A PRIMER ON PROVABILITY LOGIC

RYAN KAVANAGH

ABSTRACT. The K4LR and GL systems of modal logic will be presented in the context of a Hilbert-style system of sentential logic. Löb's theorem and Löb's Derivability Criterion will be proven. Similarities between properties of Bew and GL's $\Box$ will be drawn, before proving that $\Box$ in GL can be interpreted as Bew in Peano arithmetic by means of realisations. The soundness of this interpretation will be proven by Solovay's arithmetical completeness theorem. From this, applications of GL will be considered, including a proof of Gödel's Second Incompleteness Theorem.

1. Introduction

A provability logic is a modal logic studying what formal arithmetics can express about their provability predicates.[4] Provability logics trace their roots to Gödel's 1933 paper, where it was first hinted that provability could be treated as a modal operator. They also have as roots the quests of Gödel, Henkin, Löb and Tarski to discover what formal arithmetic could express about the truth or the provability of its own sentences. Although numerous provability logics have been advanced and studied, including GL, GLS, PrL, and K4LR[3, 4], in this paper we focus on GL, using GLS and K4LR only as tools to prove properties of GL.

The provability logic GL, named in honour of Kurt Gödel and Martin Löb, is an extension of the modal logic K and has two important results. The first is Solovay's arithmetical completeness theorem, which states that the theorems of GL are provable in Peano arithmetic under all substitutions of sentences of PA for modal sentence letters.[1] This makes GL valuable as a provability logic since any theorem proven in the general context of GL will hold for any "translation" into PA, and proving in this context is typically a much easier feat than proving each possible translation directly in PA. We prove part of this theorem, the remainder being beyond the scope of this primer. The second is the fixed-point theorem, which can be seen as GL's analogue of Peano arithmetic's Diagonal Lemma, with the added feature of fixed points being logically equivalent.[1, 4] It will not be presented, although those interested should see [3, p. 76] and [1, p. 104].

We start our primer by presenting GL's syntax and proof theory, deviating from traditional accounts by presenting it in the context of a Hilbert-style deduction system. We also present the provability logic K4LR, which will be crucial in proving part of Solovay's arithmetical completeness theorem. Several useful theorems and lemmas will be proven at this point, before taking a brief interlude into Peano arithmetic. Here we prove several key properties of the provability relation known as the Löb Derivability Conditions, which simplify proving Gödel's Second Incompleteness Theorem and Löb's Theorem. We also prove Löb's theorem, which answers Henkin's question of whether or not fixed points of the provability relation are provable, i.e., it establishes the relation between $PA \vdash S \leftrightarrow \mathrm{Bew}(\ulcorner S \urcorner)$ and $PA \vdash S$.[4] To tie everything together, we proceed with a partial proof of Solovay's arithmetical completeness theorem, concluding with applications of GL, including a proof of Gödel's Second Incompleteness Theorem.

2. Modal Logic

Modal logic is typically presented in the context of a suitable system of sentential calculus, with the addition of two formal symbols, $\Box$ and $\Diamond$. Classically, these two symbols have been interpreted through Kripke semantics as "it is necessary that" and "it is possible that", with one as a primitive symbol and the other as defined notation. For example, one could take $\Box$ as the primitive symbol and define $\Diamond$ as an abbreviation for $\neg \Box \neg$, or take $\Diamond$ as the primitive symbol and define $\Box$ as an abbreviation for $\neg \Diamond \neg$. We take $\Box$ to be our primitive symbol and will make no use of $\Diamond$. The addition of this formal symbol entails additional inference rules, presented below.

Most presentations of modal logic include as axioms all tautologies. In our presentation, we instead use a Hilbert-style deduction system, mostly as presented in [2]. Although both approaches generate the same theorems by the Tautology Theorem [2, 7.1], we find our approach preferable because of its simplicity. For reasons which will soon be clear, we introduce an additional symbol, $\bot$, to which we always assign the truth value false. Thus, "$\rightarrow$" is our adequate connective and, since they are truth-functionally equivalent, we redefine $(\neg A)$ to be an abbreviation of $(A \rightarrow \bot)$.

Letting A, B, C, ..., be metavariables ranging over sentences, we can thus recursively redefine the syntax of our sentential calculus' sentences to be as follows:

- $\bot$ is a sentence;
- each sentence letter is a sentence; and
- if A and B are sentences, then so is $(A \rightarrow B)$.

We retain the following Hilbert-style axioms from [2]:

(SA1) $A \rightarrow (B \rightarrow A)$

(SA2) $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$

(SA3) $(\neg A \rightarrow \neg B) \rightarrow (B \rightarrow A)$

and modus ponens,

(MP) If $\vdash A$ and $\vdash A \rightarrow B$, infer $\vdash B$,

as the sentential calculus' sole inference rule.

In presenting modal logic, we expand our sentential calculus' syntax to obtain a recursive definition of modal sentences:

- if A is a sentence, then so is $\Box(A)$.

As usual, we omit parentheses where no ambiguity ensues to alleviate notation, taking $\Box$ to be the tightest binding operator. That's to say, $\Box A \to B$ is to be interpreted as $(\Box(A) \to B)$ rather than $\Box(A \to B)$. Unless otherwise specified, we will henceforth take "sentence" to mean "modal sentence" and let A, B, C, ..., range over modal sentences.

We now deal with substitution. If F is a sentence, the result of substituting A for p in F, $F[A/p]$, may be defined recursively as follows:[1]

- if $F = p$, then $F[A/p]$ is A;
- if $F = q$ and $q \neq p$, then $F[A/p]$ is A;
- if $F = \bot$, then $F[A/p]$ is $\bot$;
- $(F \to G)[A/p]$ is $(F[A/p] \to G[A/p])$; and
- $\Box(F)[A/p]$ is $\Box(F[A/p])$.

Having dealt with our logics' syntax, we are now free to present our first system of modal logic, GL. We take S to be a given set of sentences, usually GL or K4LR. We introduce an inference rule known as necessitation,

(N) If $S \vdash A$, infer $S \vdash \Box(A)$,

a distribution axiom,

(DA) $(\Box(A \to B)) \to (\Box A \to \Box B)$,

and the axiom:

(L) $\Box(\Box A \to A) \to \Box A$.

That's to say, for any modal sentences A and B, we have $\mathrm{GL} \vdash (\Box(A \to B)) \to (\Box A \to \Box B)$ and $\mathrm{GL} \vdash \Box(\Box A \to A) \to \Box A$.

Our second system, K4LR, retains (N) and (DA), drops (L), introduces the axiom

(F) $\Box A \to \Box\Box A$,

and introduces the inference rule

(LR) If $S \vdash (\Box A \to A)$, infer $S \vdash \Box(A)$.

To gain a feel for the workings of GL and K4LR, we will prove a few theorems which we will find useful later when proving properties of GL and K4LR. To avoid proving these theorems twice, once for each system, we notice that GL and K4LR have a few immediate resemblances (in fact, we will soon show GL and K4LR to have the same theorems): each contains all tautologies, all instances of the distribution axiom, and is closed under modus ponens, necessitation, and substitution. We call any such system *normal* and denote it by L.[1] That's to say, if $L \vdash A$, then $\mathrm{GL} \vdash A$ and $\mathrm{K4LR} \vdash A$.

Lemma 1 (Substitution Lemma). *If* $L \vdash A \leftrightarrow B$*, then* $L \vdash F[A/p] \leftrightarrow F[B/p]$.

Proof. By induction on complexity. Omitted. $\Box$

The following two theorems enable us to prove the third, which says that GL can prove K4LR's axiom (F). Their proofs are straightforward.

Theorem 2. *If* $\mathrm{L} \vdash A \to \mathrm{B}$ *then* $\mathrm{L} \vdash \Box A \to \Box \mathrm{B}$.

Proof.

(1) $\mathrm{L} \vdash A \to \mathrm{B}$	hypoth.
(2) $\mathrm{L} \vdash \Box(A \to \mathrm{B})$	(1), (N)
(3) $\mathrm{L} \vdash \Box(A \to \mathrm{B}) \to (\Box A \to \Box \mathrm{B})$	(DA)
(4) $\mathrm{L} \vdash \Box A \to \Box \mathrm{B}$	(2), (3), (MP) □

Theorem 3. $\mathrm{L} \vdash \Box(A \wedge \mathrm{B}) \leftrightarrow (\Box A \wedge \Box \mathrm{B})$

Proof.

(1) $\mathrm{L} \vdash (A \wedge \mathrm{B}) \to A$	taut.
(2) $\mathrm{L} \vdash (A \wedge \mathrm{B}) \to \mathrm{B}$	taut.
(3) $\mathrm{L} \vdash \Box(A \wedge \mathrm{B}) \to \Box A$	(1), 2
(4) $\mathrm{L} \vdash \Box(A \wedge \mathrm{B}) \to \Box \mathrm{B}$	(2), 2
(5) $\mathrm{L} \vdash A \to (\mathrm{B} \to (A \wedge \mathrm{B}))$	taut.
(6) $\mathrm{L} \vdash \Box A \to \Box(\mathrm{B} \to (A \wedge \mathrm{B}))$	(5), 2
(7) $\mathrm{L} \vdash \Box(\mathrm{B} \to (A \wedge \mathrm{B})) \to (\Box \mathrm{B} \to \Box(A \wedge \mathrm{B}))$	(DA)
(8) $\mathrm{L} \vdash \Box A \to (\Box \mathrm{B} \to \Box(A \wedge \mathrm{B}))$	(6), (7), [2, (9.2)]
(9) $\mathrm{L} \vdash (\Box A \wedge \Box \mathrm{B}) \to \Box(A \wedge \mathrm{B})$	(8), truth funct.
(10) $\mathrm{L} \vdash \Box(A \wedge \mathrm{B}) \to (\Box A \wedge \Box \mathrm{B})$	(3), (4), truth funct.
(11) $\mathrm{L} \vdash \Box(A \wedge \mathrm{B}) \leftrightarrow (\Box A \wedge \Box \mathrm{B})$	(9), (10), abbrev. □

Theorem 4. $\mathrm{GL} \vdash \Box A \to \Box \Box A$

Proof. We make use of the following tautology:

(†) $$A \to ((\mathrm{B} \wedge \mathrm{C}) \to (\mathrm{C} \wedge A))$$

(1)	$\mathrm{GL} \vdash A \to ((\Box\Box A \wedge \Box A) \to (\Box A \wedge A))$	(†)
(2)	$\mathrm{GL} \vdash A \to ((\Box(\Box A \wedge A)) \to (\Box A \wedge A))$	(1), 3
(3)	$\mathrm{GL} \vdash \Box(A \to ((\Box(\Box A \wedge A)) \to (\Box A \wedge A)))$	(2), (N)
(4)	$\mathrm{GL} \vdash \Box A \to \Box((\Box(\Box A \wedge A)) \to (\Box A \wedge A))$	(3), (DA)
(5)	$\mathrm{GL} \vdash \Box(\Box(\Box A \wedge A) \to (\Box A \wedge A)) \to \Box(\Box A \wedge A)$	(L)
(6)	$\mathrm{GL} \vdash \Box A \to \Box(\Box A \wedge A)$	(4), (5), [2, (9.2)]
(7)	$\mathrm{GL} \vdash \Box(\Box A \wedge A) \to \Box\Box A$	3
(8)	$\mathrm{GL} \vdash \Box A \to \Box\Box A$	(6), (7), [2, (9.2)] □

3. Peano Arithmetic

We must prove several additional theorems about the provability relation in Peano Arithmetic. We take throughout Bew to be $\mathrm{Thm}_{\mathrm{PA}}$ and take Prv to be $\mathrm{Prv}_{\mathrm{PA}}$.

Theorem 5 (Löb's Derivability Criterion)**.** *The provability relation,* Bew*, has the following properties:*

(i) If $\mathrm{PA} \vdash S$*, then* $\mathrm{PA} \vdash \mathrm{Bew}(\ulcorner S \urcorner)$

Proof. This is a consequence of [2, Corollary 22.12]. □

(ii) $\mathrm{PA} \vdash \mathrm{Bew}(\ulcorner(S \to T)\urcorner) \to (\mathrm{Bew}(\ulcorner S \urcorner) \to \mathrm{Bew}(\ulcorner T \urcorner))$

Proof. By [2, Corollary 22.11] and the following observation:

$$\mathrm{PA} \vdash \mathrm{Prv}(\ulcorner S \to T \urcorner, y) \wedge \mathrm{Prv}(\ulcorner S \urcorner, y') \to \mathrm{Prv}(\ulcorner T \urcorner, y * y' * \langle \ulcorner T \urcorner \rangle).$$ □

(iii) $\mathrm{PA} \vdash \mathrm{Bew}(\ulcorner S \urcorner) \to \mathrm{Bew}(\ulcorner \mathrm{Bew}(\ulcorner S \urcorner) \urcorner)$

Proof. Omitted. □

Together, these properties allow us to prove the following fascinating and useful theorem:

Theorem 6 (Löb's Theorem)**.** $\mathrm{PA} \vdash \mathrm{Bew}(\ulcorner S \urcorner) \to S$ *if and only if* $\mathrm{PA} \vdash S$*.*

Proof. The right-to-left direction is trivial.[3]

For the sakes of brevity and clarity, we'll abbreviate "$\mathrm{Bew}(\ulcorner X \urcorner)$" by "$\mathrm{B}\,X$".

By the diagonal lemma, there exists a sentence A such that $\mathrm{PA} \vdash A \leftrightarrow (\mathrm{B}\,A \to S)$. Then,

(1)	$\mathrm{PA} \vdash A \leftrightarrow (\mathrm{B}\,A \to S)$	[2, 21.6]
(2)	$\mathrm{PA} \vdash A \to (\mathrm{B}\,A \to S)$	(1)
(3)	$\mathrm{PA} \vdash \mathrm{B}(A \to (\mathrm{B}\,A \to S))$	5(i)
(4)	$\mathrm{PA} \vdash \mathrm{B}(A \to (\mathrm{B}\,A \to S)) \to (\mathrm{B}\,A \to \mathrm{B}(\mathrm{B}\,A \to S))$	5(ii)
(5)	$\mathrm{PA} \vdash \mathrm{B}\,A \to \mathrm{B}(\mathrm{B}\,A \to S)$	(3), (4), (MP)
(6)	$\mathrm{PA} \vdash \mathrm{B}(\mathrm{B}\,A \to S) \to (\mathrm{B}\,\mathrm{B}\,A \to \mathrm{B}\,S)$	5(ii)
(7)	$\mathrm{PA} \vdash \mathrm{B}\,A \to (\mathrm{B}\,\mathrm{B}\,A \to \mathrm{B}\,S)$	(5), (6), [2, (9.2)]
(8)	$\mathrm{PA} \vdash \mathrm{B}\,A \to \mathrm{B}\,\mathrm{B}\,A$	5(iii)
(9)	$\mathrm{PA} \vdash \mathrm{B}\,A \to \mathrm{B}\,S$	(7), (8), truth funct.
(10)	$\mathrm{PA} \vdash \mathrm{B}\,S \to S$	hypoth.
(11)	$\mathrm{PA} \vdash \mathrm{B}\,A \to S$	(9), (10), [2, (9.2)]
(12)	$\mathrm{PA} \vdash A$	(1), (11), (MP)
(13)	$\mathrm{PA} \vdash \mathrm{B}\,A$	5(i)
(14)	$\mathrm{PA} \vdash S$	(11), (12), (MP) □

4. Relation between GL and K4LR

We notice that GL and K4LR are very similar, they differ only on account of (L) and (LR), as we have already shown in Theorem 4 that $\mathrm{GL} \vdash \Box A \to \Box\Box A$, K4LR's axiom (F). In fact, as the following theorem shows, GL and K4LR have the same theorems.

Theorem 7. *GL and K4LR have the same theorems.*

Proof. The proof is by Boolos.[1]

We notice that by Theorem 4, $\mathrm{GL} \vdash \Box A \to \Box\Box A$. Moreover, GL is closed under the Löb rule, since:

(1)	$\mathrm{GL} \vdash \Box A \to A$	hypoth.
(2)	$\mathrm{GL} \vdash \Box(\Box A \to A)$	(1), (N)
(3)	$\mathrm{GL} \vdash \Box(\Box A \to A) \to \Box A$	(L)
(4)	$\mathrm{GL} \vdash \Box A$	(2), (3), (MP)
(5)	$\mathrm{GL} \vdash A$	(1), (4), (MP)

Thus, since GL can prove all of the axioms of K4LR and is closed under its inference rules, if $\mathrm{K4LR} \vdash A$, then $\mathrm{GL} \vdash A$.

Conversely, let $B = \Box(\Box A \to A)$, $C = \Box A$ and $D = B \to C$. We will show that $K4LR \vdash D$, that's to say, that K4LR can prove GL's axiom (L). We have that:

(1)	$K4LR \vdash \Box(B \to C) \to (\Box B \to \Box C)$	(DA)
(2)	$K4LR \vdash \Box D \to (\Box B \to \Box C)$	(1), abbrev.
(3)	$K4LR \vdash \Box(\Box A \to A) \to (\Box\Box A \to \Box A)$	(DA)
(4)	$K4LR \vdash B \to (\Box C \to C)$	(3), abbrev.
(5)	$K4LR \vdash \Box(\Box A \to A) \to \Box\Box(\Box A \to A)$	4
(6)	$K4LR \vdash B \to \Box B$	(5), abbrev.
(7)	$K4LR \vdash \neg(\Box B \to \Box C) \to \neg\Box D$	(6), [2, 6.11(b)]
(8)	$K4LR \vdash (\neg\Box C \to \neg\Box B) \to \neg\Box D$	(7), 1, [2, 6.11(b)]
(9)	$K4LR \vdash \neg\Box B \to B$	(6), [2, 6.11(b)]
(10)	$K4LR \vdash (\neg\Box C \to \neg B) \to \neg\Box D$	(8), (9), [2, (9.2)]
(11)	$K4LR \vdash \neg(B \to \Box C) \to \neg\Box D$	(10), 1, [2, 6.11(b)]
(12)	$K4LR \vdash \Box D \to (B \to \Box C)$	(11), [2, 6.11(b)]
(13)	$K4LR \vdash \Box D \to (B \to C)$	(4), (12), truth funct.
(14)	$K4LR \vdash \Box D \to D$	(13), abbrev.
(15)	$K4LR \vdash D$	(14), (LR)

We thus see that if $GL \vdash A$, then $K4LR \vdash A$. □

5. Relation between GL and Peano arithmetic

We now show how K4LR and GL can be used as a provability logics for Peano arithmetic. Readers may have noticed the strong tie between the axioms and inference rules of K4LR and GL, and the theorems and properties proven about PA and Bew in Section 3. Namely, by interpreting □ as Bew, we notice a direct correspondence between (N) and Theorem 5(i). We further notice a direct correspondence between (DA) and Theorem 5(ii). We can also interpret (LR) as Löb's Theorem, and (L) as a formalisation in GL of Löb's Theorem. But are K4LR and GL sound in regards to this interpretation? Is every theorem of K4LR and GL provable in PA under the interpretation of □ as Bew? Solovay's arithmetical completeness theorem, below, tells us that it is so. Is the converse true? Solovay's theorem tells us that it is nearly so.

We must first establish a mapping between modal logic and PA. We do so by means of *realisations*.[1] A realisation is a function that assigns to each sentence letter in modal logic a sentence of PA[1], and we use "$*$" to range over such functions. We recursively define a *translation* A^* of a modal sentence A under a realisation $*$ as:

(1) $\bot^* = (\mathbf{0} \neq \mathbf{0})$, or your contradiction of choice;

(2) $p^* = *(p)$;
(3) $(A \to B)^* = (A^* \to B^*)$; and
(4) $\Box(A)^* = \mathrm{Bew}(\ulcorner A^* \urcorner)$.

For example, $\Box(\bot \to \bot)^* = \mathrm{Bew}(\ulcorner(\mathbf{0} \neq \mathbf{0}) \to (\mathbf{0} \neq \mathbf{0})\urcorner)$, and if we assume $*$ is a realisation taking p to the sentence $(\mathbf{s0} = \mathbf{0} + \mathbf{s0})$, then $(\Box(p) \to \Box(\Box(p)))^* = \mathrm{Bew}(\ulcorner(\mathbf{s0} = \mathbf{0} + \mathbf{s0})\urcorner) \to \mathrm{Bew}(\ulcorner\mathrm{Bew}(\ulcorner(\mathbf{s0} = \mathbf{0} + \mathbf{s0})\urcorner)\urcorner)$.

With this out of the way, we have:

Theorem 8. *If* $\mathrm{K4LR} \vdash A$, *then for every realisation* $*$, $\mathrm{PA} \vdash A^*$.

Proof. We proceed by induction on complexity.

If A is an instance of the axioms (SA1), (SA2) or (SA3), then so will be A^*, and so $\mathrm{PA} \vdash A^*$.

If A is an instance of the distribution axiom, (DA), then A is of the form $(\Box(B \to C)) \to (\Box B \to \Box C)$. Then $A^* = \mathrm{Bew}(\ulcorner B^* \to C^* \urcorner) \to (\mathrm{Bew}(\ulcorner B^* \urcorner) \to \mathrm{Bew}(\ulcorner C^* \urcorner))$, which by Theorem 5(ii) is a theorem of PA.

In the case of modus ponens, (MP), if $\mathrm{PA} \vdash (A \to B)^*$ and $\mathrm{PA} \vdash A^*$, then $\mathrm{PA} \vdash B^*$ since $(A \to B)^* = (A^* \to B^*)$.

In the case of the Löb Rule, (LR), if $\mathrm{PA} \vdash (\Box A \to A)^*$ then $\mathrm{PA} \vdash A^*$ by Löb's Theorem, since $(\Box(A) \to A)^* = \mathrm{Bew}(\ulcorner A^* \urcorner) \to A^*$.

Finally, we deal with necessitation, (N). If $\mathrm{PA} \vdash A^*$, then by Theorem 5(i), $\mathrm{PA} \vdash \mathrm{Bew}(\ulcorner A^* \urcorner)$. Thus by definition of realisations, $\mathrm{PA} \vdash (\Box(A))^*$. □

Corollary 9. *If* $\mathrm{GL} \vdash A$, *then for every realisation* $*$, $\mathrm{PA} \vdash A^*$.

Proof. GL and K4LR have the same theorems by Theorem 7. □

Interestingly, this relation between GL and PA implies that GL can only prove truths (relative to the intended model $\mathfrak{N}$) about PA. In fact, Solovay's theorem is even stronger and tells us that the provability logic GLS—whose axioms are all the theorems of GL and all sentences of the form $\Box A \to A$, with modus ponens as its sole inference rule[1]—can only prove truths about PA, and that the converse is true. We present the theorem here in simplified form:

Theorem 10 (Solovay's arithmetical completeness theorem). *For every modal sentence* A *of GLS and every realisation* $*$, $\mathrm{GLS} \vdash A$ *if and only if* $\mathfrak{N} \models A^*$.

Proof. The proof is by Boolos. Assume that $\mathrm{GLS} \vdash A$. Since by [2, 12.11], every theorem of PA is true under the intended model if $\mathrm{Bew}(\ulcorner A^* \urcorner)$ is true, then A^* is a theorem of PA and A^* is true. Thus for every realisation $*$ and every modal sentence A, $(\Box A \to A)^*$ is true. By Corollary 9, if A is a theorem of GL, then A^* is a theorem of PA, and again by [2, 12.11], A^* is true. Thus, if $\mathrm{GLS} \vdash A$, then $\mathfrak{N} \models A$.

The converse's proof is non-trivial and omitted. See [1] and [3] for details. □

Corollary 11. *If* $\mathrm{GL} \vdash A$*, then for every realisation* $*$, $\mathfrak{N} \models A^*$.

Proof. Immediate from Theorem 10 and the definition of GLS. □

The above theorems are useful, not only as means of proving truths about PA, but also of proving that a sentence is not a theorem of GL. For example, assume that p is a theorem of GL. Then by Theorem 10, under any realisation $*$ such that $*(\mathrm{p}) = (\mathbf{0} \neq \mathbf{0})$, $\mathfrak{N} \models (0 \neq 0)$, which is obviously false, and so p is not a theorem of GL. Now assume that $\Box\,\mathrm{p} \to \mathrm{q}$ is a theorem of GL. Then by Theorem 9, under any realisation taking p to $(\mathbf{0} = \mathbf{0})$ and q to $(\mathbf{0} \neq \mathbf{0})$ in PA, $\mathsf{PA} \vdash \mathrm{Bew}(\ulcorner(\mathbf{0} = \mathbf{0})\urcorner) \to (\mathbf{0} \neq \mathbf{0})$. Since $(\mathbf{0} = \mathbf{0})$ is a theorem of PA, by Theorem 5(i), $\mathsf{PA} \vdash \mathrm{Bew}(\ulcorner(\mathbf{0} = \mathbf{0})\urcorner)$. But then by modus ponens, $\mathsf{PA} \vdash (\mathbf{0} \neq \mathbf{0})$, contradicting the consistency of PA. Therefore $\Box\,\mathrm{p} \to \mathrm{q}$ is not a theorem of GL.

6. Applications of GL

It is now easy to prove Gödel's Second Incompleteness Theorem:

Theorem 12 (Gödel's Second Incompleteness Theorem)**.** *If* PA *is consistent, then* $\mathsf{PA} \nvdash \mathrm{Bew}(\ulcorner(\mathbf{0} \neq \mathbf{0})\urcorner)$.

Proof. We can formalise the above statement as

$$\mathsf{PA} \vdash \neg\,\mathrm{Bew}(\ulcorner(\mathbf{0} \neq \mathbf{0})\urcorner) \to \neg\,\mathrm{Bew}(\ulcorner\neg\,\mathrm{Bew}(\ulcorner(\mathbf{0} \neq \mathbf{0})\urcorner)\urcorner).$$

But this can easily be reached through realisation:

(1) $\mathrm{GL} \vdash \Box(\Box\bot \to \bot) \to \Box\bot$	(L)
(2) $\mathrm{GL} \vdash \neg\,\Box\bot \to \neg\,\Box(\Box\bot \to \bot)$	(1), [2, 6.11(b)]
(3) $\mathrm{GL} \vdash \neg\,\Box\bot \to \neg\,\Box(\neg\,\Box\bot)$	(2), abbrev.
(4) $\mathsf{PA} \vdash (\neg\,\Box\bot \to \neg\,\Box(\neg\,\Box\bot))^*$	(3), 9
(5) $\mathsf{PA} \vdash \neg\,\mathrm{Bew}(\ulcorner(\mathbf{0} \neq \mathbf{0})\urcorner) \to \neg\,\mathrm{Bew}(\ulcorner\neg\,\mathrm{Bew}(\ulcorner(\mathbf{0} \neq \mathbf{0})\urcorner)\urcorner)$	(4), 9 □

This leads us to an interesting corollary by Boolos:

Corollary 13. *The following assertion is provable in* PA*:*

> *If the inconsistency of arithmetic is not provable, then the consistency of arithmetic is undecidable.*

Proof. The assertion is equivalent to

$$\mathsf{PA} \vdash \neg\,\mathrm{Bew}(\ulcorner\mathrm{Bew}(\ulcorner(\mathbf{0} \neq \mathbf{0})\urcorner)\urcorner) \to (\neg\,\mathrm{Bew}(\ulcorner\neg\mathrm{Bew}(\ulcorner(\mathbf{0} \neq \mathbf{0})\urcorner)\urcorner) \wedge \neg\,\mathrm{Bew}(\ulcorner\neg\neg\,\mathrm{Bew}(\ulcorner(\mathbf{0} \neq \mathbf{0})\urcorner)\urcorner)),$$

which is easily derivable using GL:

(1)	$\mathrm{GL} \vdash \Box\bot \to \Box\Box\bot$	4
(2)	$\mathrm{GL} \vdash \neg\Box\Box\bot \to \neg\Box\bot$	(1), [2, 6.11(b)]
(3)	$\mathrm{GL} \vdash \neg\Box\bot \to \neg\Box\neg\Box\bot$	12
(4)	$\mathrm{GL} \vdash \neg\Box\Box\bot \to \neg\Box\neg\Box\bot$	(2), (3), [2, (9.2)]
(5)	$\mathrm{GL} \vdash \neg\Box\Box\bot \to \neg\Box\neg\neg\Box\bot$	taut.
(6)	$\mathrm{GL} \vdash \neg\Box\Box\bot \to (\neg\Box\neg\Box\bot \wedge \neg\Box\neg\neg\Box\bot)$	(4), (5), truth funct.

The assertion readily follows by means of realisation of (6). □

References

[1] George Boolos, *The logic of provability*, Cambridge University Press, Cambridge England New York, NY, USA, 1995.

[2] Ole A. Nielsen, *An introduction to formal arithmetic: Incompleteness, consistency, and computability*, 2012.

[3] C. Smoryński, *Self reference and modal logic*, Springer-Verlag, New York, 1985 (eng). Bibliography: p. [330]-333.

[4] Rineke (L.C.) Verbrugge, *Provability logic*, The stanford encyclopedia of philosophy, 2010.