Understanding Constructive Semantics
(Spinoza Lecture)

Sergei N. Artemov
Cornell and Moscow University
http://www.cs.cornell.edu/home/artemov

August 17, 1999

Abstract

Is there an alternative mathematics? In particular, does intuitionism yield an essentially new approach that cannot be specified within classical mathematics? The intended informal meaning of intuitionistic logic **Int** was given in the 1930s by the Brouwer-Heyting-Kolmogorov semantics which understands intuitionistic truth as provability. Moreover, Kolmogorov (and later Gödel) suggested interpreting **Int** via *classical* provability and thus providing a meaningful semantics for **Int** independent of intuitionistic assumptions. Natural attempts to formalize this semantics met serious difficulties related to Gödel's incompleteness phenomenon. In this lecture we will talk about recent advances in this area that have bridged the incompleteness gap and provided an adequate formalization of the propositional Brouwer-Heyting-Kolmogorov semantics based on classical provability.

Plan

1. Brouwer - Heyting - Kolmogorov provability semantics for intuitionistic logic
2. Defining intuitionistic logic in classical provability logic
3. Explicit vs. implicit approaches
4. Proof polynomials and Logic of Proofs
5. Solution of Gödel's problem and the propositional *BHK* problem
6. First order case
7. Discussion

1 Brouwer - Heyting - Kolmogorov provability semantics for intuitionistic logic

According to Brouwer (1907 and 1918), intuitionistic truth means provability. Here is a summary in this issue taken from A. Troelstra and D. van Dalen *Constructivism in Mathematics. An Introduction*, v. 1 (1988). page 4.

> "It does not make sense to think of truth or falsity of a mathematical statement independently of our knowledge concerning the statement. A statement is *true* if we have a proof of it, and *false* if we can show that the assumption that there is a proof for the statement leads to a contradiction."

In 1931-32 Heyting and Kolmogorov made Brouwer's definition of intuitionistic truth explicit, though informal, by introducing what is now known as *Brouwer-Heyting-Kolmogorov (BHK) semantics*. Now *BHK* semantics is widely recognized as the intended semantics for intuitionistic logic **Int**[1]. According to *BHK* a statement is true if it has a proof, and a proof of a logically compound statement is given in terms of the proofs of its components. The description uses the unexplained primitive notions of *construction* and *proof*. It stipulates that

- a proof of a proposition $A \wedge B$ consists of a proof of A and a proof of B,
- a proof of $A \vee B$ is given by presenting either a proof of A or a proof of B[2],
- a proof of $A \rightarrow B$ is a construction which, given a proof of A returns a proof of B,
- absurdity $\perp$ is a proposition which has no proof and a proof of $\neg A$ is a construction which, given a proof of A, would return a proof of $\perp$.

Here are minimal *a priori* requirements to a formal *BHK* semantics for intuitionistic logic.

1. It should be based on real proofs in a certain background formal theory (or a class of theories). In particular,

[1] In this talk by **Int** we understand intuitionistic propositional logic also known as **IPC**. The provability semantics problem for **Int** was central in the papers A. Kolmogoroff, "Zur Deutung der intuitionistischen Logik." - *Mathematische Zeitschrift*, v. 35 (1932), pp. 58-65 and K. Gödel, "Eine Interpretation des intuitionistischen Aussagenkalkuls", *Ergebnisse eines mathematischen Kolloquiums*, v. 4 (1933), p. 39-40.

[2] Nowhere in the original Heyting or Kolmogorov writings could I find the well-known extra condition on the disjunction: a proof of a disjunction should also specify which one of the disjuncts it is a proof of. This condition is clearly redundant for the usual notion of a proof: since the predicate "p is a proof of F" is decidable given a proof p we always know which one of the disjuncts p is a proof of. Kreisel (1965) suggested some further modifications of the *BHK* semantics. In our talk we consider the original *BHK* formulation by Heyting and Kolmogorov.

a) the predicate *Proof(p,F)* meaning "p is a *BHK* proof of F" should be decidable,
b) *BHK* proofs should enumerate theorems of the background theory T, i.e.

$$T \vdash F \ \Leftrightarrow\ \textit{Proof(p,F)} \text{ for some } p$$

2. It should be non-circular. For example, *BHK* proofs should not be derivations in a formal system based on **Int** itself.

Until recently there were no sound semantics for **Int** suggested which met these minimal *BHK* requirements. Dirk van Dalen in the chapter "Intuitionistic Logic" in *Handbook of Philosophical Logic*, v. 3. (1986), p. 243, writes:

> "The intended interpretation of intuitionistic logic as presented by Heyting, Kreisel and others[3] so far has proved to be rather elusive. ... However, ever since Heyting's formalization, various, more or less artificial, semantics have been proposed."

There is an important distinction between Heyting's and Kolmogorov's descriptions of the *BHK* semantics. Despite strong technical similarities their approaches had fundamentally different objectives. Presumably, Heyting explained **Int** in terms of the intuitionistic understanding of constructions and proofs. Kolmogorov in 1932 (and then Gödel in 1933 and 1938) intended to interpret intuitionistic logic on the basis of the usual mathematical notion of proof (problem solution), and thus to provide a *definition* of **Int** within classical mathematics independent of the intuitionistic assumptions. For purposes of formalization of *BHK* semantics it is important to distinguish between Heyting and Kolmogorov - Gödel interpretations. We will use the names *intuitionistic BHK semantics* for the former and *classical BHK semantics* for the latter. In this talk we will be interested in the classical *BHK* semantics.

Intuitionistically acceptable semantics for the intuitionistic logic was studied by Kreisel, Kripke, Dyson, van Dalen, Leivant, Veldman, de Swart, Dummet, Troelstra, H. Friedman, Visser, and others. Those studies met considerable technical difficulties (cf. D. van Dalen's chapter "Intuitionistic Logic" in *Handbook of Philosophical Logic*, v. 3. (1986)). To the best of our knowledge none of the suggested interpretations satisfies the minimal requirements to a formal *BHK* semantics above.

Here is the list of major known classical semantics for intuitionistic logic.

1. Algebraic semantics (Birkhoff, 1935)
2. Topological semantics (Stone, 1937; Tarski, 1938)
3. Realizability semantics (Kleene, 1945)
4. Beth models (1956)
5. Dialectica Interpretation (Gödel, 1958)
6. Curry - Howard isomorphism (1958)

[3] I.e. the *BHK* semantics. – S.A.

7. Medvedev's logic of problems (1962)
8. Kripke models (1965)
9. Kuznetsov - Muravitsky - Goldblatt - Boolos provability interpretation (1976)
10. Categorical semantics (Goldblatt, 1979)

Those interpretations have shown to be extremely fruitful for understanding intuitionistic logic. However, none of them may be considered as a *BHK* type semantics.

Semantics 1 – 5, 7, 8, 10 are not connected to provability. In particular, Kleene realizability provides a computational but not provability semantics of intuitionistic logic[4]. Indeed, the predicate "x realizes F" is not decidable, Kleene realizers do not enumerate theorems of any formal theory. It is also worth of mentioning that Kleene realizability is not an adequate semantics for **Int**, i.e. there are realizable propositional formulas not derivable in **Int**.

Curry - Howard isomorphism transliterates natural derivations in **Int** to the corresponding λ-terms. This is a powerful device connecting proofs and programs which may be regarded as a sort of a computational semantics for **Int**. However, its foundational significance is rather limited. From the *BHK* point of view Curry - Howard isomorphism provides the trivial semantics which defines "F is intuitionistically true" as "F is derivable in **Int**" and therefore is obviously circular.

Kuznetsov - Muravitsky - Goldblatt - Boolos semantics for **Int** translates a propositional formula F into F^- by prefixing all atoms and all implications in F by the modal operator $\Box$ (McKinsey - Tarski translation) and then decodes $\Box A$ as "A and *Provable(A)*" where *Provable* is the predicate of formal provability in the first order arithmetic **PA**. **Int** is known to be sound and complete with respect to this semantics. This semantics, however, is highly nonconstructive since it appeals to the unrestricted notion of classical truth for arithmetical formulas. For example, it stipulates that $A \wedge B$ is intuitionistically true iff A and B are both classically true and provable in **PA**. In addition, it has nothing to do with *BHK* since there are no individual proofs and operations on proofs present whatsoever.

An attempt to formalize *BHK* semantics directly was made by Kreisel in 1962 and 1965 in his theory of constructions. Kreisel's original variant of the theory turned out to be inconsistent, and the problem occurred already at the propositional level. Goodman (1970) fixed that gap but his solution involved a stratification of constructions into levels which ruined the *BHK* character of this semantics. In particular, a proof of $A \rightarrow B$ was no longer a function that could be applied to any proof of A. A comprehensive account of Kreisel - Goodman theory could by found in the paper by S. Weinstein, "The intended interpretation of intuitionistic logic", Journal of Philosophical Logic, v. 12 (1983), pp. 261-270, which concludes that

> "The interpretation of intuitionistic theories in terms of the notions of proof and construction ... has yet, however, failed to receive a definitive formulation."

[4]Kleene himself denied any connection of his realizability with *BHK* interpretation.

In this talk we will demonstrate that the propositional classical *BHK* semantics admits an exact mathematical formalization, which indeed provides an adequate specification of **Int** on the basis of the usual classical notion of proof independent of any intuitionistic assumptions. This solves the problem studied by Kolmogorov (1932) and Gödel (1933).

Along with the obvious foundational[5], historical[6] and mathematical[7] motivations for tackling this problem, I would like to mention two more.

1. Modal logic and λ-terms provide two parallel languages describing provability. Modality permits iterations, λ-terms are explicit and more informative. Why don't we try to do both?

2. There is a number of questions in modal logic, typed theories, knowledge representation, constructive semantics, theory of verification, etc. related to the notion of probability, which have not been addressed by the traditional theory of formal (implicit) provability.

2 Defining intuitionistic logic in classical provability logic

Perhaps, the first paper on formal provability semantics for intuitionistic logic was written in 1928 by Orlov in Russian[8]. Referring to Brouwer's papers on intuitionism he suggested prefixing all subformulas of a given propositional intuitionistic formula by $\Box$ with the informal reading of $\Box F$ as "F is provable", and understanding the logical connectives in the usual classical way. His modal axioms for provability coincide with the Gödel axioms for the modal logic **S4** (1933), though Orlov's system was weaker than **S4** because he chose a certain proper fragment of classical logic on the background.

Gödel in 1933 independently introduced the modal calculus of provability (which turned out to be another axiomatization of one of the Lewis modal systems **S4**) and defined **Int** in this logic. Gödel's provability logic admits all axioms and rules of classical logic and has the modal axioms and rules

$\Box F \rightarrow F$,
$\Box(F \rightarrow G) \rightarrow (\Box F \rightarrow \Box G)$,
$\Box F \rightarrow \Box\Box F$,
$F \vdash \Box F$ (*necessitation* rule).

Gödel considered the translation *t(F)* of an intuitionistic formula F into the classical modal language similar to the Orlov translation: "box each subformula of F". Both apparently

[5] A loophole in the foundations of constructive logic.
[6] One of the oldest well-known problems in logic.
[7] A challenge: new approaches were needed.
[8] I.E. Orlov. "Izchislenie sovmesntosti predlozhenii" *Matematicheskii sbornik* (i.e. "The calculus of compatibility of propositions", *Mathematics of the USSR, Sbornik*), v. 35 (1928), pp.263-286 (in Russian).

considered such a translation to be a fair formalization of the Brouwer thesis

$$\textit{intuitionistic truth} = \textit{provability}.$$

Indeed, a consistent substituting "provable" for "true" in the usual inductive definition the truth of a logical formula F leads to *t(F)*. Gödel established that

$$\mathbf{Int} \vdash F \qquad \Rightarrow \qquad \mathbf{S4} \vdash t(F),$$

thus providing an exact reading of the **Int** formulas as statements about provability in classical mathematics. He conjectured that the converse $\Leftarrow$ also holds. This conjecture was eventually confirmed in 1948 by McKinsey and Tarski. However, the ultimate goal of defining **Int** via the notion of a proof in classical mathematics had not been achieved because **S4** was left without an exact intended semantics of the provability operator $\Box$.

$$\mathbf{Int} \hookrightarrow \mathbf{S4} \hookrightarrow \ldots \quad ? \quad \ldots \hookrightarrow \textit{REAL PROOFS}$$

By *REAL PROOFS* here we understand any rigorously defined system of proofs in sufficiently rich formal mathematical theories. In particular, we expect such a system to be represented by a binary predicate *Proof(p,F)* (a shorthand for "p is a proof of F") satisfying the minimal *BHK* requirements above. Model case: the standard proof predicate $\textit{Proof}(x, y)$ in the first order arithmetic **PA** denoting the decidable relation "x is the code of a proof of the formula having a code y".

Gödel himself was the first who addressed the issue of provability semantics for **S4** and figured out that there was a problem there. He pointed out that the straightforward reading of $\Box F$ as *Provable(F)* contradicted his incompleteness theorem.

> Let $\bot$ be the boolean constant *false*; then the **S4**-axiom $\Box\bot \rightarrow \bot$ corresponds to the statement *Consis* **PA**, expressing consistency of **PA**. By necessitation, **S4** derives $\Box(\Box\bot \rightarrow \bot)$. The latter formula expresses the assertion that *Consis* **PA** is provable in **PA**, which is false according to the second Gödel incompleteness theorem.

The issue of the intended provability semantics for **S4** was addressed by Lemmon (1957), Kripke (1963), Montague (1963), Mints (1974), Kuznetsov & Muravitsky (1977), Goldblatt (1978), Boolos (1979, 1993), Buss (1990), Artemov (1990), and many others. However, the problem of finding an adequate provability semantics for **S4** remained open.

3 Explicit vs. implicit approaches

A problem with the reading **S4** modality $\Box F$ as the formal provability predicate *Provable(F)* was caused by the existential quantifier over proofs in $\textit{Provable}(y)$. The latter is a shorthand for $\exists x Proof(x,y)$, where $Proof(x,y)$ is the standard arithmetical formula saying "x is the code of a proof of a formula with the code y". In a given model of arithmetic the formula $\exists x Proof(x,F)$ does not necessarily mean the existence of a proof of F. An element that instantiates the existential quantifier may be nonstandard. In that case $\exists x Proof(x,F)$ is true in the model, but there is no "real" **PA**-derivation behind such an x. This explains why the reflection principle $Provable(F) \rightarrow F$ is not derivable in **PA**: the formula $Provable(F)$ does not deliver a "real" proof of F.

On the other hand, the explicit reflection

$$Proof(n,F) \ \rightarrow\ F$$

for each natural number n is internally provable. Indeed, if $Proof(n,F)$ holds, then F is provable. If $Proof(n,F)$ does not hold then its negation $\neg Proof(n,F)$ is provable, since $Proof(x,y)$ is a decidable relation. In both cases $Proof(n,F) \rightarrow F$ is provable.

This consideration suggests the idea of introducing a kind of explicit provability logic by switching from the formulas $\exists x Proof(x,F)$ to the formulas *Proof(t,F)* and replacing the existential quantifier on proofs in the former by Skolem style operations on proofs in the latter. The usual Skolem technique, however, does not work here, since one cannot move quantifiers off the scope of the provability operator.

> Some of these operations appeared in the proof of Gödel's second incompleteness theorem. Within that proof in order to establish what are now known as Hilbert-Bernays-Löb derivability conditions one constructs computable functions $\mathbf{m}(x,y)$ and $\mathbf{c}(x)$ such that
>
> $\mathbf{PA} \vdash Proof(s, F \rightarrow G) \wedge Proof(t,F) \ \rightarrow\ Proof(\mathbf{m}(s,t), G);$
>
> $\mathbf{PA} \vdash Proof(t,F) \rightarrow Proof(\mathbf{c}(t), Proof(t,F)).$
>
> Later in the proof these facts were relaxed to their simplified versions
>
> $\mathbf{PA} \vdash Provable(F \rightarrow G) \wedge Provable(F) \ \rightarrow\ Provable(G),$
>
> $\mathbf{PA} \vdash Provable(F) \rightarrow Provable(Provable(F)),$
>
> sufficient to establish the incompleteness theorem.

In one of his lectures in 1938 (first published in 1995) Gödel mentioned the possibility of building an explicit version of **S4** with basic propositions "t is a proof of F" ($t:F$ in the modern notation) and thus getting a semantics of proofs for **Int**. Though neither definitions nor axiomatization were given, Gödel's suggestion specified the format $t:F$ of an expected solution of the provability semantics problem for **S4** and for the *BHK* problem[9]. It turned out that one more operation on proofs is needed to capture the whole of Gödel's provability logic **S4**.

[9] The author began working on logics with the atoms "t is a proof of F" and discovered the Logic of Proofs **LP** below before Gödel's paper of 1938-1995 became known. The first papers by the author on the logics with the atoms $t:F$ but without operations on proofs appeared in 1992 (joint work with T. Strassen). An early version of Logic of Proofs was finished during author's extended visit to the Amsterdam University in the fall of 1994. The system **LP** was first presented in 1994 at logic seminars in Amsterdam and Münster.

4 Proof polynomials and Logic of Proofs

Definition The language of Logic of Proofs (**LP**) contains the usual language of classical propositional logic along with

proof variables $x_0, \ldots, x_n, \ldots$ and proof constants $a_0, \ldots, a_n, \ldots$,
function symbols ! (monadic), $\cdot$ and $+$ (binary),
a formation symbol ":".

Proof terms in **LP** (called proof polynomials) are constructed from variables and constants by the operations $\cdot, +, !$. We shall denote proof polynomials by $p, s, t, \ldots$. Formulas in **LP** are built from the propositional atoms by the usual boolean connectives and by the new formation rule: if t is a proof polynomial and F a formula, then $t\!:\!F$ is a formula.

The intended semantics for $p\!:\!F$ is *p is a proof of F*, which will be formalized below. Note that proof systems which provide a formal semantics for $p\!:\!F$ are *multi-conclusion* ones, i.e. p may denote a proof of several different F's[10].

Definition The system **LP** along with the classical propositional logic contains the axioms:

A1. $t\!:\!F \rightarrow F$	*"verification"*
A2. $t\!:\!(F \rightarrow G) \rightarrow (s\!:\!F \rightarrow (t\cdot s)\!:\!G)$	*"application"*
A3. $t\!:\!F \rightarrow\ !t\!:\!(t\!:\!F)$	*"proof checker"*
A4. $s\!:\!F \rightarrow (s+t)\!:\!F, \quad t\!:\!F \rightarrow (s+t)\!:\!F$	*"choice"*

and the rule of inference:

R. $\vdash c\!:\!\mathbf{A}$ *if* $\mathbf{A}$ *is an axiom A0 - A4, and c a proof constant* *"axiom necessitation"*.

A *Constant Specification (CS)* is a finite set of formulas $c_1 : A_1, \ldots, c_n : A_n$ such that c_i is a constant, and A_i an axiom *A0 – A4*. Each derivation in **LP** naturally generates the *CS* consisting of all formulas introduced in this derivation by the *axiom necessitation* rule. Proof constants in **LP** stand for proofs of "simple facts", namely propositional axioms and axioms *A1 – A4*. Proof constants behave like atomic constant terms (*combinators*) of typed combinatory logic. A constant c_1 specified as $c_1\!:\!(A \rightarrow (B \rightarrow A))$ can be identified with the combinator $\mathbf{k}^{A,B}$ of the type $A \rightarrow (B \rightarrow A)$. A constant c_2 such that $c_2\!:\![(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))]$ corresponds to the combinator $\mathbf{s}^{A,B,C}$ of the type $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$. The proof variables may be regarded as term variables of combinatory logic and the operation

[10] The difference between single conclusion and multi-conclusion proof systems is mostly cosmetic. Usual proof systems (Hilbert or Gentzen style) may be considered as single conclusion ones if we assume that 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 stipulating that a given proof derives all formulas assigned to the nodes of this proof tree. The logic of strictly single conclusion proof systems **FLP** also admits (V. Krupski) a complete axiomatization. **FLP** is not compatible with the usual modal logic. For example, in **FLP** the principle $t\!:\!A \rightarrow \neg t\!:\!(A \rightarrow A)$ holds. The forgetful projection of this principle is $\Box A \rightarrow \neg\Box(A \rightarrow A)$ which is inconsistent with any normal system of modal logic. Therefore, strictly single conclusion proof systems are not directly relevant to the problem of a provability semantics for **S4**. Provability as a modal operator corresponds to multi-conclusion proof systems.

"$\cdot$" as the application of terms. In general an **LP**-formula $t{:}F$ can be read as a combinatory term t of the type F. Typed combinatory logic $\mathbf{CL}_{\rightarrow}$ thus corresponds to a fragment of **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 "$\rightarrow$" only.

There is no restriction on the choice of a constant c in R within a given derivation. In particular, R allows us to introduce a formula $c{:}A(c)$, or to specify a constant several times as a proof of different axioms from *A0 – A4*.

The following constructive form of the necessitation rule is admissible in **LP**:

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

Here p is nothing but the blueprint of a given derivation of F in **LP**. Therefore **LP** is a propositional system capable of internalizing its own proofs.

No single operator "$t:$" in **LP** is a modality since none of them satisfies the property $t{:}(P \rightarrow Q) \rightarrow (t{:}P \rightarrow t{:}Q)$. This makes **LP** essentially different from polymodal logics where the modality is upgraded by some additional features. In **LP** the modality is *decomposed* into a family of proof polynomials.

5 Solution of Gödel's problem and the propositional classical *BHK* problem

Under the standard provability interpretation of **LP** proof polynomials are evaluated by natural numbers, a formula $t{:}F$ is evaluated as $\mathit{Proof}(t^*, \ulcorner F^* \urcorner)$, where *Proof(x,y)* is any multi-conclusion proof predicate in **PA**, t^* and F^* are the evaluations of t and F respectively, $\ulcorner G \urcorner$ is the Gödel number of G. The operations "$\cdot$" and "!" are interpreted as Gödel's operations $\mathbf{a}(x,y)$ and $\mathbf{c}(x)$ respectively. The operation $s+t$ is an analogue of a concatenation of s and t, which is assumed to be present for a given proof predicate *Proof(x,y)*.

Definition Let *CS* be a constant specification. An interpretation *respects CS* if all formulas from *CS* are valid under this interpretation.

Completeness theorem for LP[11]

F is derivable in **LP** *with a constant specification CS*	$\Leftrightarrow$	*F is valid for any interpretation that respects CS*

The completeness theorem says that **LP** contains all the logical tautologies concerning proof polynomials. In the above notations

$$\mathbf{LP} \hookrightarrow \textit{REAL PROOFS}$$

[11] I found the first version of the completeness theorem concerning some call-by-name semantics for **LP** in 1994. In 1998 I established the completeness theorem for the call-by-value semantics above.

It is easy to see that the forgetful projection of **LP** is correct with respect to **S4**. Indeed, substituting $\Box$ for all occurrences of "$t{:}$" converts each **LP** derivation into a **S4** derivation. A much less trivial fact is that **LP** suffices to realize any **S4** theorem.

Definition By an **LP**-*realization* of a modal formula F we mean an assignment of proof polynomials to all occurrences of the modality in F. Let F^r be the image of F under a realization r.

In a provability context $\Box F$ is intuitively understood as "*there exists a proof x of F*". After a skolemization, all negative occurrences of $\Box$ produce arguments of Skolem functions, whereas positive ones give functions of those arguments. For example, $\Box A \to \Box B$ should be read informally as

$\exists x$ " *x is a proof of A*" $\to \exists y$ " *y is a proof of B*",

with the Skolem form

" *x is a proof of A*" $\to$ " *f(x) is a proof of B*".

The following definition captures this feature.

Definition A realization r is *normal* if all negative occurrences of $\Box$ are realized by proof variables.

Realization theorem[12]

If **S4** $\vdash F$, *then* **LP** $\vdash F^r$ *for some normal realization* r.

It was not *a priori* clear how to build such a realization. Indeed, the naive induction on a derivation in **S4** fails: if $A \to B$ is realizable and A is realizable then we still cannot conclude that B is realizable since those two occurrences of A may well have different realizations. In fact it takes an iterative procedure which operates with the whole derivation of F in **S4** to construct such a realization.

Here is an example which demonstrates the choice operation "+" at work. We first consider a derivation in **S4** of the formula $(\Box A \vee \Box B) \to \Box(A \vee B)$:

1. $A \to (A \vee B),\ \ B \to (A \vee B)$ — propositional axioms
2. $\Box(A \to A \vee B),\ \ \Box(B \to A \vee B)$ — from 1, by Necessitation
3. $\Box(A \to A \vee B) \to (\Box A \to \Box(A \vee B)),\ \ \Box(B \to A \vee B) \to (\Box B \to \Box(A \vee B))$ — **S4** axioms
4. $\Box A \to \Box(A \vee B),\ \ \Box B \to \Box(A \vee B)$ — from 2 and 3
5. $(\Box A \vee \Box B) \to \Box(A \vee B)$ — from 4, by propositional logic

In **LP** the corresponding derivation is

1. $A \to A \vee B,\quad B \to A \vee B$ — by $A0$,
2. $a{:}(A \to A \vee B),\quad b{:}(B \to A \vee B)$ — by R,

[12] The author, 1994

3. $x{:}A \to (a{\cdot}x){:}(A\vee B)$, $\quad y{:}B \to (b{\cdot}y){:}(A\vee B)$ from 2, by *A2*,
4. $(a{\cdot}x){:}(A\vee B) \to (a{\cdot}x+b{\cdot}y){:}(A\vee B)$, $\quad (b{\cdot}y){:}(A\vee B) \to (a{\cdot}x+b{\cdot}y){:}(A\vee B)$ by *A4*,
5. $(x{:}A \vee y{:}B) \to (a{\cdot}x+b{\cdot}y){:}(A\vee B)$ from 4, by propositional logic.

S4 may be considered as a higher level language on the top of **LP**. A general recipe for using **S4** as a provability logic might be the following: derive in **S4** and then translate the result into **LP** to recover its provability meaning.

The Realization theorem above links **S4** and **LP** thus connecting the chain of exact embeddings

$$\mathbf{Int} \hookrightarrow \mathbf{S4} \hookrightarrow \mathbf{LP} \hookrightarrow \textit{REAL PROOFS}$$

Definition A modal formula is *proof realizable* if there is a realization of it by proof polynomials valid in arithmetic.

Corollary 1. (Gödel's problem of provability semantics for **S4**).

A modal formula is proof realizable if and only if it is derivable in **S4**.

We believe there is a sufficient evidence that here we have "the solution" rather than "a solution" to the problem. Godel in 1938 introduced the **LP** format for understanding **S4**. Given this format proof polynomials appear as the minimal system of proof terms sufficient for realization of all operations on proofs that can be specified by a propositional condition. In turn, the proof polynomials completely determine the axiom system for **LP**, which is substantiated by the completeness theorem above.

Definition A propositional formula F is *proof realizable* if the corresponding modal formula $t(F)$ is proof realizable.

Corollary 2. (The classical *BHK* problem for propositional logic).

A propositional formula is proof realizable iff it is derivable in **Int**

In what sense proof realizability of the propositional language meets the requirements to a formal *BHK* semantics? Firstly, the proof realizability semantics is *BHK* compliant. Indeed, by the axiom *A2* of **LP** a proof polynomial realizing $A \to B$ acts as an operation that given a proof of A returns a proof of B. A proof realizer of $A \wedge B$ yields proofs of both A and B. A proof realizer of $A \vee B$ produces either a proof realizer of A or a proof realizer of B. The latter is supported by the fact that

$$\mathbf{S4} \vdash \Box(A \vee B) \to (\Box A \vee \Box B)$$

for all A and B prefixed by $\Box$, and by its explicit version in **LP**. Secondly, the proof realizability semantics is based on real proof systems, it is not circular, and it provides an exact specification of **Int**.

We wish to think that here we also have "the solution" rather than "the first solution" to the problem. Gödel's (and Orlov's) translation is nothing but the straightforward classical formalization of Brouwer's suggestion to understand intuitionistic truth as provability. Therefore **Int** is a definable fragment of **S4**. Since proof polynomials provide the intended provability semantics for **S4** they do the same for **Int** as well.

6 First order case

Theories based on the first order **S4** were studied by Hintikka, Mints, Myhill, Goodman, H. Friedman, Flagg, Scedrov, S. Shapiro, and others.

In the first order logic of proofs constants and proof letters depend on individual variables: $u(\vec{x})$, $c(\vec{x}), \ldots$ and are interpreted as provably recursive arithmetical terms. Here are some examples of valid principles accompanied by their plain modal projections.

$$\begin{array}{ll} c(y):(\forall x A(x) \to A(y)) & \Box(\forall x A(x) \to A(y)) \\ u:\forall x A(x) \to (c(y)\cdot u):A(y) & \Box\forall x A(x) \to \Box A(y) \\ u:\forall x A(x) \to \forall y((c(y)\cdot u):A(y)) & \Box\forall x A(x) \to \forall y \Box A(y) \end{array}$$

In a recent joint paper with Tanya Sidon-Yavorskaya we have shown that the first order logic of proofs is hyperarithmetical (in fact, $\Pi^0_1(\mathbf{TA})$ complete). In particular, this means that such logic does not admit a complete axiomatization. Similar results hold for the fragment of the first order logic of proofs with constants and proof variables not depending on individual variables.

7 Discussion

LP is an advanced system of combinatory logic that accommodates not only the "application" operation, but also "proof checker" and "choice". These operations subsume the simply typed λ-calculus together with the modal logic **S4**, and thus the whole of modal λ-calculus. In particular, **LP** creates the environment where modality and λ-terms are objects of the same nature, namely proof polynomials. Another way to look at it: modal logic is a forgetful projection of the typed combinatory logic enriched by the operations "proof checker" and "choice".

There was a major difficulty standing in the way of presenting modality via a system of terms: such a presentation should be self-referential and accommodate types containing terms of any type, including its own, for example, $x:F(x)$. The choice of the combinatory logic format for **LP** versus the obvious λ-term one in fact allows us to come with the concise representation of this self-referentiality. The natural λ-term system doing the same job would require an infinite supply of new term constructors and is less manageable.

The realization of **S4** in **LP** provides a fresh look at modal logic and its applications in general. Proof polynomials reveal the dynamic character of modality. In recent papers by V. Brezhnev, E. Kazakov, D. Shapiro and the author explicit counterparts of the modal logics **K**, **K4**, and **S5** were found and supplied with the provability semantics.

Such areas as modal λ-calculi, polymorphic second order λ-calculi, λ-calculi with types depending on terms, non-deterministic λ-calculi, etc., could benefit from semantics similar to the one delivered by **LP**.

Gabbay's Labelled Deductive Systems may serve as a natural framework for **LP**. Intuitionistic Type Theory by Martin-Löf also makes use of the format $t\!:\!F$ with its informal provability reading. **LP** may also be regarded as a basic epistemic logic with explicit justifications; a problem of finding such systems was raised by van Benthem.

The studies of the modal logics of formal provability (Solovay's systems **GL**, **S**, etc.) have given a valuable experience in arithmetical self-referential semantics for a variety of logical languages. Neither completeness theorem nor realization theorem above apply results or technique of the formal provability logics. However a substantial methodological influence of those studies on the logics of explicit provability is undeniable.