Provability Logic and the Arithmetics of a Theory

Albert Visser

Theoretical Philosophy, Department of Philosophy,
Faculty of the Humanities, Utrecht University

Special Session on Proof Theory
Logic Colloquium 2012

Thursday, June 12, 2012

Overview

Provability Logic

Solovay's Theorem

An Example

Overview

Provability Logic

Solovay's Theorem

An Example

Overview

Overview

Provability Logic

Solovay's Theorem

An Example

The Logic GL

The Logic GL is the normal modal logic given by the following principles.

G1 $\vdash \phi \ \Rightarrow \vdash \Box\phi$

G2 $\vdash \Box(\phi \rightarrow \psi) \rightarrow (\Box\phi \rightarrow \Box\psi)$

G3 $\vdash \Box\phi \rightarrow \Box\Box\phi$

G4 $\vdash \Box(\Box\phi \rightarrow \phi) \rightarrow \Box\phi$

G3 follows from the other axioms

The logic GL is complete for finite, transitive, irreflexive Kripke Frames.

Degrees of Falsehood

We define:

- $\Box^0 \bot := \bot$,
- $\Box^{n+1} \bot := \Box \Box^n \bot$,
- $\Box^\infty \bot := \top$.

Shavrukov calls these *lies*.

Let a range over $0, 1, \ldots \infty$. GL_a is $\mathrm{GL} + \Box^a \bot$.

Arithmetical Interpretations of GL

Consider any interpretation $N : \mathsf{S}^1_2 \rightarrow U$, where U is Δ^{b}_1-axiomatized. We call N an *arithmetic in U*.

We consider the arithmetical formula giving the axioms of a theory U as part of the data for U. Source and target theory are part of the data for an interpretation.

An arithmetical interpretation of GL in N is a mapping σ from the formulas of GL to the sentences of U, that commutes with the propositional connectives, such that:

- $(\Box\phi)^\sigma := (\Box_U \phi^\sigma)^N := (\mathsf{prov}_U(\underline{\ulcorner \phi^\sigma \urcorner}))^N$.

Universiteit Utrecht

The Provability Logic of a Theory

We define:

- $\phi \in \mathrm{prl}(N)$ iff, for all N-translations σ, $U \vdash \phi^\sigma$,
- $\phi \in \mathrm{prl}_{\mathrm{all}}(U)$ iff, for all arithmetics N in U, $\phi \in \mathrm{prl}(N)$.
- $\deg(N) := \min(\{a \mid \Box^a\bot \in \mathrm{prl}(N)\})$.
- $\deg_{\mathrm{all}}(U) := \min(\{a \mid \Box^a\bot \in \mathrm{prl}_{\mathrm{all}}(U)\})$.

If there are no arithmetics in U, then $\deg_{\mathrm{all}}(U) = 0$.

if $N : \mathrm{S}^1_2 \to U$ is an identical embedding $\mathcal{E}_{\mathrm{S}^1_2, U}$, we speak also of the provability logic $\mathrm{prl}(U)$ of U.

Theorem
GL is always part of $\mathrm{prl}(N)$, for an arbitrary arithmetic N in any theory U.

Universiteit Utrecht

Overview

Provability Logic

Solovay's Theorem

An Example

Solovay's Theorem for Single Arithmetics

Let (N, Γ)-comp be the principle $\vdash A \rightarrow \Box_U A^N$, for A in Γ. Here Γ is a set of arithmetical sentences.

Let $\exists\Pi_1^{\mathrm{b,sent}}$ be the class of all $\exists\Pi_1^{\mathrm{b}}$-sentences.

Solovay's Theorem
Let N be an arithmetic in U such that

$$U \vdash (\mathrm{T}_2^1 + (N, \exists\Pi_1^{\mathrm{b,sent}})\text{-comp})^N.$$

Then $\mathrm{prl}(N) = \mathrm{GL}_{\mathrm{deg}(N)}$.

The proof uses the careful analysis of the Solovay argument due to De Jongh, Jumelet and Montagna.

The substitution instances are disjunctions of conjunctions of $\forall\Delta_1^{\mathrm{b}}$-sentences and $\exists\Pi_1^{\mathrm{b}}$-sentences.

Other Results in the Same Niche 1

Theorem
Suppose U contains a Σ^0_1-sound arithmetic N. Then, there is an arithmetic M in U, such that $\mathrm{prl}(M) = \mathrm{GL}$.

By bootstrapping and by the second incompleteness theorem U interprets $\mathrm{T}^1_2 + \mathrm{incon}(U)$. So, a fortiori, U interprets

$$W := \mathrm{T}^1_2 + \{(K, \exists\Pi^{\mathrm{b,sent}}_1)\text{-comp} \mid K \text{ is an arithmetic in } U\}.$$

Since, U contains a Σ^0_1-sound arithmetic, by results of Per Lindström, we can find a faithful interpretation M of W. Since W is a true theory, it follows that $\mathrm{prl}(M) = \mathrm{GL}$.

Universiteit Utrecht

Other Results in the Same Niche 2

Theorem
Suppose A is a finitely axiomatized sequential theory. Then, there is an arithmetic M in A, such that $\mathrm{prl}(M) = \mathrm{GL}$.

By results of Harvey Friedman and, independently, Jan Krajíček, the theory A contains a Σ^0_1-sound arithmetic.

Other Results in the Same Niche 3

The theory CFL is introduced by A. Cordón-Franco, A. Fernández-Margarit and F. F. Lara-Martin as an axiomatization of the boole(Σ_1)-consequences both of $\mathrm{I}\Pi_1^-$ and of EA.

CFL is $\mathrm{I}\Delta_0$ plus

- $\vdash \exists x\, S_0(x) \rightarrow \exists x\, \exists y\, (2^x = y \wedge S_0(x))$.

where S_0 is $\Sigma_1(x)$.

CFL is incomparable with S^1_2. If we replace S^1_2 by CFL in our definition of arithmetic, we get Solovay's full theorem.

The theory CFL is locally interpretable in Q but not globally interpretable.

Great Open Problems

- What is the provability logic of S^1_2?
- What is the provability logic of $\mathsf{S}^1_2 + \exists\Pi_1^{b,\mathrm{sent}}$-comp?
- What is the provability logic of T^1_2?
- What is the provability logic of $\mathsf{S}_2 = \mathrm{I}\Delta_0 + \Omega_1$?

Verbrugge and Razborov:
If $\mathsf{S}^1_2 \vdash \exists\Pi_1^{b,\mathrm{sent}}$-comp, then $\mathsf{NP} \cap \text{co-}\mathsf{NP} = \mathsf{P}$.

Universiteit Utrecht

The Initial Arithmetic Ordering

Consider arithmetics N and M in U. We define $N \preceq M$ if there is a U-definable and U-verifiable initial embedding F of N in M.

A theory U is *sequential* if it has good sequence coding.

Theorem (Pudlák-Dedekind)
Suppose U is sequential. Then, for all arithmetics N and M in U, there is an arithmetic K in U such that $K \preceq N$ and $K \preceq M$.

Theorem (Visser)
Consider a finite set of Σ^0_1-sentences $\mathcal{S}$, a theory U and an arithmetic N in U. Then, there is an arithmetic $M \preceq N$, such that

$$U \vdash (\mathrm{T}^2_1 + \mathcal{S}\text{-comp})^M.$$

Solovay's Theorem for All Arithmetics of a Given Theory

Theorem
Consider any theory U. We have: $\mathrm{prl}_{\mathrm{all}}(U) = \mathrm{GL}_{\mathrm{deg}_{\mathrm{all}}(U)}$.

The proof uses the previous theorem in combination with the work of De Jongh, Jumelet and Montagna.

The theorem also works when U does not contain any arithmetic.

Overview

The Example

Suppose A is a finitely axiomatized sequential theory. We consider the theory:

- $W := A + \{(\Box_A^{\# N}\bot)^N \mid N \text{ is an arithmetic in } A\}$.

WARNING: sloppy formulation.

We have:

- $\mathrm{deg}_{\mathrm{all}}(W) = \infty$,
- for any arithmetic N in W, $\mathrm{deg}(N) < \infty$.
- The predicate logic of W is complete Π^0_2.
- $A \not\rhd W$, $A \rhd_{\mathrm{mod}} W$.

The Lemma 1

Consider a sequential sentence A.

- N is Σ^0_1*-veracious in* A iff

$$\mathrm{S}^1_2 \vdash \forall S \in \Sigma^0_1\text{-sent}\,(\Box_A S^N \to \Box_{\mathrm{S}^1_2}(\mathrm{con}_{\rho(A)}(A) \to S)).$$

  So Σ^0_1-veracity is the S^1_2-verifiable Σ^0_1-conservativity of N over $\mathrm{ID}_{\mathrm{S}^1_2+\mathrm{con}_{\rho(A)}(A)}$.
- N is *strong in* A iff $A \vdash \mathrm{con}^N_{\rho(A)}(A)$.
- N is *deep in* A iff N is both Σ^0_1-veracious and strong in A.

Theorem
Suppose that A is a sequential sentence and N is Σ^0_1-veracious in A. Then,

$$\mathrm{I}\Delta_0 + \mathrm{supexp} \vdash \forall S \in \Sigma^0_1\text{-sent}\,((\mathrm{con}(A) \wedge \Box_A S^N) \to \mathrm{true}(S)).$$

Here true is a Σ^0_1 truth predicate.

The Lemma 2

Theorem
Suppose N is a deep arithmetic in A. We have:

$$\mathrm{S}^1_2 \vdash \forall S \in \Sigma^0_1\text{-sent}\,(\Box_A S^N \leftrightarrow \Box_{\mathrm{S}^1_2}(\mathrm{con}_{\rho(A)}(A) \rightarrow S)).$$

Theorem
Both Σ^0_1-veracity and strength are downwards closed w.r.t. $\preceq$.

Theorem
For every arithmetic N in A, there is a deep arithmetic M in A with $M \preceq N$.

Theorem
Suppose N is Σ^0_1-veracious in A. We have:

$$\mathrm{S}^1_2 \vdash \Box_A \Box^{N,n}_A \bot \leftrightarrow \Box^n_{\mathrm{S}^1_2} \Box_A \bot.$$

Strange but True

Suppose N is a deep arithmetic in GB. Then, (suppressing the von Neumann interpretation):

$$\mathrm{GB} + \mathrm{con}(\mathrm{GB}) \vdash \mathrm{con}(\mathrm{GB} + \mathrm{con}^N(\mathrm{GB})).$$

This is *not* an example of a theory proving its own consistency! We *do* have:

$$\mathrm{GB} + \mathrm{con}(\mathrm{GB}) \nvdash \mathrm{con}^N(\mathrm{GB} + \mathrm{con}(\mathrm{GB})).$$

and:

$$\mathrm{GB} + \mathrm{con}^N(\mathrm{GB}) \nvdash \mathrm{con}^N(\mathrm{GB} + \mathrm{con}^N(\mathrm{GB})).$$