of arithmetic U.

Obviously, **GL** is the least logic of formal provability. the Solovay Theorem provides another example of such a logic: $S=L_\alpha(TA)$ where $\|\alpha\|=PA$ and TA is the set of all true arithmetic sentences.

There exists continually many logics of provability [Art79], [Art80]. A Classification Theorem for logics of provability was accomplished by L.Beklemishev in [Bek].

3 A DEFINITION FOR THE MODALITY OF INTUITIVE PROVABILITY

In [Kuz&Mur77], [Gol], [Kuz&Mur86], [Boo80], [Art86b], [Boo79] and other papers there was considered a translation of $\Box A$ as $A\wedge\Delta A$, that provides an arithmetical provability interpretation of $\Box$-language, therefore, **Int**-language. It turns out that logics **Int** and **Grz** are complete under this interpretation. More precisely, let B^Δ denote the decoding of $\Box P$ as $P\wedge\Delta P$ in all subformulas $\Box P$ of a formula B.

Theorem 5. i.(A.Grzegorczyk [Grz]) *For an* **Int**-*formula* B

$$\mathbf{Int}\vdash B \iff \mathbf{Grz}\vdash tr(B).$$

ii.(A.V.Kuznetsov & A.Yu.Muravitskii [Kuz&Mur77],86]; R.Goldblatt [Gol]) *For a* $\Box$-*formula* B

$$\mathbf{Grz}\vdash B \iff \mathbf{GL}\vdash B^\Delta,$$

iii.(G.Boolos [Boo80]) *For a* $\Box$-*formula* B

$$\mathbf{Grz}\vdash B \iff \mathbf{S}\vdash B^\Delta.$$

Are there any reasons for adopting the definition $\Box P := P \wedge \Delta P$? The modality $\Box$ doesn't have an explicit mathematical model; it had been introduced as a modality for an intuitive notion of mathematical provability. On the contrary the modality Δ has an exact mathematical definition as an operator of formal provability $Pr(.)$ on the set of arithmetical sentences. Thus there is no way to prove that $\Box P = P \wedge \Delta P$; one can only hope to find some arguments in order to declare a

Thesis: $\Box P := P \wedge \Delta P$ (**)

(like the Church Thesis for computable functions). Gödel himself in [Göd] tried the obvious idea to define $\Box Q$ as ΔQ but noticed that this definition led to a contradiction between his axioms and rules for $\Box$ and the already known Gödel Second Incompleteness Theorem. Can one nevertheless give a reasonable definition of $\Box$ via Δ? The most optimistic expectations are

to find a Δ-formula $B(p)$ which satisfies known properties of $\Box p$ (first of all axioms and rules of $S4$) and such that for each other Δ-formula $C(p)$ with these properties

$$GL \vdash B(p) \leftrightarrow C(p).$$

In this case we have the right to declare a definition $\Box Q := B(p)$ as a Thesis. It turns out that this situation holds with $p \wedge \Delta p$ as $B(p)$. The main ideas of the proof of the following theorem were taken from [Kuz&Mur86].

Theorem 6. *For a given Δ-formula $C(p)$ if*

1. all axioms and rules of $S4$ for $C(p)$ as $\Box p$ are arithmetically valid (derivable in S) and

2. $GL \vdash C(p) \rightarrow \Delta p$ (this principle says that any "real" mathematical proof can be finitely transformed into a formal proof)

then

$$GL \vdash C(p) \leftrightarrow (p \wedge \Delta p).$$

Proof. Let $\top$ denotes the propositional constant "truth" so $\top \in Int, S4, Grz, GL, S$. Obviously, $S4 \vdash \Box \top$ and by the conditions of Theorem 6

1) $S \vdash C(\top)$,

2) $S \vdash C(C(p) \rightarrow p)$ (because $S4 \vdash \Box(\Box p \rightarrow p)$),

3) for each Δ-formula F that contains modality symbols only in combinations of a type $C(.)$

$$S \vdash F \quad \Rightarrow \quad S \vdash C(F),$$

(because of the necessitation rule for $S4$: $S4 \vdash Q \Rightarrow S4 \vdash \Box Q$),

4) $GL \vdash C(p) \to \Delta p$ (condition *2.* of the theorem).
We will show that

$$GL \vdash C(p) \leftrightarrow (p \wedge \Delta p)$$

and thus this formula is deducible in all logics of formal provability. According to 2)

$$S \vdash C(C(p) \to p),$$

thus ($GL \subseteq S$, condition *2.* of the theorem)

$$GL \vdash \Delta(C(p) \to p)$$

and

$$GL \vdash C(p) \to p.$$

Together with 4) this gives

$$GL \vdash C(p) \to p \wedge \Delta p.$$

Lemma. *For each Δ-formula* $D(p)$

$$GL \vdash (p \wedge \Delta p) \to (D(p) \leftrightarrow D(\top)).$$

The proof is an induction on the complexity of D. The basis step and induction steps for Boolean connectives are trivial. Let $D(p)$ be $\Delta E(p)$. By the induction hypothesis

$$GL \vdash (p \wedge \Delta p) \to (E(p) \leftrightarrow E(\top)).$$

The necessitation rule for GL and the commutativity of Δ with $\to$ and $\wedge$ give

$$GL \vdash (\Delta p \wedge \Delta\Delta p) \to (\Delta E(p) \leftrightarrow \Delta E(\top)).$$

Together with $GL \vdash \Delta p \to \Delta\Delta p$ this implies

$$GL \vdash (p \wedge \Delta p) \to (D(p) \leftrightarrow D(\top)).$$

By 2) $S \vdash C(\top)$ and according to 3),4), $S \vdash C(C(\top))$, $S \vdash \Delta C(p)$ and $GL \vdash C(p)$. Because of the lemma we have

$$GL \vdash (p \wedge \Delta p) \to C(p), \quad \text{whence} \quad GL \vdash C(p) \leftrightarrow (p \wedge \Delta p).$$

Remark. Without condition *2.* of the theorem we lose the uniqueness of the definition (**): $C(p) := p$ also fits.

Below we assume the *Thesis* (**). Theorems 3 and 5 may now be considered as an affirmation of Kolmogorov's conjecture on the Completeness of **Int** with respect to his *problem's* semantics where one understands *a problem* as *a problem to prove* and a *provability* operator $\Box(.)$ as $(.) \wedge \Delta(.)$.

Since the *Thesis* provides a provability interpretation for the **Int**-language we can extend the notion of provability logics to this language. We use the notation $\mathcal{L}$**Int** for the lattice of all logics containing **Int**, $\mathcal{L}$**Grz** for the lattice of all extensions of **Grz**, and $\mathcal{L}$**GL** for the lattice of extensions of **GL**.

Let us consider a mapping ρ ([Mak&Ryb]) from $\mathcal{L}$**Grz** to $\mathcal{L}$**Int** which is determined by the Gödel translation **tr**: for each logic **m** from $\mathcal{L}$**Grz** we put

$$\rho(\mathbf{m})=\{F \mid F \text{ is an } \mathbf{Int}\text{-formula and } \mathbf{m}\vdash \mathbf{tr}(F)\}.$$

We can also consider a mapping μ ([Kuz&Mur86]) from $\mathcal{L}$**GL** to $\mathcal{L}$**Grz**: for each logic $\mathbf{m}\in\mathcal{L}\mathbf{GL}$, we set

$$\mu(\mathbf{m})=\{F \mid F \text{ is a } \Box\text{-formula and } \mathbf{m}\vdash F^{\Delta}\}.$$

We say that a logic **l** in an **Int**-language has *a provability interpretation* iff there exists a numeration α and an extension of the arithmetic **U** such that

$$\mathbf{l}=\rho\circ\mu\circ \mathbf{L}_{\alpha}(\mathbf{U}).$$

In this situation the logic **l** describes those laws of the provability $\mathbf{Pr}_{\alpha}$ that can be expressed on the **Int**-language and justified by means of the theory **U**.

By Theorems 3 and 5 the logic **Int** has a provability interpretation and **Int** is the least such logic in this language. There are continually many logics extending **Int** in the language of **Int**. Which of them have a provability interpretation?

The following theorem provides a Classification of all logics in **Int**-language that have a provability interpretation. We denote by $\mathbf{LP}_n, n\le\omega$, a logic $\mathbf{Int}+\mathbf{Q}_n$, where

$$\mathbf{Q}_0=\bot,\ \mathbf{Q}_{n+1}=\mathbf{p}_{n+1}\vee(\mathbf{p}_{n+1}\to\mathbf{Q}_n),$$

and $\mathbf{LP}_{\omega}=\mathbf{Int}$. Obviously

$$\mathbf{LP}_0\supset\mathbf{LP}_1\supset\ldots\supset\mathbf{LP}_{\omega}=\mathbf{Int}$$

In fact $\mathbf{LP}_n$, $n\in\omega$, are the smallest logics in *finite slices* $\mathbf{s}_n$ by Hosoi-Ono and each of these logics is decidable. We note that $\mathbf{LP}_0$ is inconsistent, $\mathbf{LP}_1$ is the classical logic and the logics $\mathbf{LP}_n$, $n\ge 1$, have properties close to those of the classical one.

Theorem 7. ([Art86b]) *Among logics in the language of* **Int** *only*

$$\mathbf{LP}_0,\mathbf{LP}_1,\ldots\mathbf{LP}_{\omega}=\mathbf{Int}$$

have a provability interpretation.

This theorem shows that classical propositional logic **Cl** also has a provability interpretation.

Corollary. *The logic*

$$\mathbf{I}=\rho\circ\mu\circ\mathbf{L}_{\alpha}(\mathbf{U}).$$

is classical iff

$$\mathbf{U}\supseteq\mathbf{PA}+\{\mathbf{F}\rightarrow\mathbf{Pr}_{\alpha}[\mathbf{F}]\,|\,\mathbf{F}\text{ is an arithmetical sentence}\}$$

Thus, the classical logic **Cl** corresponds to those theories in which *the completeness principle* "all statements that are true are provable" for **PA** is derivable. This consideration shows a reasonable correspondence of formal results with intuition in classical propositional logic.

4 UNIFORMIZATION THEOREM

The following theorem extends the Uniform Arithmetical Completeness for **GL** (Theorem 4) to simultaneous uniformization for **GL,S,Grz,Int** and all $\mathbf{LP}_n, n\in\omega$. For simplicity we assume below that $\|\alpha\|=\mathbf{PA}$ and thus $\mathbf{Pr}(x)$ signifies a standard provability formula for **PA**. In [Art79], [Art80] it was pointed out that the logic **S** is arithmetically complete with respect to an extension of **PA** by the Local Reflection Principle:

$$\mathbf{PA'}=\mathbf{PA}+\{\mathbf{Pr}[\phi]\rightarrow\phi\,|\,\phi\in\mathbf{St}_{\mathbf{PA}}\}.$$

Moreover if $\mathbf{S}\nvdash\mathbf{Q}_0$ then one can choose a realization **f** for which $\mathbf{PA'}\nvdash\mathbf{fQ}$ and $\mathbf{fQ}\in\Sigma^0_2$.

A provability interpretation of logics $\mathbf{LP}_n, n\in\omega$, assigns to each of these logics a theory $\mathbf{PA}+\mathbf{Pr}^n[\bot]$, i.e.

$$\mathbf{LP}_n=\rho\circ\mu\circ\mathbf{L}_{\alpha}(\mathbf{PA}+\mathbf{Pr}^n[\bot]).$$

Here $\mathbf{Pr}^0[\phi]=\phi$, $\mathbf{Pr}^{n+1}[\phi]=\mathbf{Pr}[\mathbf{Pr}^n[\mathbf{F}]]$.

Theorem 8. *There exists a realization* **f** *such that for each* Δ*-formula* **B**

$$\mathbf{GL}\vdash\mathbf{B}\iff\mathbf{PA}\vdash\mathbf{fB}\quad\text{and}\quad\mathbf{S}\vdash\mathbf{B}\iff\mathbf{PA'}\vdash\mathbf{fB},$$

for each $\Box$*-formula* **B**

$$\mathbf{Grz}\vdash\mathbf{B}\iff\mathbf{PA}\vdash\mathbf{f}(\mathbf{B}^{\Delta}),$$

for each **Int**-*formula* **B**

$$\mathbf{Int}\vdash\mathbf{B}\iff\mathbf{PA}\vdash\mathbf{f}([\mathbf{tr}(\mathbf{B})]^{\Delta}),$$

$$\mathbf{LP}_n\vdash\mathbf{B}\iff\mathbf{PA}+\mathbf{Pr}^n[\bot]\vdash\mathbf{f}([\mathbf{tr}(\mathbf{B})]^{\Delta}).$$

Proof. We prove a unformization theorem for the logic **S** first and then show that this uniform realization also fits for all other logics mentioned in the Theorem.

Lemma. *There exists a realization* f *such that for each* Δ*-formula* B

$$S\vdash B \iff PA'\vdash fB.$$

Proof is based on an improved version of Montagna's method from [Mon79]. For a Δ-formula $R(p_0,\dots,p_n)$ and any arithmetic formulae $B_0,\dots,B_n$ let $R(B_0,\dots,B_n)$ denote fR with a realization f such that $fp_i=B_i$, $i=0,\dots,n$.

Let $H[x,y,z,]$ mean that the following 3 conditions hold:

1. x is the Gödel number of an arithmetical formula $B(t)$ with one free variable, say;
2. y is the Gödel number of a Δ-formula $Q(p_0,\dots,p_n)$, which is not a theorem of S;
3. z is the Gödel number of a proof of $Q(B(0),\dots,B(n))$ in PA' and non of natural $v<z$ is the Gödel number of a proof in PA' of any $R(B(0),\dots,B(k))$ with some $R\not\supseteq S$.

Obviously $H[x,y,z]$ is recursive. Let $H(x,y,z)$ is its representation in PA. Usual properties of such representations give that if $H[x,y,z,]$ then

$$PA\vdash\forall x,y(H(k,x,y,)\leftrightarrow x=m\wedge y=n).$$

Consider a recursive procedure which for any Δ-formula R not deducible in S constructs a realization g such that $T_1\nvdash gR$.

For such R and g let p_i^R denote an arithmetical formula gp_i.

Let us also define a recursive function $F(x,y)$ as follows:

if x is a number of some formula $R(p_0,\dots,p_n)$ not deducible in S and $y\le n$, then $F(x,y)=\ulcorner p_y^R\urcorner$; in all other cases $F(x,y)=0$.

Let also the formula $G(x,y,z)$ represent a function $F(x,y)$ in PA. Then $F(m,n)=k$ implies

$$PA\vdash\forall z(G(m,n,z)\to z=k).$$

Let $U(x,y)$ denote the arithmetical formula

$$\forall z,v(H(x,v,z)\to\forall w(G(v,y,w)\to Tr_s(w))),$$

where $Tr_2(x)$ is a standard formula defining truth for all Σ_2^0-sentences of arithmetic, i.e.

$$PA\vdash E\leftrightarrow Tr_2(\ulcorner E\urcorner)$$

for each $E\in\Sigma^0_2$. By the fixed-point lemma for PA one can get an arithmetic formula $B(y)$ such that

$$PA\vdash B(y)\leftrightarrow\forall v,z(H(\ulcorner B\urcorner,v,z)\to\forall w(G(v,y,w)\to Tr_2(w))).$$

We can show now that $B(0),B(1),\ldots$ is a desired Uniform realization for S and PA'.

Suppose now that for some Δ-formula $Q(p,\ldots,p)$, $S\nvdash Q$ and $PA'\vdash Q(B(0),\ldots,B(n))$. Let k be the least number which is a number of some derivation in PA' of an arithmetical formula $R(B(0),\ldots,B(m))$ such that $I\nvdash R$. Then $H[\ulcorner B\urcorner,\ulcorner R\urcorner,k]$ holds, therefore

$$PA\vdash\forall v,z(H(\ulcorner B\urcorner,v,z)\leftrightarrow v=\ulcorner R\urcorner\wedge z=k).$$

Thus for each i, $0\le i\le m$,

$$PA\vdash B(i)\leftrightarrow\forall v,z(v=\ulcorner R\urcorner\wedge z=k\to\forall w(G(v,i,w)\to Tr_2(w))).$$

Therefore

$$PA\vdash B(i)\leftrightarrow\forall w(G(\ulcorner R\urcorner,i,w)\to Tr_2(w)).$$

As $F(\ulcorner R\urcorner,i)=\ulcorner p^R_i\urcorner$ we get

$$PA\vdash\forall w(G(\ulcorner R\urcorner,i,w)\leftrightarrow w=\ulcorner p^R_i\urcorner).$$

Thus

$$PA\vdash B(i)\leftrightarrow Tr_2(\ulcorner p^R_i\urcorner)$$

and

$$PA\vdash B(i)\leftrightarrow p^R_i.$$

So

$$PA\vdash R(B(0),\ldots,B(m))\leftrightarrow R(p^R_0,\ldots,p^R_m)$$

and

$$S\vdash R(p^R_0,\ldots,p^R_m).$$

This contradicts the definition of p^R_i.

The Lemma is thus proved.

Let f be a uniform realization for S and PA'. We can show that f is a uniform realization for GL and PA. As we have already noticed $S\vdash\Delta Q$ implies $GL\vdash Q$. Thus $PA\vdash fQ$ implies $PA\vdash Pr[fQ]$ and so $PA'\vdash Pr[fQ]$ i.e. $PA'\vdash f(\Delta Q)$. The realization f is uniform for S and PA' and so $S\vdash\Delta Q$; Therefore $GL\vdash Q$.

The realization f is obviously uniform for Grz and PA: as we already noticed above $Grz=\mu(GL)$. Thus

$$Grz\vdash B \iff GL\vdash B^\Delta \iff PA\vdash f(B^\Delta).$$

Let us show now that f is also a uniform realization for logics $GL+\Delta^n\bot$ (without *necessitation*) and theories $PA+Pr^n[\bot]$. Here

$$\Delta^0F\equiv F,\quad \Delta^{n+1}F\equiv\Delta\Delta^nF.$$

So $PA+Pr^n[\bot]\vdash fQ$ gives $PA\vdash Pr^n[\bot]\rightarrow fQ$ and $PA\vdash f(\Delta^n\bot\rightarrow Q)$. The realization f is uniform for GL and PA. Thus $GL\vdash\Delta^n\bot\rightarrow Q$ and $GL+\Delta^n\bot\vdash Q$.

According to [Art86b] and [Art88]

$$LP_n\equiv\rho\circ\mu(GL+\Delta^n\bot)$$

and thus f is a uniform realization for LP_n and $PA+Pr^n[\bot]$:

$$LP_n\vdash B \iff GL+\Delta^n\bot\vdash[tr(B)]^\Delta \iff PA+Pr^n[\bot]\vdash f([tr(B)]^\Delta).$$

Theorem 8 is thus proved.

5 PROVABILITY INTERPRETATION OF THE PREDICATE LANGUAGE

The Gödel translation tr can be easily extended to the first order language: for each predicate formula F let tr(F) be a result of prefixing an operator □ to each subformula of *F*.

The notion of an arithmetical *realization* of Δ-language has also a natural extension to the predicate language ([Mon84],[Art85], [Var]). We assume that the predicate Δ-language does not contain equality and function symbols. By *a realization* we mean now a mapping f that associates with every predicate formula an arithmetic formula with the same free variables and that commutes with the operation of substitution for free variables and with the Boolean connectives and the quantifiers- In addition, let

$$f\Delta R(x_1,\dots,x_n)=Pr[fR(x_1,\dots,x_n)].$$

Here, for any formula F of PA, Pr[F] is the formula of PA with the same free variables as F that expresses the PA-provability of the result of substituting for each variable free in F the numeral for the value of that variable. For the details of the construction of Pr[F], the reader may consult [Boo79], p.42.

Thus each predicate Δ-formula can be thought of as a "provability law", where the predicate letters are treated universally and the modality signifies the provability in PA.

Let U be an extension of PA. We set

$$QL(U)=\{P\,|\,P \text{ is a predicate } \Delta\text{-formula and } U\vdash fP \text{ for each realization } f\}.$$

The modal logic QL(U) describes the principles of the provability Pr that can be demonstrated by means of the theory U.

Unlike the propositional case the logic $QL(TA)$ that describes all true laws of provability in PA is not arithmetical ([Art85]) and the logic $QL(PA)$ that describes all PA-provable laws of provability is not enumerable ([Var]). These results can be easily extended to the $\Box$-language: $\mu \circ QL(TA)$ is not arithmetical ([Art88]) and $\mu \circ QL(PA)$ is not enumerable (recent observation by P.Naumov).

It seems very interesting to study what kind of provability semantics for the first order logic is provided via Gödel translation tr, decoding $\Box F = F \wedge \Delta F$ (see *Thesis* (**)) and a provability interpretation of the predicate Δ-language. Let us put

$$i(U)=\rho \circ \mu \circ QL(U).$$

Lemma. $i(PA)=i(TA)$.

Proof. For each first order formula P, $tr(P)$ begins with a modality $\Box$ and so it is equal to $\Box Q$ for some $\Box$-formula Q. An arithmetic formula $f([\Box Q]^{\Delta})$ thus looks like $R \wedge Pr[R]$ for some R. If $R \wedge Pr[R]$ is true then $PA \vdash R$. Thus $PA \vdash Pr[R]$ and $PA \vdash R \wedge Pr[R]$.

According to the provability interpretation, each first order formula can be considered as a predicate principle of "provability problems" where the Gödel provability operator $\Box(.)$ is interpreted as "$(.)$ is true and provable in arithmetic". The lemma shows that there exists a set of first order formulae which for every correct extension of the arithmetic U (i.e. $U \subseteq TA$) coincides with the set of provability principles demonstrated by means of U.

Thus we may define a Quantified Logic of the Provability Problems

$$I := i(PA) \ (=i(TA)=i(U) \text{ for any } U \text{ such that } PA \subseteq U \subseteq TA).$$

The following theorem shows that the provability interpretation provides a correct semantics for HPC.

Logicians often say that it is still unclear what system is to be accepted as the right one for *Intuitionistic Predicate Logic.* The provability interpretation may be considered as an attempt to give an independent definition for an intuitionistic first order logic. As we have seen above, this approach gives the traditional intuitionistic system Int in the propositional case.

Theorem 9. $HPC \subseteq I$.

Proof is obtained by a routine testing of axioms and rules of HPC to have translations correct in arithmetic.

Recently N.Pankrat'ev proved that $\mathbf{HPC} \neq \mathbf{I}$. His result actually states that $\mathbf{HPC}+\mathbf{P} \subseteq \mathbf{I}$ and $\mathbf{HPC} \nvdash \mathbf{P}$, where

$$P = \forall u \exists v ((Q(u) \to Q(v)) \to Q(u)) \to \forall u Q(u)$$

and Q is a monadic predicate letter. D.Skvortsov and P.Naumov noticed that the Gabbay's formula

$$G = \neg\neg\forall u (Q(u) \vee \neg Q(u))$$

also fits, i.e. $\mathbf{HPC}+\mathbf{G} \subseteq \mathbf{I}$ and $\mathbf{HPC} \nvdash \mathbf{G}$. Pankrat'ev has shown that $\mathbf{HPC}+\mathbf{P} \vdash \mathbf{G}$ and $\mathbf{HPC}+\mathbf{G} \nvdash \mathbf{P}$. These examples provide a kind of "lower bound" for the logic **I**.

Theorem 9 and the Kripke completeness of **HPC** with respect to reflexive and transitive frames imply that each first order formula which is valid in all such Kripke models belongs to **I**. The following theorem shows however that the difference between **I** and **HPC** can not be discerned by the finite Kripke models.

Theorem 10. *If a first order formula* **F** *fails in some finite Kripke model (reflexive, transitive) than* $\mathbf{F} \notin \mathbf{I}$.

Proof. A Kripke model for **HPC** (**HPC**-model) is a system $\mathcal{K}=(K,\preccurlyeq,\{V_i\}_{i\in K},\Vdash)$ such that

1. K is a nonempty set (called "the set of worlds");
2. $\preccurlyeq$ is a transitive and reflexive relation on K; we can even assume that $\preccurlyeq$ is a partial ordering on K;
3. $\{V_i\}_{i\in K}$ are nonempty sets (called "the domains") indexed by elements of K such that if $i \preccurlyeq j$ then $V_i \subseteq V_j$.
4. $\Vdash$ is a (forcing) relation between worlds $i \in K$ and closed formulas with parameters in V_i: for each formula F

$$i \Vdash F \text{ and } i \preccurlyeq j \;\Rightarrow\; j \Vdash F$$

and $\Vdash$ deals with connectives and quantifiers in a usual intuitionistic way

$i \Vdash P \wedge Q \iff i \Vdash P$ and $i \Vdash Q$,
$i \Vdash P \vee Q \iff i \Vdash P$ or $i \Vdash Q$,
$i \Vdash P \to Q \iff$ for every j if $i \preccurlyeq j$ then $j \Vdash Q$ or $j \nVdash P$,
$i \nVdash \bot$,
$i \Vdash \forall x P(x) \iff$ for each j if $i \preccurlyeq j$ then for each $a \in V_j$ $j \Vdash P(a)$,
$i \Vdash \exists x P(x) \iff$ for some $a \in V_i$ $i \Vdash P(a)$.

A Kripke model for Δ-language (Δ-model) is a system $\mathcal{K}=(K,\prec,\{V_i\}_{i\in K},\Vdash)$ such that $\prec$ is a transitive and irreflexive relation on K and a forcing relation $\Vdash$ satisfies conditions

$i \nVdash \bot$,

$i\Vdash P \to Q$ iff $i\nVdash P$ or $i \Vdash Q$,
$i\Vdash \forall x P(x)$ iff $i\Vdash P(k)$ for all $k\in V_i$,
$i\Vdash \Delta P$ iff for every j if $i\prec j$ then $j\Vdash P$.

We say that a closed predicate formula Q is valid in the model $\mathcal{K}=(K,\prec,\{V_i\}_{i\in K},\Vdash)$ iff $i\Vdash Q$ for every $i\in K$.

There is an obvious way to transform a HPC-model $\mathcal{K}$ into a Δ-model $\mathcal{K}'$ just replacing $\preccurlyeq$ by $\prec$, where $i\prec j$ may be defined as "$i\preccurlyeq j$ but not $j\preccurlyeq i$". The following natural lemma holds:

Lemma. *For every first order sentence* P, HPC-*model* $\mathcal{K}$ *and* $i\in K$

$$i\Vdash P \text{ (in a model } \mathcal{K}) \iff i\Vdash'(trP)^{\Delta} \text{ (in a model } \mathcal{K}').$$

Proof is a routine induction on the complexity of P.

We call a model *finite* iff K and every $V_i, i\in K$, are finite. It is clear that a transformation of a finite HPC-model is a finite Δ-model.

In order to complete the proof of Theorem 10 let us consider a main result of the paper [Art&Dzh] (a detailed proof is to appear in the Journal of Symbolic Logic in the paper "Finite Kripke models and predicate logics of provability"):

If a closed predicate Δ*-formula* R *is not valid in some predicate finite* Δ*-model then there exists a realization* f *such that* $PA\nvdash fR$.

Thus if F fails in a finite HPC-model $\mathcal{K}$ then we transform $\mathcal{K}$ into a finite Δ-model $\mathcal{K}'$ where F also fails by the lemma. Therefore there exists a realization f such that $PA\nvdash f[(trF)^{\Delta}]$. This implies $F\notin I$.

This theorem provides a kind of "upper bounds" for I. Let Gr denote a Grzegorczyk's formula

$$\forall x(P(x)\vee q) \to \forall x P(x)\vee q$$

where P is a monadic letter and q is a propositional one. We consider also the Markov Principle MP

$$[\forall x(P(x)\vee\neg P(x))\wedge\neg\neg\exists x P(x)] \to \exists x P(x).$$

It is well known that both of these formulae Gr and MP fail in corresponding finite HPC-models.

Corollary. Gr,MP$\notin$I.

The main problem here: whether I is enumerable?

References.

S.N.Artemov. Extensions of arithmetic and connected with them modal theories. VI LMPS Congress, Gannover, Abstracts, Sec.1-4, pp.15-9 (1979)

S.N.Artemov. Arithmetically Complete Modal Theories. Semiotika i Informatika, VINITI, Moscow, v.14, pp.115-133 (1980) (Russian). English transl.: Amer.Math.Soc.Transl. (2), v.135, pp.39-54 (1987)

S.N.Artemov. Nonarithmeticity of truth predicate logics of provability. Dokl.Akad.Nauk SSSR, vol.284, pp.270-271 (1985); English transl.in Soviet Math.Dokl. vol.33,pp.403-405 (1986)

S.N.Artemov. Numerically correct provability logics. Dokl.Akad. Nauk SSSR v.290, No.6, pp.1289-92 (1986) English transl.:Soviet Math.Dokl.v.34, No.2,pp.384-387 (1987)

S.N.Artemov. Superintuitionistic logics having a provability interpretation. Dokl.Akad.Nauk SSSR v.291,No.6, pp.1289-91 (1986) English transl.:Soviet Math.Dokl.v.34, No.3,pp.596-598 (1987)

S.N.Artemov. On logics having a provability interpretation. in: S.I.Adian, ed., Voprosy Kibernet., Complexity of calculations and algorithms, Nauka, Moscow, pp.5-22 (Russian) (1988)

S.N.Artemov & G.K.Dzhaparidze. On effective predicate logics of provability, Dokl.Akad.Nauk SSSR, vol.297, No.3, pp.521-523 (Russian) (1987)

L.D.Beklemishev. On Classification of Provability Logics. Izvest. AN SSSR, ser.matemat. v.53, No.5 (Russian)(1989)

G.Boolos. The Unprovability of Consistency; An Essay in Modal Logic. Cambridge University Press, Cambridge (1979)

G.Boolos. On systems of modal logics with provability interpretations. Theoria, v.46, No.1, pp.7-18 (1980)

G.Boolos. Extremely undecidable sentences. Journ.Symb.Logic, v.47, No.1, pp.191-196 (1982).

S.Feferman. Arithmetization of metamathematics in a general setting. Fundamenta Mathematicae, v.49, pp.35-92 (1960)

K.Gödel, Eine Interpretation des intuitionistischen Aussagenkalkuls, Ergebnisse Math. Colloq. 4, 39-40 (1933)

R.Goldblatt. Arithmetical necessity, provability and intuitionistic logic. Theoria, v.44, No.1, pp.38-46 (1978)

A.Grzegorczyk. Some relational systems and the associated topological spaces. Fundamenta Mathematicae, v.60,pp.223-31 (1967)

A.Kolmogoroff. Zur Deutung der intuitionistischen Logik. Math. Ztschr.,35,S.58-65 (1932)

A.V.Kuznetsov & A.Yu.Muravitsky. Magari algebras. Fourteenth All-Union Algebra Conf., Abstracts, Part 2: Rings, Algebraic Structures, Novosibirsk Univ., Novosibirsk, pp.105-6. (Russian) (1977)

A.V.Kuznetsov & A.Yu.Muravitsky. On superintuitionistic logics as fragments of proof logic. Studia Logica, v.XLV, No.1,pp.76-99 (1986)

L.L.Maksimova & V.V.Rybakov. On the lattice on normal modal logics.Algebra i Logika,v.13,No.2,pp.188-216 (Russian) (1974)

J.C.C.McKinsey & A.Tarski. Some theorems about the sentential calculi of Lewis and Heyting. Journ.Symb.Logic, v.13, No.1, pp.1-15 (1948)

F.Montagna. On the diagonilizable algebra of Peano arithmetic. Boll.della Unione Math.Ital.,v.66-B, pp.795-812 (1979)

F.Montagna. The predicate modal logic of provability. Notre Dame Journal of Formal Logic, v.25, No.2, pp.179-189 (1984)

R.M.Solovay. Provability interpretations of modal logic. Israel Journal of Math.,v.25, pp.287-304 (1976)

V.A.Vardanyan. Arithmetic complexity of predicate logics of provability and their fragments. Dokl.Akad.Nauk SSSR, v.288, No.1, pp.11-14 (1986); English transl. in Soviet Math. Dokl., vol.33, pp.569-572 (1986)

A.Visser. Aspects of diagonalization and provability. Ph.D. Thesis, Utrecht, (1981)

A.Visser. The provability logics of recursively enumerable theories extending Peano arithmetic at arbitrary theories extending Peano arithmetic. Journal of Philosoph. Logic, v.13, pp.97-113 (1984)