Logic Colloquium 2008
Bern University

Logic of Strong Provability and Explicit Proofs

Elena Nogina

City University of New York

July 4, 2008

Gödel's axiomatic approach to provability

Gödel (1933) introduced the modal logic S4 as the system axiomatizing provability in classical mathematics:

Axioms and rules of classical propositional logic

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

$\Box F \rightarrow F$ *Reflexivity*

$\Box F \rightarrow \Box\Box F$ *Transitivity*

Necessitation Rule: $\dfrac{\vdash F}{\vdash \Box F}$

Gödel's provability semantics for modality

Gödel also considered the interpretation of $\Box F$ as

$$F \textit{ is provable in Peano Arithmetic } \text{PA}$$

and noticed that this semantics is inconsistent with S4.

Indeed, $\Box(\Box F \to F)$ can be derived in S4. On the other hand, interpreting $\Box$ as the predicate *Provable* of formal provability in Peano Arithmetic PA and F as *falsum* $\bot$, converts this formula into the false statement that the consistency of PA is internally provable in PA:

$$\textit{Provable } (\textit{Consis PA}) \ .$$

Gödel's paper left open two problems

(1) Find a modal logic of formal provability *Provable*,

'**a provability semantics without a calculus**'

(2) Find a precise provability semantics for S4,

'**a provability calculus without a semantics**'

Problem (1) was solved in 1976 by Solovay, who found the logic of formal provability GL.

Problem (2) was solved in 1995 by Artëmov's Logic of Proofs LP which provided a semantics of explicit proofs for S4.

The provability logic GL is given by the following list of postulates:

Axioms and rules of classical propositional logic

$\Box(F \to G) \to (\Box F \to \Box G)$ *Normality*

$\Box(\Box F \to F) \to \Box F$ *Löb Axiom*

$\Box F \to \Box\Box F$ *Transitivity*

Necessitation Rule: $$\frac{\vdash F}{\vdash \Box F}$$

Formal provability (arithmetical) **interpretation** of a modal language is a mapping $*$ from the set of modal formulas to the set of arithmetical sentences such that $*$ agrees with Boolean connectives and constants and

$$(\Box G)^* = \textit{Provable } G^* \ .$$

Solovay's completeness theorem:

GL $\vdash F$ *iff* *for all interpretations* $*$, PA $\vdash F^*$.

As was noticed by Gödel, the formal provability predicate does not model the very notion of mathematical provability in a satisfactory way. For example, the basic reflexivity principle of mathematical provability,

if F is provable, then F is true,

which Gödel included in his basic provability logic S4, fails in the logic of formal provability GL.

S4-preserving provability interpretation:

$$(\Box G)^* = G^* \wedge \mathit{Provable}\ (G^*)$$

Complete axiomatization:

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

The studies of the logics of strong provability (Kuznetsov, Muravitsky, Goldblatt, Boolos, Artemov, Esakia, Yavorskaya, and others) are helping to connect Provability Logic to Epistemology.

Alternative Gödel's format for provability

In his lecture in Vienna in 1938 Gödel mentioned a possibility of building an explicit version of S4 with basic propositions "t is a proof of F":

$$\mathit{Proof}(t, F)$$

This Gödel's lecture remained unpublished until 1995. By that time the full Logic of Proofs was already discovered by Artëmov.

Logic of Proofs LP

Proof polynomials are terms built from *proof variables* $x, y, z, \ldots$ and *proof constants* $a, b, c, \ldots$ by means of two binary operations: *application* '$\cdot$' and *union* '$+$', and one unary *proof checker* '!'.

Using t to stand for any proof polynomial and S for any sentence letter, the **formulas of the Logic of Proofs** are defined by the grammar

$$A = S \mid A \rightarrow A \mid A \wedge A \mid A \vee A \mid \neg A \mid t{:}A \ .$$

Axioms and rules of the Logic of Proofs $\mathrm{LP}_{\emptyset}$

LP0 Axioms and rules of classical propositional logic

LP1 $t{:}(F \to G) \to (s{:}F \to (t \cdot s){:}G)$ *Application*

LP2 $t{:}F \to !t{:}(t{:}F)$ *Proof Checker*

LP3 $s{:}F \to (s+t){:}F, \quad t{:}F \to (s+t){:}F$ *Sum*

LP4 $t{:}F \to F$ *Reflexivity*

Constant Specification CS is a set of formulas

$$\{c_1{:}A_1, c_2{:}A_2, c_3{:}A_3, \ldots\}$$

where each A_i is an axiom and each c_i is a proof constant.

$$\mathsf{LP}_{CS} \quad = \quad \mathsf{LP}_{\emptyset} \; + \; CS.$$

$$\mathsf{LP} \quad = \quad \mathsf{LP}_{CS}, \text{ such that}$$

$$CS = \{c{:}A \mid c \text{ is any constant, } A \text{ is any axiom}\}$$

Each derivation in LP is a derivation in LP_{CS} for some finite constant specification CS.

Internalization (Gödel, Artëmov)

If LP $\vdash F$ *then for some proof polynomial* p, LP $\vdash p{:}F$

Realization of S4 **in the Logic of Proofs** LP **(Artëmov)**:

For each theorem F *of* S4 *one can recover a witness (proof polynomial) for each occurrence of* $\Box$ *in* F *in such a way that the resulting formula* F^r *is derivable in* LP*.*

Realization gives a semantics of proofs for S4**.**

$$\mathsf{S4} \vdash F \quad \Leftrightarrow \quad \exists r\ \mathsf{LP} \vdash F^r$$

Natural semantics of LP **in real proofs**

Interpretation $*$ is determined by

1. a proof formula $\mathit{Proof}(x, y)$ with natural operations on proofs for $\cdot$, $+$, and !;

2. an interpretation of proof variables and constants by numerals;

3. an interpretation of propositional variables by arithmetical sentences.

Interpretation respects Boolean connectives and

$$(p{:}F)^* \quad = \quad \mathit{Proof}(p^*, F^*).$$

Artëmov's arithmetical completeness theorem

LP *specifies all valid logical principles about proofs in its language, i.e., for finite constant specifications* CS,

$$\mathsf{LP}_{CS} \vdash F \text{ } \textit{iff for every} * \textit{respecting } CS, \mathsf{PA} \vdash F^*$$

Joining languages GL **and** LP

Certain principles require a mixture of both provability and explicit proofs, e.g., negative introspection.

Sorcates: "I know nothing except the fact of my ignorance".

Its purely **modal** formulation $\neg\Box F \rightarrow \Box\neg\Box F$ **is not valid** as a provability principle. Indeed, let F be $\bot$. Then $\neg\Box\bot$ reads as *Consis PA* and the whole formula as

$$\textit{Consis PA} \rightarrow \textit{Provable}\ (\textit{Consis PA}),$$

which is false, by Gödel's Second Incompleteness Theorem.

There is no explicit negative introspection either

The principle $\neg x{:}S \to t{:}(\neg x{:}S)$, where x is a proof variable and S is a propositional variable, cannot be valid. Otherwise, fix an interpretation $*$ of x and t and the Goedel proof predicate. Then there are infinitely many arithmetical instances of S for which the antecedent holds. Hence t^* is a proof of infinitely many theorems, which is impossible.

The mixed language of proofs and provability fits negative introspection

The principle

$$\neg x{:}F \to \Box(\neg x{:}F)$$

is arithmetically provable, by Σ-completeness of PA.

Arithmetically complete logics of proofs and provability.

- B (Artëmov, 1994): GL + LP**, no operations on proofs**.
- GrzB (Nogina, 1994): Grz + LP**, no operations on proofs**.
- LPP (Sidon-Yavorskaya, 1997): GL + LP + **extra operations on proofs**.
- GLA (Nogina, 2005): GL + LP.

In this talk we introduce GrzA = Grz + LP

The language of GrzA

Proof polynomials for GrzA are the same as for LP.

Formulas of GrzA are built according to the grammar

$$A = S \mid A \to A \mid A \wedge A \mid A \vee A \mid \neg A \mid \Box A \mid t{:}A \ .$$

Axioms and rules of $\mathsf{GrzA}_\emptyset$:

Axioms and rules of both Grz and LP and

C1 $t{:}F \to \Box F$ *Explicit-Implicit Connection*

C2 $\neg t{:}F \to \Box \neg t{:}F$ *Negative Introspection*

Constant Specification CS for GrzA is defined as the one for LP.

Note that since GrzA has more axioms than LP does, there are more possibilities to specify constants in GrzA than in LP. This makes proof polynomials in GrzA more expressive.

$$\mathsf{GrzA}_{CS} \;=\; \mathsf{GrzA}_{\emptyset} \;+\; CS$$

GrzA is GrzA_{CS} for 'total' CS., i.e.,

$CS = \{c{:}A \mid c \text{ is any constant, } A \text{ is any axiom}\}$

Internalization theorem.

If GrzA $\vdash F$ *then for some proof polynomial* p, GrzA $\vdash p{:}F$.

Proof. Induction on a derivation of F.

Base: F is an axiom. Then use Constant Specification.

In this case, p is a proof constant.

Induction step: by internalized rules of GrzA.

Internalization of Necessitation rule $\vdash F \Rightarrow \vdash \Box F$:

For each F *there is* $t(x)$ *such that* GrzA $\vdash x{:}F \to t(x){:}\Box F$

1. $x{:}F \to \Box F$ - Explicit-Implicit Connection
2. $a{:}(x{:}F \to \Box F)$ - by Constant Specification
3. $x{:}F \to !x{:}(x{:}F)$ - Proof Checker
4. $!x{:}(x{:}F) \to (a{\cdot}!x){:}\Box F$ - from 2, by Application
5. $x{:}F \to (a{\cdot}!x){:}\Box F$ - from 3,4, by propositional logic.

Now put $t(x) = a{\cdot}!x$.

More examples

Positive Introspection: $\mathsf{GrzA}_{\emptyset} \vdash t{:}F \rightarrow \Box(t{:}F)$

1. $t{:}F \rightarrow !t{:}(t{:}F)$ - Proof Checker
2. $!t{:}(t{:}F) \rightarrow \Box(t{:}F)$ - Explicit-Implicit Connection
3. $t{:}F \rightarrow \Box(t{:}F)$ - from 1,2, by propositional logic

Stability of proof assertions: $\mathsf{GrzA}_{\emptyset} \vdash \Box(t{:}F) \vee \Box(\neg t{:}F)$

4. $\neg t{:}F \rightarrow \Box(\neg t{:}F)$ - Negative Introspection
5. $\Box(t{:}F) \vee \Box(\neg t{:}F)$ - from 3,4, by propositional logic

Kripke-style models for $\mathsf{GrzA}_\emptyset$: $\mathcal{M} = (W, \preceq, \mathcal{E}, \Vdash)$.

$(W, \preceq)$ is the usual Grz-frame, i.e.,

- W is a non-empty set of *possible worlds*,
- $\preceq$ is a finite rooted partial order (reflexive, transitive, and antisymmetric) on W.

Evidence relation $\mathcal{E}$ is a relation between proof polynomials and formulas; $\mathcal{E}$ enjoys the following closure properties:

applicaiton: *if* $\mathcal{E}(s, F \to G)$ *and* $\mathcal{E}(t, F)$*, then* $\mathcal{E}(s \cdot t, G)$
sum: *if* $\mathcal{E}(s, F)$ *then* $\mathcal{E}(s + t, F)$ *and* $\mathcal{E}(t + s, G)$
proof checker: *if* $\mathcal{E}(t, F)$ *then* $\mathcal{E}(!t, t{:}F)$

We read $\mathcal{E}(t, F)$ as

t *serves as a possible evidence for* F*.*

Forcing: $\Vdash$ is a forcing relation which is Kripkean on Boolean connectives and modality $\Box$:

- $\Vdash$ respects Boolean connectives at each world ($u \Vdash F \wedge G$ iff $u \Vdash F$ and $u \Vdash G$; $u \Vdash \neg F$ iff $u \nVdash F$, etc.);
- $u \Vdash \Box F$ iff $v \Vdash F$ for every $v \in W$ with $u \prec v$,

and

- $u \Vdash t{:}F$ iff 1. $v \Vdash F$ **for every** $v \in W$,
  2. $\mathcal{E}(t, F)$.

GrzA$_{CS}$-model is a GrzA$_{\emptyset}$-model in which all formulas from a given Constant Specification CS hold.

Kripke soundness and completeness

GrzA$_{CS} \vdash F$ *iff* F *holds in each* GrzA$_{CS}$*-model.*

Example: *For any propositional variable P and proof polynomial t,* GrzA $\nvdash \Box P \rightarrow t{:}P$.

Consider the minimal evidence relation $\mathcal{E}$ that contains

$$\{<c, A> \mid c \text{ is a constant and } A \text{ is an axiom}\}.$$

Note that if $\mathcal{E}(s, F)$, then GrzA $\vdash s{:}F$, Since a propositional variable P is not provable in GrzA, GrzA $\nvdash t{:}P$. Therefore $\mathcal{E}(t, P)$ is false. Consider the singleton GrzA-model $\mathcal{M}$ in which P holds and which has this evidence relation $\mathcal{E}$. Then $\Box P$ holds in $\mathcal{M}$, and $t{:}P$ does not. Hence $\mathcal{M}$ is a countermodel for $\Box P \rightarrow t{:}P$.

Arithmetical interpretation

The union of the intended arithmetical interpretations for Grz and LP. In particular,

$$(\Box G)^* = G^* \wedge \mathit{Provable}\ (G^*);$$
$$(p{:}F)^* \quad = \quad \mathit{Proof}\,(p^*, F^*).$$

An interpretation $*$ is a CS interpretation, if for all $F \in CS$, F^* holds in PA.

Absorbing finite constant specifications

For any finite constant specification CS,

$$\mathsf{GrzA}_{CS} \vdash F \quad \text{iff} \quad \mathsf{GrzA}_{\emptyset} \vdash \bigwedge CS \to F.$$

Finite CS's are sufficient for representing any derivation in GrzA. For any finite CS, arithmetical completeness of $\mathsf{GrzA}_{\emptyset}$ easily extends to GrzA_{CS}. With an infinite CS, GrzA_{CS} can be not arithmetically sound.

Arithmetical Completeness

For any finite constant specification CS,
$\mathsf{GrzA}_{CS} \vdash F$, *iff for each* CS*-interpretation* $*$, $\mathsf{PA} \vdash F^*$.

Hence GrzA specifies the set of all principles of proofs and strong provability in the joint language of Grz and LP. GrzA serves as a useful theoretical prototype of logics of knowledge with justifications.