A Survey of Provability Logic

Magnus Boman
SYSLAB / FIST

Federated Information Systems Technology

Internal Working Note No.46[1]
February 1992
Department of Computer and Systems Sciences
The Royal Institute of Technology and Stockholm University
Electrum 230, S-164 40 KISTA SWEDEN
Phone: (+46 8) 161678
E-mail: mab@dsv.su.se

Abstract

Provability logic is a kind of modal logic obtained by interpreting the alethic operator for necessity as an operator of provability. It is used mainly for proving results about self-referential sentences in arithmetic. Very few writers have contributed to the topic of provability logic, especially considering its potential applications to deductive databases and distributed problem solving. This short survey is to a large extent based on publications by Boolos and Smorynski.

[1] This paper replaces Working Paper No.170, “A Survey of Provability Logic and a Note on its Relevance to Nonmonotonic Federated Information Systems”, published in June, 1990. Since then the author has given up on his ideas on using recursion theory for solving problems with nonmonotonic federated information systems. Because of the demand for WP170 over the last 18 months, it seems only fair to exclude those bits that do not seem relevant, and to concentrate on presenting a survey, now that WP170 is out of print. The author has taken this opportunity to revise the paper with respect to language and layout. He would also like to thank Paul Johannesson for comments on drafts of WP170, and also the people who have helped distribute that paper to the far corners of this world.

1. Background

Very few writers have contributed to the topic of provability logic, especially considering its potential applications to the fields of deductive databases (cf. [Börger-87], [Minker-88]), and distributed and cooperated problem solving (cf. [Bond-88], [Deen-91], [Kambayashi-91]). Apart from the works of Boolos and Smorynski often referred to in this paper, there are the more popular but excellent “puzzle books” by Smullyan, especially [Smullyan-82] and [Smullyan-87]. Though seldom treated in textbooks on logic, provability logic are given chapters in [Boolos-80] and [Epstein-90]. There are also papers, including [Leivant-81], [Avron-84], and [Montagna-84], presenting sequential calculi for different modal systems related to provability logic. These papers were inspired mainly by Robert Solovay´s paper [Solovay-76] publishing results from the early seventies which gave new life to the topic. Leivant gives sequential calculi for the system *G* for provability logic, presented below, and [Avron-84] extends (and corrects) Leivant´s paper. Avron also shows that the most natural sequential formulation of the quantified version of *G* is not cut-free, a property the propositional version has. This is in turn extended in [Montagna-84], which presents further negative results on quantified provability logic.

The first time a modal system was constructed by extending a classical base of propositional logic, in which all tautologies could be proved, was in [Gödel-33]. Gödel´s method has since then become standard. The modal axiom schemata in Gödel´s extension contained a provability operator, Bew (for *Beweisbar*), which we represent here as Bew. This system was proven by McKinsey and Tarski in 1948 to be an axiomatization of the system *S4*.[2] We will show that this proof is not the only indication of a resemblance between logics of provability and classical modal logics.

Shortly before [Gödel-33], Gödel had published some papers on his two *incompleteness theorems*, the most important paper

[2] The system *S4* was put forth in [Lewis-32]. For details, see for example [Hughes-68].

being [Gödel-31]. These are usually proven with respect to *Peano Arithmetic (PA)*, and the proof of the second incompleteness theorem reduces to a proof of the first, given the three *Hilbert-Bernays derivability conditions*.[3] As explained in [Smorynski-85], the latter are formalizations based on the definition of provability, and they were introduced in order to facilitate the proof of the second incompleteness theorem, and not in order to analyze the notion of provability. For this reason, they are very hard to understand and use for the latter purpose.

In [Löb-55], Löb came up with an alternative set of three derivability conditions, with the important difference to the earlier ones being that the *Löb Derivability Conditions (LDC)* were expressions of modal propositional logic, instead of predicate logic formulas:[4]

In the system PA, it holds for all sentences ϕ, ψ, where $\ulcorner\phi\urcorner$ denotes the Gödel number of ϕ (in PA), i.e. the result of assigning a numerical code to ϕ, that:[5]

---

[3]Following [Boolos-79], we will define the language of PA in the usual way, i.e. as consisting of the individual constant **0**, the unary function symbol for successor, ', and the two binary function symbols for sum, **+** and product, . The theorems of PA are the logical consequences of the universal closures of the recursion axioms for the functions, and instances of the usual induction axiom schema.

The Hilbert-Bernays derivability conditions were introduced in their “Grundlagen der Mathematik” (in the 2nd ed., 1968, on p.295). They are in a sense equivalent to the Löb derivability conditions (presented below), as explained in [Smorynski-85], p.8. We will not present the former here, only note that they are formalizations of some of the properties of the proof predicate Bew(x). We will also leave out completely the Diagonalisation Theorem in our presentation, and the reader is deferred to [Smorynski-81] for an extensive investigation of this important result.

[4]In *Journal of Symbolic Logic*, Volume 17, Number 2 (1955), Leon Henkin stated the following problem. “If Σ is any standard formal system adequate for recursive number theory, a formula (having a certain integer q as its Gödel number) can be constructed which expresses the proposition that the formula with Gödel number q is provable in Σ. Is this formula provable or independent in Σ?”. This was the problem solved in [Löb-55], and in the process Löb changed Bernays´ definition of the derivability conditions.

[5]We need not fix any code numbering, many different Gödel numberings work.

(i) If $\vdash \phi$, then $\vdash \mathrm{Bew}(\ulcorner \phi \urcorner)$;

(ii) $\vdash ((\mathrm{Bew}(\ulcorner \phi \urcorner) \wedge \mathrm{Bew}(\ulcorner \phi \rightarrow \psi \urcorner)) \rightarrow \mathrm{Bew}(\ulcorner \psi \urcorner))$;

(iii) $\vdash (\mathrm{Bew}(\ulcorner \phi \urcorner) \rightarrow \mathrm{Bew}(\ulcorner \mathrm{Bew}(\ulcorner \phi \urcorner) \urcorner))$.

George Boolos has suggested that $\mathrm{Bew}(\ulcorner \phi \urcorner)$ should be referred to as the sentence that asserts that ϕ is provable. More formally, $\mathrm{Bew}(x)$ is a predicate, and $\mathrm{Bew}(\ulcorner \phi \urcorner)$ results from substituting $\ulcorner \phi \urcorner$ for the variable x in $\mathrm{Bew}(x)$. Boolos also comments on Löb´s definition: "According to the first condition, if a sentence S is provable, then so is the sentence that asserts that S is provable. According to the second condition, it is always provable in PA that if a conditional and its antecedent are provable, then so is its consequent. According to the third condition, it is always provable that a sentence S satisfies the first condition".[6] In [Smorynski-85], the verification that y codes a proof of a sentence coded by x is expressed within the object language as a formula $\mathrm{Prov}(y,x)$, and $\mathrm{Bew}(x)$ is then defined by $\exists y \mathrm{Prov}(y,x)$.

The above definition, and the formulas satisfying it, will be the starting point for our survey. In the following section, we will see how it relates the notion of provability to a system of modal logic.

2. The Notion of Minimality in Modal Logic

The (semantically) minimal modal logic system is called *K*, after Kripke, and its axioms all have the form of one of the following.

Ax-P: The tautologies of propositional logic

Ax-K: The axiom schema $\Box\phi \rightarrow (\Box(\phi \rightarrow \psi) \rightarrow \Box\psi)$

Ax-P includes the tautological modal propositions with occurrences of the modal operator for necessity, $\Box$. This "box-operator" is applied to propositions, as in $\Box\phi$ above, to mean "ϕ is necessary (or necessarily true)". Ax-K is called the *distribution axiom* for $\Box$, since it governs the distribution of $\Box$ over implication. Moreover, the system has two rules:

R-MP: $\{\phi, (\phi \rightarrow \rho)\} \vdash \rho$

R-N: If $\vdash \phi$, then $\vdash \Box\phi$

---

[6] [Boolos-79], p.7.

The system has the usual definitions of abbreviations, omission of parentheses, and substitution. We will follow the new standard definition of the notion of normality which says that a modal system L is normal iff the set of theorems of L contains the propositional logic tautologies, all instances of the distribution axiom for $\Box$, and is closed under R-MP, R-N, and substitution.[7] Note that the Deduction Theorem can only be applied to derivations which do not use R-N, since otherwise the unacceptable $\vdash \phi \rightarrow \Box\phi$ would follow.[8]

The minimality of *K* is explained by its semantical properties as follows. Every normal system of modal propositional logic can be studied by means of models. A *Kripke model* is an ordered triple $<W,R,V>$, where W is any non-empty set of elements (called *worlds*), R is the binary *accessibility relation*, $R \subseteq W \times W$, and V is a value assignment function. Any model $<W,\mathrm{R},V>$ is *based on the frame* $<W,R>$. A modal proposition A is *valid in the Kripke model* $<W,R,V>$ iff $V(A,W)$ = T, for every $w \in W$. Now, the theorems of *K* are precisely the propositions valid in all models in which no restriction is enforced on *R*, not even that it is non-empty. For all extensions of *K*, there will be such restrictions, for example that R is reflexive, as will be seen below.

There is, however, also a notion of syntactic minimality, which is explained in [Smorynski-85] as follows. The modal part of a system´s definition can be viewed as a non-logical simulation of the LDC, such that Ax-K corresponds to case (ii) in the definition above, and R-N to case (i). Ax-P and R-MP correspond to ordinary propositional logic. A syntactically minimal system thus consists of modal counterparts of the tautologies, modus ponens, and the LDC; it remains to find an analogue of case (iii). This analogue is the well-known modal axiom called 4, by which we now extend *K*:

Ax-4: The axiom schema $\Box\phi \rightarrow \Box\phi$

[7]The previous standard was to define a system as normal iff all substitution instances of $\Box\phi\rightarrow\phi$ were contained in the set of theorems. This idea came from [Kripke-63].

[8]Cf. [Smorynski-84], p.455, where a "Modified Deduction Theorem" is given.

The syntactical minimality of the system *K4* now reached is justified by the fact that the LDC, together with Löb´s theorem presented below, constitute a complete analysis of the properties of the notion of provability.

3. Löb´s Theorem and the System *G* for Provability Logic

In order to study the logic of provability, the (syntactically) minimal logic, *K4*, has to be extended by another axiom. Like the other rules and axioms of *K4*, it has an analogue in the proof theory of arithmetic, namely *Löb´s Theorem*.[9] In [Smorynski-85], it is presented (and proved in three different ways) as in the following definition.

Löb´s Theorem:

$\vdash (\mathrm{Bew}(\ulcorner \mathrm{Bew}(\ulcorner \phi \urcorner) \rightarrow \phi \urcorner) \rightarrow \mathrm{Bew}(\ulcorner \phi \urcorner))$, for any sentence ϕ

We will let Bew[ϕ] denote $\mathrm{Bew}(\ulcorner \phi \urcorner)$, where ϕ has no free variables. Bew[ϕ] $\rightarrow \phi$ is called the *reflection principle* for ϕ. Thus, Löb´s Theorem says that for all sentences ϕ in arithmetic, ϕ is provable if the reflection principle for ϕ is provable. The analogue then, naturally, becomes:

Ax-W: The axiom schema $\Box(\Box\phi \rightarrow \phi) \rightarrow \Box\phi$

The name of this extension of *K4* is *G*.[10] The system *G* is equivalent to the system obtained by adding to *K4* the following rule of inference:

If $\vdash \Box\phi \rightarrow \phi$, then $\vdash \phi$.[11]

---

[9] An argument which shows that Löb´s Theorem is a direct consequence of Gödel´s second incompleteness theorem can be found in [Boolos-79], p.11. In fact, Löb´s Theorem is the contrapositive of it, for all finite extensions of PA. However, Smorynski (cf. [Smorynski-84], p.452) stresses the fact that even though Löb´s extension is easy, it is by no means obvious...

[10] The name *W* for this axiom schema was originally chosen to abbreviate *well*, as in *well-founded*, *well-capped*, and *(anti-)well-ordered*. The *G* is for Gödel, and it is sometimes called *GL* for "Gödel-Löb". Albert Visser, in his thesis, gave it the alternative name PRL for PRovability Logic, and in [Smorynski-79] it is called *L*.

[11] This inference rule is in turn obtained from the unformalised version of Löb´s Theorem: If $\vdash (\ulcorner \mathrm{Bew}(\ulcorner \phi \urcorner) \rightarrow \phi \urcorner)$, then $\vdash \phi$, for any sentence ϕ. The formalised version is usually chosen, since an axiom schema is generally

Today, the axiom Ax-4 is usually excluded, since it is derivable from the others. We will cite the proof here, for the purpose of illustration:[12]

$\vdash_G A \to ((\Box A \wedge \Box A) \to (A \wedge \Box A))$ (Tautology)

$\vdash_G \Box(A \wedge \Box A) \leftrightarrow (\Box A \wedge \Box A)$ (An instance of the well known theorem in *K*, and thus in *G*: $\Box(\phi \to \psi) \leftrightarrow (\Box\phi \wedge \Box\psi)$, for all sentences ϕ, ψ.)

$\vdash_G A \to (\Box(A \wedge \Box A) \to (A \wedge \Box A))$ (By prop. logic)

$\vdash_G \Box A \to \Box(\Box(A \wedge \Box A) \to (A \wedge \Box A))$ (By normality)

$\vdash_G \Box(\Box(A \wedge \Box A) \to (A \wedge \Box A)) \to \Box(A \wedge \Box A)$ (Inst. of Ax-W)

$\vdash_G \Box A \to \Box(A \wedge \Box A)$ (By prop. logic)

$\vdash_G \Box A \to \Box A \wedge \Box A$ (By prop. logic)

$\vdash_G \Box A \to \Box A$ (By prop. logic)

Q.E.D.

A system *L* is said to be *extended by* a different system *L'* iff every theorem of *L* is a theorem of *L'*. Of the modal systems usually studied, *K* and *K4* are both extended by *G*, but *G* is not extended by any other system, since it is not extended by *S5* (and all the other systems: *T*, *B*, and *S4*, are).

Another interesting thing to note is that when $\Box$ is taken to mean "it is provable that", then the dual alethic modality operator for possibility, , comes to mean "it is consistent that". We can thus prove that *G* is consistent by showing that $\Box\phi \to \phi$ is not a theorem of *G*, as shown in [Boolos-79]; if $\vdash_G \Box\phi \to \phi$, we could apply R-N to get the antecedent of Ax-W, and so $\vdash_G \Box\phi$, by R-MP. By R-MP again on $\Box\phi \to \phi$, we get ϕ, and by substituting $\perp$ for ϕ, we have shown *G* to be inconsistent. Moreover, Boolos notes that no modal proposition of the form ϕ is a theorem of *G*.

easier to handle model theoretically than an inference rule, cf. [Smorynski-84], p.457-458. The equivalence result was proved in [Macintyre-73].

[12]This proof was originally presented in [Boolos-79], p.30.

4. The Connection Between Modal Logic and Arithmetic

To investigate in more detail the modal simulations of the LDC and Löb´s Theorem, we need some new terminology. Our presentation will follow that of [Boolos-79].

A *realization* is a function that assigns to each sentence letter of modal logic a sentence of PA. A *translation* to a sentence in arithmetic from a sentence in modal logic is defined inductively, relative to a realization, as follows.

> Given a realization Ξ, the translation of a sentence A of modal logic is obtained from the following cases (and only from these):

(i) If A is $\bot$, then $A^{\Xi} = \bot$;

(ii) If A is a sentence letter, then $A^{\Xi} = \Xi(A)$;

(iii) If A is $B \to C$, then $A^{\Xi} = B^{\Xi} \to C^{\Xi}$;

(iv) If A is $\Box B$, then $A^{\Xi} = \mathrm{Bew}(\ulcorner B^{\Xi} \urcorner)$.

The most interesting translation is the one from Ax-W to Löb´s Theorem. If A is a sentence of modal logic and $A^{\Xi} = S$, then $(\Box(\Box A \to A) \to \Box A)^{\Xi} = (\mathrm{Bew}(\ulcorner \mathrm{Bew}(\ulcorner S \urcorner) \to \ulcorner S \urcorner) \to \mathrm{Bew}(\ulcorner S \urcorner))$, the latter being the sentence of PA that asserts that S is provable if $\mathrm{Bew}(\ulcorner S \urcorner) \to S$ is provable. Boolos writes: "Thus every translation of each axiom of G of the form $\Box(\Box A \to A) \to \Box A$ asserts that some particular instance of Löb´s theorem holds. Each such translation ... is itself provable, and indeed, *every translation of each theorem of G is a theorem of arithmetic*." The theorem which establishes this last result, i.e. if for every realization Ξ, $\vdash_{PA} A^{\Xi}$, then $\vdash_{G} A$, is *Solovay´s Completeness Theorem* for G, published in [Solovay-76].

To be able to learn things about arithmetic by studying G, we need the notion of *arithmetization*: Suppose that S and S' are sentences of the language of arithmetic, and let $\mathrm{Bew}[\phi]$ denote $\mathrm{Bew}(\ulcorner \phi \urcorner)$, where ϕ has no free variables. Let the connectives other than $\to$ and $\bot$ be abbreviations of these two in the usual manner. Then the arithmetization of the assertion that:

S is provable (in arithmetic) is the sentence Bew[*S*];
S is consistent is ¬Bew[¬*S*];
S is unprovable is ¬Bew[*S*];
S is disprovable (refutable) is Bew[¬*S*];
S is undecidable is (¬Bew[*S*] ∧ ¬Bew[¬*S*]);
S is equivalent to *S*' is Bew[*S* ↔ *S*'];
S implies *S*' (*S*' is deducible from *S*) is Bew[*S* → *S*'];
Arithmetic is consistent is ¬Bew[⊥];
Arithmetic is inconsistent is Bew[⊥].

By means of arithmetizations, we can learn things about arithmetic by studying the modal logic system *G*, such as the fascinating result that both of Gödel´s incompleteness theorems are provable in it. Lots of effort has lately been put into proving things that have to do with self-reference (cf. e.g. [Smorynski-79], [Smorynski-84], [Smorynski-85]), and characterizing properties of modal systems by means of fixed points. The most important result is perhaps the *De Jongh-Sambin Theorem*, which says that every sentence in *G* has a unique, explicitly definable fixed point.[13] This, in turn, shows something important about paradoxes: self-referential sentences have genuine meanings determinable without resort to self-reference (cf. [Smorynski-84]).

It is also possible to extend the studies into multi-modal logic by adding to the above definition arithmetizations of other predicates. For instance, in [Smorynski-85], a "substitutability" predicate ρ(x) is introduced.[14] Two new axiom schemata are added to *G*; □(φ ↔ ψ) → (∇φ ↔ ∇ψ), where ∇ is a

[13] A sentence *S* such that *S* ↔ *P*(⌈*S*⌉) is provable is called a fixed point of *P*(*x*). Gödel showed how to construct a fixed point in arithmetic of the predicate ¬Bew(*x*). Such a sentence, *S* ↔ ¬Bew(⌈*S*⌉), is called a Gödel sentence. With this fixed point notion, we can formulate truths such as: If PA is consistent, then no fixed point of ¬Bew(*x*) is provable. For a presentation and proof of the De Jongh-Sambin Theorem, see e.g. [Boolos-79], p.141, or [Smorynski-84], p.464. [Smorynski-79] is entirely devoted to techniques for calculating fixed points, while [Leivant-81] relates fixed points to interpolation, in the process of presenting several sequent calculi for *G*.

[14] On p.168, Smorynski defines ρ(v) as any substitutable formula of a certain kind. The important thing to understand here is not this notion, however, but rather that it is possible to analyze other predicates than provability with fruitful results.

new modal operator simulating $\rho(x)$, and another *mixing axiom* $\nabla\phi \rightarrow \Box\nabla\psi$. A mixing axiom earns its name from the fact that it consists of two or more different (primitive) modal operators. Part of the analysis of substitutability now carries over from the analysis of provability.

It is even possible that one could construct interesting predicates other than provability, which do not violate the LDC or Löb´s Theorem. Multi-modal logic is a very active research area right now, especially systems mixing different operators of temporal logic are common, and also systems mixing operators of knowledge and belief as in [Boman-90]. Some systems are multi-modal even if they only use one kind of operator, since it is relativized to any agent. Thus, the number of modal operators in any such system is (at least) equal to the number of agents in the system.

5. On the Soundness, Completeness, and Decidability of the System *G* for Provability Logic

It comes as no surprise that the semantics of *G* is not as natural as the semantics of the most common modal systems, since *G* was not constructed because of its semantical properties, but for syntactic reasons. However, its semantics can be characterized in the same way as the other systems, i.e. by noting that the theorems of *G* are precisely the sentences valid in all models in which a certain restriction is enforced on *R*.

For the needed terminology, we cite [Boolos-79]: "... a sentence is said to be *valid in a frame* if it is valid in all models based on the frame. Thus a sentence is valid in all frames iff valid in all models, valid in all transitive frames iff valid in all transitive models, etc. Every tautology is true at each world in each model; therefore all tautologies are valid in all models. And every distribution axiom is likewise valid in all models because it is true at each world in each model...". For instance, Ax-4 is valid in a frame $<W,V>$ iff *R* is a transitive relation on *W*. Such a frame (or model) is called *appropriate* to *K4*. Appropriate frames are easily found for the other classical modal systems, e.g. *T*, *B*, *S4*, *S5*. Naturally, every frame is appropriate to *K*. We must now determine which frames are appropriate to *G*. First, some more terminology. Let $R^{\cup}$ denote the converse of *R*, i.e. *aRb* iff $bR^{\cup}a$. We then have the following.[15]

> A relation, *E*, is said to be *well-founded* iff there is no infinite sequence a_0, a_1, a_2,... such that ...$a_2Ea_1Ea_0$.
>
> A relation *E* is *well-capped* iff $E^{\cup}$ is well-founded.
>
> A relation *E* is a *strict partial well-ordering* iff
>
> *E* is transitive and well-founded.
>
> Theorem:
>
> A frame <*W*,*R*> is appropriate to *G* iff *R* is transitive and well-capped, or alternatively iff $R^{\cup}$ is a strict partial well-ordering (since a relation is transitive iff its converse is).

In the very proof of this soundness theorem for *G* lies most of the intuition behind it, but the important thing is that we can characterize the semantics of system *G* by means of the properties of its accessibility relation. Unfortunately, well-cappedness is a second-order property, and it can be shown that no first-order formula that describes the class of transitive, well-capped frames exist.[16] It turns out, however, that this is not a problem, for the following reason.

The completeness theorem for *G* says that the theorems of *G* are precisely the modal propositions valid in all models in which *R* is transitive and well-capped. This theorem can be strengthened by inserting “finite” before the word “models”. Now, transitive, well-capped models whose domain is finite can alternatively be characterized by models <*W*,*R*,*V*> such that *W* is finite and *R* is a transitive, irreflexive relation on *W*. The frames of such models, with finite domains and transitive, irreflexive accessibility relations, are called *finite strict partial orderings*. Since irreflexivity is a first-order property, the problem vanishes. This stronger completeness theorem for *G*

[15]Cf. [Boolos-79], Chapter 5.

[16]This proof can be found in [Boolos-79], p.84. For a discussion on (non-modal) first-order characterizations of modal propositional logic, see [Hughes-84], chapter 3.

was proved in 1971, by Krister Segerberg.[17]

The idea is that if a modal proposition ϕ is not a theorem in *G*, then ϕ is invalid in some finite strict partial ordering. The decidability of *G* now follows from the fact that ϕ is not a theorem of *G* iff there is a finite transitive and irreflexive model with a finite domain in which ϕ is not valid. Boolos has presented an effective algorithm which checks a modal proposition for theoremhood in *G*.[18] So, *G* is sound and complete with respect to the class of models that are transitive, irreflexive, and well-founded. Finally, the predicate logic version of *G*, usually called *QGL*, is not complete with respect to any class of models. This, and other negative results on *QGL*

---

[17]In [Segerberg-71], p.86. Segerberg´s name for *G* is *K4W*. A similar proof is given in [Hughes-84], p.145, and a proof using truth-trees is presented in [Boolos-79], Chapter 8. An interesting difference between *G* and the other normal systems usually studied is that G is not a *canonical system*. This notion was introduced in [Segerberg-71], although he called such systems *natural*. It is in turn based on a special kind of model, called a *canonical model*, introduced in [Lemmon-77], and explained in detail in e.g. [Hughes-84]. Completeness is today usually proven by means of canonical models; given any system S, if the frame of the canonical model for S is a frame for S itself, then S is a canonical system. From the fact that S is canonical, its completeness easily follows. But, and we cite [Hughes-84], p.56: “We cannot, however, equate being canonical with being complete; for it is conceivable that a system might be characterized by *some* class of frames, even though the frame of its canonical model was not a frame for the system”. As shown in [Hughes-84], p.100, *G* is such a non-canonical, but complete, system.

[18]See [Boolos-79], Chapters 7 and 8. On page 99, Boolos writes: “To decide upon the theoremhood of any given sentence *A*, we (effectively) enumerate all the theorems of *G* and all models <*W*,*R*,*P*> in which *W* is a finite set of integers, *R* is a transitive and irreflexive relation on *W*, and *P* is a function that assigns a truth-value to each pair consisting of a member of *W* and a sentence letter in *A*. As theorems appear, we check each one to see whether or not it is identical to *A*. As models appear, we calculate the truth-value of *A* in all of the finitely many worlds of each model and determine whether *A* is false at at least one of them. (The determination can of course be effectively performed.) Either we shall eventually come upon *A* in the enumeration of theorems, or we shall not; but in the latter case, as our main theorem will show, we shall come upon a model at one of whose worlds *A* is false, and we shall then know that *A* is not a theorem of *G*. ... The proof of the main theorem will show that if *A* is a modal sentence with *n* subsentences that is not a theorem of *G*, then there is a finite strict partial ordering in which *A* is invalid, *whose domain contains* 2^n *worlds*”.

can be found in [Montagna-84].

References

[Avron-84]
Arnon Avron: "On Modal Systems having Arithmetical Interpretations" in *Journal of Symbolic Logic*, pp. 935-942, Vol.49, 1984.

[Boman-90]
Magnus Boman & Paul Johannesson: "Axiomatic Epistemic Systems for Federated Information Systems", in *Data Management*, pp.195-213, Ed. Prakash, Tata McGraw-Hill Publ. Co., New Delhi 1990.

[Bond-88]
Alan H. Bond & Les Gasser: "An Analysis of Problems and Research in DAI" in *Readings in Distributed Artificial Intelligence*, pp.3-35, Eds. Bond, Gasser, Morgan Kaufmann Publishers Inc. 1988.

[Boolos-79]
George Boolos: The Unprovability of Consistency, Cambridge University Press 1979.

[Boolos-80]
George Boolos & Richard C. Jeffrey: Computability and Logic, 2nd ed., Cambridge University Press 1980.

[Börger-87]
Egon Börger: Current Trends in Theoretical Computer Science, Ed. Börger, Computer Science Press 1987.

[Deen-91]
M.Deen: Cooperating Knowledge Based Systems 1990, Ed. Deen, Springer-Verlag 1991.

[Epstein-90]
Richard Epstein: The Semantic Foundations of Logic Volume 1: Propositional Logics, Nijhoff International Philosophy Series, Vol.35, Kluwer Academic Publishers, Dordrecht 1990.

[Gödel-31]
Kurt Gödel: "Über Formal Unentscheidbare Sätze der Principia Mathematica und Verwandter Systeme I", in *Monatshefte für Mathematik und Physik,* pp. 173-198, Vol.38, 1931.

[Gödel-33]
Kurt Gödel: "Eine Interpretation des Intuitionistischen Aussagenkalküls", in *Ergebnisse eines Mathematischen Kolloquiums* 4, pp.39-40, 1933. Also (with English translation) in *Collected Works (Volume 1),* Oxford University Press 1986.

[Hughes-68]
G.E. Hughes & M.J. Cresswell: An Introduction to Modal Logic, Methuen, London 1968.

[Hughes-84]
G.E. Hughes & M.J. Cresswell: A Companion to Modal Logic, Methuen, London 1984.

[Kambayashi-91]
Kambayashi et.al.: Proceedings of the First International Workshop on Interoperability in Multidatabase Systems, Eds. Kambayashi, Rusinkiewicz, and Sheth, IEEE Computer Society Press, Los Alamitos, California 1991.

[Kripke-63]
Saul Kripke: “Semantical Analysis of Modal Logic I: Normal propositional Calculi”, in *Zeitschrift für Mathematische Logik und Grundlagen der Mathematik*, Vol.9, pp.67-96, 1963.

[Leivant-81]
Daniel Leivant: “On the Proof Theory of the Modal Logic for Arithmetic Provability”, in *Journal of Symbolic Logic*, pp. 531-538, Vol.46, 1981.

[Lemmon-77]
E.J. Lemmon in collaboration with Dana Scott, and edited by Krister Segerberg: An Introduction to Modal Logic, in *American Philosophical Quarterly Monograph Series*, Ed. Rescher, Oxford 1977. Manuscript written in 1966.

[Lewis-32]
C.I. Lewis & C.H. Langford: Symbolic Logic, Dover, Mineola, New York 1932.

[Löb-55]
M.H. Löb: “Solution of a Problem of Leon Henkin”, in *Journal of Symbolic Logic*, pp. 115-118, Vol.20, 1955.

[Macintyre-73]
Macintyre & Simmons: “Gödel´s Diagonalization Technique and Related Properties of Theories”, *Colloquium Mathematicum* 28, pp. 165-180, 1973.

[Minker-88]
Jack Minker et.al.: Foundations of Deductive Databases and Logic Programming, Ed. Minker, Morgan Kaufmann Publishers Inc. 1988.

[Montagna-84]
Franco Montagna: “The Predicate Modal Logic of Provability”, in *Notre Dame Journal of Formal Logic*, pp. 179-189, Vol.25, 1984.

[Segerberg-71]
Krister Segerberg: An Essay in Classical Modal Logic, Filosofiska Föreningen, Uppsala, Sweden 1971.

[Smorynski-79]
Craig Smorynski: “Calculating Self-referential Statements, I: Explicit Calculations”, in *Studia Logica*, pp. 17-36, Vol.38, 1979.

[Smorynski-81]
Craig Smorynski: “Fifty Years of Self-reference in Arithmetic”, in *Notre Dame Journal of Formal Logic*, pp. 357-374, Vol.22, 1981.

[Smorynski-84]
Craig Smorynski: “Modal Logic and Self-Reference”, in *Handbook of Philosophical Logic, Volume II: Extensions of Classical Logic*, pp. 441-495, Eds. Gabbay, Guenthner, Synthese Library, D. Reidel Publishing Company, Dordrecht 1984.

[Smorynski-85]
Craig Smorynski: Self-Reference and Modal Logic, Springer-Verlag 1985.

[Smullyan-82]
Raymond Smullyan: The Lady or the Tiger?, Knopf, New York 1982.

[Smullyan-87]
Raymond Smullyan: Forever Undecided, Knopf, New York 1987.

[Solovay-76]
Robert Solovay: “Provability Interpretations of Modal Logic”, in *Israel Journal of Mathematics*, Vol.25, pp. 287-304, 1976.