On the Proof Theory of the modal logic $\underline{G}$.

By

Daniel Leivant

TR79-380

July, 1979

Department of Computer Science
Cornell University
Ithaca, NY   14853

On the Proof Theory of the modal logic <u>G</u> .

Daniel Leivant
Department of Computer Science
Cornell University, Ithaca NY 14853

July 1979

1. An arithmetic interpretation $*$ of propositional formulas (fls) is determined by interpreting atoms p_i by arithmetic sentences p_i^*. This may be extended to the language of modality by a suitable interpretation of the "necessity" connective $\Box$. Of special interest is the interpretation of $\Box$ as (arithmetized) provability in, say, Peano's arithmetic <u>PA</u> ; i.e., one defines, given $\{p_i^*\}_i$, $\bot^* :\equiv \bot$, $(\varphi \circ \psi)^* :\equiv \varphi^* \circ \psi^*$ for each binary connective $\circ$, and $(\Box\varphi)^* :\equiv Pr(\ulcorner \varphi^* \urcorner)$, where Pr is a (canonical) provability predicate for <u>PA</u> .

Under any such interpretation, any instance of the following schemas becomes a theorem or rule of <u>PA</u> :

(A1) $\Box(\varphi \to \psi) \to . \Box\varphi \to \Box\psi$

(A2) $\Box\varphi \to \Box\Box\varphi$

(R1) $\vdash \varphi \Rightarrow \vdash \Box\varphi$.

In fact, these are the derivability conditions used in the proof of Gödel's incompleteness theorems. While these schemas are valid also for trivial interpretations of $\Box$ (e.g., as a vacuous operator), the self-referential mechanism of <u>PA</u> yields as a theorem of <u>PA</u> also each $*$ interpretation of

(A3) $\Box(\Box\varphi \to \varphi) \to \Box\varphi$

(Löb [5]).

Let $\underline{G}$ (for Gödel) be the extension of classical propositional logic $\underline{Cp}$ with (A1) - (A3), (R1). We indicated that each $*$-interpretation of a theorem of $\underline{G}$ is a theorem of $\underline{PA}$. Solovay [8] proved the converse: if $\vdash_{\underline{PA}} \varphi^*$ for all $*$, then $\vdash_{\underline{G}} \varphi$. The logic $\underline{G}$ is discussed _in extenso_ by Boolos [1] and Smoryński [6] (where it is denoted $\underline{L}$).

De Jongh, Sambin and Kripke have independently shown that (A2) is derived in $\underline{G}^- := \underline{G}$ - (A2). (cf. [1], p. 30.)

2. _An alternative axiomatization of_ $\underline{G}$. Let $\underline{G'}$ be like $\underline{G}$, except that (A3) is replaced by the inference rule

(R2) $\qquad \vdash \Box\varphi \to \varphi \;\Rightarrow\; \vdash \varphi .$

We show that $\underline{G'}$ is equivalent to $\underline{G}$.

2.1. _LEMMA_. $\vdash_{\underline{G}} \Box\varphi \;\Rightarrow\; \vdash_{\underline{G}} \varphi$.

Proof: Assume $\vdash_{\underline{G}} \Box\varphi$; then $\vdash_{\underline{PA}} Pr\ulcorner\varphi^*\urcorner$ for any $*$, so $\vdash_{\underline{PA}} \varphi^*$ by the soundness of $\underline{PA}$, and hence $\vdash_{\underline{G}} \varphi$ by Solovay's completeness theorem. ☒

2.2. _PROPOSITION_. $\vdash_{\underline{G'}} \varphi \;\Rightarrow\; \vdash_{\underline{G}} \varphi$.

Proof: We only have to verify that $\underline{G}$ is closed under (R2). Assume $\vdash_{\underline{G}} \Box\varphi \to \varphi$; then $\vdash_{\underline{G}} \Box(\Box\varphi \to \varphi)$ by (R1), so $\vdash_{\underline{G}} \Box\varphi$ by (A3), and $\vdash_{\underline{G}} \varphi$ by 2.1. ☒

2.3. PROPOSITION. $\vdash_{\underline{G}} \varphi \Rightarrow \vdash_{\underline{G'}} \varphi$.

Proof: We only have to prove in $\underline{G'}$ every instance of (A3), say

$$\psi \equiv \Box(\Box\varphi \to \varphi) \to \Box\varphi .$$

By (P2) it suffices to derive $\Box\psi \to \psi$. Arguing in $\underline{G'}$, assume (1) $\Box\psi$ and (2) $\Box(\Box\varphi \to \varphi)$. Then (3) $\Box\Box(\Box\varphi \to \varphi)$ by (2), (A2); also (4) $\Box\Box(\Box\varphi \to \varphi) \to \Box\Box\varphi$ by (1), (A1); so (5) $\Box\Box\varphi$ by (3), (4); (6) $\Box\Box\varphi \to \Box\varphi$ by (2), (A1), and $\Box\varphi$ by (5), (6). ⌛

3. A sequential calculus for $\underline{G}$. Let Γ, Δ stand for finite sets of fls. A sequent is an ordered pair $\Gamma:\Delta$. Write Γ, Δ for $\Gamma \cup \Delta$; Γ, φ for $\Gamma \cup \{\varphi\}$; $\Box\Gamma$ for $\{\Box\varphi \mid \varphi \in \Gamma\}$. We define $\underline{G}_0$ as the sequential calculus built on the following inference rules.

$$p:p \quad ; \quad \bot: \quad ; \quad :\top$$

$$\underline{\to L}: \quad \frac{\Gamma:\varphi,\Delta \qquad \Sigma,\psi:\Xi}{\Gamma,\Sigma,\varphi \to \psi:\Delta,\Xi} \quad ; \quad \underline{\to R}: \quad \frac{\Gamma,\varphi:\psi,\Delta}{\Gamma:\varphi \to \psi,\Delta}$$

The usual rules for $\wedge$ and $\vee$ (if one wishes to refer to these connectives)

$$\underline{\text{cut}}: \quad \frac{\Gamma:\varphi,\Delta \qquad \Sigma,\varphi:\Xi}{\Gamma,\Sigma:\Delta,\Xi} \quad ; \quad \underline{\text{thin}}: \quad \frac{\Gamma:\Delta}{\Gamma,\Sigma:\Delta,\Xi}$$

$$\underline{\Box I}: \quad \frac{\Gamma:\varphi}{\Box\Gamma:\Box\varphi}$$

Clearly, $\underline{G}_o$ is the same as $\underline{Cp}$ + (A1) + (R1). Let $\underline{G}_1 := \underline{G}_o$ + (A2), and $\underline{G}_2 := \underline{G}_1 + (\underline{L})$ where $\underline{L}$ is the rule:

$$\underline{L} \quad \frac{\Box\varphi:\varphi}{:\varphi}$$

Then $\underline{G}_2$ is the same as $\underline{G}'$, and hence the same as $\underline{G}$.

3.1. LEMMA. (Cut-elimination) Every theorem of $\underline{G}_o$ has a proof in $\underline{G}_o$ without cut.

Proof: Same as the standard cut-elimination argument for $\underline{Cp}$ (cf. e.g. [3] p. 454). Permutation of cut over $\underline{\Box I}$ is never needed, since all fls are active in the conclusion of $\underline{\Box I}$. When both active occurrences of a cut formula are derived by $\underline{\Box I}$, we have

$$\frac{\dfrac{\Gamma:\varphi}{\Box\Gamma:\Box\varphi} \qquad \dfrac{\Sigma,\varphi:\psi}{\Box\Sigma,\Box\varphi:\Box\psi}}{\Box\Gamma,\Box\Sigma:\Box\psi}\ .$$

This is reduced to $\dfrac{\dfrac{\Gamma:\varphi \qquad \Sigma,\varphi:\psi}{\Gamma,\Sigma:\psi}}{\Box\Gamma,\Box\Sigma:\Box\psi}$. ⊠

We do not have cut elimination for either $\underline{G}_1$ or $\underline{G}_2$. However, the simple axiomatization of $\underline{G}_2$ over $\underline{G}_o$ permits some interesting applications of 3.1. This is done via the following lemma.

3.2. LEMMA. (i) If $\Gamma \vdash_{\underline{G}} \Delta$, then $\Sigma,\Box\Xi,\Gamma \vdash_{\underline{G}_o} \Delta$, where each $\sigma \in \Sigma$ is an instance of (A2), and each $\xi \in \Xi$ is a theorem of $\underline{G}$.

(ii) Let $\underline{G}_2^- := \underline{G}_2 - (A2)$. If $\Gamma \vdash_{\underline{G}_2^-} \Delta$ then $\Box\Xi, \Gamma \vdash_{\underline{G}_0} \Delta$ where each $\xi \in \Xi$ is a theorem of $\underline{G}_2^-$.

Proof: (i) If $\Gamma \vdash_{\underline{G}} \Delta$ then there is a proof π in $\underline{G}_0 + (\underline{L})$ deriving $\Gamma, \Sigma : \Delta$ for Σ as above. Skipping in π each instance $\frac{\Box\varphi : \varphi}{: \varphi}$ of $(\underline{L})$ and collecting $\Box\varphi$ in all antecedents below such an instance we obtain the result. The proof of (ii) is the same. ⊠

4. Closure under rules. Cut-free systems are useful in demonstrating closure under rules. We give two examples.

4.1. PROPOSITION. If $\Box\Gamma \vdash_{\underline{G}} \Box\Delta, \Box\Delta'$ then $\Gamma, \Box\Gamma \vdash_{\underline{G}} \Delta, \Box\Delta'$.

Proof: Assume $\Box\Gamma \vdash_{\underline{G}} \Box\Delta, \Box\Delta'$. Then, by 3.2(i), 3.1, there is a cut free proof π of $\underline{G}_0$ deriving

$$(*) \qquad \Sigma, \Box\Xi, \Box\Gamma : \Box\Delta, \Box\Delta'$$

where $\Sigma = (\Box\psi_i \to \Box\Box\psi_i)_i$ and each $\xi \in \Xi$ is a theorem of $\underline{G}$. We show by induction on the height h of π that (**) $\Gamma, \Box\Gamma \vdash_{\underline{G}} \Delta, \Box\Delta'$.

Basis. $h = 1$. (*) has no premise. Case (a). $\Box\delta \in \Box\Xi$ for some $\delta \in \Delta \cup \Delta'$; then $\vdash_{\underline{G}} \delta$ and $\vdash_{\underline{G}} \Box\delta$. (b) $\Box\delta \in \Box\Gamma$; then $\Gamma \vdash_{\underline{G}} \delta$, and $\Box\Gamma \vdash_{\underline{G}} \Box\delta$.

Ind. Step. $h > 1$. Case 1. (*) is derived by $\to\underline{L}$:

$$\frac{\Sigma, \Box\Xi, \Box\Gamma : \Box\Delta, \Box\Delta', \Box\psi \qquad \Sigma, \Box\Box\psi, \Box\Xi, \Box\Gamma : \Box\Delta, \Box\Delta'}{\Sigma, \Box\psi \to \Box\Box\psi, \Box\Xi, \Box\Gamma : \Box\Delta, \Box\Delta'}$$

By ind. hyp. applied to the premises,

$$\Gamma, \Box\Gamma \vdash_{\underline{G}} \Delta, \Box\delta', \Box\psi \quad \text{and} \quad \Gamma, \Box\Gamma, \Box\psi, \Box\Box\psi \vdash_{\underline{G}} \Delta, \Box\Delta'$$

So $\Gamma, \Box\Gamma \vdash_{G} \Delta, \Box\delta'$

<u>Case 2</u>. (*) is derived by <u>thin</u>; trivial.

<u>Case 3</u>. (*) is derived by $\underline{\Box I}$:

$$\frac{\Xi, \Gamma : \delta}{\Box\Xi, \Box\Gamma : \Box\delta}$$

then $\Gamma \vdash_{\underline{G}} \delta$ and $\Box\Gamma \vdash_{\underline{G}} \Box\delta$. Since π is cut-free, these are the only possible cases. ⊠

4.2. <u>COROLLARY</u>. If $\Box\Box\Gamma \vdash_{\underline{G}} \Box\Delta$ then $\Box\Gamma \vdash_{\underline{G}} \Delta$. ⊠

4.3. <u>PROPOSITION</u>. If $\Box\Gamma \vdash_{\underline{G}_2^-} \Box\Delta$ then $\Gamma \vdash_{\underline{G}_2^-} \Delta$.

<u>Proof</u>: Similar to (and simpler than) 4.1., using 3.2(ii) in place of 3.2(i). ⊠

4.4. <u>COROLLARY</u>. $\Box p \nvdash_{\underline{G}_2^-} \Box\Box p$. ⊠

This contrasts with the derivability of (A2) in $\underline{G}^- = \underline{G} - (A2)$, mentioned in §1.

We now give a second example of a rule under which $\underline{G}$ is closed.

4.5. <u>PROPOSITION</u>. If $\Box\Gamma \vdash_{\underline{G}} \Box\Delta, \Lambda$, where each $\lambda \in \Lambda$ is a propositional letter, then $\Box\Gamma \vdash_{\underline{G}} \varphi$ for some $\varphi \in (\Box\Delta, \Lambda)$.

<u>Proof</u>: Using the conventional notations of 4.1, it suffices to show that $\Box\Gamma \vdash_{\underline{G}} \varphi$ whenever there is a cut-free proof π of $\underline{G}_0$ deriving $(*)$ $\Sigma, \Box\Xi, \Box\Gamma : \Box\Delta, \Lambda$. We proceed, again, by induction on the height of π. The basis is trivial.

<u>Ind. Step</u>. <u>Case 1</u>. $(*)$ is derived by $\underline{\to L}$.

$$\frac{\Sigma, \Box\Xi, \Box\Gamma : \Box\Delta, \Lambda, \Box\psi \qquad \Sigma, \Box\Xi, \Box\Gamma, \Box\Box\psi : \Box\Delta, \Lambda}{\Sigma, \Box\psi \to \Box\Box\psi, \Box\Xi, \Box\Gamma : \Box\Delta, \Lambda} .$$

By ind. hyp. applied to the left premise, if $\Box\Gamma \nvdash_{\underline{G}} \varphi$ for $\varphi \in (\Box\Delta, \Lambda)$, then $\Box\Gamma \vdash_{\underline{G}} \Box\psi$. And by ind. hyp. for the right premise, $\Box\Gamma, \Box\Box\psi \vdash_{\underline{G}} \varphi$ for some $\varphi \in (\Box\Delta, \Lambda)$. Hence $\Box\Gamma \vdash_{\underline{G}} \varphi$. <u>Case 2</u>: <u>thin</u>; trivial. <u>Case 3</u>. $\underline{\Box I}$; then the succedent of $(*)$ must consist of a single fl to start with. ⊠

Some examples of application of 4.5: (1) $\Box(p \vee q) \nvdash_{\underline{G}} \Box p \vee \Box q$ (2) $\Box(p \vee \Box p \vee \ldots \vee \Box^n p) \nvdash_{\underline{G}} p \vee \Box p \vee \ldots \vee \Box^n p$. Here $\Box^0 p :\equiv p$, $\Box^{n+1} p :\equiv \Box\Box^n p$.

5. <u>The reflection principle</u>. This is the schema $\Box\varphi \to \varphi$. By (A3), $\vdash_{\underline{G}} \Box\varphi \to \varphi$ iff $\vdash_{\underline{G}} \varphi$. The next result shows that the reflection principle is not finitely axiomatizable over $\underline{G}$. This has been shown model-theoretically by Boolos [2].

5.1. <u>PROPOSITION</u>. Assume $(*)$ $\{\Box\varphi_i \to \varphi_i\}_{i=1}^{k} \vdash_{\underline{G}} \Box^n p \to p$. Then $k \geq n$.

Proof: By induction on n. Basis $n = 1$; trivial. Ind. step. $n > 1$. Using again the notational conventions of 4.1, if (*) holds, then there is a cut-free proof π of $\underline{G}_o$ deriving

$$(**) \qquad \Sigma, \Box\Xi, (\Box\varphi_i \to \varphi_i)_{i=1}^{k}, \quad \Box^n p : p .$$

(*) must be derived by thin or $\to$L. The left premise have the form $\Sigma, \Box\Xi, (\Box\varphi_i \to \varphi_i)_i, \Box^n p : \; p, \Box\phi$ and is derived again by thin or $\to$L. These inferences may be ordered at will, with a single instance of thin on the top; this is simply because such instances of $\to$L may be permuted ([4]). To recall:

$$\dfrac{\dfrac{\Gamma:\Delta,\alpha,\varphi \qquad \Gamma,\psi:\Delta,\alpha}{\Gamma,\varphi\to\psi:\Delta,\alpha} \qquad \Gamma,\varphi\to\psi,\beta:\Delta}{\Gamma,\alpha\to\beta,\varphi\to\psi:\Delta}$$

may be rearranged as

$$\dfrac{\dfrac{\Gamma:\Delta,\alpha,\varphi \qquad \Gamma,\varphi\to\psi,\beta:\Delta}{\Gamma,\varphi\to\psi,\alpha\to\beta:\Delta,\varphi} \qquad \dfrac{\Gamma,\psi:\Delta,\alpha \qquad \Gamma,\varphi\to\psi,\beta:\Delta}{\Gamma,\varphi\to\beta,\psi:\Delta}}{\Gamma,\varphi\to\psi,\alpha\to\beta:\Delta}$$

We may assume, therefore, that instances of reflection are active below active occurrences of fls in Σ; taking successively left premises of $\to$L, we then get in π a sequent $\Sigma, \Box\Xi, \Box^n p : p, (\Box\varphi_i)_{i=1}^{k}$. Hence $\Box^n p \vdash_{\underline{G}} p, (\Box\varphi_i)_{i=1}^{k}$. Since $\Box^n p \nvdash_{\underline{G}} p$, we get, by 4.5., $\Box^n p \vdash \Box\varphi_i$ for some i, say $i = k$. Since $n > 1$, $\Box^{n-1} p \vdash_{\underline{G}} \varphi_k$ by 4.2. Hence $(\Box\varphi_i \to \varphi_i)_{i=1}^{k-1} \vdash_{\underline{G}} \Box^{n-1} p \to p$. By ind. hyp. $k - 1 \geq n - 1$, and so $k \geq n$. ⊠

6. Interpolation. A system $\underline{S}$ satisfies (Craig's) interpolation if $\varphi \vdash_{\underline{S}} \psi$ implies that $\varphi \vdash_{\underline{S}} \kappa$ and $\kappa \vdash_{\underline{S}} \psi$ for some fl κ with logical constants common to φ and ψ.

6.1. PROPOSITION. $\underline{G}_o$ satisfies interpolation.

Proof: We apply cut-elimination (3.1) via Maehara's partition method (cf. [4] p. 35). The presence of the rule $\underline{\Box I}$ necessitates only two additional clauses. (1) Consider $\frac{\Gamma, \Delta : \gamma}{\Box\Gamma, \Box\Delta : \Box\gamma}$, and assume κ is an interpolant for the premise: $\Gamma \vdash \kappa, \gamma$ and $\Delta, \kappa \vdash$. Then $\Box\Gamma, \Box\neg\kappa \vdash \Box\gamma$ and $\Box\Delta \vdash \Box\neg\kappa$. So $\Box\Gamma \vdash \neg\Box\neg\kappa, \Box\gamma$ and $\Box\Delta, \neg\Box\neg\kappa \vdash$, and $\neg\Box\neg\kappa$ is an interpolant for the conclusion. (2) Similarly, if κ is an interpolant for $\Gamma, \Delta : \delta$, then $\Box\kappa$ is for $\Box\Gamma, \Box\Delta : \Box\delta$. ⊠

6.2. LEMMA. Assume $\Gamma, \Sigma_1[\vec{r}] \vdash_{\underline{G}} \Delta, \Sigma_2[\vec{r}]$, $\vec{r} = (r_1, \ldots, r_n)$. Set $\Sigma_i^{\vec{r}} = \{\sigma(\delta_1, \ldots, \delta_n) \mid \sigma \in \Sigma_i, \delta_j = \top \text{ or } \bot, j = 1, \ldots, n\}$. Then $\Gamma, \Sigma_1^{\vec{r}} \vdash_{\underline{G}} \Delta, \Sigma_2^{\vec{r}}$.

Proof: A straightforward and trivial induction on the length of the proof in $\underline{G}_2$ for $\Gamma, \Sigma_1 : \Delta, \Sigma_2$. ⊠

6.3. PROPOSITION. If $\underline{H} = \underline{G}_o + \underline{S}$, where $\underline{S}$ is a set of axioms (no rules!) closed under substition, then $\underline{H}$ satisfies interpolation.

Proof: Assume $\varphi[\vec{p}, \vec{q}] \vdash_{\underline{H}} \psi[\vec{p}, \vec{s}]$; then $\Sigma[\vec{p}, \vec{q}, \vec{s}], \varphi \vdash_{\underline{G}_o} \psi$, with $\Sigma \subset S$. So by 5.2. $\Sigma^{\vec{q}, \vec{s}}[\vec{p}], \varphi \vdash_{\underline{G}_o} \psi$. By 5.1 there is an interpolant κ in $\underline{G}_o$ for $\wedge(\Sigma^{\vec{q}, \vec{s}}) \wedge \varphi$ and ψ. Since $\Sigma^{\vec{q}, \vec{s}} \subset \underline{S}$ by our assumption on $\underline{S}$, $\varphi \vdash_{\underline{H}} \kappa$ and $\kappa \vdash_{\underline{H}} \psi$. ⊠

6.4. COROLLARY. $\underline{G}_1$ and $\underline{G}_2 = \underline{G}$ satisfy interpolation. ☒

The interpolation theorem for $\underline{G}$ was proved independently by Boolos [1] and Smoryński [7], using Kriple models for $\underline{G}$. As usual, from the interpolation theorem Beth's definability theorem for $\underline{G}$ readily follows.

REFERENCES

[1] G. Boolos: The Unprovability of Consistency, Cambridge, 1979.

[2] ________: Reflection principles and iterated consistency assertions; Jour. Symb. Logic 44 (1979) 33-35.

[3] S. C. Kleene: Introduction to Metamathematics, Amsterdam, 1952.

[4] ________: Permutability of inferences in Gentzen's calculi LK and LJ; Mem. of AMS 10, 1952.

[5] M. H. Löb: Solution of a problem of Leon Henkin; Jour. Symb. Logic 20 (1955) 115-118.

[6] C. Smoryński: Calculating self-referential statements, I: explicit calculations; to appear in Studia Logica.

[7] ________: Beth's theorem and self-referential sentences; Logic Colloquium 77 (eds. A. Macintyre et als.), Amsterdam, 1978.

[8] R. Solovay: Provability interpretations of modal logic; Israel Jour. Math 25 (1976) 287-304.

[9] G. Takeuti: Proof Theory, Amsterdam, 1978.