A bird's eye view on the logic of provability

Rineke Verbrugge, Institute of Artificial Intelligence, University of Groningen

Annual Meet on Logic and its Applications, Calcutta Logic Circle, Kolkata,
September 3, 2011

Overview

- Some pre-history of provability logic: foundations of arithmetic
- Syntax and semantics of provability logic
- Modal soundness and completeness: syntax $\equiv$ semantics
- Solovay's arithmetical completeness theorem:
  provability logic $\equiv$ provability fragment of Peano Arithmetic
- Löb's Theorem and Gödel's Second Incompleteness Theorem
- Intermezzo: Löb's paradox - prove anything you want!
- Later developments in provability logic
- Material for this talk is based on:
  Rineke Verbrugge, Provability logic, Stanford Encyclopedia of Philosophy, Ed Zalta (ed.), Winter edition 2010.

Historical developments in foundations of mathematics

- 1889 Peano defines a formal language for arithmetic.
- 1893 Frege publishes Grundgesetze der Arithmetik.
- 1901 Russell shows that Frege's system is inconsistent: the "set of all sets A that are not a member of A" leads to Russell's Paradox.
- 1910 Russell and Whitehead publish Principia Mathematica, aiming to provide solid logical foundations for mathematics, even reducing mathematics to logic.
- 1920s Hilbert's Program: Aimed at formalization of all of mathematics in axiomatic form, together with a 'finitistic' proof that this axiomatization of mathematics is consistent.

Historical developments, continued

- 1931-1932 Gödel gave a blow to Hilbert's Program by proving two incompleteness theorems.

David Hilbert (Köningsberg, 1862 - Göttingen, 1942)

Historical developments, continued

On these and related developments, read Doxiadis, Papadimitriou, Papadatos and Di Donna, Logicomix: An epic search for truth.

Russell about the set of all sets that do not contain themselves as a member.

Peano Arithmetic (1889)

The language of Peano Arithmetic contains 0, S, $+$, $\cdot$, $=$ and $\leq$.

Axioms:

$\forall x(\neg(Sx = 0))$

$\forall x \forall y(Sx = Sy \rightarrow x = y)$

$\forall x(x \neq 0 \rightarrow \exists y(y = Sx))$

$\forall x(x + 0 = x)$

$\forall x \forall y(x + Sy = S(x + y))$

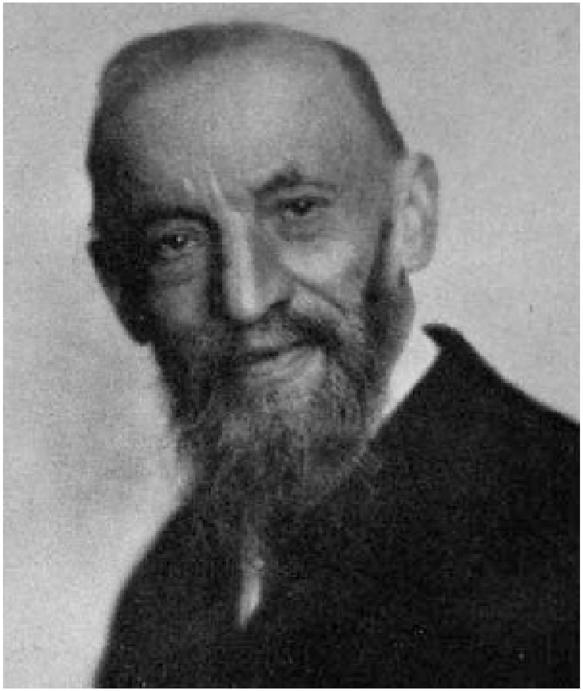
$\forall x(x \cdot 0 = 0)$

$\forall x \forall y(x \cdot Sy = (x \cdot y) + x)$

$\forall x \forall y(x \leq y \leftrightarrow \exists z(z + x = y))$

$(A(0) \wedge \forall x(A(x) \rightarrow A(Sx))) \rightarrow \forall x A(x)$ (Induction scheme)

Giuseppe Peano (Spinetta 1858 - Torino 1932)



The author of Formulario Mathematico in 1930

Gödel's meta-mathematics of Peano Arithmetic

Gödel (1931) arithmetized the formal arithmetic given in Principia Mathematica. The procedure works similarly for Peano Arithmetic.

Gödel numbering of formulas

Gödel assigned natural number to each symbol in the language of PA.

Given sequence $x_1 x_2 \ldots, x_n$ of positive integers, the Gödel encoding of the sequence is the product of the first n primes raised to the corresponding values in the sequence:

$$\mathrm{enc}(x_1 x_2 x_3 \ldots x_n) = 2^{x_1} \cdot 3^{x_2} \cdot 5^{x_3} \cdots p_n^{x_n}$$

Because any such number can be uniquely factored into prime factors, it is possible to recover the original sequence from its Gödel number.

Let $\ulcorner A \urcorner$ denote the Gödel number of arithmetical formula A, seen as sequence of symbols.

Gödel numbering of formulas and proofs

Example formula: Let the Gödel number for symbol "0" be 6, and let the Gödel number for "=" be 5. Then $\ulcorner 0 = 0 \urcorner$ is $2^6 \cdot 3^5 \cdot 5^6$.

A proof in PA is a sequence of formulas $A_1 A_2 \ldots A_m$. It can be encoded by taking Gödel numbers of the formulas, and making the Gödel encoding of the sequence: $2^{\ulcorner A_1 \urcorner} \cdot 3^{\ulcorner A_2 \urcorner} \cdot \ldots \cdot p_m^{\ulcorner A_m \urcorner}$

Gödel constructed a formalized proof predicate *Proof* of Peano Arithmetic.

Proof(y, x) stands for "Gödel number y codes a correct proof from the axioms of Peano Arithmetic of the formula with Gödel number x".

Then he constructed *Prov*(x), the formalized provability predicate for Peano Arithmetic, namely $\exists y \mathit{Proof}\,(y, x)$.

Kurt Gödel (Brno 1906 - Princeton 1978)

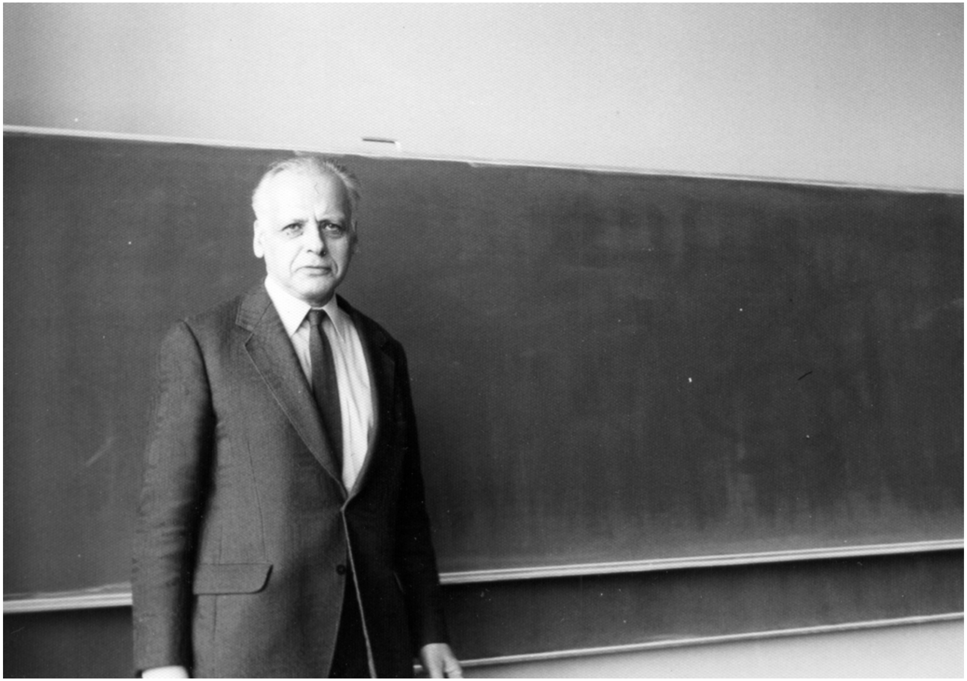
Löb's three derivability conditions

In 1955, Löb formulated three conditions on the provability predicate of Peano Arithmetic. Derivability of A from Peano Arithmetic is denoted by $PA \vdash A$:

1. If $PA \vdash A$, then $PA \vdash \mathit{Prov}(\ulcorner A \urcorner)$;
2. $PA \vdash \mathit{Prov}(\ulcorner A \to B \urcorner) \to (\mathit{Prov}(\ulcorner A \urcorner) \to \mathit{Prov}(\ulcorner B \urcorner))$;
3. $PA \vdash \mathit{Prov}(\ulcorner A \urcorner) \to \mathit{Prov}(\ulcorner \mathit{Prov}(\ulcorner A \urcorner) \urcorner)$.

These Löb conditions cry out for a modal logical investigation, where the modality $\Box$ stands for provability in PA.
Löb used them to prove that $\mathit{Prov}(\ulcorner A \urcorner) \to A$ can only be proved in PA in the trivial case that PA already proves A itself.

Martin Löb (Berlin 1921-Annen 2006)



As professor at the University of Amsterdam, 1978

Propositional provability logic: language

The logical language of propositional provability logic contains propositional atoms and the usual truth-functional operators $\wedge, \vee, \neg, \rightarrow, \leftrightarrow$, as well as the contradiction symbol $\bot$.

New is a modal operator $\Box$ with intended meaning
"is provable in T,"
where T is a sufficiently strong formal theory,
let us say Peano Arithmetic (PA).

Axioms and rules of propositional provability logic

Propositional provability logic is often called GL, after Gödel and Löb. The logic GL contains the axioms:

- All instantiations of propositional tautologies; for example, $\Box p \rightarrow \Box p$ is such an instantiation
- $\Box(A \rightarrow B) \rightarrow (\Box A \rightarrow \Box B)$
  (Distribution, corresponds to second derivability condition)
- $\Box A \rightarrow \Box\Box A$
  (Corresponds to third derivability condition)
- $\Box(\Box A \rightarrow A) \rightarrow \Box A$
  (Löb's axiom)

Axioms and rules of propositional provability logic, contd.

Furthermore, GL is closed under the following rules:

- If GL $\vdash A \rightarrow B$ and GL $\vdash A$, then GL $\vdash B$ (modus ponens)
- if GL $\vdash A$, then GL $\vdash \Box A$
  (Generalization; corresponds to first derivability condition)

NB It is in general not the case that GL $\vdash A \rightarrow \Box A$!

The notion GL $\vdash A$ denotes provability of a modal formula A in propositional provability logic.

Possible worlds semantics

A possible worlds model (or Kripke model) is a triple $M = \langle W, R, V\rangle$, where W is a set of possible worlds, R is a binary accessibility relation on W, and V is a valuation that assigns a truth value (0 or 1) to each propositional variable for each world in W.

The notion of truth of a formula A in a model M at a world $w \in W$, notation $M, w \models A$, is defined inductively:

- $M, w \models p$ iff $V_w(p) = 1$
- $M, w \models A \wedge B$ iff $M, w \models A$ and $M, w \models B$
- $M, w \models \neg A$ iff not $M, w \models A$
- (Similarly for $\vee$, $\longrightarrow$, and $\leftrightarrow$)
- $M, w \models \Box A$ iff for every v, if wRv, then $M, v \models A$

Modal soundness and completeness of GL

Krister Segerberg proved in 1971 that GL is sound and complete with respect to Kripke models on finite transitive irreflexive trees.

Soundness:
If GL $\vdash A$,
then for all Kripke models $M = \langle W, R, V\rangle$ with finite W on which R is a transitive irreflexive tree, and for all $w \in W$,
it holds that $M, w \models A$.

Completeness:
If for all Kripke models $M = \langle W, R, V\rangle$ with finite W on which R is a transitive irreflexive tree, and for all $w \in W$, it holds that $M, w \models A$,
then GL $\vdash A$.

Decidability of GL

The modal soundness and completeness theorems give rise to a decision procedure to check in a finite time for any modal formula A whether A follows from GL or not:

Enumerate all GL-proofs: $P_1, P_2, P_3 \ldots$ and
enumerate all Kripke models on finite transitive irreflexive trees: M_1, M_2, M_3 .

Check alternately for $i = 1, 2, \ldots$:
Is A the conclusion of P_i?
If not, does A have a counter-model on model M_i?
Stop as soon as you find a positive answer.

Decidability of GL in PSPACE

More precisely, GL is decidable in computational complexity class PSPACE: there is a Turing machine that, given a formula A as input, answers whether A follows from GL or not. The size of the needed memory is only polynomial in the length of A.

This procedure works by methodically constructing a semantic tableau: a possible counter-model against A, on a finite tree.

Arithmetical soundness and completeness

GL is an adequate modal logic for Peano Arithmetic:
GL proves everything about provability that can be expressed in a propositional modal language and can be proved in PA.

More precisely: Let a translation be a function f that assigns to each propositional atom of modal logic a sentence of arithmetic, where:

- $f(\bot) = (0 = 1)$
- $f(A \wedge B) = f(A) \wedge f(B)$ (and f similarly respects $\vee, \neg, \rightarrow, \leftrightarrow$)
- $f(\Box A) = Prov(\ulcorner f(A) \urcorner)$

Solovay's arithmetical completeness theorem (1976)
GL $\vdash A$ iff for all translations f, PA $\vdash f(A)$

Robert Solovay (1938 -)

Solavay in 1972

Arithmetical soundness, part 2: Diagonalization

Gödel's Diagonalization lemma
For any arithmetical formula $C(x)$ there is an arithmetical formula B such that:

$$\mathrm{PA} \vdash B \leftrightarrow C(\ulcorner B \urcorner)$$

Formula B says "I have property C." (Self-reference)

For Gödel's First Incompleteness Theorem, one uses a formula B with:

$$\mathrm{PA} \vdash B \leftrightarrow \neg \mathit{Prov}(\ulcorner B \urcorner),$$

"I am not provable from PA". It turns out that B is not provable in PA, and is therefore true in the standard model.

Arithmetical soundness, part 3: Löb's Theorem

Löb's theorem

Suppose that PA $\vdash Prov(\ulcorner A \urcorner) \rightarrow A$, then PA $\vdash A$.

Proof By the Diagonalization lemma, there is a formula B such that

PA $\vdash B \leftrightarrow (Prov(\ulcorner B \urcorner) \rightarrow A)$.

From this it follows by Löb's first and second derivability conditions plus some propositional reasoning that:

PA $\vdash Prov(\ulcorner B \urcorner) \rightarrow Prov(\ulcorner Prov(\ulcorner B \urcorner) \rightarrow A \urcorner)$.

Thus, again by Löb's second condition,

PA $\vdash Prov(\ulcorner B \urcorner) \rightarrow (Prov(\ulcorner Prov(\ulcorner B \urcorner) \urcorner) \rightarrow Prov(\ulcorner A \urcorner))$.

Arithmetical soundness, part 4: Löb's Theorem, cntd.

So far, PA $\vdash \mathit{Prov}(\ulcorner B \urcorner) \rightarrow (\mathit{Prov}(\ulcorner \mathit{Prov}(\ulcorner B \urcorner) \urcorner) \rightarrow \mathit{Prov}(\ulcorner A \urcorner))$.

On the other hand, Löb's third condition gives:

PA $\vdash \mathit{Prov}(\ulcorner B \urcorner) \rightarrow \mathit{Prov}(\ulcorner \mathit{Prov}(\ulcorner B \urcorner) \urcorner)$, thus

PA $\vdash \mathit{Prov}(\ulcorner B \urcorner) \rightarrow \mathit{Prov}(\ulcorner A \urcorner)$.

Together with the assumption that
PA $\vdash \mathit{Prov}(\ulcorner A \urcorner) \rightarrow A$, this gives
PA $\vdash \mathit{Prov}(\ulcorner B \urcorner) \rightarrow A$.

Finally, the equation produced by Diagonalization implies that
PA$\vdash B$, so PA $\vdash \mathit{Prov}(\ulcorner B \urcorner)$, thus, applying Modus Ponens,

PA $\vdash A$, as desired. QED

Intermezzo: Löb's paradox - proving any A you want

Let A be any sentence (for example, of Peano Aritmetic). Let B be the sentence "If B is true, then A". Now we reason as follows:

1 B is true (assumption)

2 If B is true, then A (by definition of B)

3 A (from 1 and 2, by modus ponens)

So we proved that 3 follows from assumption 1. But that means that we derive, without any assumption:

4 If B is true, then A

5 B is true (4 is just what B says!)

6 A (from 4 and 5, by modus ponens)

What’s wrong in the “proof” of Löb’s paradox?

It seems to use diagonalization for a formalized Truth predicate such that $\mathit{True}(x)$ stands for “Gödel number x codes a sentence of PA that is true in the standard model”.

But such a formalized Truth predicate cannot exist, as Tarski proved in his undefinability theorem (1936):

There is no PA-formula $\mathit{True}(\mathrm{x})$ such that for every PA-formula A, $\mathit{True}(\ulcorner A \urcorner)$ iff A is true in the standard model.

Proof idea: Reductio ad absurdum. Suppose such a Truth predicate True does exist. By diagonalization, there is a B such that
$PA \vdash B \leftrightarrow \neg \mathit{True}(\ulcorner B \urcorner)$, but then
$B \leftrightarrow \neg \mathit{True}(\ulcorner B \urcorner)$ should be true in the standard model. But if True were a truth predicate, we would have that $B \leftrightarrow \mathit{True}(\ulcorner B \urcorner)$ should be true in the standard model - contradiction.

Proof of Gödel's Second Incompleteness Theorem

Gödel's Second Incompleteness Theorem says:

If PA is consistent, then PA cannot prove its own consistency.

Formally:

Gödel's Second Incompleteness Theorem
If not PA $\vdash 0 = 1$, then not PA $\vdash \neg \mathit{Prov}(\ulcorner(0 = 1)\urcorner)$

Proof
Löb's Theorem says:
If PA $\vdash \mathit{Prov}(\ulcorner A \urcorner) \rightarrow A$, then PA $\vdash A$.

Substituting $0 = 1$ for A in Löb's theorem, we derive that

PA $\vdash \neg \mathit{Prov}(\ulcorner 0 = 1 \urcorner)$ implies PA $\vdash 0 = 1$,

which is just the contraposition of Gödel's Second Incompleteness theorem.

Later developments: boundaries of provability logic

Weaker systems than Peano Arithmetic may correspond to functions computable in interesting complexity classes.

Δ_0-formulas are arithmetical formulas in which all quantifiers are bounded by a term, for example
$\forall y \leq SS0\, \forall z \leq y\, \forall x \leq y+z\, (x+y \leq (y+(y+z)))$.

The arithmetical theory $\mathrm{I}\Delta_0$ is similar to Peano Arithmetic, except that induction, $(A(0) \wedge \forall x(A(x) \rightarrow A(Sx))) \rightarrow \forall x A(x)$,
is restricted to Δ_0-formulas A.

Let EXP be the formula expressing that for each x, its power 2^x exists.

Let Ω_1 be the formula expressing that for each x, its power $x^{\log(x)}$ exists.

Is GL the provability logic of weak systems of arithmetic?

For such weak theories T, the translation f should translate $\Box$ to the relevant $Prov_T$.

De Jongh, Jumelet and Montagna (1991) proved that arithmetical completeness holds for T= IΔ_0+EXP:

GL $\vdash A$ iff
for all translations f, IΔ_0+EXP $\vdash f(A)$

Open question
Does arithmetical completeness also hold for T =I$\Delta_0 + \Omega_1$?
(Partial answers in Berarducci and Verbrugge 1993).

Philosophical aspects of provability logic

Provability logic withstands Quine's critique of modal notions as unintelligible, because of its unambiguous arithmetical interpretation. Even for predicate provability logic (with quantifiers and equality), interpretation is unproblematic.

Example $\forall x \Box \exists y (y = x)$:

For each natural number n, we have $PA \vdash \exists y (y = I_n)$, where $I_n = SS \dots S0$ with n occurrences of successor operator S. This is true in the standard model. Even: $PA \vdash \forall x \Box \exists y (y = x)$.

Take care The arithmetical interpretation of the Barcan formula $\forall x \Box A(x) \rightarrow \Box \forall x A(x)$ is not true, let alone provable!

For example, for all n, $PA \vdash \neg \mathit{Proof}(I_n, \ulcorner 0 = 1 \urcorner)$ is true, but $PA \nvdash \forall x \neg \mathit{Proof}(x, \ulcorner 0 = 1 \urcorner)$ (Gödel's 2nd incompleteness theorem)

Conclusion

- For PA and many other arithmetical theories, provability logic proves everything you always wanted to prove about provability.
- This gives a nice decidable sub-theory of the undecidable theory of PA.

Further reading

Foundations of mathematics

- Doxiadis, A., Papadimitriou, C., Papadatos, A. and Di Donna, A., Logicomix: An Epic Search for Truth.
- Hofstadter, D., 1979, Gödel, Escher, Bach.
- Nagel, E. and Newman, J.R., 1958, Gödel's Proof.
- Hájek, P. and Pudlák, P., 1993, Meta-mathematics of First-order Arithmetic.

Provability logic

- Boolos, G., 1993, The Logic of Provability.
- Smorynski, C., 1995, Self-reference and Modal Logic.

- Verbrugge, R., 2010, Provability logic, Stanford Encyclopedia of Philosophy. (Just Google “provability logic”)

Epilogue

Thou hast made me known to friends whom I knew not.
Thou hast given me seats in homes not my own.
Thou hast brought the distant near and made a brother of the stranger.

From Rabindranath Tagore, Gitanjali (1910, 1913)