Provability Logics and Applications
Day 1
Provability as modality

David Fernández Duque[1] and Joost J. Joosten[2]

1: Universidad de Sevilla;
2: Universitat de Barcelona

Monday 13-08-2012
ESSLLI Tutorial, Opole

What is provability logic?

Idea: Given a formal theory T over a language L, we interpret $\Box\phi$ as

"ϕ is provable in T".

In symbols we write $T \vdash \phi$.

This interpretation of modal logic was first suggested by Kurt Gödel.

It can be used to reason about Gödel's famous incompleteness theorems.

Some history: 1930s

Gödel suggests that provability may be seen as an interpretation of modal logic: $\Box\phi \equiv$ "ϕ is provable"

Some history: 1930s

Gödel suggests that provability may be seen as an interpretation of modal logic: $\Box\phi \equiv$ "ϕ is provable"

- $\vdash \phi \leftrightarrow \neg\Box\phi$: Liar paradox

Some history: 1930s

Gödel suggests that provability may be seen as an interpretation of modal logic: $\Box\phi \equiv$ "ϕ is provable"

- $\vdash \phi \leftrightarrow \neg\Box\phi$: Liar paradox
- $\Diamond\top \to \Diamond\Box\bot$: Second incompleteness theorem

Some history: 1950s

Henkin asks, “What can we say about formulas that assert their own provability”?

Truth-teller paradox: $\phi \leftrightarrow \Box\phi$

Some history: 1950s

Henkin asks, “What can we say about formulas that assert their own provability”?

Truth-teller paradox: $\phi \leftrightarrow \Box\phi$

Löb answers Henkin’s question (they are themselves derivable) and gives basic modal-like axioms for a provability predicate

Some history: 1950s

Henkin asks, “What can we say about formulas that assert their own provability”?

Truth-teller paradox: $\phi \leftrightarrow \Box\phi$

Löb answers Henkin’s question (they are themselves derivable) and gives basic modal-like axioms for a provability predicate

Löb’s rule: $\dfrac{\Box\phi \to \phi}{\phi}$

Some history: 1960s-1970s

1963 Smiley formulates the modal version of Löb's axiom: $\Box(\Box\phi \to \phi) \to \Box\phi$ in a paper about ethics!

Some history: 1960s-1970s

1963 Smiley formulates the modal version of Löb's axiom: $\Box(\Box\phi \to \phi) \to \Box\phi$ in a paper about ethics!

1971 Segerberg proves Kripke completeness.

Some history: 1960s-1970s

1963 Smiley formulates the modal version of Löb's axiom: $\Box(\Box\phi \to \phi) \to \Box\phi$ in a paper about ethics!

1971 Segerberg proves Kripke completeness.

1975 De Jongh and Sambin proved the fixpoint theorem:

Some history: 1960s-1970s

1963 Smiley formulates the modal version of Löb's axiom: $\Box(\Box\phi \to \phi) \to \Box\phi$ in a paper about ethics!

1971 Segerberg proves Kripke completeness.

1975 De Jongh and Sambin proved the fixpoint theorem:

If p appears only “boxed” in $\psi(p)$ then

$$\exists\phi \mathsf{GL} \vdash \phi \leftrightarrow \psi(\phi)$$

Some history: The arithmetical completeness theorem

Kripke completeness is useful, but is provability logic complete for its intended interpretation?

$$\Box\phi \mapsto \text{“PA} \vdash \phi\text{”}$$

Some history: The arithmetical completeness theorem

Kripke completeness is useful, but is provability logic complete for its intended interpretation?

$$\Box\phi \mapsto \text{“PA} \vdash \phi\text{”}$$

In 1976, Solovay proves completeness for the arithmetical interpretation of provability logic.

Some history: The arithmetical completeness theorem

Kripke completeness is useful, but is provability logic complete for its intended interpretation?

$$\Box\phi \mapsto \text{“PA} \vdash \phi\text{”}$$

In 1976, Solovay proves completeness for the arithmetical interpretation of provability logic.

$$\mathrm{GL} \vdash \phi \Leftrightarrow \forall f\big(\mathbb{N} \models f(\phi)\big)$$

Some history: 1980s

1981 Esakia proposes the topological derived-set semantics.

Some history: 1980s

1981 Esakia proposes the topological derived-set semantics.

1985 Abashide shows that GL is complete for its topological interpretation on any ordinal $\geq \omega^\omega$

Some history: 1980s

1981 Esakia proposes the topological derived-set semantics.

1985 Abashide shows that GL is complete for its topological interpretation on any ordinal $\geq \omega^\omega$

1986 Japaridze proposes a polymodal version of provability logic.

Some history: 1980s

1981 Esakia proposes the topological derived-set semantics.

1985 Abashide shows that GL is complete for its topological interpretation on any ordinal $\geq \omega^\omega$

1986 Japaridze proposes a polymodal version of provability logic.

No Kripke models!

Some history: 1990s

1990 Blass shows that it is consistent with standard set theory that GL_2 has no non-trivial canonical ordinal models.

Some history: 1990s

1990 Blass shows that it is consistent with standard set theory that GL_2 has no non-trivial canonical ordinal models.

More recently,

- Beklemishev showed that it is also consistent that GLP_2 is complete for its canonical ordinal models

Some history: 1990s

1990 Blass shows that it is consistent with standard set theory that GL_2 has no non-trivial canonical ordinal models.

More recently,

- Beklemishev showed that it is also consistent that GLP_2 is complete for its canonical ordinal models
- Bagaria has related existence of non-trivial ordinal models of GLP_n to a family of large cardinal axioms.

Some history: 1990s

1990 Blass shows that it is consistent with standard set theory that GL_2 has no non-trivial canonical ordinal models.

More recently,

- Beklemishev showed that it is also consistent that GLP_2 is complete for its canonical ordinal models
- Bagaria has related existence of non-trivial ordinal models of GLP_n to a family of large cardinal axioms.

1993 Ignatiev gives Kripke models for the closed fragment.

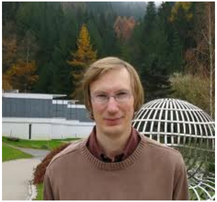
Some history: Ordinal analysis

Gödel's provability logic does not distinguish well between reasonably strong formal theories, but Japaridze's extension does.

Some history: Ordinal analysis

Gödel's provability logic does not distinguish well between reasonably strong formal theories, but Japaridze's extension does.

In 2004, Lev Beklemishev showed how Japaridze's system GLP_ω can be used to give an ordinal analysis of Peano Arithmetic.



Some history: Recent times

2005 Beklemishev proposes extending to GLP_Λ, which uses transfinite modalities.

Some history: Recent times

2005 Beklemishev proposes extending to GLP_Λ, which uses transfinite modalities.

2009 Icard defines topological models of the closed fragment.

Some history: Recent times

2005 Beklemishev proposes extending to GLP_Λ, which uses transfinite modalities.

2009 Icard defines topological models of the closed fragment.

2011 Beklemishev and Gabelaia prove topological completeness for GLP_ω

Present and future

We have been generalizing many of these results to GLP_Λ.

- Ignatiev models
- Icard topologies
- Fixpoint theorem
- …

With this we hope to use provability logics to analyze stronger and stronger theories.

Basic ingredients

We will need:

1. A formal language L to speak about arithmetic.
2. A formal theory T that reasons about arithmetic
3. A provability predicate $\mathtt{Prv}_T$ which talks about provability within L
4. A modal logic where $\Box \approx \mathtt{Prv}_T$

Arithmetic languages

An arithmetic interpretation of a first- or higher-order language L is an L-model $\mathfrak{N} = \langle \mathbb{N}, I \rangle$ such that:

- there is an L-term $\mathtt{0}$ with $I(\mathtt{0}) = 0$
- there is a unary function symbol S such that for all $n \in \mathbb{N}$, $I(\overline{n}) = n$, where

$$\overline{n} = \underbrace{\mathtt{SS}\ldots\mathtt{S}}_{n}\mathtt{0}$$

- there are binary function symbols $\mathtt{plus}$, $\mathtt{times}$, $\mathtt{exp}$ such that, given $n, m \in \mathbb{N}$,
  - $I\big(\mathtt{plus}(\overline{n}, \overline{m})\big) = n + m$
  - $I\big(\mathtt{times}(\overline{n}, \overline{m})\big) = n \times m$
  - $I\big(\mathtt{exp}(\overline{n}, \overline{m})\big) = n^m$

  We will usually write $\mathbb{N} \models \phi$ instead of $\mathfrak{N} \models \phi$.

The arithmetic hierarchy

A bounded quantifier is one of the form $\forall x(x < t \to \phi)$ or $\exists x(x < t \wedge \phi)$.

A formula ϕ is elementary or Δ_0 if all quantifiers appearing in ϕ are bounded.

Then, define by induction:

- $\Pi_0 = \Sigma_0 = \Delta_0$
- if $\phi \in \Sigma_n$ then $\forall x_0 \forall x_1 \ldots \forall x_m \phi \in \Pi_{n+1}$
- if $\phi \in \Pi_n$ then $\exists x_0 \exists x_1 \ldots \exists x_m \phi \in \Sigma_{n+1}$

Fact: Every first-order formula is provably equivalent in FOL to either a Π_n-formula or a Σ_n-formula.

Sequences are numbers too

Any finite sequence of numbers

$$n_1, n_2, \ldots n_k$$

can itself be represented as a natural number.

There are many ways to do this:

- use binary and twos as commas
- products of prime powers
- using the Chinese remainder theorem

The representation can be picked so there are formulas

- $\mathrm{seq}(x)$ expressing "x represents a sequence"
- $\mathrm{len}(x, y)$ expressing "y is the length of x"
- $\mathrm{entry}(x, y, z)$ expressing "y is the z^{th} entry of x"

Gödel numbers

A Gödel numbering is an assignment $\phi \mapsto \ulcorner\phi\urcorner$ mapping an L-formula to a natural number.

This allows us to reason about formal languages within arithmetic.

Trick:

1. Enumerate all symbols
2. View formulas as sequences of symbols

Substitution

Many standard syntactic operations are primitive recursive and hence can be represented by a Δ_0 formula.

Proposition

In any arithmetical language L *there is a* Δ_0 *formula* $\mathtt{subs}(\mathtt{w}, \mathtt{x}, \mathtt{y}, \mathtt{z})$ *such that for all tuples of natural numbers* a, b, n, m*,*

$$\mathbb{N} \models \mathtt{subs}(\overline{a}, \overline{b}, \overline{n}, \overline{m})$$

if and only if there is is a formula α*, a term* t *and a variable* v *with*

$$a = \ulcorner \alpha \urcorner \qquad n = \ulcorner t \urcorner \qquad m = \ulcorner v \urcorner$$

and

$$b = \ulcorner \alpha[x/t] \urcorner.$$

Formal theories

A formal theory T is usually presented as a family of *rules* and *axioms*.

Definition

A derivation of ϕ is a sequence $\langle \phi_0, \dots \phi_N \rangle$ such that $\phi_N = \phi$ and each ϕ_n is either an axiom or follows by the rules from $\phi_0, \dots, \phi_{n-1}$.

If ϕ is derivable in T we write $T \vdash \phi$.

All theories will be assumed closed under generalization and modus ponens:

$$\frac{\phi}{\forall x \phi} \qquad \frac{\phi \qquad \phi \to \psi}{\psi}$$

Arithmetic theories

L is an arithmetically interpreted language, T is a theory over L.

Definition

The theory T is arithmetically sound if whenever T $\vdash \phi$, $\mathbb{N} \models \phi$
The theory T is arithmetically complete if, whenever $\mathbb{N} \models \phi$, T $\vdash \phi$.

There are also relative versions of these notions. For example, if Γ is a set of formulas, *T* is Γ-sound if every theorem of *T* that also belongs to Γ is true.

We will be mainly interested in arithmetically sound theories.

Peano arithmetic

Abbreviated PA, it is axiomatized by FOL and:

- $\forall \mathtt{x}(\mathtt{x} = \mathtt{x})$
- $\forall \mathtt{x} \forall \mathtt{y} \forall \mathtt{z}(\mathtt{x} = \mathtt{y} \wedge \mathtt{y} = \mathtt{z} \to \mathtt{x} = \mathtt{z})$
- $\forall \mathtt{x} \forall \mathtt{y}(\mathtt{x} = \mathtt{y} \leftrightarrow \mathtt{Sx} = \mathtt{Sy})$
- $\neg \exists \mathtt{x}(\mathtt{0} = \mathtt{Sx})$
- $\forall \mathtt{x}\, \mathtt{sum}(\mathtt{x}, \mathtt{0}) = \mathtt{x}$
- $\forall \mathtt{x} \forall \mathtt{y}(\mathtt{sum}(\mathtt{x}, \mathtt{Sy}) = \mathtt{S}(\mathtt{sum}(\mathtt{x}, \mathtt{y})))$
- $\forall \mathtt{x}\, \mathtt{times}(\mathtt{x}, \mathtt{0}) = \mathtt{0}$
- $\forall \mathtt{x} \forall \mathtt{y}\, \mathtt{times}(\mathtt{x}, \mathtt{Sy}) = \mathtt{sum}(\mathtt{times}(\mathtt{x}, \mathtt{y}), \mathtt{x})$
- $\forall \mathtt{x}\, \mathtt{exp}(\mathtt{x}, \mathtt{0}) = \mathtt{S0}$
- $\forall \mathtt{x} \forall \mathtt{y}\, \mathtt{exp}(\mathtt{x}, \mathtt{Sy}) = \mathtt{times}(\mathtt{exp}(\mathtt{x}, \mathtt{y}), \mathtt{x})$

Induction: $\phi(\mathtt{0}) \wedge \forall \mathtt{x}(\phi(\mathtt{x}) \to \phi(\mathtt{Sx})) \to \forall \mathtt{x} \phi(\mathtt{x})$.

Elementarily presented theories

Reasonable requirement: Proofs are checkable.

Better: Easy to check.

Checkable	$\approx$	Σ_1	$=$	recursively enumerable.
Easy to check	$\approx$	Δ_0	$=$	elementarily presented.

Craig's trick: If the axioms and rules of T are Σ_1-definable, then there is an elementarily presented family of axioms and rules which give the same theorems as T.

Provability predicates

Derivations are sequences of formulas so they can be assigned Gödel numbers too, which allows us to study logic within any arithmetically interpreted language.

Proposition (Gödel)

If T is elementarily presented there is a Δ_0-formula $\mathtt{prv}_T(\mathtt{x},\mathtt{y})$ such that for all $n, m \in \mathbb{N}$, $\mathbb{N} \models \mathtt{prv}_T(\overline{n}, \overline{m})$ if and only if there is a derivation d of a formula ϕ with $n = \ulcorner \phi \urcorner$ and $m = \ulcorner d \urcorner$.

With this we can define

- ϕ is provable in T:

$$\mathtt{Prv}_T(x) := \exists \mathtt{y}\, \mathtt{prv}_T(x, y).$$

- T is consistent:

$$\mathtt{Cons}(T) := \neg \mathtt{Prv}_T(\overline{\ulcorner \mathtt{0} = \mathtt{S0} \urcorner})$$

Self-reference in natural language

Self-reference often leads to paradox:

- This sentence is false.
- The smallest number not definable with ten words or less.
- The result of substituting this sentence for x in "The sentence "x" is true" is false.

Fortunately, this is impossible to do directly in arithmetic.

Indirect self-reference

Gödel numbers do lead to an indirect version of self-reference:

1. There are infinitely many prime numbers.
2. Every number has a unique sucessor.
3. Two plus two is five.

⋮

1000. Sentence 1000 is not provable.

This type of self-reference is available in arithmetic.

The fixpoint lemma

Proposition

Given an arithmetic formula $\psi(\mathrm{n}, \vec{\mathrm{x}})$*, there exists a formula* ϕ *such that*

$$T \vdash \forall \vec{\mathrm{x}} \big(\phi \leftrightarrow \psi(\overline{\ulcorner \phi \urcorner}, \vec{\mathrm{x}}) \big)$$

for every sound and sufficiently strong arithmetic theory T*.*

Theorem (First incompleteness theorem)

No elementarily presentable theory is arithmetically sound and complete.

Theorem (First incompleteness theorem)

No elementarily presentable theory is arithmetically sound and complete.

Theorem (Second incompleteness theorem)

If an elementarily presentable theory T is arithmetically sound and provably Σ_1-complete, then

$$T \nvdash \mathtt{Cons}(T).$$