The Basic Logic of Proofs

Sergei Artëmov*
Steklov Mathematical Institute,
Vavilov str. 42,
117966 Moscow, Russia.
e-mail: art@log.mian.su

Tyko Straßen†
University of Berne, IAM,
Länggassstr. 51,
CH- 3012 Berne.
e-mail: strassen@iam.unibe.ch

Abstract

Propositional Provability Logic was axiomatized in [7]. This logic describes the behaviour of the arithmetical operator "y is provable". The aim of the current paper is to provide propositional axiomatizations of the predicate "x is a proof of y" by means of modal logic, with the intention of meeting some of the needs of computer science.

1 Introduction

The Propositional Provability Logic GL was axiomatized in [7]. This logic describes the behaviour of the arithmetical operator "y is provable" by means of modal logic. Although some properties of this logic are relevant for computer science (e.g. various forms of Gödel's incompleteness theorem for consistency proofs in databases), GL is rather a mathematical domain. One reason is that in computer science not only the *provability* of a statement is of interest, but also in many cases the *proofs themselves*, respectively informations about the time or memory expenditure for a proof are known. These considerations lead to a different situation. For example it is well-known that a powerful machine cannot prove its own consistency, but it is very well possible for such a machine to demonstrate that a given proof does not derive $0 = 1$, or that no computation within a fixed time comes to that answer. The studies on the Logic of Proofs have been initiated by a series of questions by G. Jäger related to this topic. One was to give an arithmetically complete propositional axiomatization of the predicate "x is a proof of y". The modal systems $\mathcal{P}$, $\mathcal{PF}$ and $\mathcal{PFM}$ introduced below solve this problem.

Most definitions in this introduction are in accordance with those of classical Provability Logic [7]. Nevertheless, the Basic Logic of Proofs is entirely different from Provability Logic, and its arithmetical completeness proof does not use the Solovay argument.

*Supported by the Swiss Nationalfonds (project 21-27878.89) during a stay at the University of Berne in January 1992.

†Financed by the Union Bank of Switzerland (**UBS/SBG**) and by the Swiss Nationalfonds (projects 21-27878.89 and 20-32705.91).

1.1 Definition The modal language contains two sorts of variables,

$$p_0, p_1, \ldots \text{ (called } \textit{proof variables}\text{)},$$
$$S_0, S_1, \ldots \text{ (called } \textit{sentence variables}\text{)},$$

the usual boolean connectives, truth values $\top$ (for truth) and $\bot$ (for absurdity), and the labeled modality symbol $\Box_{p_i}$ for each proof variable p_i. The modal language is generated from the atoms $\top, \bot, S_0, S_1, \ldots$ by the boolean connective $\to$ as usual, and by the unary modal operators $\Box_{p_0}(\cdot), \Box_{p_1}(\cdot), \ldots$ as follows: if p is a proof variable and A a modal formula then $\Box_p(A)$ ($\Box_p A$ for short) is a modal formula.

Parentheses are avoided whenever possible by the usual conventions on precedence along with the modal convention that $\Box_{p_i}(\cdot)$ is given the minimal scope. Small letters $p, q, r, \ldots$ are used for proof variables, capital letters $S, T, \ldots$ for sentence variables and $A, B, C, \ldots$ for modal formulas.

The clear intention is to interpret $\Box_p A$ as "p is a proof of A". In order to allow iterations of modalities, which is an essential principle of the Logic of Proofs, the modal language must be interpreted in theories, which are able to link theorems and proofs after some natural coding. These considerations lead to the notion of the *arithmetical interpretation* of the modal language.

1.2 Definition Let the theory T be a recursive extension of $\mathrm{I}\Sigma_1$ which is valid in the standard model of arithmetic, for example let T be Peano Arithmetic $\mathtt{PA}$. Greek letters φ, ψ, ... denote arithmetical formulas. In this paper it will not be distinguished between the number n and its numeral $\overline{n}$.

1.3 Definition An arithmetical formula $Prf(\cdot,\cdot)$ is called a *proof predicate* in T iff

- $Prf(x, y)$ is (provably-in-T equivalent to) a recursive formula in x and y.
- $\mathsf{T} \vdash \varphi \iff \exists n \in \mathbb{N}: \; Prf(n, \ulcorner\varphi\urcorner)$ for all arithmetical formulas φ.

A proof predicate is thus nothing but a recursive enumeration of the theorems of T.

1.4 Example

1. A *standard Gödel proof predicate* $\widetilde{Prf}(\cdot,\cdot)$ for the theory T is a recursive formula which complies with the following specification:

   $$\widetilde{Prf}(x, y) \text{ is true} \quad :\Longleftrightarrow \quad \begin{array}{l} x \text{ is the Gödel number of a proof in } \mathsf{T} \\ \text{of the formula with the Gödel number } y. \end{array}$$

   A formal representation of $\widetilde{Prf}(\cdot,\cdot)$ can be found for example in [3] or [6]. Note that with respect to $\widetilde{Prf}(\cdot,\cdot)$ each theorem has infinitely many proofs.

2. A modification $Prf_1(\cdot,\cdot)$ of $\widetilde{Prf}(\cdot,\cdot)$ is obtained if one allows not only proofs as first argument, but also programs which enumerate the theorems of T. This generalization leads to a different proof predicate: If $\widetilde{Prf}(x, y)$ holds, one may assume that $x \geq y$, provided the usual Gödel numbering is used (cf. remark 1.7). Differently, short programs can compute long theorems such that $Prf_1(x, y)$ does not necessarily imply $x \geq y$.

3. In the context of *resource bounded reasoning* one can construct a proof predicate $Prf_2(\cdot,\cdot)$ by

$$Prf_2(x,y) \;:=\; \exists p \leq x :\; Prf_1(p,y)$$

with the intention that $Prf_2(x,y)$ holds iff the formula (with Gödel number) y is computable by a program which size (i.e. Gödel number) is bounded by x. The proof predicate $Prf_2(\cdot,\cdot)$ differs from $\widetilde{Prf}(\cdot,\cdot)$ and $Prf_1(\cdot,\cdot)$ in the sense that there may be several formulas $\varphi_1, \varphi_2, \ldots$ such that $Prf_2(n, \ulcorner \varphi_i \urcorner)$ is true for a fixed n.

1.5 Definition A proof predicate is called *functional* iff for all $n, k_1, k_2 \in \mathbb{N}$:

$$\text{If} \;\; Prf(n,k_1) \;\; \text{and} \;\; Prf(n,k_2) \;\; \text{then} \;\; k_1 = k_2.$$

So functional proof predicates are just injective recursive enumerations of the theorems of $\mathbf{T}$. The standard Gödel proof predicate $\widetilde{Prf}(\cdot,\cdot)$ and $Prf_1(\cdot,\cdot)$ from example 1.4 are examples of such functional proof predicates.

The standard Gödel proof predicate $\widetilde{Prf}(\cdot,\cdot)$ enjoys an additional property, namely to be monotonic:

1.6 Definition A proof predicate is called *monotone* iff for all $n, k \in \mathbb{N}$:

$$\text{If} \;\; Prf(n,k) \;\; \text{then} \;\; n \geq k.$$

1.7 Remark It is assumed that the Gödel numbering of formulas and proofs satisfies the following conditions:

- if $n \in \mathbb{N}$ then $n \leq \ulcorner n \urcorner$,
- if a term t occurs in the formula φ then $\ulcorner t \urcorner < \ulcorner \varphi \urcorner$, and if p is a proof of the formula φ then $\ulcorner p \urcorner \geq \ulcorner \varphi \urcorner$.

1.8 Definition Let $Prf(\cdot,\cdot)$ be a proof predicate in $\mathbf{T}$, and let ϕ be a function that assigns to each proof variable p_i some $n \in \mathbb{N}$ and to each sentence variable S_i a sentence of $\mathbf{T}$. An *arithmetical interpretation* (*interpretation* for short) $(\cdot)^*$ is a pair $(Prf(\cdot,\cdot), \phi)$ of such $Prf(\cdot,\cdot)$ and ϕ. The arithmetical interpretation $(A)^*$ (A^* for short) of a modal formula A is the extension of ϕ to all modal formulas by:

- $\top^* := (0=0) \quad \bot^* := (0=1) \quad p_i{}^* := \phi(p_i) \quad S_i{}^* := \phi(S_i)$
- $(A \to B)^* := A^* \to B^*$
- $(\Box_p A)^* := Prf(p^*, \ulcorner A^* \urcorner)$

1.9 Definition Let "$\equiv$" denote the syntactical identity of formulas (e.g. $\varphi \equiv \varphi$, but $\varphi \wedge \varphi \not\equiv \varphi$, $S_0 \not\equiv S_1$ and $\Box_{p_0}\top \not\equiv \Box_{p_1}\top$). An arithmetical interpretation $(\cdot)^* = (Prf(\cdot,\cdot), \phi)$ is called *functional* iff $Prf(\cdot,\cdot)$ is functional and $(\cdot)^*$ is injective, which means that $A^* \equiv B^*$ implies $A \equiv B$. An arithmetical interpretation $(\cdot)^* = (Prf(\cdot,\cdot), \phi)$ is called *monotone* iff $Prf(\cdot,\cdot)$ is a monotonic proof predicate. A *standard* interpretation is an interpretation which is functional and monotonic.

1.10 Example Consider the formula $\neg\Box_p\neg\Box_p\top$. Its arithmetical interpretation is $\neg Prf(p^*, \ulcorner\neg Prf(p^*, \ulcorner 0=0\urcorner)\urcorner)$, depending on $Prf(\cdot,\cdot)$ and the interpretation of the proof variable p.

Assume first that $Prf(\cdot,\cdot)$ is a standard proof predicate, for example the Gödel one $\widetilde{Prf}(\cdot,\cdot)$. As p^* occurs in $\neg Prf(p^*, \ulcorner 0=0\urcorner)$ and by the convention on Gödel numbering it follows that $p^* < \ulcorner\neg Prf(p^*, \ulcorner 0=0\urcorner)\urcorner$. Hence, by the monotonicity property $Prf(p^*, \ulcorner\neg Prf(p^*, \ulcorner 0=0\urcorner)\urcorner)$ cannot be true, and as this is a recursive sentence it follows that $\neg Prf(p^*, \ulcorner\neg Prf(p^*, \ulcorner 0=0\urcorner)\urcorner)$ is provable. So $\neg\Box_p\neg\Box_p\top$ is provable (hence true) under every standard interpretation.

Assume next that $Prf(\cdot,\cdot)$ is defined by the following fixed point equation, i.e. T proves the following equivalence:

$$Prf(x,y) \quad \longleftrightarrow \quad \left[\begin{array}{lcll} x=0 & \rightarrow & y = \ulcorner\neg Prf(0, \ulcorner 0=0\urcorner)\urcorner & \wedge \\ x>0 & \rightarrow & \widetilde{Prf}(x-1,y) & \end{array}\right]$$

Clearly $Prf(\cdot,\cdot)$ is a proof predicate: It is recursive and enumerates all theorems by $\widetilde{Prf}(\cdot,\cdot)$ and additionally the sentence $\neg Prf(0, \ulcorner 0=0\urcorner)$ which is according to the fixed point equation provable in T, too. Furthermore $Prf(\cdot,\cdot)$ is functional but no longer monotonic. Now $Prf(0, \ulcorner\neg Prf(0, \ulcorner 0=0\urcorner)\urcorner)$ is true by the fixed point equation and hence $\neg Prf(p^*, \ulcorner\neg Prf(p^*, \ulcorner 0=0\urcorner)\urcorner)$ is false with $p^* = 0$. So there exists a functional interpretation which makes $\neg\Box_p\neg\Box_p\top$ false.

The Basic Logic of Proofs is not concerned with occasional details about the coding of proofs in T by means of one fixed $Prf(\cdot,\cdot)$. Rather the Basic Logic of Proofs describes those basic principles which are true for *all* proof predicates of a given class.

In this paper the decidable modal logics $\mathcal{P}$, $\mathcal{PF}$ and $\mathcal{PFM}$ are introduced ($\mathcal{M}$ stands for Monotonicity and $\mathcal{F}$ for Functionality), with axioms and rules of inference as follows:

$$\left.\begin{array}{ll} \textbf{(A1)} & \text{All (boolean) tautologies} \\ \textbf{(A2)} & \Box_p A \longrightarrow A \\ \textbf{(R1)} & \dfrac{A \qquad A \rightarrow B}{B} \\ \textbf{(A3)} & \Box_p A \longrightarrow \neg\Box_p B \quad (A \not\equiv B) \\ \textbf{(A4)} & \neg[\Box_{q_1} A_2(q_2) \wedge \Box_{q_2} A_3(q_3) \wedge \ldots \wedge \Box_{q_n} A_1(q_1)] \end{array}\right\} \begin{array}{l} \mathcal{P} \\ \\ \\ \mathcal{PF} \\ \\ \mathcal{PFM} \end{array}$$

where A, B are modal formulas, p is a proof variable and $A_i(q_i)$ is a modal formula in which the proof variable q_i occurs. The scheme (A4) includes $\neg\Box_{q_1} A_1(q_1)$. (A2) is the *Reflexivity Axiom*, (A3) the *Functionality Axiom* and (A4) the *Monotonicity Axiom*.

The main result of the paper claims that for each modal formula A the following hold:

$$\begin{array}{rcl} \mathcal{P} \vdash A & \Longleftrightarrow & A^* \text{ is true for every interpretation } (\cdot)^* \\ \mathcal{PF} \vdash A & \Longleftrightarrow & A^* \text{ is true for every functional interpretation } (\cdot)^* \\ \mathcal{PFM} \vdash A & \Longleftrightarrow & A^* \text{ is true for every standard interpretation } (\cdot)^* \end{array}$$

Moreover, for each of these completeness theorems a proof predicate $Prf(\cdot,\cdot)$ can uniformly be chosen, and $\mathcal{PFM}$ even is complete with respect to all interpretations which use a fixed standard proof predicate, for example the Gödel one $\widetilde{Prf}(\cdot,\cdot)$.

None of $\mathcal{P}$, $\mathcal{PF}$ and $\mathcal{PFM}$ can be regarded as a *normal* modal logic as none of them is closed under the necessitation rule

$$\frac{A}{\Box_p A}$$

The substitution rule

$$\frac{A \leftrightarrow B}{\Box_p A \leftrightarrow \Box_p B}$$

obviously fails under arithmetical interpretations, too.

In section 2 the soundness and completeness for $\mathcal{P}$ is proved, in sections 3 and 4 the same is done for $\mathcal{PF}$ resp. $\mathcal{PFM}$, and section 5 is devoted to uniform proof predicates.

2 The basic modal system $\mathcal{P}$

The aim of this section is to prove soundness and completeness of the modal system $\mathcal{P}$ with respect to arithmetical interpretations.

2.1 Example $\mathcal{P} \vdash \neg\Box_p\bot,\ \neg\Box_p\Box_q\bot,\ \Box_p\neg A \to \neg\Box_q A,\ \ldots$
and $\mathcal{P}$ proves neither $\Box_p\top$ nor $\neg\Box_p\top$ nor $\Box_p A \to \Box_p(A \wedge A)$.

2.2 Soundness of $\mathcal{P}$ Let A be a modal formula. Then

$$\begin{array}{lcll} \mathcal{P} \vdash A & \Longrightarrow & \forall^* : \ \mathsf{T} \vdash A^* & \text{and therefore} \\ & & \forall^* : \ A^* \text{ is true} & \end{array}$$

Proof Let $(\cdot)^*$ be some arithmetical interpretation. One has to show that $\mathsf{T} \vdash A^*$. Induction on the complexity of the $\mathcal{P}$-proof of A:

(A1) and (R1) straightforward.

(A2) 1st case: $\mathsf{T} \vdash Prf(p^*, \ulcorner A^* \urcorner)$. It follows $\mathsf{T} \vdash A^*$, hence $\mathsf{T} \vdash Prf(p^*, \ulcorner A^* \urcorner) \to A^*$.
2nd case: $\mathsf{T} \nvdash Prf(p^*, \ulcorner A^* \urcorner)$. As $Prf(\cdot,\cdot)$ is recursive $\mathsf{T} \vdash \neg Prf(p^*, \ulcorner A^* \urcorner)$, hence $\mathsf{T} \vdash Prf(p^*, \ulcorner A^* \urcorner) \to A^*$.

■

The main aim to the end of this section is to prove the arithmetical completeness of $\mathcal{P}$ (i.e. the converse of theorem 2.2). In the following subsection 2.1 a sequential version of $\mathcal{P}$ is presented together with a structural analysis (Saturation Lemma). Subsection 2.2 then deals with the arithmetical part of the completeness proof by constructing arithmetical interpretations (countermodels). An overview of the obtained results is presented in subsection 2.3 .

2.1 Gentzen style system for $\mathcal{P}$

In the following, a *sequent* is a formal expression $\Gamma \supset \Delta$, where Γ and Δ are finite sets of modal formulas. If $\Gamma = A_1, \ldots, A_k$ then $\bigwedge \Gamma := A_1 \wedge \ldots \wedge A_k$; analogous definition for $\bigvee \Delta$.

2.3 Definition $\mathcal{P}_\mathcal{G}$ is the sequent calculus with axioms and rules of inference as follows:

- Sequent calculus for classical propositional logic including the cut-rule.
- $\dfrac{A, \Gamma \supset \Delta}{\Box_p A, \Gamma \supset \Delta}\,\mathrm{refl}$

$\mathcal{P}_\mathcal{G}^-$ is the system $\mathcal{P}_\mathcal{G}$ without the cut rule.

2.4 Soundness of $\mathcal{P}_\mathcal{G}$ w.r.t. $\mathcal{P}$ For each sequent $\Gamma \supset \Delta$:

$$\mathcal{P}_\mathcal{G} \vdash \Gamma \supset \Delta \qquad \Longrightarrow \qquad \mathcal{P} \vdash \bigwedge \Gamma \to \bigvee \Delta$$

Proof Straightforward induction on the complexity of the $\mathcal{P}_\mathcal{G}$-proof of $\Gamma \supset \Delta$. ■

2.5 Definition The sequent $\Gamma \supset \Delta$ is called *saturated*, if the following statements hold for all modal formulas A, B and for all proof variables p:

1. $A \to B \in \Delta$ implies $A \in \Gamma$ and $B \in \Delta$,
2. $A \to B \in \Gamma$ implies $B \in \Gamma$ or $A \in \Delta$,
3. $\Box_p A \in \Gamma$ implies $A \in \Gamma$.

2.6 Saturation Lemma Let $\Gamma \supset \Delta$ be a sequent such that $\mathcal{P}_\mathcal{G}^- \not\vdash \Gamma \supset \Delta$. Then there exists a saturated sequent $\Gamma' \supset \Delta'$ such that

(i) $\Gamma \subset \Gamma'$, $\Delta \subset \Delta'$,

(ii) $\Gamma \cup \Delta$ and $\Gamma' \cup \Delta'$ have the same subformulas,

(iii) $\Gamma' \supset \Delta'$ is not an axiom, i.e. $\bot \notin \Gamma'$, $\top \notin \Delta'$ and $\Gamma' \cap \Delta' = \emptyset$,

(iv) $\mathcal{P}_{\mathcal{G}}^{-} \not\vdash \Gamma' \supset \Delta'$.

Furthermore $\Gamma' \supset \Delta'$ is effectively computable from $\Gamma \supset \Delta$.
Such a $\Gamma' \supset \Delta'$ is called a *saturation* of $\Gamma \supset \Delta$.

Proof This is a fairly standard lemma. Here just a recursive algorithm is given, which accepts a sequent as input and which saturates this sequent provided it is not $\mathcal{P}_{\mathcal{G}}^{-}$-provable, otherwise the algorithm fails.

2.7 Saturation Algorithm Given $\Gamma \supset \Delta$, for each subformula S of $\Gamma \cup \Delta$ nondeterministically try to perform one of the following steps:

- if $S = A \to B \in \Delta$ then $\Gamma := \Gamma \cup \{A\}$ and $\Delta := \Delta \cup \{B\}$.
- if $S = A \to B \in \Gamma$ then either $\Gamma := \Gamma \cup \{B\}$ and branch, or $\Delta := \Delta \cup \{A\}$ and branch.
- if $S = \Box_p A \in \Gamma$ then $\Gamma := \Gamma \cup \{A\}$.
- if $\bot \in \Gamma$ or $\top \in \Delta$ or $\Gamma \cap \Delta \neq \emptyset$ (i.e. $\Gamma \supset \Delta$ is an axiom) then backtrack.

Properties of the Saturation Algorithm:

- Termination: there are only finitely many subformulas in $\Gamma \cup \Delta$ and at most two branches in each step.
- (i) and (ii) clearly hold, and (iii) is a immediate consequence of (iv).
- If the algorithm fails then each branch in the computation contains an axiom, and so one can readily construct a $\mathcal{P}_{\mathcal{G}}^{-}$-proof of $\Gamma \supset \Delta$.
- If the algorithm succeeds then the resulting sequent $\Gamma' \supset \Delta'$ is saturated and not $\mathcal{P}_{\mathcal{G}}^{-}$-provable. Otherwise, assume that $\Gamma' \supset \Delta'$ is $\mathcal{P}_{\mathcal{G}}^{-}$-provable and hence, as it is saturated, an axiom. Starting with $\Gamma' \supset \Delta'$ and according to the saturation process construct a $\mathcal{P}_{\mathcal{G}}^{-}$-proof of $\Gamma \supset \Delta$.

■

2.2 Arithmetical completeness

2.8 Main Lemma for $\mathcal{P}$ Let $\Gamma' \supset \Delta'$ be a saturated sequent which is not $\mathcal{P}_{\mathcal{G}}^{-}$-provable. Then there exists an arithmetical interpretation $(\cdot)^*$ which makes all formulas in Γ' true and all formulas in Δ' false, i.e.

$$(\bigwedge \Gamma' \to \bigvee \Delta')^* \quad \text{is false.}$$

Proof For the sentence and proof variables let $(\cdot)^*$ be defined as:

$$S_i{}^* := \begin{cases} \forall x_i(x_i = x_i) & \text{if } S_i \in \Gamma', \\ \forall x_i(x_i \neq x_i) & \text{else.} \end{cases}$$

$$p_i{}^* := 2i$$

By induction on the complexity of a modal formula it follows that $(\cdot)^*$ is an injective arithmetical interpretation of the modal language.

Write $\bigwedge \Gamma'$ as

$$\bigwedge_{i=0}^{m} \bigwedge_{j=0}^{J_i} \Box_{p_i} A_{i,j} \ \wedge \Gamma''$$

where Γ'' contains no formula of the form $\Box_p A$.

By some variant of the arithmetical fixed point argument (Diagonalization Lemma) one can find a predicate $Prf(\cdot,\cdot)$ – and this $Prf(\cdot,\cdot)$ completes the interpretation $(\cdot)^*$ – which solves the following fixed point equation: $\mathtt{T}$ proves

$$\begin{array}{lcl} Prf(u,v) & \longleftrightarrow & \forall r \leq u \Big[\\ & & \quad u = 2r+1 \ \rightarrow \ \widetilde{Prf}(r,v) \ \wedge \\ & & \quad u = 2r \ \rightarrow \ \Big[\ r = 0 \ \rightarrow \ \bigvee_{j=0}^{J_0}(v = \ulcorner A_{0,j}{}^* \urcorner) \ \wedge \\ & & \qquad\qquad \vdots \\ & & \qquad\qquad r = m \ \rightarrow \ \bigvee_{j=0}^{J_m}(v = \ulcorner A_{m,j}{}^* \urcorner) \ \wedge \\ & & \qquad\qquad r > m \ \rightarrow \ v = \ulcorner \forall x_0 \forall x_0 (x_0 = x_0) \urcorner \ \Big] \ \Big] \end{array}$$

Note that $Prf(\cdot,\cdot)$ may occur in each $A_{i,j}{}^*$ and remind that $\widetilde{Prf}(\cdot,\cdot)$ is the Gödel proof predicate for $\mathtt{T}$.

The first task is to show that $Prf(\cdot,\cdot)$ can be constructed in this way.

Let the formula F be defined as

$$\begin{array}{lcl} F(x,y,z_{0,0},z_{0,1},\ldots,z_{m,J_m}) & \longleftrightarrow & \forall r \leq x \Big[\\ & & \quad x = 2r+1 \ \rightarrow \ \widetilde{Prf}(r,y) \ \wedge \\ & & \quad x = 2r \ \rightarrow \ \Big[\ r = 0 \ \rightarrow \ \bigvee_{j=0}^{J_0}(y = z_{0,j}) \ \wedge \\ & & \qquad\qquad \vdots \\ & & \qquad\qquad r = m \ \rightarrow \ \bigvee_{j=0}^{J_m}(y = z_{m,j}) \ \wedge \\ & & \qquad\qquad r > m \ \rightarrow \ y = \ulcorner \forall x_0 \forall x_0 (x_0 = x_0) \urcorner \ \Big] \ \Big] \end{array}$$

and let $Sb_{i,j}(a,b)$ be a standard term corresponding to the primitive recursive function, determined by the following specification:

If a is the Gödel number of a formula $B(x,y,z)$ then consider the interpretation $(\cdot)^{**} := (B(x,y,b),\phi)$ where ϕ is defined on proof and sentence variables identical to $(\cdot)^*$ and put

$$Sb_{i,j}(a,b) := \ulcorner A_{i,j}{}^{**} \urcorner$$

Finally let

$$\begin{array}{rcl} B(x,y,z) & := & F(x,y,Sb_{0,0}(z,z),Sb_{0,1}(z,z),\ldots,Sb_{m,J_m}(z,z)) \\ g & := & \ulcorner B(x,y,z) \urcorner \\ Prf(x,y) & := & B(x,y,g) \end{array}$$

Now observe that $Sb_{i,j}(g,g) = \ulcorner A_{i,j}{}^{*} \urcorner$ as if $a = b = g$ then

$$\begin{array}{rcl} (\cdot)^{**} & \equiv & (B(x,y,g),\phi) \\ & \equiv & (Prf(x,y),\phi) \\ & \equiv & (\cdot)^* \end{array}$$

So it follows that

$$Prf(x,y) \equiv B(x,y,g) \equiv F(x,y,Sb_{0,0}(g,g),Sb_{0,1}(g,g),\ldots,Sb_{m,J_m}(g,g))$$

which is provably equivalent to

$$F(x,y,\ulcorner A_{0,0}{}^{*} \urcorner,\ulcorner A_{0,1}{}^{*} \urcorner,\ldots,\ulcorner A_{m,J_m}{}^{*} \urcorner)$$

Hence this so-defined $Prf(\cdot,\cdot)$ is a solution of the fixed point equation above.

The next task is to show that $(\cdot)^*$ has the desired properties, i.e. that $(\cdot)^*$ makes all formulas in Γ' true and all formulas in Δ' false, and afterwards the proof will be completed by the observation that $Prf(\cdot,\cdot)$ really is a proof predicate.

Let D be some modal formula from $\Gamma' \cup \Delta'$. Note that $Prf(\cdot,\cdot)$ is recursive. Therefore D^* is a closed, recursive arithmetical formula and

$$\begin{array}{rcl} D^* \text{ is true} & \Longleftrightarrow & \mathbf{T} \vdash D^* \\ D^* \text{ is false} & \Longleftrightarrow & \mathbf{T} \vdash \neg D^* \end{array}$$

By induction on the complexity of D it follows that:

$$\begin{array}{rcl} D \in \Gamma' & \Longrightarrow & D^* \text{ is true} \\ D \in \Delta' & \Longrightarrow & D^* \text{ is false} \end{array}$$

- $D = \top \in \Gamma'$: $D^* = (0 = 0)$ is true.
- $D = \top \in \Delta'$: this case is not possible due to the Saturation Lemma.
- $D = \bot \in \Gamma'$: this case is not possible due to the Saturation Lemma.
- $D = \bot \in \Delta'$: $D^* = (0 = 1)$ is false.

- $D = S_j \in \Gamma'$: $D^* = \forall x_i(x_i = x_i)$ is true.
- $D = S_j \in \Delta'$: $D^* = \forall x_i(x_i \neq x_i)$ is false.
- $D = (A \to B) \in \Gamma'$: As $\Gamma' \supset \Delta'$ is saturated, $B \in \Gamma'$ or $A \in \Delta'$. By the induction hypothesis B^* is true or A^* is false, hence $(A \to B)^*$ is true.
- $D = (A \to B) \in \Delta'$: As $\Gamma' \supset \Delta'$ is saturated, $A \in \Gamma'$ and $B \in \Delta'$. By the induction hypothesis A^* is true and B^* is false, hence $(A \to B)^*$ is false.
- $D = \Box_{p_i} A_{i,j} \in \Gamma'$: $(\Box_{p_i} A_{i,j})^* = Prf(p_i{}^*, \ulcorner A_{i,j}{}^* \urcorner) = Prf(2i, \ulcorner A_{i,j}{}^* \urcorner)$ is true by the fixed point equation.
- $D = \Box_{p_i} B \in \Delta'$ for some $i \leq m$: $(\Box_{p_i} B)^* = Prf(2i, \ulcorner B^* \urcorner)$ is false by the fixed point equation as $\ulcorner B^* \urcorner \neq \ulcorner A_{i,j}{}^* \urcorner$ for any $j \leq J_i$. Here is made use of the fact that Γ' and Δ' are disjoint.
- $D = \Box_{p_i} C \in \Delta'$ for some $i > m$: $(\Box_{p_i} C)^* = Prf(2i, \ulcorner C^* \urcorner)$ is false by the fixed point equation as there exists no modal formula C such that $\ulcorner C^* \urcorner = \ulcorner \forall x_0 \forall x_0(x_0 = x_0) \urcorner$.

So it remains to show that $Prf(\cdot, \cdot)$ can be used as a proof predicate in $\mathbf{T}$:

$$\mathbf{T} \vdash \varphi \qquad \Longleftrightarrow \qquad \exists n \in \mathbb{N} : \ Prf(n, \ulcorner \varphi \urcorner) \text{ is true}$$

Let $\mathbf{T} \vdash \varphi$. By the definition of the Gödel proof predicate $\widetilde{Prf}(\cdot, \cdot)$ there exists an $n_0 \in \mathbb{N}$ such that

$$\widetilde{Prf}(n_0, \ulcorner \varphi \urcorner)$$

holds, hence by the fixed point equation

$$Prf(2n_0 + 1, \ulcorner \varphi \urcorner)$$

Conversely if $Prf(n_0, \ulcorner \varphi \urcorner)$ is true for some $n_0 \in \mathbb{N}$, consider the three cases:

1st case: $n_0 = 2k{+}1$. If $Prf(2k + 1, \ulcorner \varphi \urcorner)$ then by the fixed point equation $\widetilde{Prf}(k, \ulcorner \varphi \urcorner)$, hence $\mathbf{T} \vdash \varphi$.

2nd case: $n_0 = 2k$ and $k \leq m$. By the fixed point equation $\ulcorner \varphi \urcorner = \ulcorner A_{k,j}{}^* \urcorner$ for some $\Box_{p_k} A_{k,j} \in \Gamma'$. Then, by the injectivity of the Gödel numbering $\varphi \equiv A_{k,j}{}^*$. But $A_{k,j}$ is in Γ' as $\Gamma' \supset \Delta'$ is saturated, and thus φ is true and provable in $\mathbf{T}$.

3rd case: $n_0 = 2k$ and $k > m$. It follows $\varphi \equiv \forall x_0 \forall x_0(x_0 = x_0)$ from the fixed point equation. Trivially $\mathbf{T} \vdash \varphi$.

So $Prf(\cdot, \cdot)$ is a proof predicate for $\mathbf{T}$ and the Main Lemma for $\mathcal{P}$ is proved. Even something more has been proved, namely that there exists an arithmetical interpretation which makes all formulas in Γ' provable and all formulas in Δ' refutable, i.e.

$$\mathbf{T} \vdash \neg(\bigwedge \Gamma \to \bigvee \Delta)^*$$

■

2.9 Corollary Let $\Gamma \supset \Delta$ be a sequent. Then

$$\left[\forall^*: \ (\bigwedge \Gamma \to \bigvee \Delta)^* \text{ is true}\right] \quad \Longrightarrow \quad \mathcal{P}_{\mathcal{G}}^- \vdash \Gamma \supset \Delta$$

Proof Assume that $\mathcal{P}_{\mathcal{G}}^- \nvdash \Gamma \supset \Delta$. By the Saturation Lemma there exists a saturated sequent $\Gamma' \supset \Delta'$ which is not $\mathcal{P}_{\mathcal{G}}^-$-provable. Hence by the Main Lemma there exists an arithmetical interpretation $(\cdot)^*$ which makes $\bigwedge \Gamma' \to \bigvee \Delta'$ false. But as $\Gamma \subset \Gamma'$ and $\Delta \subset \Delta'$, this interpretation falsifies also $\bigwedge \Gamma \to \bigvee \Delta$.
■

2.3 The Main Theorem for $\mathcal{P}$

So far, it has been shown that for any sequent $\Gamma \supset \Delta$ the following diagram is valid:

$$\begin{array}{ccccc}
\forall^*: \ (\bigwedge \Gamma \to \bigvee \Delta)^* \text{ is true} & \Longleftarrow & \forall^*: \ \mathbf{T} \vdash (\bigwedge \Gamma \to \bigvee \Delta)^* \\
\Big\Downarrow & & \Big\Uparrow \\
\mathcal{P}_{\mathcal{G}}^- \vdash \Gamma \supset \Delta & \Longrightarrow & \mathcal{P}_{\mathcal{G}} \vdash \Gamma \supset \Delta & \Longrightarrow & \mathcal{P} \vdash \bigwedge \Gamma \to \bigvee \Delta
\end{array}$$

Hence an immediate consequence is the soundness and completeness of the proof system $\mathcal{P}$ with respect to arithmetical interpretations:

2.10 Main Theorem for $\mathcal{P}$

- $\mathcal{P}$ is arithmetically sound and complete, i.e. for any modal formula A:

$$\begin{array}{lll}
\mathcal{P} \vdash A & \Longleftrightarrow & \forall^*: \ \mathbf{T} \vdash A^* \qquad \text{and moreover} \\
& \Longleftrightarrow & \forall^*: \ A^* \text{ is true}
\end{array}$$

- $\mathcal{P}$ is decidable.
- $\mathcal{P}_{\mathcal{G}}$ is equivalent to $\mathcal{P}$ and admits cut elimination.

Proof Decidability: Apply the saturation algorithm 2.7 to the sequent $\supset A$. If the algorithm finds a saturation then there exists an arithmetical interpretation which makes A false, otherwise A is true in all arithmetical interpretations.
■

3 Functionality

This section is devoted to the modal system $\mathcal{PF}$ which corresponds to functional arithmetical interpretations. The proofs go along the lines of the previous section on the basic system $\mathcal{P}$.

3.1 Example $\mathcal{PF} \vdash \neg\Box_p\bot,\ \Box_p S_0 \to \neg\Box_p S_1,\ \Box_p A \to \neg\Box_p(A \wedge A),\ \ldots$

and $\mathcal{PF}$ proofs $\neg\Box_p\Box_p\top$ for some proof variable p:

Axiom (A2):	$\Box_p\Box_p\top \to \Box_p\top$	(1)
Axiom (A3):	$\Box_p\Box_p\top \to \neg\Box_p\top$	(2)
From (1) and (2):	$\neg\Box_p\Box_p\top$	

3.2 Remark In the sequel it will be shown that $\mathcal{PF}$ (as $\mathcal{P}$) does not prove any modal formula of the form $\Box_p A$. But $\mathcal{PF}$ (as $\mathcal{P}$) proves $\neg\Box_p A$ for some formulas A. In the case of $\neg\Box_p\bot$ it is due to the refutability of $\bot$, and in the case of $\neg\Box_p\Box_p\top$ it is due to the functional behaviour of $\Box_p(\cdot)$ which, according to (A3) does not allow both $\Box_p A$ and $\Box_p B$ to hold simultaneously for syntactically different A and B.

3.3 Soundness of $\mathcal{PF}$ Let A be a modal formula. Then

$$\mathcal{PF} \vdash A \quad \Longrightarrow \quad \begin{array}{ll} \forall^*(\text{functional}): & \mathsf{T} \vdash A^* \\ \forall^*(\text{functional}): & A^* \text{ is true} \end{array} \quad \text{and therefore}$$

Proof In view of theorem 2.2 it remains to verify the soundness of the Functionality Axiom:

(A3) 1st case: $\mathsf{T} \vdash Prf(p^*, \ulcorner A^* \urcorner)$. As $\ulcorner A^* \urcorner \not\equiv \ulcorner B^* \urcorner$ $(A \not\equiv B)$ and by the functionality condition $\mathsf{T} \vdash \neg Prf(p^*, \ulcorner B^* \urcorner)$, hence $\mathsf{T} \vdash Prf(p^*, \ulcorner A^* \urcorner) \to \neg Prf(p^*, \ulcorner B^* \urcorner)$.
2nd case: $\mathsf{T} \nvdash Prf(p^*, \ulcorner A^* \urcorner)$. As $Prf(\cdot,\cdot)$ is recursive $\mathsf{T} \vdash \neg Prf(p^*, \ulcorner A^* \urcorner)$, hence $\mathsf{T} \vdash Prf(p^*, \ulcorner A^* \urcorner) \to \neg Prf(p^*, \ulcorner B^* \urcorner)$.

■

3.1 Gentzen style system for $\mathcal{PF}$

3.4 Definition $\mathcal{PF}_\mathcal{G}$ is a sequent calculus with axioms and rules of inference as follows:

- Sequent calculus for classical propositional logic including the cut-rule.
- $\dfrac{A, \Gamma \supset \Delta}{\Box_p A, \Gamma \supset \Delta}\text{refl} \qquad \dfrac{\Gamma \supset \Delta, \Box_p A}{\Box_p B, \Gamma \supset \Delta}\text{func} \quad (A \not\equiv B)$

$\mathcal{PF}_{\mathcal{G}}^{-}$ is the system $\mathcal{PF}_{\mathcal{G}}$ without the cut rule.

3.5 Soundness of $\mathcal{PF}_{\mathcal{G}}$ w.r.t. $\mathcal{PF}$ For each sequent $\Gamma \supset \Delta$:

$$\mathcal{PF}_{\mathcal{G}} \vdash \Gamma \supset \Delta \qquad \Longrightarrow \qquad \mathcal{PF} \vdash \bigwedge \Gamma \to \bigvee \Delta$$

■

3.6 Definition The sequent $\Gamma \supset \Delta$ is called *functionally saturated*, if the following statements hold for all modal formulas A, B and for all proof variables p:

1. $A \to B \in \Delta$ implies $A \in \Gamma$ and $B \in \Delta$,
2. $A \to B \in \Gamma$ implies $B \in \Gamma$ or $A \in \Delta$,
3. $\Box_p A \in \Gamma$ implies $A \in \Gamma$ and $\Box_p B \in \Delta$ for each subformula $\Box_p B$ of $\Gamma \cup \Delta$ such that $A \not\equiv B$.

3.7 Saturation Lemma for $\mathcal{PF}_{\mathcal{G}}$ Let $\Gamma \supset \Delta$ be a sequent such that $\mathcal{PF}_{\mathcal{G}}^{-} \nvdash \Gamma \supset \Delta$. Then there exists a functionally saturated sequent $\Gamma' \supset \Delta'$ such that

(i) $\Gamma \subset \Gamma'$, $\Delta \subset \Delta'$,

(ii) $\Gamma \cup \Delta$ and $\Gamma' \cup \Delta'$ have the same subformulas,

(iii) $\bot \notin \Gamma'$ and $\top \notin \Delta'$ and $\Gamma' \cap \Delta' = \emptyset$, and for each proof variable p there are no distinct formulas A and B such that both $\Box_p A$ and $\Box_p B$ are in Γ'.

(iv) $\mathcal{PF}_{\mathcal{G}}^{-} \nvdash \Gamma' \supset \Delta'$.

Furthermore $\Gamma' \supset \Delta'$ is effectively computable from $\Gamma \supset \Delta$.
Such a $\Gamma' \supset \Delta'$ is called a *functional saturation* of $\Gamma \supset \Delta$.

Proof The Saturation Algorithm for $\mathcal{PF}_{\mathcal{G}}$ works similarly to that for $\mathcal{P}_{\mathcal{G}}$:

- if $S = A \to B \in \Delta$ then $\Gamma := \Gamma \cup \{A\}$ and $\Delta := \Delta \cup \{B\}$.
- if $S = A \to B \in \Gamma$ then either $\Gamma := \Gamma \cup \{B\}$ and branch, or $\Delta := \Delta \cup \{A\}$ and branch.
- if $S = \Box_p A \in \Gamma$ then $\Gamma := \Gamma \cup \{A\}$ and $\Delta := \Delta \cup \{\Box_p B\}$ for each subformula $\Box_p B$ of $\Gamma \cup \Delta$ such that $A \not\equiv B$.
- if $\bot \in \Gamma$ or $\top \in \Delta$ or $\Gamma \cap \Delta \neq \emptyset$ then backtrack.

The required properties (i) to (iv) are proved in the same way as in the Saturation Lemma 2.6 for $\mathcal{P}$.
■

3.2 Arithmetical completeness

3.8 Main Lemma for $\mathcal{PF}$ Let $\Gamma' \supset \Delta'$ be a functionally saturated sequent which is not $\mathcal{PF}^-_{\mathcal{G}}$-provable. Then there exists a functional interpretation $(\cdot)^*$ which makes all formulas in Γ' true and all formulas in Δ' false, i.e.

$$(\bigwedge \Gamma' \to \bigvee \Delta')^* \quad \text{is false.}$$

Proof For the sentence and proof variables let $(\cdot)^*$ be defined as in case of $\mathcal{P}$, namely:

$$S_i^* \;:=\; \begin{cases} \forall x_i(x_i = x_i) & \text{if } S_i \in \Gamma', \\ \forall x_i(x_i \neq x_i) & \text{else.} \end{cases}$$

$$p_i^* \;:=\; 2i$$

Again it follows that $(\cdot)^*$ is an injective arithmetical interpretation of the modal language.

Now write $\bigwedge \Gamma'$ as

$$\bigwedge_{i=0}^{m} \Box_{p_i} A_i \;\wedge \Gamma''$$

where Γ'' contains no formula of the form $\Box_p A$. This notion is possible, as, due to the functional saturation and non-provability of $\Gamma' \supset \Delta'$, there is no proof variable p such that both $\Box_p A$ and $\Box_p B$ may be contained in Γ' for distinct A and B.

Again let $\widetilde{Prf}(\cdot,\cdot)$ be a standard proof predicate for $\mathtt{T}$. The *fixed point equation* for $Prf(\cdot,\cdot)$ is simply a special case of that for $\mathcal{P}$: $\mathtt{T}$ proves

$$\begin{array}{lcl@{\quad}l@{\quad}l@{\quad}l} Prf(u,v) & \longleftrightarrow & \forall r \le u \Big[& & & \\ & u = 2r+1 & \to & \widetilde{Prf}(r,v) & \wedge & \\ & u = 2r & \to & \Big[\; r = 0 & \to \; v = \ulcorner {A_0}^* \urcorner & \wedge \\ & & & \vdots & & \\ & & & r = m & \to \; v = \ulcorner {A_m}^* \urcorner & \wedge \\ & & & r > m & \to \; v = \ulcorner \forall x_0 \forall x_0 (x_0 = x_0) \urcorner & \Big] \Big] \end{array}$$

Clearly $Prf(\cdot,\cdot)$ is functional.

The remaining part of the proof is exactly as in the case for $\mathcal{P}$, and again it is clear that this interpretation $(\cdot)^*$ even has the property that

$$\mathtt{T} \vdash \neg(\bigwedge \Gamma \to \bigvee \Delta)^*$$

■

3.9 Corollary Let $\Gamma \supset \Delta$ be a sequent. Then

$$\Big[\forall^*(\text{functional}) : \quad (\bigwedge \Gamma \to \bigvee \Delta)^* \;\text{ is true}\Big] \quad \Longrightarrow \quad \mathcal{PF}^-_{\mathcal{G}} \vdash \Gamma \supset \Delta$$

■

3.3 The Main Theorem for $\mathcal{PF}$

So far, it has been shown that for any sequent $\Gamma \supset \Delta$ the following diagram is valid:

$$\begin{array}{ccccc}
\forall^*(\text{functional}): \ (\bigwedge\Gamma \to \bigvee\Delta)^* \text{ is true} & \Longleftarrow & \forall^*(\text{functional}): \ \mathsf{T} \vdash (\bigwedge\Gamma \to \bigvee\Delta)^* \\
\Downarrow & & \Uparrow \\
\mathcal{PF}_{\mathcal{G}}^{-} \vdash \Gamma \supset \Delta & \Longrightarrow & \mathcal{PF}_{\mathcal{G}} \vdash \Gamma \supset \Delta & \Longrightarrow & \mathcal{PF} \vdash \bigwedge\Gamma \to \bigvee\Delta
\end{array}$$

3.10 Main Theorem for $\mathcal{PF}$

- $\mathcal{PF}$ is arithmetically sound and complete, i.e. for any modal formula A:

$$\begin{array}{lll}
\mathcal{PF} \vdash A & \Longleftrightarrow & \forall^*(\text{functional}): \ \mathsf{T} \vdash A^* \qquad \text{and moreover} \\
& \Longleftrightarrow & \forall^*(\text{functional}): \ A^* \text{ is true}
\end{array}$$

- $\mathcal{PF}$ is decidable.
- $\mathcal{PF}_{\mathcal{G}}$ is equivalent to $\mathcal{PF}$ and admits cut elimination.

Proof Decidability: The modal formula A is true in all arithmetical interpretations iff the Saturation Algorithm for $\mathcal{PF}$ fails to find a functional saturation of $\supset A$.
■

4 Monotonicity. The logic of the standard proof predicate

The example 1.10 from the Introduction demonstrates that the logic of standard proof predicates does not coincide with $\mathcal{PF}$. In this section the logic $\mathcal{PFM}$ is introduced, and it is shown that $\mathcal{PFM}$ is sound and complete with respect to all standard interpretations.

A further result of the completeness proof is that an arbitrary standard proof predicate can be fixed, and that $\mathcal{PFM}$ is sound and complete with respect to all interpretations which use this fixed proof predicate. This property holds in particular for the Gödel proof predicate. So $\mathcal{PFM}$ is not only another specialization in the studies of proof predicates but differs in a fundamental property from $\mathcal{P}$ respectively $\mathcal{PF}$.

4.1 Hilbert style system for $\mathcal{PFM}$

The formula $\neg\Box_p\neg\Box_p\top$ from the Introduction is an example of the monotonicity scheme (A4). Thus, $\mathcal{PFM}$ is a proper extension of $\mathcal{PF}$.

4.1 Soundness of $\mathcal{PFM}$ Let A be a modal formula. Then

$$\mathcal{PFM} \vdash A \quad \Longrightarrow \quad \begin{array}{ll} \forall^*(\text{standard}): & \mathsf{T} \vdash A^* \\ \forall^*(\text{standard}): & A^* \text{ is true} \end{array} \quad \text{and therefore}$$

Proof In view of theorem 3.3 it remains to verify the soundness of the Monotonicity Axiom:

(A4) Assume that T does not prove $(\neg[\Box_{q_1}A_2(q_2) \wedge \Box_{q_2}A_3(q_3) \wedge \ldots \wedge \Box_{q_n}A_1(q_1)])^*$. It follows that the sentences

$$Prf(q_1{}^*, \ulcorner(A_2(q_2))^*\urcorner),\ Prf(q_2{}^*, \ulcorner(A_3(q_3))^*\urcorner),\ \ldots,\ Prf(q_n{}^*, \ulcorner(A_1(q_1))^*\urcorner)$$

are true. $Prf(q_i{}^*, \ulcorner(A_j(q_j))^*\urcorner)$ implies by definition 1.6 that $q_i{}^* \geq \ulcorner(A_j(q_j))^*\urcorner$. By the convention on Gödel numbering (remark 1.7) – as q_j is a subterm of $A_j(q_j)$ – it follows that $q_j{}^* \leq \ulcorner q_j{}^*\urcorner < \ulcorner(A_j(q_j))^*\urcorner$. Hence

$$q_1{}^* \geq \ulcorner(A_2(q_2))^*\urcorner > q_2{}^* \geq \ulcorner(A_3(q_3))^*\urcorner > \cdots > q_n{}^* \geq \ulcorner(A_1(q_1))^*\urcorner > q_1{}^*$$

which is a contradiction.

■

4.2 Gentzen style system for $\mathcal{PFM}$

4.2 Definition $\mathcal{PFM}_{\mathcal{G}}$ is a sequent calculus with axioms and rules of inference as follows:

- Sequent calculus for classical propositional logic including the cut-rule.
- $\dfrac{A, \Gamma \supset \Delta}{\Box_p A, \Gamma \supset \Delta}\text{refl} \qquad \dfrac{\Gamma \supset \Delta, \Box_p A}{\Box_p B, \Gamma \supset \Delta}\text{func} \quad (A \not\equiv B)$
- $\Box_{q_1}A_2(q_2), \Box_{q_2}A_3(q_3), \ldots, \Box_{q_n}A_1(q_1) \supset \qquad \text{mon}$

As usual, $\mathcal{PFM}_{\mathcal{G}}^-$ denotes the system $\mathcal{PFM}_{\mathcal{G}}$ without the cut rule.

■

The frame of the proof for the Main Theorem for $\mathcal{PFM}$ is the same as for $\mathcal{PF}$ in subsection 3.3 . The following statements are easy to prove.

4.3 Soundness of $\mathcal{PFM}_{\mathcal{G}}$ w.r.t. $\mathcal{PFM}$ For each sequent $\Gamma \supset \Delta$:

$$\mathcal{PFM}_{\mathcal{G}} \vdash \Gamma \supset \Delta \quad \Longrightarrow \quad \mathcal{PFM} \vdash \bigwedge \Gamma \to \bigvee \Delta$$

■

4.4 Saturation Lemma and Algorithm The definition 3.6 of a saturated sequent for $\mathcal{PF}_\mathcal{G}$ is still valid for $\mathcal{PFM}_\mathcal{G}$. The Saturation Lemma 3.7 for $\mathcal{PF}_\mathcal{G}$ can be extended by the statement that if $\Gamma' \supset \Delta'$ is a saturated sequent which is not $\mathcal{PFM}_\mathcal{G}^-$-provable then Γ' contains no *nonmonotonic witness*; a nonmonotonic witness is a configuration $\Box_{q_1} A_2(q_2), \Box_{q_2} A_3(q_3), \ldots, \Box_{q_n} A_1(q_1)$ where $A_i(q_i)$ is a modal formula which contains an occurrence of the proof variable q_i. Consequently, the Saturation Algorithm for $\mathcal{PFM}_\mathcal{G}$ is essentially the same as for $\mathcal{PF}_\mathcal{G}$, the only new step is to check whether Γ contains a nonmonotonic witness; if *yes*, then the sequent is $\mathcal{PFM}_\mathcal{G}^-$-provable and one has to backtrack; if *no*, then the saturation procedure can be continued.

■

4.5 Main Lemma for $\mathcal{PFM}$ Let $\Gamma' \supset \Delta'$ be a functionally saturated sequent which is not $\mathcal{PFM}_\mathcal{G}^-$-provable. Then there exists a standard interpretation $(\cdot)^*$ which makes all formulas in Γ' true and all formulas in Δ' false, i.e.

$$(\bigwedge \Gamma' \to \bigvee \Delta')^* \quad \text{is false.}$$

Proof Due to the Monotonicity Axiom this lemma can and has to be proved in a rather different and somewhat simpler way compared to $\mathcal{P}$ respectively $\mathcal{PF}$: The $\Box$ is interpreted independently from $\Gamma' \supset \Delta'$ as a fixed standard proof predicate. On the contrary, the proof variables cannot be interpreted in a fixed way any more as section 5 about uniformization demonstrates; they are defined stepwise by means of an ordering on the proof variables defined below.

The binary relation "$\prec$" is defined on the proof variables occurring in $\Gamma' \cup \Delta'$ as:

$$\begin{array}{lll} p \prec q & :\Longleftrightarrow & \text{there exist proof variables } q = q_1, \ldots, q_n = p \quad (n > 1) \\ & & \text{such that } \Box_{q_1} A_2(q_2), \ldots, \Box_{q_{n-1}} A_n(q_n) \in \Gamma' \end{array}$$

"$\prec$" is a strict, well-founded ordering on the proof variables:
It is irreflexive, since if $\Box_{q_1} A_2(q_2), \ldots, \Box_{q_{n-1}} A_1(q_1) \in \Gamma'$ then $\mathcal{PFM}_\mathcal{G}^- \vdash \Gamma' \supset \Delta'$. The transitivity follows directly from the definition, and the relation is well-founded as $\Gamma' \supset \Delta'$ contains only finitely many proof variables.

The function $s(\cdot)$ is defined on the proof variables occurring in $\Gamma' \cup \Delta'$ as:

$$s(p) \;:=\; \begin{cases} 1 + \max\{s(q) \mid q \prec p\} & \text{if there exists some } q \text{ such that } q \prec p, \\ 1 & \text{else.} \end{cases}$$

It is clear that $s(\cdot)$ is well-defined for all proof variables occurring in $\Gamma' \cup \Delta'$. In particular, $s(p) = 1$ for all isolated and minimal (with respect to "$\prec$") proof variables p, e.g. for all those which do not occur in Γ'. Next $s(A)$ is defined for all modal formulas A occurring in $\Gamma' \cup \Delta'$:

$$s(A) \;:=\; \begin{cases} 0 & \text{for } \Box\text{-free } A, \\ \max\{s(p) \mid p \text{ is a proof variable which occurs in } A\} & \text{else.} \end{cases}$$

Again, it is clear that $s(\cdot)$ is well-defined. The main property that is used in connection with this ordering is, that if $\Box_p A \in \Gamma'$ and $s(\Box_p A) = k$ then $s(A) < k$.

The interpretation $(\cdot)^*$ is defined for sentence variables as:

$$S_i^* \quad := \begin{cases} \forall x_i (x_i = x_i) & \text{if } S_i \in \Gamma', \\ \forall x_i (x_i \neq x_i) & \text{else.} \end{cases}$$

So it is already clear that the interpretation of a modal formula is recursive. As mentioned before, the $\Box$ is interpreted as an arbitrary standard proof predicate, for example the Gödel one:

$$(\Box_p A)^* = \widetilde{Prf}(p^*, \ulcorner A^* \urcorner)$$

So $(\cdot)^*$ is a standard interpretation.

By an induction on $k = 0, 1, \ldots$ and for every formula D contained in $\Gamma' \cup \Delta'$ such that $s(D) = k$,

(i) D^* is defined, i.e. the interpretation for all proof variables occurring in D is fixed,

(ii) it is proved that

$$\begin{array}{lll} \text{if } D \in \Gamma' & \text{then} & D^* \text{ is true, and} \\ \text{if } D \in \Delta' & \text{then} & D^* \text{ is false.} \end{array}$$

If D is a Boolean constant, a sentence variable or a Boolean combination of formulas then part (ii) is proved as in the case for $\mathcal{P}$ (Main Lemma 2.8 for $\mathcal{P}$).

induction base: $s(D) = 0$, so D is $\Box$-free and D^* is independent from the interpretation of the proof variables, hence well-defined.

induction step: Let (i) and (ii) be fulfilled for every formula E such that $s(E) < k$, and let D be of the form $\Box_{p_i} A$ with $s(D) = k$. As $\Gamma' \supset \Delta'$ is functionally saturated, if $\Box_{p_i} A \in \Gamma'$ then $\Box_{p_i} A \notin \Delta'$ and there is no $\Box_{p_i} B$ in Γ' when A and B are distinct.

If $\Box_{p_i} A \in \Gamma'$ then $A \in \Gamma'$ and $s(A) < k$. Hence A^* is a true recursive formula and so $\mathsf{T} \vdash A^*$. Let ${p_i}^*$ be the Gödel number of a proof of A^* in T. So $(\Box_{p_i} A)^* = \widetilde{Prf}({p_i}^*, \ulcorner A^* \urcorner)$ is defined and true.

If $\Box_{p_i} A \in \Delta'$ and $\Box_{p_i} B \in \Gamma'$ for some modal formula B then ${p_i}^*$ is already defined and $(\Box_{p_i} A)^* = \widetilde{Prf}({p_i}^*, \ulcorner A^* \urcorner)$ is false, as $\widetilde{Prf}(\cdot, \cdot)$ is functional and ${p_i}^*$ is the Gödel number of a proof of B^* which is different from A^*.

If $\Box_{p_i} A \in \Delta'$ and there is no modal formula B such that $\Box_{p_i} B \in \Gamma'$ then let ${p_i}^*$ be the Gödel number of a proof of the sentence $\forall x_i \forall x_i (x_i = x_i)$ in T. So $(\Box_{p_i} A)^* = \widetilde{Prf}({p_i}^*, \ulcorner A^* \urcorner)$ is defined and false, as $\widetilde{Prf}(\cdot, \cdot)$ is functional and there is no modal formula A such that $\ulcorner A^* \urcorner = \ulcorner \forall x_i \forall x_i (x_i = x_i) \urcorner$.

The induction is done and it has been shown that for every modal formula D contained in $\Gamma' \cup \Delta'$, D^* is recursive, and

$$\begin{array}{ll} \text{if } D \in \Gamma' & \text{then} \quad D^* \text{ is true,} \\ \text{if } D \in \Delta' & \text{then} \quad D^* \text{ is false.} \end{array}$$

Therefore $(\bigwedge \Gamma' \to \bigvee \Delta')^*$ is a false recursive formula and thus not provable in T.

It is clear that not only the Gödel proof predicate $\widetilde{Prf}(\cdot,\cdot)$ can be used as a fixed proof predicate for this interpretation $(\cdot)^*$ but any standard one.
■

4.6 Main Theorem for $\mathcal{PFM}$

- $\mathcal{PFM}$ is arithmetically sound and complete, i.e. for any modal formula A:

$$\begin{array}{lll} \mathcal{PFM} \vdash A & \iff & \forall^*(\text{standard}): \quad \mathsf{T} \vdash A^* \qquad \text{and moreover} \\ & \iff & \forall^*(\text{standard}): \quad A^* \text{ is true} \end{array}$$

- $\mathcal{PFM}$ is decidable.
- $\mathcal{PFM}_{\mathcal{G}}$ is equivalent to $\mathcal{PFM}$ and admits cut elimination.
- Let $\widehat{Prf}(\cdot,\cdot)$ be a standard proof predicate. Then for every modal formula A:

$$\mathcal{PFM} \vdash A \quad \iff \quad A^* \text{ is true for each } (\cdot)^* \text{ based on } \widehat{Prf}(\cdot,\cdot)$$

Proof A decision procedure is given by the Saturation Algorithm 4.4 above.
■

5 Uniform proof predicates

A natural question is whether there exists a uniform proof predicate for $\mathcal{P}$ resp. $\mathcal{PF}$ too, i.e. whether there exists a fixed proof predicate $Prf(\cdot,\cdot)$ under which for every modal formula A

$$\mathcal{P} \vdash A \iff \forall^*: \quad \mathsf{T} \vdash A^*$$

respectively, if there exists a fixed functional proof predicate under which

$$\mathcal{PF} \vdash A \iff \forall^*: \quad \mathsf{T} \vdash A^*$$

So in this case $\forall^*$ quantifies only proof and sentence variables. Uniform proof predicates are in a certain sense proof predicates *without any special properties*. For example, a uniform proof predicate for $\mathcal{P}$ may not be functional for obvious reasons.

The main result of this section is that there exist uniform proof predicates for $\mathcal{P}$ and $\mathcal{PF}$. The construction of a uniform proof predicate for $\mathcal{PF}$ will be described in the following; the case of $\mathcal{P}$ can be treated similarly.

5.1 Theorem There exists a functional proof predicate $\widehat{Prf}(\cdot,\cdot)$ such that for every modal formula A:

$$\mathcal{PF} \vdash A \iff \mathtt{T} \vdash A^* \text{ for each } (\cdot)^* \text{ based on } \widehat{Prf}(\cdot,\cdot)$$

Proof If $\mathcal{PF} \vdash A$ then it follows by theorem 3.3 that $\mathtt{T} \vdash A^*$ for each functional interpretation $(\cdot)^*$. Trivially $\mathtt{T} \vdash A^*$ holds also for each interpretation, which has $\widehat{Prf}(\cdot,\cdot)$ as its functional proof predicate. So assume that A is not $\mathcal{PF}$-provable. The proof will follow the outline of the proofs for theorems 2.8 and 3.8, but in this case the fixed point equation must be independent from A.

From the proof of Lemma 3.7 it follows that the saturation procedure for $\mathcal{PF}$ is primitive recursive, i.e. that $\mathcal{PF}$ is primitive recursive. Let $A_0, A_1, \ldots$ be a primitive recursive list of all modal formulas not provable in $\mathcal{PF}$, and let $\Gamma_0 \supset \Delta_0, \Gamma_1 \supset \Delta_1, \ldots$ be a primitive recursive list of sequents such that for every i, $\Gamma_i \supset \Delta_i$ is a saturation of $\supset A_i$. Let $<\cdot,\cdot>$ be a primitive recursive pairing function and let $(\cdot)_1$, $(\cdot)_2$ be the corresponding projection functions. Let $C(x)$ be a natural formalization of

"There exists a modal formula B such that $\Box_{p_{(x)_2}} B \in \Gamma_{(x)_1}$".

Note that $C(x)$ is primitive recursive, since the existential quantifier occurring in it can be bounded primitive recursively in x (cf. remark 1.7). The construction of Lemma 3.8 gives primitive recursively, for each formula A_n, a proof predicate and an interpretation of the sentence and proof variables such that $A_n{}^*$ is false.

For each n let the interpretation ϕ_n of the sentence and proof variables be defined as:

$$\phi_n(S_i) := \begin{cases} \forall x_i(x_i = x_i) & \text{if } S_i \in \Gamma_n, \\ \forall x_i(x_i \neq x_i) & \text{else.} \end{cases}$$

$$\phi_n(p_i) := 2\cdot<n,i>$$

Notice that the interpretation of both proof and sentence variables depends from n.

The predicate $\widehat{Prf}(\cdot,\cdot)$ can now be defined by the following *fixed point equation*:

$$\begin{array}{lll} \widehat{Prf}(u,v) & \longleftrightarrow & \forall r \leq u \Big[\\ \quad u = 2r+1 & \rightarrow & \widetilde{Prf}(r,v) \quad \wedge \\ \quad u = 2r & \rightarrow & \Big[\; C(r) \rightarrow v = \ulcorner B^* \urcorner \text{ for a modal formula } B \text{ such that } \Box_{p_{(r)_2}} B \in \Gamma_{(r)_1} \text{ (such a formula } B \text{ is unique as } \Gamma_{(r)_1} \supset \Delta_{(r)_1} \text{ is functionally saturated) and the interpretation } (\cdot)^* = (\widehat{Prf}(\cdot,\cdot), \phi_{(r)_1}). \\ & & \quad \neg C(r) \rightarrow v = \ulcorner \forall x_0 \forall x_0 (x_0 = x_0) \urcorner \quad \Big] \Big] \end{array}$$

5.2 Lemma Let D be a modal formula contained in $\Gamma_n \cup \Delta_n$. Then:

$$\begin{array}{lll} D \in \Gamma_n & \Longrightarrow & D^* \text{ is true} \\ D \in \Delta_n & \Longrightarrow & D^* \text{ is false} \end{array}$$

Proof Induction on the complexity of D:

- D is atomic: by the definition of $(\cdot)^*$.
- The case of Boolean connectives is straightforward.
- $D = \Box_{p_i} B \in \Gamma_n$. Then

$$(\Box_{p_i} B)^* = \widehat{Prf}(2^{\cdot} <n, i>, \ulcorner B^* \urcorner)$$

  is true according to the fixed point equation.
- $D = \Box_{p_i} B \in \Delta_n$. Then $C(<n, i>)$ is violated, and $\ulcorner B^* \urcorner = \ulcorner \forall x_0 \forall x_0 (x_0 = x_0) \urcorner$ is also false as there exists no modal formula B such that $B^* \equiv \forall x_0 \forall x_0 (x_0 = x_0)$. Therefore $\widehat{Prf}(2^{\cdot} <n, i>, \ulcorner B^* \urcorner)$ is false, too.

■

5.3 Lemma

(a) $\widehat{Prf}(\cdot, \cdot)$ is primitive recursive and functional.

(b) $\mathsf{T} \vdash \varphi \iff \widehat{Prf}(n, \ulcorner \varphi \urcorner)$ for some n.

Proof

(a) It is easy to see that the right side of the fixed point equation is provably equivalent to a primitive recursive formula because all the quantifiers in the descriptions of functions and predicates are bounded by the corresponding primitive recursive functions. Thus $\widehat{Prf}(\cdot, \cdot)$ is primitive recursive. Obviously, $\widehat{Prf}(\cdot, \cdot)$ is functional, too.

(b) Let $\mathsf{T} \vdash \varphi$ and m be the Gödel number of the proof of φ in T. Then $\widetilde{Prf}(m, \ulcorner \varphi \urcorner)$ holds and thus $\widehat{Prf}(2m + 1, \ulcorner \varphi \urcorner)$. Let now $\widehat{Prf}(k, \ulcorner \varphi \urcorner)$ for some k.

If $k = 2m + 1$ then $\widetilde{Prf}(m, \ulcorner \varphi \urcorner)$ holds, so m is the Gödel number of a proof of φ, hence $\mathsf{T} \vdash \varphi$.

If $k = 2m$ and $C(m)$ then $\varphi \equiv D^*$ for some modal formula D such that $D \in \Gamma_{(m)_1}$ and the interpretation $(\cdot)^*$ corresponding to $\Gamma_{(m)_1} \supset \Delta_{(m)_1}$. By lemma 5.2, D^* is a true primitive recursive formula; again $\mathsf{T} \vdash \varphi$.

If $k = 2m$ and not $C(m)$ then $\varphi \equiv \forall x_0 \forall x_0 (x_0 = x_0)$ and so trivially $\mathsf{T} \vdash \varphi$.

By the formalization of (b) one can also prove that

$$\mathsf{T} \vdash \forall y \; (\widehat{Pr}(y) \leftrightarrow \widetilde{Pr}(y))$$

■

Thus theorem 5.1 is proved.

■

This proof predicate $\widehat{Prf}(\cdot, \cdot)$ is also uniform for the truth interpretation of $\mathcal{PF}$, i.e. for every modal formula A:

$$\mathcal{PF} \vdash A \iff A^* \text{ is true for each } (\cdot)^* \text{ based on } \widehat{Prf}(\cdot, \cdot)$$

After the uniformization of the proof predicate in $\mathcal{P}$, $\mathcal{PF}$ and $\mathcal{PFM}$, the natural question arises whether it is also possible to choose a fixed interpretation for the sentence or proof variables. Such kind of uniformity for the Provability Logic GL has been established independently in [1, 2], [4], [5] and [8]. This question will be answered up to the end of this section.

To recall the definition, each interpretation $(\cdot)^*$ consists of three natural parts:

(i) a (functional/standard) proof predicate $Prf(\cdot,\cdot)$ for $\mathtt{T}$,

(ii) an evaluation α of proof variables as natural numbers,

(iii) an evaluation β of sentence variables as sentences of $\mathtt{T}$.

So the completeness theorems 2.10 and 3.10 state that

$$\forall A:\ \exists \alpha, \beta, Prf(\cdot,\cdot):\ (\mathtt{T} \vdash A^* \ \Rightarrow\ \mathcal{P}/\mathcal{PF} \vdash A)$$

Theorem 5.1 shows that also

$$\exists Prf(\cdot,\cdot):\ \forall A:\ \exists \alpha, \beta:\ (\mathtt{T} \vdash A^* \ \Rightarrow\ \mathcal{P}/\mathcal{PF} \vdash A)$$

As the proofs of theorems 2.8 and 3.8 demonstrate, the interpretation α of the proof variables alone is uniformizable in $\mathcal{P}$ and $\mathcal{PF}$ (e.g. $p_i{}^* = 2i$). These completeness theorems can therefore be formulated as

$$\exists \alpha:\ \forall A:\ \exists \beta, Prf(\cdot,\cdot):\ (\mathtt{T} \vdash A^* \ \Rightarrow\ \mathcal{P}/\mathcal{PF} \vdash A)$$

It is not possible to use a uniform proof predicate in addition to α. Assume that

$$\exists \alpha, Prf(\cdot,\cdot):\ \forall A:\ \exists \beta:\ (\mathtt{T} \vdash A^* \ \Rightarrow\ \mathcal{P}/\mathcal{PF} \vdash A)$$

and let $\widehat{\alpha}$ be such an α and $\widehat{Prf}(\cdot,\cdot)$ be such a $Prf(\cdot,\cdot)$. As $\mathcal{P}/\mathcal{PF} \nvdash \Box_{p_0}\top$ it follows that $\mathtt{T} \nvdash \widehat{Prf}(p_0{}^{\widehat{\alpha}}, \ulcorner 0=0 \urcorner)$ and then $\mathtt{T} \vdash \neg\widehat{Prf}(p_0{}^{\widehat{\alpha}}, \ulcorner 0=0 \urcorner)$. But this is equivalent to $\mathcal{P}/\mathcal{PF} \vdash \neg\Box_{p_0}\top$, which is known to be false.

The interpretation α of the proof variables is not uniformizable in the case of $\mathcal{PFM}$. Assume that

$$\exists \alpha:\ \forall A:\ \exists \beta, Prf(\cdot,\cdot):\ (\mathtt{T} \vdash A^* \ \Rightarrow\ \mathcal{PFM} \vdash A)$$

and let $\widehat{\alpha}$ be such a fixed α. Let A be a modal formula $\neg\Box_{p_0}B$ with $B := \top\wedge\top\wedge\ldots\wedge\top$ such that $\ulcorner B^* \urcorner > p_0{}^{\widehat{\alpha}}$. As $\mathcal{PFM} \nvdash \neg\Box_{p_0}B$, it follows that there exists a standard proof predicate $Prf(\cdot,\cdot)$ such that $\mathtt{T} \nvdash \neg Prf(p_0{}^{\widehat{\alpha}}, \ulcorner B^* \urcorner)$ which is equivalent to $\mathtt{T} \vdash Prf(p_0{}^{\widehat{\alpha}}, \ulcorner B^* \urcorner)$. But a consequence of $Prf(p_0{}^{\widehat{\alpha}}, \ulcorner B^* \urcorner)$ is that $p_0{}^{\widehat{\alpha}} \geq \ulcorner B^* \urcorner$, which is a contradiction.

The interpretation β of the sentence variables is not uniformizable at all. Assume that

$$\exists \beta:\ \forall A:\ \exists \alpha, Prf(\cdot,\cdot):\ (\mathtt{T} \vdash A^* \ \Rightarrow\ \mathcal{P}/\mathcal{PF}/\mathcal{PFM} \vdash A)$$

and let $\widehat{\beta}$ be such a fixed β. As $\mathcal{P}/\mathcal{PF}/\mathcal{PFM} \nvdash \neg\Box_{p_0} S_0$, this implies that $\exists\alpha, Prf(\cdot,\cdot) :$ $\mathtt{T} \nvdash \neg Prf(p_0{}^{\alpha}, \ulcorner S_0{}^{\widehat{\beta}} \urcorner)$ which is equivalent to $\exists\alpha, Prf(\cdot,\cdot) :$ $\mathtt{T} \vdash Prf(p_0{}^{\alpha}, \ulcorner S_0{}^{\widehat{\beta}} \urcorner)$, from which follows that $\mathtt{T} \vdash S_0{}^{\widehat{\beta}}$. As a consequence, $\forall\alpha, Prf(\cdot,\cdot) :$ $\mathtt{T} \nvdash Prf(p_0{}^{\alpha}, \ulcorner \neg S_0{}^{\widehat{\beta}} \urcorner)$, hence $\forall\alpha, Prf(\cdot,\cdot) :$ $\mathtt{T} \vdash \neg Prf(p_0{}^{\alpha}, \ulcorner \neg S_0{}^{\widehat{\beta}} \urcorner)$, which implies $\mathcal{P}/\mathcal{PF}/\mathcal{PFM} \vdash \neg\Box_{p_0} \neg S_0$, but again this is known to be false.

The situation can therefore be summarized as:

> In the cases of $\mathcal{P}$ and $\mathcal{PF}$ one can either choose a uniform proof predicate as $\widehat{Prf}(\cdot,\cdot)$ in this section, or one can choose a uniform interpretation of the proof variables as in sections 2 and 3.
>
> In the case of $\mathcal{PFM}$ every standard proof predicate is a uniform one, but the uniformization of the proof variables is not possible.
>
> All other combinations of uniformization, including those of the sentence variables, are not possible.

References

[1] S. Artëmov, "Extensions of arithmetic and connected with them modal theories," *VI LMPS Congress, Hannover*, pp. 15–19, 1979. Section 1.

[2] S. Artëmov, "Arifmeticheski polnyje modal'nyje teorii; Russian (Arithmetically complete modal theories)," *Semiotika i informatika (Semiotics and Information Science)*, vol. 14, no. 14, pp. 115–133, 1980. Translation: AMS Transl. (2), vol 135, 1987, pp. 39-54, Akad. Nauk SSSR, VINiTI, Moscow.

[3] G. Boolos, *The unprovability of consistency: an essay in modal logic*. Cambridge: Cambridge University Press, 1979.

[4] G. Boolos, "Extremely undecidable sentences," *Journal of Symbolic Logic*, vol. 47, pp. 191–196, Mar. 1982.

[5] F. Montagna, "On the diagonalizable algebra of Peano arithmetic," *Bollettino della Unione Matematica Italiana*, vol. 16-B, no. 5, pp. 795–812, 1979.

[6] C. Smoryński, "The incompleteness theorems," in *Handbook of Mathematical Logic* (J. Barwise, ed.), ch. D.1, pp. 821–865, North-Holland, Amsterdam, 1977.

[7] R. M. Solovay, "Provability interpretations of modal logic," *Israel Journal of Mathematics*, vol. 25, pp. 287–304, 1976.

[8] A. Visser, *Aspects of Diagonalization and Provability*. PhD thesis, University of Utrecht, 1981.