Kurt Gödel Research Center

First-Order Logic of Proofs

Sergei Artemov & Tatiana Yavorskaya (Sidon)

Vienna, April 27, 2011

BHK semantics

The intended semantics of intuitionistic logic is the semantics of proofs, also known as Brouwer-Heyting-Kolmogorov (BHK) semantics.

- a proof of $A \wedge B$ 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,
- a proof of $A \to B$ is a construction which, given a proof of A, returns a proof of B,
- a proof of $\forall x A(x)$ is a function converting c into a proof of $A(c)$,
- a proof of $\exists x A(x)$ is a pair (c, d) where d is a proof of $A(c)$.

Kolmogorov (1932), and Gödel (1933,1938), viewed BHK-proofs as proofs in classical mathematics. Gödel discussed the possibility of builidng a classical logic of proofs. Kolmogorov intended "to construct a unified logical apparatus dealing with objects of two types – propositions and problems."

Gödel's embedding

In 1933 Gödel embedded IPC into modal logic S4, viewed as a modal logic for classical provability, in a way that respects the informal provability reading of S4:

$$\mathsf{IPC} \vdash F \quad \textit{iff} \quad \mathsf{S4} \vdash tr(F),$$

where $tr(F)$ is obtained from F by prefixing each subformula of F with $\Box$. When parsing Gödel's translation $tr(F)$ of some formula F, we encounter a provability modality before each subformula, which forces us to read said subformula as provable rather then true. Therefore, Gödel's translation reflects the fundamental intuitionistic paradigm that intuitionistic truth is provability. Gödel's and Kolmogorov's approach views intuitionstic truth as *classical provability* thus making this version of BHK a non-circular semantics for intuitionistic logic. A similar position was taken by P.S. Novikov in his book "Constructive mathematical logic from the viewpoint of the classical one" (in Russian).

Logic of Proofs as BHK

At that stage, the problem of finding a BHK-type semantics of proof for IPC was reduced to developing such a semantics for S4. The next step was taken in the propositional Logic of Proofs LP with new atoms $t{:}F$ for

$$t \textit{ is a proof of } F$$

was introduced. The Realization Theorem demonstrated that each S4 theorem conceals an explicit statement about proofs, e.g.,

$$\Box F \to \Box G$$

reads as

$$u{:}F \to t(u){:}G$$

i.e., *if u is a proof of F, then $t(u)$ is a proof of G*, for an appropriate proof term $t(u)$. The Realization Theorem allows for the extension of this kind of explicit reading of modalities to all theorems of S4, so S4 has a semantics of LP proofs as anticipated by Gödel. Since proof terms in LP can be naturally interpreted as mathematical proofs, e.g., in Peano Arithmetic PA, S4 and IPC received an exact provability semantics consistent with BHK-requirements.

Lessons to learn from LP

Proofs are represented in LP by *proof terms* constructed from *proof variables* and *proof constants* by means of functional symbols for elementary computable operations on proofs, binary $\cdot$, $+$, and unary $!$. The formulas of LP are the usual propositional formulas and those of the form $t{:}F$ where t is a *proof term* and F is a formula. The operations of LP are specified by the following schemas:

$t{:}(A \to B) \to (s{:}A \to (t \cdot s){:}B)$ *application*

$t{:}A \to (t + s){:}A, \quad s{:}A \to (t + s){:}A$ *choice*

$t{:}A \to !t{:}t{:}A$ *proof checker.*

LP is axiomatized over the classical propositional calculus by the above schemas, the principle

$t{:}A \to A$ *reflexivity*

and the *axiom necessitation rule*, which allows for the specification of proof constants as proofs of the concrete axioms

$$\vdash c{:}A, \quad \text{where } c \text{ is an axiom constant, } A \text{ is an axiom of LP.}$$

Lessons to learn from LP

The intended semantics for LP is provided by proof predicates in Peano Arithmetic PA. The proof terms of the LP-language are interpreted by codes of arithmetical derivations. Operations $\cdot$, $+$, and unary ! become total recursive functions on such codes. Formulas of LP are interpreted by closed arithmetical formulas; and $t{:}F$ is interpreted by an arithmetical proof predicate in PA. LP is complete with respect to such provability semantics.

The following Realization Theorem shows that LP is an exact counterpart of Gödel's provability logic S4.

> *A modal formula F is provable in* S4 *iff there exists an assignment (called a "realization") of proof terms to all occurrences of* $\Box$ *in F such that the resulting formula is provable in* LP.

The proof of the Realization Theorem treats $\Box$ in the style of Skolem as the existential quantifier on proofs. Negative occurrences of $\Box$'s are assumed to hide universal quantifiers and hence are realized by proof variables, and positive occurrences of $\Box$'s are realized as existential quantifiers, i.e., by proof terms depending on these variables.

The Realization Theorem provides S4, and therefore IPC, with the exact BHK-style provability semantics, thus completing Gödel's project of 1933.

Quantification and LP

The arithmetical provability semantics for the Logic of Proofs LP, naturally generalizes to a first-order version with conventional quantifiers, and to a version with quantifiers over proofs. In both cases, axiomatizability questions were answered negatively.

> *The first-order logic of proofs is not recursively enumerable* (Artemov & Yavorskaya, 2001. *The logic of proofs with quantifiers over proofs is not recursively enumerable* (Yavorsky 2001).

Earlier this year, Artemov & Yavorskaya found the first-order logic of proofs FOLP capable of realizing first-order modal logic FOS4 and, therefore, the first-order intuitionistic logic HPC. Two kinds of proof semantics for FOLP have been offered: *parametric semantics*, in which proof objects are interpreted as derivations with parameters, and *generic semantics* with proof terms interpreted as provably computable functions from parameters to formal derivations. Both provide semantics of proofs for first-order S4 and a first-order Brouwer-Heyting-Kolmogorov-style semantics for HPC.

FOS4 may be viewed as a general purpose first-order justification logic; it opens the door to a general theory of first-order justification.

First-order LP: format

In the language FOLP, the proof predicate is represented by formulas of the form

$$t{:}_X A$$

where X is the set of individual variables that are considered global parameters. Variables from X and only them are free in $t{:}_X A$. All occurrences of variables from X that are free in A are also free in $t{:}_X A$. All other free variables of A are considered local and hence bound in $t{:}_X A$.

Proofs are represented by proof terms which do not contain individual variables. An arithmetical interpretation $*$, commutes with the Boolean connectives and quantifiers and

$$(t{:}_X F)^* = \mathit{Prof}\,(t^*(\underline{X}), F^*(\underline{X})),$$

i.e., $(t{:}_X F)^*$ is evaluated by the natural arithmetical formula asserting that t is a proof of F with global variables X.

First-order LP: axioms

FOLP is axiomatized by the following schemas. Here A, B are formulas, s, t are terms, X is a set of individual variables, and y is an individual variable.

A1 classical axioms of first-order logic

A2 $t{:}_X{}_y A \to t{:}_X A, \quad y$ is not free in A

A3 $t{:}_X A \to t{:}_X{}_y A$

B1 $t{:}_X A \to A$

B2 $s{:}_X (A \to B) \wedge t{:}_X A \to (s \cdot t){:}_X B$

B3 $t{:}_X A \to (t+s){:}_X A, \quad s{:}_X A \to (t+s){:}_X A$

B4 $t{:}_X A \to !t{:}_X t{:}_X A$

B5 $t{:}_X A \to \Box_x(t){:}_X \forall x A,\ x \notin X$

FOLP has the following inference rules:

R1 $\vdash A, A \to B \ \to \vdash B$ *Modus Ponens*

R2 $\vdash A \ \to \vdash \forall x A$ *generalization*

R3 $\vdash c{:}A$, where A is an axiom, c is a proof constant *axiom necessitation.*

First-order LP: example

Deriving an explicit converse Barcan Formula $\Box\forall xA \rightarrow \forall x\Box A$.

1. $\forall xA \rightarrow A$ - logical axiom;
2. $c{:}(\forall xA \rightarrow A)$ - axiom necessitation;
3. $c{:}_{\{x\}}(\forall xA \rightarrow A)$ - from 2, by axiom A3;
4. $c{:}_{\{x\}}(\forall xA \rightarrow A) \rightarrow (u{:}_{\{x\}}\forall xA \rightarrow (c\cdot u){:}_{\{x\}}A)$ - axiom B2;
5. $u{:}_{\{x\}}\forall xA \rightarrow (c\cdot u){:}_{\{x\}}A$ - from 3, 4, by Modus Ponens;
6. $u{:}\forall xA \rightarrow u{:}_{\{x\}}\forall xA$ - by axiom A3;
7. $u{:}\forall xA \rightarrow (c\cdot u){:}_{\{x\}}A$ - from 5, 6;
8. $\forall x[u{:}\forall xA \rightarrow (c\cdot u){:}_{\{x\}}A]$ - from 7, by generalization;
9. $u{:}\forall xA \rightarrow \forall x(c\cdot u){:}_{\{x\}}A$ - since x is not free in the antecedent.

Internalization

Internalization Theorem. *Let $p_0, \ldots, p_k$ be proof variables, $X_0, \ldots, X_k$ be sets of individual variables, and $X = X_0 \cup X_1 \cup \ldots \cup X_k$. Suppose that in* FOLP

$$p_0{:}_{X_0} A_0, \ldots, p_k{:}_{X_k} A_k \vdash F.$$

Then there exists a proof term $t(p_0, p_1, \ldots, p_k)$ such that

$$p_0{:}_{X_0} A_0, \ldots, p_k{:}_{X_k} A_k \vdash t{:}_X F.$$

Proof. Induction on derivation of F from $p_0{:}_{X_0} A_0, \ldots, p_k{:}_{X_k} A_k$.

...

Case 4. F follows by *generalization*, i.e., $F = \forall x G$ for some x not occurring free in the set of hypotheses. In particular, $x \notin X$. By IH, $s{:}_X G$ for some s. By B5, $s{:}_X G \to \mathsf{gen}_x(s){:}_X \forall x G$, hence $\mathsf{gen}_x(s){:}_X \forall x G$. Take $t = \mathsf{gen}_x(s)$.

...

In particular, given $\vdash F$, there is a proof term t containing no proof or individual variables such that $\vdash t{:}F$. Such t can be chosen $+$-free.

Realization

By *realization* of a formula A we mean a formula A^r of the language of FOLP that is obtained from A by replacing all occurrences of subformulas of A of the form $\Box B$ by $t{:}_X B^r$ for some proof terms t and such that $X = FVar(B)$. A realization is *normal* if all negative occurrences of $\Box$ are assigned proof variables.

We define the forgetful projection $(\cdot)^0$ of FOLP to the first-order modal language by induction on an FOLP-formula. For atomic formulas, we stipulate $F^0 = F$, forgetful projection commutes with Boolean connectives and quantifiers, and for proof assertions,

$$(t{:}_X F)^0 = \Box \forall y_0 \ldots \forall y_k F^0, \text{ where } \{y_0, \ldots, y_k\} = FVar(F) \setminus X.$$

Correctiness *If* FOLP $\vdash F$, *then* F^0 *is derivable in* FOS4.

Realization Theorem.
If FOS4 $\vdash A$, *then there is a normal realization* A^r *such that* FOLP $\vdash A^r$.

Realization

Proof. The proof is similar to that in the propositional case, with additional care given to individual variables. We consider the Gentzen-style calculus for FOS4 and prove that for every sequent $\Gamma \Rightarrow \Delta$ that is provable in FOS4, there exists a realization $(\Gamma \Rightarrow \Delta)^r$ such that FOLP $\vdash (\wedge\Gamma \rightarrow \vee\Delta)^r$. For this purpose, we take a cut-free derivation of $\Gamma \Rightarrow \Delta$ and construct realization for the whole derivation.

The sequential calculus for FOS4 has the same rule as the first order logic with additional 'modal' rules

$$\frac{\Box\Gamma \Rightarrow A}{\Box\Gamma \Rightarrow \Box A} \quad (R\Box), \qquad \frac{\Gamma, A \Rightarrow \Delta}{\Gamma, \Box A \Rightarrow \Delta} \quad (L\Box).$$

The following connection between FOS4 and its Gentzen-style version $\mathcal{G}$FOS4 takes place:

$$\mathcal{G}\mathsf{FOS4} \vdash \Gamma \Rightarrow \Delta \quad \text{iff} \quad \mathsf{FOS4} \vdash \bigwedge \Gamma \rightarrow \bigvee \Delta.$$

Cut-elimination holds in $\mathcal{G}$FOS4: if $\mathcal{G}\mathsf{FOS4} \vdash \Gamma \Rightarrow \Delta$, then $\Gamma \Rightarrow \Delta$ can be derived in $\mathcal{G}$FOS4 without using the cut-rule.

Realization

Lemma *If* $\mathcal{G}$FOS4 $\vdash \Gamma \Rightarrow \Delta$, *then there exists a normal realization such that* FOLP $\vdash (\bigwedge \Gamma \rightarrow \bigvee \Delta)^r$.

Proof Suppose that $\mathcal{D}$ is a cut-free derivation in FOS4. We will construct a realization for each sequent $\Gamma \Rightarrow \Delta$ in $\mathcal{D}$ in such a way that the formula $\bigwedge \Gamma^r \rightarrow \bigvee \Delta^r$ is provable in FOLP.

As in the propositional case, we split all occurrences of $\Box$'s in derivation $\mathcal{D}$ into families of related ones. Namely, two occurrences of $\Box$ are related if they occur in related subformulas of premises and conclusions of rules; we extend this relationship by reflexivity and transitivity. All the rules of $\mathcal{G}$FOS4 respect polarities, hence all $\Box$'s in every family have the same polarity. So we can speak about *positive and negative families of* $\Box$*'s*. If f is a positive family, then all $\Box$'s from f are introduced either by weakening on the right or by the rule $(R\Box)$. If at least one $\Box$ in f is introduced by $(R\Box)$, then we call f an *essential* family, otherwise f is called *inessential family*.

Step 1. Initialization. To every negative or inessential positive family f we assign a fresh proof variable p_f. Replace all $\Box A$, where $\Box$ is from f, by $p_f{:}_X A$ with $X = FVar(A)$.

Realization

Suppose that f is an essential positive family. We enumerate the rules $(R\Box)$ which introduce $\Box$'s from the family f. Let $n(f)$ be the total number of such rules for the family f. For the $(R\Box)$–rule number k in a family f where $k = 1, \ldots, n(f)$, we take a fresh proof variable u_k called *a provisional variable*. Finally, replace all $\Box A$ from the family f by

$$[u_1 + \ldots + u_{n(f)}]{:}_X A$$

with $X = FVar(A)$.

After initialization is completed, all nodes in the resulting tree $\mathcal{D}'$ are assigned formulas of the logic FOLP.

Step 2. Realization. Now we travel along derivation $\mathcal{D}'$ from leaves to root and replace all provisional variables by FOLP–terms. We retain the notation u_j for both provisional variables and terms substituted for them. The resulting tree is denoted by $\mathcal{D}^r$. By induction on the depth of a node in $\mathcal{D}'$, we prove that after the process passes the node $\Gamma \Rightarrow \Delta$ in $\mathcal{D}'$ and replaces it by $\Gamma^r \Rightarrow \Delta^r$,

1. sequent $\Gamma^r \Rightarrow \Delta^r$ is derivable in FOLP;
2. for every subformula B occurring in Γ, Δ, we have $FVar(B^r) = FVar(B)$.

Realization

The only case in which we alter realization is in rule $(R\Box)$. Suppose that $\Gamma \Rightarrow \Delta$ is obtained by rule $(R\Box)$:

$$\frac{\Box A_1, \ldots, \Box A_k \Rightarrow A}{\Box A_1, \ldots, \Box A_k \Rightarrow \Box A}\,.$$

The symbol $\Box$ introduced by this rule belongs to an essential positive family f. Let this rule have the number i among rules $(R\Box)$ which introduce $\Box$'s from this family f, and $n = n(f)$.

Currently in $\mathcal{D}^r$, the node corresponding to the premise of this rule is assigned a sequent $q_1{:}_{X_1}B_1, \ldots, q_k{:}_{X_k}B_k \Rightarrow B$ which, by the Induction Hypothesis, is provable in FOLP. The node corresponding to the conclusion is assigned a sequent

$$q_1{:}_{X_1}B_1, \ldots, q_k{:}_{X_k}B_k \Rightarrow [u_1 + \ldots + u_i + \ldots + u_n]{:}_X B$$

where all q_j are proof variables, all u_j are either provisional variables or terms, u_i is a provisional variable, and $X = FVar(B)$.

Realization

By Internalization Lemma, it follows that there exists a term t such that FOLP derives

$$q_1{:}_{X_1} B_1, \ldots, q_k{:}_{X_k} B_k \Rightarrow t{:}_Y B$$

where $Y = X_1 \cup X_2 \cup \ldots \cup X_n$. Using axiom A2, we remove from Y all variables that are not in $FVar(B)$ and obtain $Y' = Y \cap FVar(B)$. Then, by A3, add to Y' all free variables of B that were not yet there and obtain X. The resulting sequent

$$q_1{:}_{X_1} B_1, \ldots, q_k{:}_{X_k} B_k \Rightarrow t{:}_X B$$

is provable in FOLP. Therefore, by B3,

$$q_1{:}_{X_1} B_1, \ldots, q_k{:}_{X_k} B_k \Rightarrow [u_1 + \ldots + u_{i-1} + t + u_{i+1} + \ldots + u_n]{:}_X B.$$

Replace provisional variable u_i by t everywhere in $\mathcal{D}^r$. By the Substitution Lemma, this substitution respects provability in FOLP.

FOS4 = projection of FOLP

Corollary 1 FOS4 *is the forgetful projection of* FOLP.

Corollary 2 *F is derivable in* HPC *if and only if its Gödel translation is realizable in* FOLP.

Example 1 Consider formula

$$\neg\forall x A(x) \to \exists x \neg A(x) \quad \text{where } A(x) \text{ is atomic.} \tag{1}$$

This is not derivable in intuitionistic first-order logic HPC. Its Gödel translation (in an equivalent simplified form $(\cdot)^\circ$, cf. [18], Section 9.2.1) is

$$\Box\neg\Box\forall x A(x) \to \exists x \Box\neg\Box A(x). \tag{2}$$

By Corollary 2, modal formula (2) is not realizable in FOLP.

Open variables in derivations

The role of X in $t{:}_X F$ is to provide a substitutional access to derivation t and formula F for all variables from X, in a sense, to keep variables in X "global" in $t{:}_X F$. We have to define "free variables of a derivation":

> *if a derivation $\mathcal{D}(x)$ with a "free variable x" is a proof of a formula $F(x)$, then for each n, $\mathcal{D}(n)$ is a derivation of $F(n)$.*

Example. Let $F(x)$ be a logical axiom with a free variable x. Consider a derivation

$F(x)$ - axiom;
$\forall x F(x)$ - generalization;
$F(x) \to (\forall x F(x) \to F(x) \wedge \forall x F(x))$ - conjunction axiom;
$\forall x F(x) \to F(x) \wedge \forall x F(x)$ - Modus Ponens;
$F(x) \wedge \forall x F(x)$ - Modus Ponens.

Question: is the very first occurrence of x free in this derivation?
Answer 1: x is free, since it is free in $F(x)$.
Answer 2: x is not free, since substitution $(0/x)$ ruins the derivation. The generalization step is no longer legitimate: $\forall x F(x)$ does not follow from $F(0)$.

Open variables in derivations

The reason for this confusion lies in the fact that Hilbert derivations are not trees and reuse the same formulas. The true structure of this derivation is revealed by its tree-style presentation

$$\dfrac{\dfrac{F(x)\to(\forall xF(x)\to F(x)\wedge\forall xF(x))\qquad F(x)}{\forall xF(x)\to F(x)\wedge\forall xF(x)}\qquad\dfrac{F(x)}{\forall xF(x)}}{F(x)\wedge\forall xF(x)}\,.$$

As we can see, axiom $F(x)$ appears twice in this derivation in quite different substitutional contexts. In the left branch, variable x from $F(x)$ remains free until the root of the derivation. In the right branch, $F(x)$ was subjected to generalization and binding of variable x. Which occurrences of x in this derivation are open to substitution? The answer is given by the boldface occurrences $\boldsymbol{x}$:

$$\dfrac{\dfrac{F(\boldsymbol{x})\to(\forall xF(x)\to F(\boldsymbol{x})\wedge\forall xF(x))\qquad F(\boldsymbol{x})}{\forall xF(x)\to F(\boldsymbol{x})\wedge\forall xF(x)}\qquad\dfrac{F(x)}{\forall xF(x)}}{F(\boldsymbol{x})\wedge\forall xF(x)}\,.$$

Open variables in derivations

The idea of *open occurrences of a variable in a given proof tree* in PA-proofs is that it is open for substituting a number without destroying the proof tree: if x is open in a proof tree $\mathcal{T}(x)$ of a formula $A(x)$, then $\mathcal{T}(n)$ is a proof of $A(n)$.

We assume that all derivations are presented in a *regular form*, which we define as follows.

1. Derivations are supplied with a tree-like proof of each of its formulas, and

2. These trees do not overlap, i.e., each occurrence of a formula in such belongs only to one of the trees.

It is obvious that each Hilbert-style proof can be presented in a regular form which proves exactly the same formulas as the original derivation.

Parametric semantics

Let us fix a natural multi-conclusion Gödel proof predicate

$$\mathit{Proof}(x,y) \rightleftharpoons \text{“}x \textit{ is the Gödel number of a finite set of tree-like } \mathsf{PA}\textit{-derivations,}$$
$$y \textit{ is the Gödel number of a root formula of one of those derivations.”}$$

$[F(\underline{X})]$ is a natural arithmetical term for $\lambda K^{\ulcorner} F(K)^{\urcorner}$,

and

$[d(\underline{X})]$ is a term for $\lambda K^{\ulcorner} d(K)^{\urcorner}$.

Lemma 3 *For each* PA*-proof* d*, arithmetical formula* F*, and set of variables* X*, the following formulas are provable in* PA*:*

1. $\mathit{Proof}(d(\underline{X}), F(\underline{X})) \to F(X)$;
2. $\mathit{Proof}(d(\underline{Xy}), F(\underline{Xy})) \to \mathit{Proof}(d(\underline{Xy}), F(\underline{X}))$, $y \notin \mathit{FVar}(F)$;
3. $\mathit{Proof}(d(\underline{Xy}), F(\underline{Xy})) \to \mathit{Proof}(d(\underline{Xy}), F(\underline{Xy}))$.

Proof. To prove (1), reason in PA. Given X and the fact that $d(X)$ is a proof of $F(X)$, we conclude that $F(X)$ is nothing but a substitutional example of F such that d is a proof of F. Since d is a specific derivation, F follows by the standard parameter-free argument from the proof of correctness of the propositional Logic of Proofs [1, 2].

Existence of operations

There exist total recursive operations on proofs $\cdot$, $+$, $!$, and gen_x such that for any proofs d and e, formulas F and G, and a set of individual variables X, the following formulas are provable in PA:

1. $\mathit{Proof}(d(\underline{X}),(F\to G)(\underline{X}))\to(\mathit{Proof}(e(\underline{X}),F(\underline{X}))\to\mathit{Proof}((d\cdot e)(\underline{X}),G(\underline{X})))$;
2. $\mathit{Proof}(d(\underline{X}),F(\underline{X}))\vee\mathit{Proof}(e(\underline{X}),F(\underline{X}))\to\mathit{Proof}((d{+}e)(\underline{X}),F(\underline{X}))$;
3. $\mathit{Proof}(d(\underline{X},F(\underline{X})\to\mathit{Proof}(!d(\underline{X}),\mathit{Proof}(d(\underline{\underline{X}}),F(\underline{\underline{X}}))))$;
4. $\mathit{Proof}(d(\underline{X}),F(\underline{X}))\to\mathit{Proof}(\mathsf{gen}_x(d)(\underline{X}),\forall xF(\underline{X}))$, $x\notin X$.

Proof The only nontrivial case is "verifier" $!$ which works as follows. Given a proof d, it recovers the set X of all parameters open in d. Then for each subset Y of X and for each formula F proved by d, it reconstructs the formula $\mathit{Proof}(d(\underline{Y}),F(\underline{Y}))$ with free variables Y. Since d is a proof of F, these formulas are all provable in PA. Operation "!" first finds a tree-like derivation for each of those formulas and finally, for $!d$, takes the set of all such derivations. The main purpose of $!d$ is to provide the proof of $\mathit{Proof}(d(\underline{Y}),F(\underline{Y}))$ for any $Y\subseteq X$.

Interpretation

A *parametric arithmetical interpretation* for the language FOLP is defined by operations $+$, $\cdot$, $!$ and gen_x which satisfy Lemma and an evaluation $*$ that maps

- proof variables and constants to multi-conclusion arithmetical proofs and
- predicate symbols of arity n to arithmetical formulas with n free variables. We suppose that $*$ commutes with the renaming of individual variables.

For proof variables and constants, t^* is given by the evaluation $*$, and we take $(s\cdot t)^*$ to be $s^*\cdot t^*$, $(s+t)^* = s^*+t^*$, $(\mathsf{gen}_x(t))^* = \mathsf{gen}_x(t^*)$, and $(!t)^* = !(t^*)$.

For formulas, $*$ commutes with the Boolean connectives and quantifiers and

$$(t{:}_X F)^* = \mathit{Proof}(t^*(\underline{X}), F^*(\underline{X})),$$

i.e., $(t{:}_X F)^*$ is evaluated by the natural arithmetical formula asserting that t is a proof of F with global variables X.

Soundness

Each derivation in FOLP generates *constant specification*, which is a (finite) set of formulas $c{:}A$ introduced by the axiom necessitation rule R3. We say that interpretation $*$ respects constant specification *CS*, if all formulas from *CS* are true (hence provable in PA).

Theorem 1 [Arithmetical soundness] *If* FOLP $\vdash A$ *with a constant specification CS, then for every parametric arithmetical interpretation* $*$ *respecting CS,* PA $\vdash A^*$.

Corollary 3 *If* FOS4 *proves* F, *then*

a) F *is realizable in* FOLP, *and*

b) a realization of F *is a parametric provability tautology.*

Corollary 4 *If* HPC *proves* F, *then*

a) the Gödel translation of F, $tr(F)$, *is provable in* FOS4,

b) $tr(F)$ *is realizable in* FOLP, *and*

c) a realization of $tr(F)$ *is a parametric provability tautology.*

Example

Consider intuitionistic theorem

$$\exists x A(x) \rightarrow \neg \forall x \neg A(x) \quad \text{(where } A(x) \text{ is atomic).}$$

Its simplified Gödel translation is

$$\Box \exists x \Box A(x) \rightarrow \neg \Box \forall x \neg \Box A(x),$$

which is provable in FOS4. By the Realization Theorem, there is its realization provable in FOLP. We leave it as an exercise to derive in FOLP the following realization

$$u{:}\exists x v{:}_{\{x\}} A(x) \rightarrow \neg w{:}\forall x \neg v{:}_{\{x\}} A(x).$$

It is easy to see that with $F = \forall x \neg v :_{\{x\}} A(x)$, the latter formula states $u{:}\neg F \rightarrow \neg w{:}F$ which is obviously provable in FOLP.

Accidental tautologies

Arithmetical interpretation based on a specific proof predicate may yield tautologies that appear as a result of the specifics of numbering of proofs.

Example. Consider the formula

$$\neg u{:}\neg u{:}\bot. \tag{3}$$

Intuitively, this does not seem right, since the arithmetical translation of $\neg u{:}\bot$ is a true decidable statement clearly provable in PA, and there is no reason to rule out a sophisticated u that can prove $\neg u{:}\bot$. However, this intuition is not supported by the parametric semantics in which (3) is vacuously valid. Indeed, the standard Gödel numbering of formulas and proofs is monotonic and the code of a whole is strictly greater than the code of its proper part. Therefore, if $(u{:}\neg u{:}\bot)^*$ were true, then the code of u^* would be less than the code of $(\neg u{:}\bot)^*$ which is less than the code of u^* - a contradiction.

In order to avoid such "identities," we introduce the notion of *invariant parametric interpretation* which accepts as valid only those principles that hold for all legitimate numerations of proofs.

Invariant semantics

We consider the class of all proof predicates that are provably equivalent to the standard proof predicate but allow different numeration of proofs.

A *proof predicate* is a provably Δ_1-formula *Prf(x,y)* for which there are provably total recursive functions $\alpha(n)$ and $\beta(n)$ such that

$\mathsf{PA} \vdash \forall x, y(\mathit{Proof}(x, y) \leftrightarrow \mathit{Prf}(\alpha(x), y))$, and

$\mathsf{PA} \vdash \forall x, y(\mathit{Proof}(\beta(x), y) \leftrightarrow \mathit{Prf}(x, y))$.

Informally, α and β are computable translators from proofs in *Prf* to proofs of the same theorems in *Proof*, and vice versa.

For each *Prf*-proof d and each set X of individual variables, $d(X)$ is a natural arithmetical term for a primitive recursive function that, for each value N of X, recovers $\beta(d)$ - the Gödel number of a regular *Proof*-derivation corresponding to d, substitutes N for X in $\beta(d)$, and computes back the *Prf*-number of the resulted derivation:

$$d(X) = \alpha(\beta(d)(X)). \tag{4}$$

Invariant semantics works

Let us reconsider formula (3) and show that it is not valid in the invariant parametric semantics. For this we have to find a proof predicate Prf and interpretation $*$ such that $(u{:}\neg u{:}\bot)^*$ holds (provable in PA).

In what follows we assume that an injective numeration of the joint syntax of FOLP and PA is given. Consider the following fixed-point equation that defines an arithmetical predicate $Prf(x, y)$.

$$Prf(x, y) \leftrightarrow Proof(x, y) \vee (x = \ulcorner u \urcorner \wedge y = \ulcorner \neg Prf(\ulcorner u \urcorner, \ulcorner \bot \urcorner) \urcorner). \qquad (5)$$

From (5), it immediately follows that $Prf(x, y)$ is provably Δ_1. Moreover, it is also clear from (5) that $\neg Prf(\ulcorner u \urcorner, \ulcorner \bot \urcorner)$ holds and let p be the Gödel number of its proof. So, $Proof(p, \ulcorner \neg Prf(\ulcorner u \urcorner, \ulcorner \bot \urcorner) \urcorner)$. Let α and β be identity functions except for

$$\beta(\ulcorner u \urcorner) = p \quad \text{and} \quad \alpha(p) = \ulcorner u \urcorner.$$

We now define the interpretation $*$ that interprets u as $\ulcorner u \urcorner$. From (5), $(u{:}\neg u{:}\bot)^*$ holds (provable in PA), hence formula (3) is not a valid provability principle in the invariant parametric semantics.

Barcan is valid

Proposition *$\forall y(t{:}_{X_y}A) \to t{:}_X A$ is valid in parametric/invariant semantics.*

Lemma *Let $A(x)$ and $B(x)$ be arithmetical formulas, and suppose for two distinct numerals n_1 and n_2, $A(n_i)$ syntactically coincides with $B(n_i)$. Then $A(x)$ coincides with $B(x)$.*

Lemma *Let $p(x)$ be a derivation in* PA*, and $Q(x)$ an arithmetical formula. If for all $n = 0, 1, 2, ...$, $p(n)$ is a derivation for $Q(n)$, then p is a derivation for Q with x as a local variable.*

Proof Suppose $p(x)$ proves $F_1(x), F_2(x), ..., F_k(x)$. Since for each n there is an i such that $Q(n) = F_i(n)$, by the Pigeonhole Principle, there is an i such that $Q(n) = F_i(n)$ for two different n's. By the previous Lemma, $Q(x) = F_i(x)$.

Principle $\forall y(t{:}_{X_y}A) \to t{:}_X A$ is derivable in PA for each parametric evaluation $*$. Indeed, both Lemmas are formalizable in PA. Reason in PA. Suppose for all y, $t^*(X, y)$ is a proof of $A^*(X, y)$. Then $A^*(X, y)$ is in $t^*(X)$ where y is a local variable. Therefore, $t^*(X)$ is a proof of $A^*(X)$. This transfers to the invariant semantics directly.

Corollary *The explicit Barcan formula $\forall x(t{:}_{Xx}A) \to \mathsf{gen}_x(t){:}_X \forall x A$ is valid in parametric/invariant semantics.*

The main thing is yet to come...

In parametric/invariant semantics, proof terms are interpreted as specific derivations with open variables. As a result, an explicit version of the Barcan formula holds. However, the intuitive provability semantics for first-order modal logic offers a somewhat different account of the Barcan formula

$$\forall x \Box A \rightarrow \Box \forall x A.$$

According to this intuition, if $A(x)$ is provable for each x, it does not guarantee that $\forall x A(x)$ is provable. In this section, we offer a generic provability semantics for FOLP that accommodates this intuition.

Generic proof(X)

Definition Given a proof predicate Prf and a set of individual variables X, a *proof function* is a pair $(p(X), \mathcal{F})$ such that

1. $p(X)$ is a provably total recursive function from the set of values of X to Prf-proofs, fairly represented in PA by a term $p(X)$; $\mathcal{F} = (F_1, \ldots, F_n)$ is a finite set of arithmetical formulas (thought as formulas provable by this proof function).

2. PA "knows" that for different values of X, $p(X)$ proves substitutional examples of formulas from $\mathcal{F}$ and only them, that is,

$$\mathsf{PA} \vdash Prf(p(X), y) \leftrightarrow \bigvee_{i=1}^{n} (y = [F_i(\underline{X})]); \tag{7}$$

3. PA "knows" that each formula provable by $p(X)$ actually holds, i.e., for each formula F (not necessarily from $\mathcal{F}$),

$$\mathsf{PA} \vdash Prf(p(X), F(\underline{X})) \rightarrow F. \tag{8}$$

As a notational convention, we will speak about a proof function $p(X)$ and the set of formulas $\widehat{p(X)}$ as $\mathcal{F}$ from the definition.

Generic proofs

Definition Fix a proof predicate Prf, finite set of variables Y. By a *proof form* $\{p_X(X)\}$ we understand a set of proof functions $p_X(X)$, one for each $X \subseteq Y$ such that the following two properties are provable in PA:

- *Monotonicity* : $Prf(p_X(X), A(\underline{X}))) \to Prf(p_{Xy}(Xy), A(\underline{Xy}))$. This reflects a basic observation that any instance of a provable formula is itself provable.

- *Coherence*: if y is not free in A, then

$$Prf(p_{Xy}(Xy), A(\underline{X})) \to Prf(p_X(X), A(\underline{X})).$$

  This reflects another basic observation that substitutions for a variable that is not free in A do not change A.

Note that for each Prf-proof p and each Y the set of invariant Prf-proofs $\{p(X)\}$ is a legitimate proof form.

In parametric semantics, proof terms are interpreted as real derivations with a mechanism of opening/closing variables, and operations on poof terms as operations on these derivations. In generic semantics, we have to define standard operations $\{+, \cdot, !, \mathsf{gen}_x\}$ on proof forms.

Two-way Gödel's Lemma

The principal tool of defining proof functions and operations:

Two-way Gödel's Lemma For each provably Δ_1-formula $\sigma(X)$, there is a provably recursive function $t(X)$ such that

$$\mathsf{PA} \vdash \mathit{Proof}\,(t(X), \sigma(\underline{X})) \leftrightarrow \sigma(X).$$

Proof Direction "$\leftarrow$" is similar to the classical Gödel's Lemma. A tedious analysis of the proof of Gödel's Lemma shows that the converse implication is also provable. However, we offer here an alternative shorter proof. Given $g(X)$ from the Gödel's Lemma, define $t(X)$ to be a natural arithmetical term for a provably recursive function that is equal to $g(X)$ if $\sigma(X)$ holds, and to 0 (which is a proof of nothing) otherwise. Therefore,

$$\mathsf{PA} \vdash \sigma(X) \rightarrow \mathit{Proof}\,(t(X), \sigma(\underline{X})).$$

We claim that

$$\mathsf{PA} \vdash \neg\sigma(X) \rightarrow \neg\mathit{Proof}\,(t(X), \sigma(\underline{X}))$$

as well. Reason in PA. If not $\sigma(X)$, then $t(X) = 0$, hence $t(X)$ is not a proof of $\sigma(X)$.

Operations on proof forms

The following lemma was the principal technical effort:

Lemma *For each finite set Y of parameters and each proof predicate there exist operations $+, \cdot, !, \mathsf{gen}_x$ of proof forms that provably satisfy axioms of* FOLP.

Proof heavily relies on the two-way Gödel's Lemma. Preserving reflexivity, monotonicity, and coherence was a challenge.

This lemma gives a convenient tool for defining arithmetical interpretations $*$ inductively: it suffices to define $*$ on atomic formulas and atomic proof terms.

Generic semantics

A *generic arithmetical interpretation* of the language FOLP is

- a proof predicate Prf, finite set of variables Y, and operations $\{+, \cdot, !, \mathsf{gen}_x\}$ on proof forms for given Y;
- an evaluation $*$ that maps proof variables and constants p to proof forms $\{p_X(X)\}$ and predicate symbols of arity n to arithmetical formulas with n free variables. We suppose that $*$ commutes with renaming of individual variables.

For each X, interpretation $*$ commutes with Prf-operations on proofs, the Boolean connectives, and quantifiers. For proof assertions,

$$(t{:}_X F)^* = Prf(t^*(X), F^*(\underline{X})).$$

Soundness Theorem *If* FOLP $\vdash F$ *with a constant specification CS, then for every generic arithmetical interpretation* $*$ *respecting CS,* PA $\vdash F^*$.

Barcan fails

The explicit Barcan formula $\forall x(p{:}_{\{x\}}A(x)) \to \mathsf{gen}_x(p){:}\forall x A(x)$ is not valid.

Fix the set of variables $Y = \{x\}$, the standard proof predicate *Proof* with the standard operations, and define $A^*(x)$ as $\neg \mathit{Proof}(x, \ulcorner \bot \urcorner)$ which is a provably Δ_1-formula. By the two-way Gödel Lemma, there is a provably recursive term $g(x)$ such that for each x it returns the code of a proof of $A(x)$. Moreover,

$$\mathsf{PA} \vdash \mathit{Proof}(g(x), A^*(\underline{x})) \to A^*(x).$$

Consider a proof function $g(x)$ with $\widehat{g(x)} = \{A^*(x)\}$. Define the interpretation $*$ of proof variables as follows: $p^*(x)$ is the proof function $g(x)$, and $*$ makes all other atomic proof terms 0. It is easy to check that each proof variable u is mapped to a proof form. Under this interpretation $*$, the explicit Barcan formula is false. Indeed, its antecedent,

$$\forall x \mathit{Proof}(g(x), \neg \mathit{Proof}(\underline{x}, \ulcorner \bot \urcorner))$$

is true, by Gödel's Lemma, whereas its succedent, $\mathit{Proof}(\mathsf{gen}_x(p)^*, \ulcorner \forall x A^* \urcorner)$, is false since $\forall x A$ is equivalent to the consistency of PA.

BHK intuition seems to work too

Intuitionistically unsound principle

$$\neg\forall x A(x) \to \exists x \neg A(x)$$

is not valid with respect to the generic provability semantics either. The simplified Gödel translation of this formula is equivalent to

$$\Box\neg\Box\forall x A(x) \to \exists x \Box\neg\Box A(x). \tag{10}$$

Note that (10) is provable in PA if $\Box$ is interpreted as the **provability** operator "*there exists a proof that ...*." Indeed, since $\mathsf{PA} \vdash \Box\neg\Box\varphi \to \Box\neg\Box\bot$, the antecedent of (10) implies $\Box\neg\Box\bot$, which, by the formalized Gödel's second incompleteness theorem, is equivalent to $\Box\bot$. In modal logic, $\Box\bot \to \exists x \Box\neg\Box A(x)$, which proves (10) in PA. This observation demonstrates that the formal provability reading of modal operators does not conform to intuitionistic logic in terms of Gödel's translation.

We show that under any normal realization of (10), there is a generic arithmetical interpretation that renders its realization not provable in PA. The proof of this fact requires yet another fixed-point construction.

Completeness is not attainable

To simplify formulations but without a loss of generality, we consider the languages of LP and FOLP without proof constants and logics LP, FOLP without the axiom necessitation rule. Let PAR, INV, and GEN be sets of FOLP-formulas valid under the parametric, invariant parametric, and generic semantics correspondingly. From what we have already learned, it follows that

$$\mathsf{FOLP} \subsetneq \mathsf{GEN} \subsetneq \mathsf{INV} \subsetneq \mathsf{PAR}.$$

Theorem *Neither of* GEN, PAR, *or* INV *is recursively enumerable.*

Corollary FOLP *is not complete with respect to any of the aforementioned provability semantics: parametric, invariant parametric, or generic.*

Conclusions

On the theoretical side, FOLP answers a cluster of long standing foundational questions, e.g., a BHK semantics for first-order intuitionistic logic, a provability semantics for first-order S4, a general logic of proofs and propositions.

In addition, FOLP may be viewed as a general purpose justification logic; it opens the door to a general theory of first-order justification in which we anticipate a variety of FOLP-like systems equipped with appropriate epistemic semantics.

Thank You!