Syntactical Models and Fixed Points for the Basic Logic of Proofs

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

Abstract

This report describes syntactical models for the Basic Logic of Proofs, which are closely related to canonical models. For each system of this class of logics soundness and completeness are proved. Moreover, some principles of the Basic Logic of Proofs, mainly concerning fixed points, are investigated.

1 Introduction

The Propositional Provability Logic GL for Peano Arithmetic PA was axiomatized in [8]. GL describes the behaviour of the arithmetical operator "A is provable" by means of modal logic. Since GL is decidable, one has an elegant and efficient tool for studying subjects centered around Gödel's incompleteness theorems, e.g. Löb's theorem, substitutions, fixed points and formalizations.

The Basic Logic of Proofs is defined exactly in the same environment as GL. But instead of having modal formulas of the form $\Box A$ and interpreting $\Box A$ as "A is provable", the language of the Basic Logic of Proofs contains labeled modalities $\Box_p A$ which are interpreted e.g. as "p is a proof of A", "p is a proof which contains A", "p is a program which computes A", or "A is computable by a program which size is bounded by p".

The goal of this report is to provide the Basic Logic of Proofs with syntactical models and then investigate some basic properties, mainly concerning fixed points.

In the remaining of this section, a summary of the definitions of the Basic Logic of Proofs is given. Most definitions are in accordance with those of the classical Provability Logic ([8]). Next, appropriate axiom systems are presented. And finally, the syntactical models are defined.

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

In section 2, the soundness and completeness of the proof systems with respect to the syntactical models are proved. Section 3 is devoted to the decidability of the models, and in section 4, fixed points for the Basic Logic of Proofs are discussed.

1.1 Definition The modal language contains two sorts of variables, $p_0, p_1, \ldots$ (called *proof variables*), $S_0, S_1, \ldots$ (called *sentence variables*), the connectives $\neg$, $\wedge$, and the labeled modality symbol $\Box_{p_i}$ for each proof variable p_i. The modal language is generated from the sentence variables $S_0, S_1, \ldots$ by the boolean connectives $\neg$, $\wedge$ 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. The truth values $\bot$ (for absurdity), $\top$ (for truth) and the other boolean connectives are defined in their usual way. 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. Sentence variables and formulas of the form $\Box_p A$ are called *quasiatomic*. 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.

Let $\mathtt{PA}$ be Peano Arithmetic. Greek letters φ, ψ, ... denote arithmetical formulas. In this paper we do not distinguish between the number n and its numeral $\overline{n}$.

1.2 Definition An arithmetical formula $Prf(\cdot,\cdot)$ is called a *proof predicate* in $\mathtt{PA}$ iff

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

The proof predicate $Prf(\cdot,\cdot)$ is called *functional* iff for all $n, k_1, k_2 \in \mathbb{N}$:

- If $Prf(n, k_1)$ and $Prf(n, k_2)$ then $k_1 = k_2$.

The proof predicate $Prf(\cdot,\cdot)$ is called *monotone* iff for all $n, k \in \mathbb{N}$:

- If $Prf(n, k)$ then $n \geq k$.

1.3 Definition Let $Prf(\cdot,\cdot)$ be a proof predicate in $\mathtt{PA}$, 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 $\mathtt{PA}$. 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:

- ${p_i}^* := \phi(p_i) \quad {S_i}^* := \phi(S_i)$
- $(\neg A)^* := \neg A^* \quad (A \wedge B)^* := A^* \wedge B^*$
- $(\Box_p A)^* := Prf(p^*, \ulcorner A^* \urcorner)$

1.4 Definition An arithmetical interpretation $(\cdot)^* = (Prf(\cdot,\cdot), \phi)$ is called *functional* iff $Prf(\cdot,\cdot)$ is functional. An arithmetical interpretation $(\cdot)^* = (Prf(\cdot,\cdot), \phi)$ is called *monotone* iff $Prf(\cdot,\cdot)$ is monotonic.

In some situations it is useful to consider functional interpretations $(\cdot)^* = (Prf(\cdot,\cdot), \phi)$ where ϕ is injective. Such interpretations will be called *i-functional*. An i-functional interpretation has the property that if A and B are modal formulas, then $A^* \equiv B^*$ iff $A \equiv B$ (here "$\equiv$" denotes the syntactical identity of formulas, e.g. $\varphi \wedge \varphi \not\equiv \varphi$, and $S_0 \not\equiv S_1$).

1.5 Definition $\mathcal{P}$, $\mathcal{PF}$, $\mathcal{PU}$, $\mathcal{PM}$, $\mathcal{PFM}$ and $\mathcal{PUM}$ are the modal theories with axioms and rules of inference as follows: (e.g. $\mathcal{PUM}$ consists of (A1), (A2), (R1), (A3) and (A4))

$$\left.\begin{array}{ll} \textbf{(A1)} & \text{All (boolean) tautologies} \\ \textbf{(A2)} & \Box_p A \longrightarrow A \\ \textbf{(R1)} & \dfrac{A \qquad A \to B}{B} \end{array}\right\} \mathcal{P}$$

$$\left.\begin{array}{ll} \textbf{(A3)} & \Box_p A \wedge \Box_p B \wedge F \longrightarrow G \qquad (F = G \pmod{A = B}) \end{array}\right\} \mathcal{U}$$

$$\left.\begin{array}{ll} \textbf{(A3')} & \neg(\Box_p A \wedge \Box_p B) \qquad (A \not\equiv B) \end{array}\right\} \mathcal{F}$$

$$\left.\begin{array}{ll} \textbf{(A4)} & \neg[\Box_{q_1} A_2(q_2) \wedge \Box_{q_2} A_3(q_3) \wedge \ldots \wedge \Box_{q_n} A_1(q_1)] \end{array}\right\} \mathcal{M}$$

where A, B, F, G are modal formulas, $p, q_1, \ldots, q_n$ are proof variables, and $A_i(q_i)$ is a modal formula in which q_i occurs. The scheme (A4) includes $\neg\Box_{q_1} A_1(q_1)$. The relation $F = G \pmod{A = B}$ is defined as $\forall\theta : (A\theta \equiv B\theta \to F\theta \equiv G\theta)$, where θ denotes a substitution which substitutes proof variables for proof variables and modal formulas for sentence variables. (A2) is the *Reflexivity Axiom*, (A3) the *Unification Axiom*, (A3') the *Functionality Axiom* and (A4) the *Monotonicity Axiom*.

The main result of [1] is that

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

the main result of [3] is that

$$\begin{array}{rcl} \mathcal{PM} \vdash A & \Longleftrightarrow & A^* \text{ is true for every monotonic interpretation } (\cdot)^*, \\ \mathcal{PFM} \vdash A & \Longleftrightarrow & A^* \text{ is true for every i-functional and monotonic } (\cdot)^*, \end{array}$$

and in [2] it is shown that

$$\begin{array}{rcl} \mathcal{PU} \vdash A & \Longleftrightarrow & A^* \text{ is true for every functional interpretation } (\cdot)^*, \\ \mathcal{PUM} \vdash A & \Longleftrightarrow & A^* \text{ is true for every functional and monotonic } (\cdot)^*. \end{array}$$

Alternatively, as it is done in [3], in the case of $\mathcal{PFM}$ and $\mathcal{PUM}$ the operator $\Box_p A$ can be interpreted as "$proof(p^*) \wedge (p^*)_{lh(p^*)} = \ulcorner A^* \urcorner$" (Gödel proof predicate), and in the case of $\mathcal{PM}$ the operator $\Box_p A$ can be interpreted as "$proof(p^*) \wedge \exists i \leq lh(p^*) : (p^*)_i = \ulcorner A^* \urcorner$" (nonfunctional Gödel proof predicate). Here $lh(s)$ and $(s)_i$ are recursive terms which compute the length and the i'th component of a sequence s, respectively, and $proof(x)$ is a standard arithmetical term for the recursive predicate "x is the Gödel number of

a proof in PA". A formal description of $proof(\cdot)$ can be found for example in [4] or [7]. So in this version, $\forall^*$ quantifies only the proof and sentence variables.

The definition 1.2 of a proof predicate makes it possible to use the Basic Logic of Proofs in a wide range of applications. The formula $\Box_p A$ can be interpreted for example as:

- p is a proof of A (monotonic and functional interpretation),
- p is a proof which contains A (monotonic interpretation),
- p is a program which computes A; regard that short programs can compute long theorems (functional interpretation),
- A is computable by a program which size is bounded by p (arbitrary interpretation).

As none of these logics is closed under the labeled necessitation $A \vdash \Box_p A$, or under the substitution rule $A \leftrightarrow B \vdash \Box_p A \leftrightarrow \Box_p B$, the usual technique of Kripke models cannot be applied here.

1.6 Definition Let w be a set of quasiatomic formulas. We define the consequence relation $w \models A$ (read: A is true in w) for all formulas A as follows:

- $w \models A$ iff $A \in w$ (when A is quasiatomic),
- $w \models \neg A$ iff not $w \models A$,
- $w \models A \wedge B$ iff both $w \models A$ and $w \models B$.

A $\mathcal{P}$-*model* (or just *model*) is a finite set w of quasiatomic formulas such that

- if $\Box_p A \in w$ then $w \models A$.

A $\mathcal{PF}$-*model* is a model w such that

- if $\Box_p A, \Box_p B \in w$ then $A \equiv B$.

A $\mathcal{PU}$-*model* is a model w such that

- there exists an underlying $\mathcal{PF}$-model w' and a substitution σ, such that for all formulas A: if $w \models A$ then $w' \models A\sigma$.
  In this case we say that w is *based* on w' and σ.

A $\mathcal{PM}$-*model* is a model w such that

- the relation $q_1 \prec q_2 :\Leftrightarrow \Box_{q_2} A_1(q_1) \in w$ (defined on the proof variables) is cycle-free. Again, $A_1(q_1)$ denotes a formula in which q_1 occurs.

A $\mathcal{PFM}$-*model* is a model which is both a $\mathcal{PF}$- and a $\mathcal{PM}$-model.

A $\mathcal{PUM}$-*model* is a $\mathcal{PU}$-model w which is based on a $\mathcal{PFM}$-model w'.

We write $\mathcal{P} \models A$ iff $w \models A$ for all $\mathcal{P}$-models w; analogously, $\mathcal{PF} \models A$ iff $w \models A$ for all $\mathcal{PF}$-models w; etc. Notice that if B is a (boolean) tautology, then $w \models B$ for each model w. Notice also, that if w is a $\mathcal{PU}$-model based on w' and σ, then for all

formulas A, $w \models A$ iff $w' \models A\sigma$: From $w \not\models A$ follows $w \models \neg A$, hence $w' \models \neg A\sigma$, and so $w' \not\models A\sigma$.

Thus, $\mathcal{P}$-models correspond to arbitrary interpretations, $\mathcal{PU}$-models to functional interpretations (letter $\mathcal{U}$), $\mathcal{PF}$-models to those functional interpretations that are injective (letter $\mathcal{F}$), and $\mathcal{PM}$-models to monotonic interpretations (letter $\mathcal{M}$).

1.7 Example

(i) $\mathcal{P} \models \Box_p A \to A$ for every formula A: Let w be an arbitrary model. Then $w \models \Box_p A \to A$, as from $w \models \Box_p A$ follows $\Box_p A \in w$, hence $w \models A$.

(ii) $\mathcal{P} \not\models S_0 \to \Box_p S_0$: Let $w := \{S_0\}$. Then $w \models S_0$, but $w \not\models \Box_p S_0$.

(iii) $\mathcal{P} \not\models \Box_p A$ for any formula A: Let $w := \emptyset$.

1.8 Example Let $w := \{\Box_{p_0}\neg\Box_{p_1}S_0, \Box_{p_0}\neg\Box_{p_1}S_1, S_0, S_1\}$. Then w is a $\mathcal{PU}$-model based on the $\mathcal{PF}$-model $w' = \{\Box_{p_0}\neg\Box_{p_1}S_0, S_0\}$ and the substitution $\sigma = \{S_1 \leftarrow S_0\}$. As w' is a $\mathcal{PM}$-model, w even is a $\mathcal{PUM}$-model. Notice that the model $\tilde{w} := \{\Box_{p_0}\neg\Box_{p_1}S_0, \Box_{p_0}\neg\Box_{p_1}S_1, S_0\}$ is a subset of w, but is not a $\mathcal{PU}$-model.

The goal of the next section is to show that for each formula A:

$$\begin{array}{rcl} \mathcal{P} \vdash A & \Longleftrightarrow & \mathcal{P} \models A \\ \mathcal{PF} \vdash A & \Longleftrightarrow & \mathcal{PF} \models A \\ & \vdots & \\ \mathcal{PUM} \vdash A & \Longleftrightarrow & \mathcal{PUM} \models A \end{array}$$

Soundness and completeness for $\mathcal{P}$, $\mathcal{PF}$, $\mathcal{PM}$ and $\mathcal{PFM}$ are proved using the technique of canonical models, the systems $\mathcal{PU}$ and $\mathcal{PUM}$ are handled separately at the end of the section. The following definitions and results up to theorem 2.6 are fairly standard (cf. [5], pp. 9-12), so the proofs are not given in all details.

2 Soundness and Completeness

As usual we call a formula $\mathcal{P}$-consistent if its negation is not $\mathcal{P}$-provable; we call a set of formulas $\mathcal{P}$-consistent if the conjunction of any finite subset is. A set of formulas M is said to be *maximal* iff for every formula A, either $A \in M$ or $\neg A \in M$. A *maximal $\mathcal{P}$-consistent set* ($\mathcal{P}$-*MCS* for short) is a set which is both maximal and $\mathcal{P}$-consistent. The same definitions are used for $\mathcal{PF}$, $\mathcal{PM}$ and $\mathcal{PFM}$, too.

We assume familiarity with the following:

2.1 Lindenbaum's Lemma Any consistent set of formulas can be extended to a maximal consistent set.

■

2.2 Lemma Let M be a $\mathcal{P}$-MCS, then

(1) $\neg A \in M$ iff $A \notin M$,

(2) $A \wedge B \in M$ iff $A \in M$ and $B \in M$,

(3) $\Box_p A \in M$ implies $A \in M$.

If M is a $\mathcal{PF}$- or a $\mathcal{PFM}$-MCS then

(4) $\Box_p A, \Box_p B \in M$ implies $A \equiv B$.

If M is a $\mathcal{PM}$- or a $\mathcal{PFM}$-MCS then

(5) the relation $q_1 \prec q_2 :\Leftrightarrow \Box_{q_2} A_1(q_1) \in M$ contains no cycles.

Proof (1) and (2) are standard properties of MCSs. For (3) we use the Reflexivity Axiom, together with the standard property of a $\mathcal{P}$-MCS M that if $\mathcal{P} \vdash A \to B$, and $A \in M$, then $B \in M$. (4) and (5) are shown in a similar way.
■

2.3 Lemma Let A be a formula. Then $\mathcal{P} \vdash A$ iff A is contained in all $\mathcal{P}$-MCSs. The same holds for $\mathcal{PF}$, $\mathcal{PM}$ and $\mathcal{PFM}$.

Proof If $\mathcal{P} \nvdash A$, i.e. if $\{\neg A\}$ is consistent, then there exists a $\mathcal{P}$-MCS M which contains $\neg A$, hence M does not contain A. If M is a $\mathcal{P}$-MCS which does not contain A, then $\neg A \in M$. As each subset of a consistent set is also consistent, $\{\neg A\}$ is consistent, i.e. $\mathcal{P} \nvdash A$. The same argument is valid for $\mathcal{PF}$, $\mathcal{PM}$ and $\mathcal{PFM}$, too.
■

2.4 Soundness of $\mathcal{P}$, $\mathcal{PF}$, $\mathcal{PM}$ and $\mathcal{PFM}$. For each formula A:

$$\mathcal{P} \vdash A \qquad \Longrightarrow \qquad \mathcal{P} \models A$$

The same holds for $\mathcal{PF}$, $\mathcal{PM}$ and $\mathcal{PFM}$.

Proof If w is a model, then let $\overline{w} := \{A \mid w \models A\}$. We show first, that if w is a $\mathcal{P}$-model such that $w \models A$, then $\overline{w}$ is a $\mathcal{P}$-MCS which contains A (and that the same holds for $\mathcal{PF}$, $\mathcal{PM}$ and $\mathcal{PFM}$, too): By definition, $\overline{w}$ is maximal, and $\overline{w}$ contains A. Now assume that $\overline{w}$ is not $\mathcal{P}$-consistent, i.e. there exist formulas $A_1, \ldots, A_n \in \overline{w}$ such that $\mathcal{P} \vdash \neg(A_1 \wedge \ldots \wedge A_n)$. From $A_1, \ldots, A_n \in \overline{w}$ follows that $w \models A_1 \wedge \ldots \wedge A_n$, i.e. $w \not\models \neg(A_1 \wedge \ldots \wedge A_n)$. We show that for each formula B, if $\mathcal{P} \vdash B$ then $w \models B$, by induction on the length of the derivation:

- The cases where B is a (boolean) tautology, or B has been concluded by modus ponens, are straightforward.
- If B is an instance of the Reflexivity Axiom then $w \models B$ by example 1.7 (i).
- The cases of $\mathcal{PF}$, $\mathcal{PM}$ and $\mathcal{PFM}$ are shown in an analogous way.

To conclude the proof of the lemma, let $\mathcal{P} \not\models A$, i.e. there exists a $\mathcal{P}$-model w, such that $w \models \neg A$. Thus $\overline{w}$ is a $\mathcal{P}$-MCS which contains $\neg A$, and so $\overline{w}$ does not contain A. By lemma 2.3, $\mathcal{P} \not\vdash A$. The same argument is valid for $\mathcal{PF}$, $\mathcal{PM}$ and $\mathcal{PFM}$, too.
■

Let w be a $\mathcal{PM}$-model. As w is a finite set, $\prec$ (defined on w as $q_1 \prec q_2 :\Leftrightarrow \Box_{q_2} A_1(q_1) \in w$) is not only cycle-free but also well-founded. In the proof of lemma 2.4, if w is a model then $\overline{w}$ contains the same quasiatomic formulas as w. From this follows that $\prec$ defined on $\overline{w}$ is well-founded, too. This observation is useful for constructing arithmetical interpretations in the cases of $\mathcal{PM}$, $\mathcal{PFM}$ and $\mathcal{PUM}$.

2.5 Lemma Let M be a $\mathcal{P}$-MCS which contains the formula A. Then there exists a $\mathcal{P}$-model w such that $w \models A$. The same holds for $\mathcal{PF}$, $\mathcal{PM}$ and $\mathcal{PFM}$, too.

Proof Let w be the set of all quasiatomic formulas which are in M, and which are subformulas of A. As there exist only finitely many subformulas of A, w is finite. If B is a subformula of A, then it follows by induction on the complexity of B, that $B \in M$ iff $w \models B$: If B is quasiatomic, then by definition, $B \in M$ iff $w \models B$. If B is $\neg C$ then also C is a subformula of A, thus $\neg C \in M$ iff (lemma 2.2) $C \notin M$ iff (induction hypothesis) $w \not\models C$ iff $w \models \neg C$. The case where B is $C_1 \wedge C_2$ is shown in an analogous way. Therefore, if $\Box_p B \in w$, then also $B \in M$ (lemma 2.2), and B is a subformula of A, hence $w \models B$. So w is a $\mathcal{P}$-model, and $w \models A$. As w does not contain more formulas of the form $\Box_p B$ than M, it follows that w is a $\mathcal{PF}$- or a $\mathcal{PM}$-model if M is $\mathcal{PF}$- or a $\mathcal{PM}$-MCS, respectively.
■

2.6 Completeness of $\mathcal{P}$, $\mathcal{PF}$, $\mathcal{PM}$ and $\mathcal{PFM}$. For each formula A:

$$\mathcal{P} \models A \qquad \Longrightarrow \qquad \mathcal{P} \vdash A$$

The same holds for $\mathcal{PF}$, $\mathcal{PM}$ and $\mathcal{PFM}$.

Proof Let $\mathcal{P} \not\vdash A$, i.e. by lemma 2.3, there exists a $\mathcal{P}$-MCS M which does not contain A, thus by lemma 2.2 contains $\neg A$. By lemma 2.5 there exists a $\mathcal{P}$-model w such that $w \models \neg A$, and so $\mathcal{P} \not\models A$. The same proof fits for $\mathcal{PF}$, $\mathcal{PM}$ and $\mathcal{PFM}$, too.
■

The soundness and completeness proofs for $\mathcal{PU}$ and $\mathcal{PUM}$ are based on the fact that the theorems of $\mathcal{PU}$ (resp. $\mathcal{PUM}$) are exactly the theorems of $\mathcal{PF}$ (resp. $\mathcal{PFM}$) for which the substitution property holds (cf. [2]), i.e. $\mathcal{PU} \vdash A$ iff $\forall \sigma : \mathcal{PF} \vdash A\sigma$, and $\mathcal{PUM} \vdash A$ iff $\forall \sigma : \mathcal{PFM} \vdash A\sigma$. We assume that the reader is familiar with substitutions, most general unifiers, etc. (cf. [6]).

2.7 Definition Let w' be a model and σ a substitution. The set $\sigma w'$ (do not confound with $w'\sigma$) of quasiatomic formulas is defined by:

$$A \in \sigma w' \quad :\Longleftrightarrow \quad w' \models A\sigma \text{ and } A \text{ is quasiatomic}$$

We will use this definition mainly to get a more convenient description of functional models (lemma 2.10). The following lemma is purely technical, and it will help us to shorten several proofs.

2.8 Lemma Let w, w' be finite sets of quasiatomic formulas, and σ a substitution such that for all quasiatomic formulas A, $w \models A$ iff $w' \models A\sigma$. Then for all formulas A, $w \models A$ iff $w' \models A\sigma$.

Proof Induction on the complexity of A: If A is quasiatomic then we are done. If A is $\neg B$, then $w \models \neg B$ iff $w \not\models B$ iff (by the induction hypothesis) $w' \not\models B\sigma$ iff $w' \models \neg B\sigma$. The case where A is $B_1 \wedge B_2$ is shown in a similar way.
■

The next lemma describes the main property, $\sigma w'$ has been defined for.

2.9 Lemma Let w' be a $\mathcal{P}$-model and σ a substitution. Then $\sigma w'$ is a $\mathcal{P}$-model, and for all formulas A,

$$\sigma w' \models A \quad \Longleftrightarrow \quad w' \models A\sigma$$

As a consequence, if w' is a $\mathcal{PF}$-model then $\sigma w'$ is a $\mathcal{PU}$-model, and if w' is a $\mathcal{PFM}$-model then $\sigma w'$ is a $\mathcal{PUM}$-model.

Proof As for each formula B there exist only finitely many formulas A_i $(i \in I)$ such that $A_i\sigma \equiv B$ $(i \in I)$, it follows that $\sigma w'$ is a finite set of quasiatomic formulas. By definition 2.7, for all quasiatomic formulas A, $\sigma w' \models A$ iff $w' \models A\sigma$. Therefore, by lemma 2.8, for all formulas A, $\sigma w' \models A$ iff $w' \models A\sigma$. As a consequence, $\sigma w'$ is a $\mathcal{P}$-model: If $\Box_p A \in \sigma w'$ then $\sigma w' \models \Box_p A$, which is equivalent to $w' \models \Box_{p\sigma} A\sigma$. As w' is a model, we get $w' \models A\sigma$, which again is equivalent to $\sigma w' \models A$.
■

Note, that if τ and σ are substitutions, then $\sigma(\tau w') \models A$ iff $\tau w' \models A\sigma$ iff $w' \models A\sigma\tau$ iff $(\sigma\tau)w' \models A$. Therefore, $\sigma(\tau w') = (\sigma\tau)w'$, i.e. the parentheses may be omitted. Another consequence of this is that if (concerning lemma 2.9) w' is a $\mathcal{PU}$-model then $\sigma w'$ again is a $\mathcal{PU}$-model, and if w' is a $\mathcal{PUM}$-model then $\sigma w'$ is a $\mathcal{PUM}$-model.

Lemma 2.9 enables us to give another definition of *$\mathcal{PU}$-model* and *$\mathcal{PUM}$-model*:

2.10 Lemma Let w be a finite set of quasiatomic formulas, w' a $\mathcal{PF}$-model ($\mathcal{PFM}$-model) and σ a substitution. Then w is a $\mathcal{PU}$-model ($\mathcal{PUM}$-model) based on w' and σ, iff $w = \sigma w'$.

Proof The direction from right to left is a consequence of the previous lemma. For the other direction let w be a $\mathcal{PU}$-model based on w' and σ, i.e. for all formulas A, $w \models A$ iff $w' \models A\sigma$. So $A \in w$ iff both $w' \models A\sigma$ and A is quasiatomic. By definition 2.7, $w = \sigma w'$.
■

As an example, consider w' to be the $\mathcal{PF}$-model $\{\Box_p \top\}$, and let $\sigma = \{S_0 \leftarrow \top\}$. Then $\sigma w'$ is the $\mathcal{PU}$-model $\{\Box_p \top, \Box_p S_0, S_0\}$ (let $\top$ be defined as $S_1 \rightarrow S_1$).

2.11 Theorem Let A be a formula. Then $\mathcal{PU} \models A$ iff $\forall\sigma : \mathcal{PF} \models A\sigma$, and $\mathcal{PUM} \models A$ iff $\forall\sigma : \mathcal{PFM} \models A\sigma$.

Proof Follows readily from lemmas 2.9 and 2.10.
■

2.12 Soundness and Completeness of $\mathcal{PU}$ and $\mathcal{PUM}$. For each formula A:

$$\begin{array}{rcl} \mathcal{PU} \vdash A & \iff & \mathcal{PU} \models A \\ \mathcal{PUM} \vdash A & \iff & \mathcal{PUM} \models A \end{array}$$

Proof $\mathcal{PU} \vdash A$ iff (cf. [2]) $\forall\sigma : \mathcal{PF} \vdash A\sigma$ iff (soundness and completeness of $\mathcal{PF}$) $\forall\sigma : \mathcal{PF} \models A\sigma$ iff (previous theorem) $\mathcal{PU} \models A$. The same proof fits for $\mathcal{PUM}$.
■

The following easy result is listened for the completeness of the discussion on functional interpretations.

2.13 Lemma Let A be a formula and let σ be a substitution. Then $\mathcal{PU} \models A$ implies $\mathcal{PU} \models A\sigma$, and $\mathcal{PUM} \models A$ implies $\mathcal{PUM} \models A\sigma$.

Proof Let $\mathcal{PU} \not\models A\sigma$, i.e. there exists a $\mathcal{PU}$-model w such that $w \models (\neg A)\sigma$. Let w be based on the $\mathcal{PF}$-model w' and the substitution τ, hence $w' \models (\neg A)\sigma\tau$. It follows $\sigma\tau w' \models \neg A$. But $\sigma\tau w'$ again is a $\mathcal{PU}$-model, therefore $\mathcal{PU} \not\models A$.
■

Functional models have the drawback that they may be exponential in length compared to a formula they satisfy. The following example demonstrates this:

2.14 Example Let A be the formula

$$\begin{array}{lcl} \Box_{p_0} S_0 & \wedge & \Box_{p_0}\Box_{p_1}(S_1 \wedge S_1) \quad \wedge \\ \Box_{p_1} S_1 & \wedge & \Box_{p_1}\Box_{p_2}(S_2 \wedge S_2) \quad \wedge \\ \vdots & & \vdots \\ \Box_{p_{n-1}} S_{n-1} & \wedge & \Box_{p_{n-1}}\Box_{p_n}(S_n \wedge S_n) \end{array}$$

Note that A has length $O(n)$ (counting proof and sentence variables and boolean connectives). Let w be a $\mathcal{PU}$-model such that $w \models A$. If we write w as $\sigma w'$ for a substitution σ and a $\mathcal{PF}$-model w', then σ is a specialization of each of the substitutions $S_i \leftarrow \Box_{p_{i+1}}(S_{i+1} \wedge S_{i+1})$ $(i = 0 \ldots n{-}1)$. As $w \models \Box_{p_0} S_0$, $w \models S_0$, hence $w' \models S_0\sigma$. Now $S_0\sigma$ is quasiatomic and has length $O(2^n)$. Hence w' contains at least one formula of exponential length. But also w contains $S_0\sigma$ if we assume σ to be idempotent (cf. remark 3.7). So we have no direct representation of a $\mathcal{PU}$-model of linear length in which A is true.

3 Decidability

The decidability of the logics mentioned in this paper has already been achieved in an efficient manner by the cut-elimination theorem ($\mathcal{P}$ and $\mathcal{PF}$ in [1], $\mathcal{PM}$ and $\mathcal{PFM}$ in [3], $\mathcal{PU}$ and $\mathcal{PUM}$ in [2]). Furthermore, according to definition 1.6, it is easily decidable whether a given finite set $\tilde{w}$ of quasiatomic formulas is a $\mathcal{P}$-, $\mathcal{PF}$-, $\mathcal{PM}$-, or $\mathcal{PFM}$-model. So the only remaining problem in this concern is to decide whether such a set $\tilde{w}$ is a $\mathcal{PU}$-model (or $\mathcal{PUM}$-model). The solution of this problem is not straightforward: It is not sufficient to test if there exists a $\mathcal{PU}$-model w, such that $w \models \bigwedge_{A \in \tilde{w}} A$ (cf. example 1.8) as it can be done in the case of $\mathcal{P}$, $\mathcal{PF}$, $\mathcal{PM}$ and $\mathcal{PFM}$. The aim of this section is to provide a decision procedure for $\mathcal{PU}$-models. All statements are given for $\mathcal{PU}$ only; $\mathcal{PUM}$ can be treated in a similar way.

The first goal is to show, that given a model w, a $\mathcal{PF}$-model w', and a substitution σ, it is decidable whether w is a $\mathcal{PU}$-model based on w' and σ.

3.1 Lemma Let w be a finite set of quasiatomic formulas, w' a $\mathcal{PF}$-model, and σ a substitution. It is decidable whether w is a $\mathcal{PU}$-model based on w' and σ.

Proof It is easily decidable, whether w is a model. We show that a model w is a $\mathcal{PU}$-model based on w' and σ, iff for all quasiatomic formulas A and sentence variables S the following decidable statements are true:

1. $A \in w$ implies $w' \models A\sigma$,
2. $A\sigma \in w'$ implies $w \models A$,
3. $S \in dom(\sigma) \setminus w$ implies $w' \not\models S\sigma$.

If w is a $\mathcal{PU}$-model based on w' and σ, then 1. and 2. hold by lemmas 2.9 and 2.10, and if $S \in dom(\sigma) \setminus w$ then $S \notin w$, so again $w' \not\models S\sigma$. For the converse, we show that for all quasiatomic formulas A, $w \models A$ iff $w' \models A\sigma$. Then we are done, because due to lemma 2.8 it follows that for all formulas A, $w \models A$ iff $w' \models A\sigma$. Let A be quasiatomic. If $w \models A$, hence $A \in w$ then by 1., $w' \models A\sigma$. If $w' \models A\sigma$ and A is of the form $\Box_p B$ or A is a sentence variable $S \notin dom(\sigma)$, then also $A\sigma$ is quasiatomic, hence $A\sigma \in w'$, and so by 2., $w \models A$. If $w' \models A\sigma$ and A is a sentence variable $S \in dom(\sigma)$, then by 3., $w \models S$, i.e. $w \models A$.
■

The following definition gives an algorithm for deciding whether a finite set of quasiatomic formulas is a $\mathcal{PU}$-model, without having knowledge of an underlying $\mathcal{PF}$-model w' and a substitution σ as in lemma 3.1.

3.2 Definition Let w be a finite set of quasiatomic formulas. A *w-chain* is a (finite or infinite) sequence $(\varepsilon, w) = (\sigma_0, w_0), (\sigma_1, w_1), \ldots$, where each σ_i is a substitution and each w_i is a finite set of quasiatomic formulas, such that:

[success] if w_k contains no formulas $\Box_p A, \Box_p B$ $(A \not\equiv B)$, then (σ_k, w_k) is the last element of the sequence.

[failure$_a$] if w_k contains formulas $\Box_p A, \Box_p B$ $(A \not\equiv B)$ that are not unifiable, then (σ_k, w_k) is the last element of the sequence.

If none of the two previous cases takes place, then choose $\Box_p A, \Box_p B \in w_k$ $(A \not\equiv B)$, let μ be an idempotent most general unifier of A and B, and let $w' := \{A \mid \exists B \in w_k : A \equiv B\mu, \text{ and } A \text{ is quasiatomic}\}$. Then

[failure$_b$] if $w_k \neq \mu w'$, then (σ_k, w_k) is the last element of the sequence.

[step] if $w_k = \mu w'$, then let $\sigma_{k+1} := \sigma_k \mu$, and let $w_{k+1} := w'$.

3.3 Lemma Let w be a model, and let $(\varepsilon, w) = (\sigma_0, w_0), (\sigma_1, w_1), \ldots$ be a w-chain. Then for each (σ_k, w_k) in this chain w-chain, $w = \sigma_k w_k$, σ_k is idempotent, $w_k \subset w$, and w_k is a model.

Proof Induction on k. For $k = 0$ we have $w = \varepsilon w$. Now let $w = \sigma_k w_k$, where w_k is a model, $w_k \subset w$, $w = \sigma_k w_k$, and σ_k is idempotent. According to the algorithm, $w_k = \mu w_{k+1}$ for an idempotent substitution μ. We get $w = \sigma_k(\mu w_{k+1}) = (\sigma_k \mu) w_{k+1} = \sigma_{k+1} w_{k+1}$. Furthermore, σ_{k+1} is the composition of idempotent substitutions, hence itself idempotent. For the proof of the remaining claims, first note, that if A and B are formulas such that $A\mu \equiv B\mu$, then $w_k \models A$ iff $w_{k+1} \models A\mu$ iff $w_{k+1} \models B\mu$ iff $w_k \models B$. Therefore, if A is an arbitrary formula, then by the idempotence of μ, $A\mu \equiv A\mu\mu$, hence $w_k \models A$ iff $w_k \models A\mu$. Next, we show that $w_{k+1} \subset w_k$: Let $A \in w_{k+1}$. By the definition of w_{k+1}, $B\mu \equiv A$ for some formula $B \in w_k$. From $B \in w_k$ follows $w_k \models B$, hence $w_k \models B\mu$, hence $w_k \models A$, which is equivalent to $A \in w_k$. Next, we prove that w_{k+1} is a model: Clearly, w_{k+1} is a finite set of quasiatomic formulas. Let $\Box_p A \in w_{k+1}$. By definition, $\Box_p A \equiv B\mu$ for a formula $B \in w_k$, hence $\Box_p A = B\mu = B\mu\mu = (\Box_p A)\mu$, so again, $A \equiv A\mu$. From $\Box_p A \in w_{k+1}$ follows by $w_{k+1} \subset w_k$ that $\Box_p A \in w_k$, hence, as w_k is a model, $w_k \models A$, thus $w_{k+1} \models A\mu$, so finally, $w_{k+1} \models A$.
■

3.4 Lemma Let w be a model, and let $(\varepsilon, w), \ldots, (\sigma_k, w_k)$ be a w-chain which ends by [failure$_b$]. Then w is not a $\mathcal{PU}$-model.

Proof By the previous lemma we know that $w = \sigma_k w_k$, σ_k is idempotent, $w_k \subset w$, and w_k is a model. Let μ and w' be defined as in definition 3.2. Our proof has the following outline:

1. Assume that for all quasiatomic formulas D_1, D_2:
   if $D_1\sigma_k\mu \equiv D_2\sigma_k\mu$, then $w_k \models D_1\sigma_k \leftrightarrow D_2\sigma_k$.
2. From 1. follows that for all quasiatomic formulas F_1, F_2:
   if $F_1\mu \equiv F_2\mu$, then $w_k \models F_1 \leftrightarrow F_2$.
3. From 2. follows that $w_k = \mu w'$, where w' is a model.
4. If 1. does not hold, then w is not a $\mathcal{PU}$-model.

First note that, as in each step of the algorithm μ is an idempotent unifier of formulas in w_k, $dom(\mu) \subset var(w_k)$, $ran(\mu) \subset var(w_k)$, and $var(w_k) \cap dom(\sigma_k) = \emptyset$. As a consequence, $dom(\mu) \cap dom(\sigma_k) = \emptyset$, and $ran(\mu) \cap dom(\sigma_k) = \emptyset$.
Now assume that 1. holds, and that F_1, F_2 are quasiatomic formulas such that $F_1\mu \equiv F_2\mu$. If $F_1 \equiv D_1\sigma_k$ and $F_2 \equiv D_2\sigma_k$, for some formulas D_1, D_2, then also D_1, D_2 are quasiatomic, hence 1. can be applied to get $w_k \models F_1 \leftrightarrow F_2$. If F_1 is not of the form

$D_1\sigma_k$, then F_1 contains a variable of $dom(\sigma_k)$: if F_1 contains no variable of $dom(\sigma_k)$, then $F_1 \equiv F_1\sigma_k$. From this follows that $F_1\mu$ contains a variable of $dom(\sigma_k)$, thus $F_2\mu$ contains a variable of $dom(\sigma_k)$, thus F_2 contains a variable of $dom(\sigma_k)$. Consequently, F_2 is not of the form $D_2\sigma_k$, too. According to definition 3.2, $w_k := \{A \mid \exists B \in w : A \equiv B\sigma_k$, and A is quasiatomic$\}$, hence $F_1, F_2 \notin w_k$. So finally we get $w_k \models \neg F_1$ and $w_k \models \neg F_2$, hence $w_k \models F_1 \leftrightarrow F_2$. The case where F_2 is not of the form $D_2\sigma_k$, is shown in the same way.
To prove 3., first notice that from 2. it follows by exactly the same argument as in the proof of the previous lemma, that $w' \subset w_k$, and that for all formulas A, $w_k \models A$ iff $w_k \models A\mu$. We show that for all formulas A, $w_k \models A$ iff $w' \models A\mu$ by induction on the complexity of $A\mu$:

- Let $A\mu$ be quasiatomic. Then also A is quasiatomic. If $w_k \models A$, i.e. $A \in w_k$, then by the definition of w', $A\mu \in w'$, hence $w' \models A\mu$. And if $w' \models A\mu$, i.e. $A\mu \in w'$, then as $w' \subset w_k$, $w_k \models A\mu$, hence $w_k \models A$.
- If $A\mu$ is $\neg B$, then $\neg B \equiv A\mu \equiv A\mu\mu \equiv \neg B\mu$, hence $B \equiv B\mu$. Consequently, $w_k \models A$ iff $w_k \models A\mu$ iff $w_k \models \neg B$ iff $w_k \not\models B$ iff (induction hypothesis) $w' \not\models B\mu$ iff $w' \models \neg B\mu$ iff $w' \models A\mu$.
- If $A\mu$ is $B_1 \wedge B_2$, then $B_1 \wedge B_2 \equiv A\mu \equiv A\mu\mu \equiv B_1\mu \wedge B_2\mu$, hence $B_1 \equiv B_1\mu$ and $B_2 \equiv B_2\mu$. Consequently, $w_k \models A$ iff $w_k \models A\mu$ iff $w_k \models B_1 \wedge B_2$ iff $(w_k \models B_1) \wedge (w_k \models B_2)$ iff (induction hypothesis) $(w' \models B_1\mu) \wedge (w' \models B_2\mu)$ iff $w' \models B_1 \wedge B_2$ iff $w' \models A\mu$.

The proof that w' is a model is straightforward: Obviously, w' is a finite set of quasiatomic formulas. Let $\Box_p A \in w'$. By definition, $\Box_p A \equiv B\mu$ for a formula $B \in w$, hence $\Box_p A \equiv B\mu \equiv B\mu\mu \equiv (\Box_p A)\mu$, so again, $A \equiv A\mu$. From $\Box_p A \in w'$ follows that $\Box_p A \in w_k$, hence $w_k \models A$, hence $w' \models A\mu$, hence $w' \models A$.
For 4., assume that we have quasiatomic formulas D_1, D_2 such that $D_1\sigma_k\mu \equiv D_2\sigma_k\mu$, but $w_k \not\models D_1\sigma_k \leftrightarrow D_2\sigma_k$. Assume furthermore, that w is a $\mathcal{PU}$-model, i.e. $w = \sigma w''$ for a substitution σ and a $\mathcal{PF}$-model w''. Now $\sigma_k\mu$ is a most general unifier of those pairs $\Box_p A, \Box_p B \in w$ $(A \not\equiv B)$ which have been chosen by the algorithm, and σ is another unifier of these pairs by $w = \sigma w''$ and the fact that w'' is a $\mathcal{PF}$-model. It follows that $\sigma = (\sigma_k\mu)\lambda$ for a substitution λ. From $D_1\sigma_k\mu \equiv D_2\sigma_k\mu$ we get $D_1\sigma_k\mu\lambda \equiv D_2\sigma_k\mu\lambda$, i.e. $D_1\sigma \equiv D_2\sigma$. Therefore, $w'' \models D_1\sigma \leftrightarrow D_2\sigma$, hence $w'' \models (D_1 \leftrightarrow D_2)\sigma$, hence $w \models D_1 \leftrightarrow D_2$, and so $w_k \models D_1\sigma_k \leftrightarrow D_2\sigma_k$; contradiction.
■

3.5 Lemma Let w be a model. Then

(i) each w-chain is finite,
(ii) there exist only finitely many w-chains,
(iii) if there exists a w-chain which ends by success, then w is a $\mathcal{PU}$-model,
(iv) if there exists a w-chain which ends by failure, then w is not a $\mathcal{PU}$-model.

Proof Let μ and w' be defined according to the algorithm in definition 3.2. For (i) observe that if (σ_k, w_k) and (σ_{k+1}, w_{k+1}) are subsequent elements of a w-chain, then the number of different sentence and proof variables in w_{k+1} is strictly less that the number of variables in w_k, as $\mu \neq \varepsilon$. Statement (ii) holds, as each set w_k in the chain

contains only finitely many unifiable formulas $\Box_p A, \Box_p B$ $(A \not\equiv B)$, and for each pair of unifiable formulas there exist only finitely many idempotent most general unifiers. Now let w_k be the last element of the w-chain. In the case of (iii), if w_k contains no formulas $\Box_p A, \Box_p B$ $(A \not\equiv B)$, then w_k is a $\mathcal{PF}$-model, hence w is a $\mathcal{PU}$-model based on w_k and σ_k. In the case of (iv), if w_k contains formulas $\Box_p A, \Box_p B$ $(A \not\equiv B)$ which are not unifiable (i.e. [failure$_a$]), then also w contains $\Box_p A$ and $\Box_p B$. Assume that w is a $\mathcal{PU}$-model based on a $\mathcal{PF}$-model w'' and a substitution σ. It follows that $(\Box_p A)\sigma, (\Box_p B)\sigma \in w''$. But $(\Box_p A)\sigma \not\equiv (\Box_p B)\sigma$, hence w'' cannot be a $\mathcal{PF}$-model. In the case of (iv), if $w_k \neq \mu w'$ (i.e. [failure$_b$]), then by lemma 3.4, w is not a $\mathcal{PU}$-model.
■

3.6 Theorem Let w be a finite set of quasiatomic formulas. It is decidable whether w is a $\mathcal{PU}$-model.

Proof Immediate consequence of lemma 3.5.
■

3.7 Remark In the decision procedure above we have used only idempotent unifiers. It is possible to restrict the definition 1.6 of $\mathcal{PU}$-model to idempotent substitutions, too: If w is a $\mathcal{PU}$-model, then there exists a $\mathcal{PF}$-model w'' and an idempotent substitution μ such that w is based on w'' and μ. The following short argument proves this claim: Let w' be a $\mathcal{PF}$-model and σ be a substitution such that w is based on w' and σ. Let μ be an idempotent substitution and α a permutation of variables such that $\sigma = \mu\alpha$. Let $w'' := w'\alpha^{-1}$. Again, w'' is a $\mathcal{PF}$-model. Now if $w \models A$ then $w' \models A\mu\alpha$, hence $w'\alpha^{-1} \models A\mu\alpha\alpha^{-1}$, which is equivalent to $w'' \models A\mu$. And if $w'' \models A\mu$, hence $w'\alpha^{-1} \models A\mu$, then $w'\alpha^{-1}\alpha \models A\mu\alpha$, which is equivalent to $w' \models A\sigma$, from which follows $w \models A$.

4 Fixed Points

In this section some general properties of the Basic Logic of Proofs are discussed, mainly centered around fixed points. The situation is not as uniform as in the classical Provability Logic GL (cf. [4] and [7]). Among other things we show that: In $\mathcal{P}$ and $\mathcal{PF}$ fixed points do not always exist (theorem 4.4), but in $\mathcal{PM}$ and $\mathcal{PFM}$ they do (theorem 4.6). There are formulas which have in the usual way logical unique fixed points (e.g. theorem 4.5), i.e. if A is a fixed point and A is logically equivalent to B then also B is a fixed point. But there are also formulas which have syntactically unique fixed points (theorem 4.9). Finally there are formulas which have logically different fixed points (last example at the end of this section).

According to definition 1.6, a $\mathcal{PU}$-model is basically a $\mathcal{PF}$-model which is "lifted up" by a substitution. So all the properties of functionality are already available in the underlying $\mathcal{PF}$-model. For this reason we discuss in this section the fixed points of $\mathcal{P}$, $\mathcal{PF}$, $\mathcal{PM}$ and $\mathcal{PFM}$, but not of $\mathcal{PU}$ and $\mathcal{PUM}$.

Let $subf(A)$ be the set of all subformulas of a formula A.

4.1 Lemma Let w be a $\mathcal{P}$-model and A a formula such that $w \models A$, and let $w_A := w \cap subf(A)$. Then w_A is a $\mathcal{P}$-model, and $w_A \models A$. If w is a $\mathcal{PF}$-, $\mathcal{PM}$- or $\mathcal{PFM}$-model, then w_A is a $\mathcal{PF}$-, $\mathcal{PM}$- or $\mathcal{PFM}$-model, respectively (cf. example 1.8).

Proof As there exist only finitely many subformulas of A, w_A is a finite set of quasiatomic formulas. By straightforward induction on the complexity of a formula B it follows that if $B \in subf(A)$, then $w \models B$ iff $w_A \models B$ (cf. proof of lemma 2.5). To see that w_A is a model, let $\Box_p B \in w_A$. By definition, $\Box_p B \in w$, and $\Box_p B$ is a subformula of A. From the first it follows that $w \models B$, and from the second that also B is a subformula of A, hence $w_A \models B$. Obviously, if w is a $\mathcal{PF}$- and/or $\mathcal{PM}$-model, then w_A is a $\mathcal{PF}$- and/or $\mathcal{PM}$-model, respectively.
■

4.2 Lemma Let A be a formula and p a proof variable.

a) If there exists a $\mathcal{P}$-model in which A is true then there exists a $\mathcal{P}$-model in which both A and $\neg\Box_p A$ are true. This is also true for $\mathcal{PF}$-, $\mathcal{PM}$- and $\mathcal{PFM}$-models.

b) If there exists a $\mathcal{P}$-model in which A is true then there exists a $\mathcal{P}$-model in which $\Box_p A$ is true. This is not true for $\mathcal{PF}$-, $\mathcal{PM}$- and $\mathcal{PFM}$-models (take $A := \Box_p \top$).

c) If A is true in all $\mathcal{P}$-models (i.e. $\mathcal{P} \models A$) then there exists a $\mathcal{P}$-model in which $\Box_p A$ is true. This is also true for $\mathcal{PF}$-, but not true for $\mathcal{PM}$- and $\mathcal{PFM}$-models (take $A := \neg\Box_p \bot$).

Proof

a) Let w be a model such that $w \models A$, and let $w_A := w \cap subf(A)$. According to lemma 4.1, $w_A \models A$, and $w_A \models \neg\Box_p A$, as $\Box_p A$ cannot be a subformula of A.
b) Let w be a $\mathcal{P}$-model such that $w \models A$, and let $\tilde{w}_A := w \cup \{\Box_p A\}$. Then again $\tilde{w}_A$ is a $\mathcal{P}$-model, and $\tilde{w}_A \models \Box_p A$.
c) Let $w := \{\Box_p A\}$. As A is true in each $\mathcal{P}$-model, it follows that w is a $\mathcal{P}$-model. Obviously, w is also a $\mathcal{PF}$-model.

■

4.3 Corollary Let A be a formula and p a proof variable.

a) $\mathcal{P} \models A \to \Box_p A$ iff $\mathcal{P} \models \neg A$.
This is also true for $\mathcal{PF}$, $\mathcal{PM}$ and $\mathcal{PFM}$.

b) $\mathcal{P} \models \neg\Box_p A$ iff $\mathcal{P} \models \neg A$.
This is not true for $\mathcal{PF}$, $\mathcal{PM}$ and $\mathcal{PFM}$ (take $A = \Box_p \top$).

c) $\mathcal{P} \models \neg\Box_p A$ implies $\mathcal{P} \not\models A$.
This is also true for $\mathcal{PF}$, but not true for $\mathcal{PM}$ and $\mathcal{PFM}$ (take $A = \neg\Box_p \bot$).

■

First notice that in each statement of the corollary, the formula A may contain the proof variable p. Item a) expresses that a formula which asserts that it is uniformly provable by p, must be refutable. Item b) divides our logics into those which have the functionality or the monotonicity property, and into those which have it not. For the latter, i.e. $\mathcal{P}$, it says that if a formula is such that it is uniformly not provable by any proof, then it is refutable; and it is at least not provable in the case of the functional logic $\mathcal{PF}$, according to item c) .

As a variant of c) we get:

4.4 Theorem The modal scheme $\neg\Box_p(\cdot)$ has no fixed point in $\mathcal{P}$ and $\mathcal{PF}$, i.e. there exists no formula A such that $\mathcal{P} \models A \leftrightarrow \neg\Box_p A$.

Proof From $\mathcal{P} \models A \leftrightarrow \neg\Box_p A$ and from (A2) it follows that $\mathcal{P} \models A$ and $\mathcal{P} \models \neg\Box_p A$, which contradicts c) of corollary 4.3 . The same holds for $\mathcal{PF}$.
■

With the same argument it follows that $\Box_p\neg(\cdot)$ has no fixed point in $\mathcal{P}$ and $\mathcal{PF}$, too. A variant of item a) in corollary 4.3 is the following:

4.5 Theorem The modal scheme $\Box_p(\cdot)$ has the logically unique fixed point $\bot$ in $\mathcal{P}$, $\mathcal{PF}$, $\mathcal{PM}$ and $\mathcal{PFM}$, i.e. $\mathcal{P} \models \bot \leftrightarrow \Box_p\bot$, and if $\mathcal{P} \models A \leftrightarrow \Box_p A$ then $\mathcal{P} \models A \leftrightarrow \bot$.

Proof $\mathcal{P} \models A \leftrightarrow \Box_p A$ is by (A2) equivalent to $\mathcal{P} \models A \rightarrow \Box_p A$ which is by corollary 4.3 item a) equivalent to $\mathcal{P} \models \neg A$. The same holds for $\mathcal{PF}$, $\mathcal{PM}$ and $\mathcal{PFM}$, too.
■

In this context remember that in the Provability Logic GL the operator $\neg\Box(\cdot)$ (not provable) has $\neg\Box\bot$ (consistency) as its unique fixed point, and $\Box(\cdot)$ (provable) has the fixed point $\top$.

4.6 Theorem In $\mathcal{PM}$ and $\mathcal{PFM}$, fixed points always exist, i.e. if every occurrence of x in a formula $D(x)$ lies within the scope of a box then there exists a formula A such that $\mathcal{PM} \models A \leftrightarrow D(A)$.

Proof Write $D(x)$ as $D(\Box_{q_1}C_1(x), \ldots, \Box_{q_k}C_k(x))$ where x occurs in each $\Box_{q_i}C_i(x)$, $D(y_1, \ldots, y_k)$ contains no further x, and none of $y_1, \ldots, y_k$ lies within the scope of a box. Then let $A := D(\Box_{q_1}\bot, \ldots, \Box_{q_k}\bot)$. By the Monotonicity Axiom, $\mathcal{PM} \models \Box_{q_i}C_i(A) \leftrightarrow \bot$, and by the Reflexion Axiom $\mathcal{PM} \models \Box_{q_i}\bot \leftrightarrow \bot$. It follows that

$$\begin{array}{rcl} \mathcal{PM} \models A & \leftrightarrow & D(\Box_{q_1}\bot, \ldots, \Box_{q_k}\bot) \\ & \leftrightarrow & D(\Box_{q_1}C_1(A), \ldots, \Box_{q_k}C_k(A)) \\ & \leftrightarrow & D(A) \end{array}$$

■

4.7 Example According to the construction in the proof above, the formula $D(x) := \neg\Box_p(x)$ has the fixed point $A = \neg\Box_p\bot$; indeed, $\mathcal{PM} \models (\neg\Box_p\bot) \leftrightarrow \neg\Box_p(\neg\Box_p\bot)$. Notice that $\neg\Box_p\bot$ is not the only fixed point. Obviously all formulas which contain p and which are provable in $\mathcal{PM}$ are fixed points, too.

In example 1.7 (iii) we have shown that no formula of the form $\Box_p A$ is provable in $\mathcal{P}$ (or $\mathcal{PF}$, $\mathcal{PM}$, $\mathcal{PFM}$). Our next aim is to discuss the refutability of $\Box_p A$. The first such result is corollary 4.3 b), according to which $\mathcal{P} \models \neg\Box_p A$ iff A is refutable in $\mathcal{P}$. The next lemma answers this question for the other logics, too.

4.8 Lemma Let A be a formula and p be a proof variable. Then

$$\mathcal{PF} \models \neg\Box_p A \iff \mathcal{PF} \models A \to (\Box_p \bar{B}_1 \vee \ldots \vee \Box_p \bar{B}_k), \text{ where } \Box_p \bar{B}_1, \ldots, \Box_p \bar{B}_k \text{ are the subformulas of } A \text{ of the form } \Box_p B.$$

$$\mathcal{PM} \models \neg\Box_p A \iff \mathcal{PM} \models \neg A, \text{ or } A \text{ contains } p.$$

$$\mathcal{PFM} \models \neg\Box_p A \iff A \text{ contains } p, \text{ or } \mathcal{PFM} \models A \to (\Box_p \bar{B}_1 \vee \ldots \vee \Box_p \bar{B}_k), \text{ where } \Box_p \bar{B}_1, \ldots, \Box_p \bar{B}_k \text{ are the subformulas of } A \text{ of the form } \Box_p B.$$

Proof The only case from the right to the left which has to be explained is that if $\mathcal{PF} \models A \to (\Box_p \bar{B}_1 \vee \ldots \vee \Box_p \bar{B}_k)$, then $\mathcal{PF} \models \neg\Box_p A$. Assume that $\mathcal{PF} \not\models \neg\Box_p A$, i.e. there exists a $\mathcal{PF}$-model w such that $w \models \Box_p A$. Let $w_A := w \cap subf(A)$. By lemma 4.1, $w_A \models A$. As w is a $\mathcal{PF}$-model, w_A contains no formulas of the form $\Box_p B$ for the proof variable p, so $w_A \models \neg\Box_p B$ for all formulas B. As a consequence, $\mathcal{PF} \not\models A \to (\Box_p \bar{B}_1 \vee \ldots \vee \Box_p \bar{B}_k)$.

For the direction from the left to the right, we show only the proof for $\mathcal{PFM}$. The proofs for $\mathcal{PF}$ and $\mathcal{PM}$ are special cases of this one. Assume that

$$A \text{ does not contain } p, \text{ and}$$
$$\exists w : \ (w \models A \ \wedge \ \Box_p \bar{B}_1 \notin w \wedge \ldots \wedge \Box_p \bar{B}_k \notin w).$$

where w is a $\mathcal{PFM}$-model, and $\Box_p \bar{B}_1, \ldots, \Box_p \bar{B}_k$ are the subformulas of A which have the form $\Box_p B$ for the proof variable p. Let $\bar{w}$ be such a model and let $\bar{w}_A := \bar{w} \cap subf(A)$. Still, $\bar{w}_A$ is a $\mathcal{PFM}$-model and $\bar{w}_A \models A$, according to lemma 4.1. Furthermore, $\bar{w}_A$ contains no formula of the form $\Box_p B$ for the proof variable p. Now let $\tilde{w} := \bar{w}_A \cup \{\Box_p A\}$. We have to check that $\tilde{w}$ is a $\mathcal{PFM}$-model, and then we are done because $\tilde{w} \models \Box_p A$, hence $\mathcal{PFM} \not\models \neg\Box_p A$. That $\tilde{w}$ is a model follows from $\tilde{w} \models A$. That $\tilde{w}$ is a $\mathcal{PM}$-model is guaranteed by the assumption that A does not contain p. And $\tilde{w}$ is still a $\mathcal{PF}$-model, as $\bar{w}_A$ contains no formula of the form $\Box_p B$ for the proof variable p.

■

Up to the end of this section we will provide some examples of fixed points to demonstrate that several nice and desired properties of Provability Logic are not valid for the Basic Logic of Proofs.

In $\mathcal{P}$ and $\mathcal{PF}$ we have the situation that *syntactically unique* fixed points exist:

4.9 Theorem The formula $D(x) := \neg\Box_p(x) \vee \Box_p \top$ has the syntactically unique fixed point $\top$ in $\mathcal{P}$ and $\mathcal{PF}$, i.e. $\mathcal{P} \models (\top) \leftrightarrow \neg\Box_p(\top) \vee \Box_p \top$, and if $\mathcal{P} \models (A) \leftrightarrow \neg\Box_p(A) \vee \Box_p \top$ then $A \equiv \top$.

Proof Let $A \not\equiv \top$. We have to show that there exists a $\mathcal{P}$-model ($\mathcal{PF}$-model) $\tilde{w}$ such that $\tilde{w} \models A \wedge \Box_p A \wedge \neg\Box_p \top$ or $\tilde{w} \models \neg A \wedge (\neg\Box_p A \vee \Box_p \top)$. For this we consider two

cases. 1st case: If for all models w, $w \models A$, then let $\tilde{w} := \{\Box_p A\}$. Obviously, $\tilde{w}$ is a $\mathcal{P}$-model ($\mathcal{PF}$-model), as $\tilde{w} \models A$. So we have $\tilde{w} \models A$, and $\tilde{w} \models \Box_p A$, and $\tilde{w} \not\models \Box_p \top$ as $A \not\equiv \top$. 2nd case: If there exists a $\mathcal{P}$-model ($\mathcal{PF}$-model) w_0 such that $w_0 \models \neg A$, then let $\tilde{w} := w_0 \cap subf(\neg A)$. By lemma 4.1, $\tilde{w}$ still is a $\mathcal{P}$-model ($\mathcal{PF}$-model) and $\tilde{w} \models \neg A$, and $\tilde{w} \models \neg \Box_p A$.
■

Next, we show that if logically equivalent formulas A_1 and A_2 ($A_1 \not\equiv A_2$) are fixed points of $D(x)$, then not necessarily all formulas equivalent to A_1 are fixed points, too. The following example fits also for $\mathcal{PF}$, $\mathcal{PM}$ and $\mathcal{PFM}$: Let $D(x) := \Box_p(x) \vee \neg\Box_p\top \vee \neg\Box_p(\top \wedge \top)$. Then

$$\mathcal{P} \models (\top) \leftrightarrow \Box_p(\top) \vee \neg\Box_p\top \vee \neg\Box_p(\top \wedge \top), \quad \text{and also}$$
$$\mathcal{P} \models (\top \wedge \top) \leftrightarrow \Box_p(\top \wedge \top) \vee \neg\Box_p\top \vee \neg\Box_p(\top \wedge \top)$$

but e.g. $\top \wedge \top \wedge \top$ is not a fixed points. This example can easily be extended to more than two such formulas.

Another formula worth to consider is $D(x) := \neg\Box_p(x) \wedge \Box_p\top$. In $\mathcal{PF}$ a fixed point exists,

$$\mathcal{PF} \models (\Box_p\top) \leftrightarrow \neg\Box_p(\Box_p\top) \wedge \Box_p\top$$

as $\neg\Box_p\Box_p\top$ is a true statement in $\mathcal{PF}$. But in $\mathcal{P}$, this formula has no fixed point:

4.10 Theorem The formula $D(x) := \neg\Box_p(x) \wedge \Box_p\top$ has no fixed point in $\mathcal{P}$.

Proof Let A be an arbitrary formula. We have to show that there exists a $\mathcal{P}$-model $\tilde{w}$ such that $\tilde{w} \models A \wedge (\Box_p A \vee \neg\Box_p\top)$ or $\tilde{w} \models \neg A \wedge \neg\Box_p A \wedge \Box_p\top$. We consider two cases. 1st case: If for all models w, $w \models \neg A$, then let $\tilde{w} := \{\Box_p\top\}$. Then $\tilde{w} \models \neg A$, hence $\tilde{w} \models \neg\Box_p A$, and $\tilde{w} \models \Box_p\top$. 2nd case: If there exists a model w_0 such that $w_0 \models A$, then let $\tilde{w} := w_0 \cup \{\Box_p A\}$. Still, $\tilde{w}$ is a model, and $\tilde{w} \models A$, and $\tilde{w} \models \Box_p A$.
■

In $\mathcal{PF}$ another effect can take place. Let $D(x) := \neg(\Box_p(x) \wedge \Box_p\top)$, then e.g.

$$\mathcal{PF} \models (\top \wedge \top) \leftrightarrow \neg(\Box_p(\top \wedge \top) \wedge \Box_p\top)$$

but

$$\mathcal{PF} \not\models (\top) \leftrightarrow \neg(\Box_p(\top) \wedge \Box_p\top)$$

Here the situation is complementary to that of theorem 4.9; all formulas equivalent to $\top$ are fixed points, except the formula $\top$ itself. Again, this example can be easily extended: Let $D(x) := \neg(\Box_p(x) \wedge \Box_p\top) \wedge \neg(\Box_p(x) \wedge \Box_p(\top \wedge \top))$. Then all provable formulas are fixed points, except $\top$ and $\top \wedge \top$.

Finally, in none of the logics $\mathcal{P}$, $\mathcal{PF}$, $\mathcal{PM}$ and $\mathcal{PFM}$ the classical fixed point theorem is valid, i.e. fixed points are in general not unique: Let $D(x) := \Box_p(x) \vee \neg\Box_p\top$, then

$$\mathcal{P} \models (\top) \leftrightarrow \Box_p(\top) \vee \neg\Box_p\top$$

and also

$$\mathcal{P} \models (\neg\Box_p\top) \leftrightarrow \Box_p(\neg\Box_p\top) \vee \neg\Box_p\top$$

but $\top$ and $\neg\Box_p\top$ are not logically equivalent in $\mathcal{P}$, $\mathcal{PF}$, $\mathcal{PM}$ or $\mathcal{PFM}$. Notice, that all formulas which are logically equivalent to $\neg\Box_p\top$ are fixed points, too, but e.g. $\top \wedge \top$ is not a fixed point.

Acknowledgements

I want to thank Sergei Artëmov (Moscow) and Giulio Rodinò (Berne) for their many helpful suggestions and hints.

References

[1] S. Artëmov and T. Straßen, "The Basic Logic of Proofs," in *Computer Science Logic* (E. Börger, G. Jäger, H. Kleine Büning, and M.M. Richter, eds.), vol. 702 of *Lecture Notes in Computer Science*, pp. 14–28, Proceedings of the 6th Workshop, CSL'92, San Miniato, Italy, October 1992, Springer-Verlag, 1993.

[2] S. Artëmov and T. Straßen, "Functionality in the Basic Logic of Proofs," Tech. Rep. IAM 93-004, Department for computer science, University of Berne, Switzerland, January 1993.

[3] S. Artëmov and T. Straßen, "The Logic of the Gödel Proof Predicate," in *Computational Logic and Proof Theory* (G. Gottlob, A. Leitsch, and D. Mundici, eds.), vol. 713 of *Lecture Notes in Computer Science*, pp. 71–82, Proceedings of the Third Kurt Gödel Colloquium, KGC'93, Brno, Czech Republic, August 1993, Springer-Verlag, 1993.

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

[5] C. C. Chang and H. J. Keisler, *Model Theory*, vol. 73 of *Studies in Logic and the Foundations of Mathematics*. Amsterdam: North-Holland, third ed., 1990.

[6] J. Lassez, M. Maher, and K. Marriott, "Unification revisited," in *Foundations of Deductive Databases and Logic Programming* (J. Minker, ed.), ch. 15, pp. 587–625, Morgan Kaufmann Publishers, Inc., 1987.

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

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