

The Basic Logic of Proofs

Inauguraldissertation
der Philosophisch-naturwissenschaftlichen Fakultät
der Universität Bern

vorgelegt von
Tyko Strassen
von Zürich

Leiter der Arbeit: Prof. Dr. G. Jäger,
Institut für Informatik und angewandte Mathematik

Acknowledgements

There are two persons I want to thank above all.

For several years, Prof. G. Jäger taught me not only a lot of mathematics and computer science in his well-known precise and competent way. He also took great care of a perfect working environment.

As a guest of our group for three times, Prof. S. Artëmov (Steklov Mathematical Institute Moscow) introduced me to several methods related to Provability Logic and to this text. Being abroad, he spent a lot of time in assisting the major part of this work, too.

Finally, I want to thank all my colleagues and friends, among others Ursula Hadorn, Markus Marzetta, Giulio Rodinò, Michael Seyfried, Thomas Strahm, and Werner Wolff, for their support in many situations.

This work was financially supported by the *Schweizerischer Nationalfonds* (projects 21-27878.89 and 20-32705.91) and by the Union Bank of Switzerland (**UBS/SBG**).

Abstract

Propositional Provability Logic was axiomatized by R.M. Solovay in 1976. This modal logic describes the behavior of the arithmetical operator “ A is provable”. The aim of these investigations is to provide propositional axiomatizations of the predicates “ p is a proof of A ”, “ p is a proof which contains A ” and “ p is a program which computes A ” using the same semantics.

The presented systems, called the Basic Logic of Proofs, are first proved to be sound and complete with respect to arithmetical interpretations. Decidability is a consequence of a semantical cut elimination theorem. Moreover, appropriate syntactical models for the Basic Logic of Proofs are defined, which are closely related to canonical models. Finally, some general principles of the Basic Logic of Proofs, mainly concerning fixed points, are investigated.

Contents

1	Introduction	1
1.1	Motivation	1
1.2	Arithmetic, proof predicates	2
1.3	Semantics	4
1.4	Main results	6
2	Soundness	11
2.1	Soundness without unification	11
2.2	Soundness with unification	12
3	Completeness	19
3.1	Gentzen style systems	20
3.2	Soundness w.r.t. Hilbert style systems	21
3.3	Saturations	22
3.4	The general case	24
3.5	Completeness with i-functionality	29
3.6	Completeness with unification	30
3.7	Completeness with monotonicity	32
4	Uniformity	39
5	Syntactical models	45
5.1	Models without unification	46
5.2	Models with unification	49
5.3	Decidability	52
6	Fixed points	59
7	Extensions	67
	References	70
	Index	72

1 Introduction

1.1 Motivation

The Provability Logic GL was axiomatized by R.M. Solovay in [11]. This propositional modal logic gives a framework for studying properties of the provability predicate $Pr_{PA}(\cdot)$ of Peano Arithmetic PA. In this context the modal operator \Box is interpreted as $Pr_{PA}(\cdot)$, i.e. $\Box A$ can be read as “ A is provable in PA”. Solovay’s axiomatization of GL consists of all tautologies, the schemes $\Box(A \rightarrow B) \rightarrow (\Box A \rightarrow \Box B)$ and $\Box(\Box A \rightarrow A) \rightarrow \Box A$, as well as the rules modus ponens and necessitation. 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, fixed points and formalizations. Some well-known properties (cf. [5], [10], [11]) of GL related to this text are the substitution lemmas and the existence and uniqueness of fixed points. E.g. $\neg\Box(\cdot)$ has the fixed point $\neg\Box\perp$ (consistency), and $\Box(\cdot)$ has the fixed point \top .

Although some properties of GL are relevant for computer science (e.g. Gödel’s incompleteness theorems for consistency proofs in databases), this logic has mainly applications to mathematics itself. 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*, or 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 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. However, these important aspects of provability cannot be expressed in terms of $Pr_{PA}(\cdot)$.

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 can be interpreted in a wide range of applications, 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 ”. Using these logics one can easily answer questions about *proofs* in the same way as GL does for *provability*. Some simple examples of such questions are “is it provable that a given proof does not derive $0=1$?”, “is it possible that p is a

proof of φ if p is a proof of $\varphi \wedge \varphi$?”, “is it provable that p cannot be the proof of a formula containing p ?”.

Most definitions in the following introduction are in accordance with those of classical Provability Logic [11]. Nevertheless, the Basic Logic of Proofs is entirely different from Provability Logic, and its arithmetical completeness proof does not use the Solovay argument.

1.1 Definition The modal language contains two sorts of variables,

$$\begin{aligned} p_0, p_1, \dots & \text{ (called } \textit{proof variables}), \\ S_0, S_1, \dots & \text{ (called } \textit{sentence variables}), \end{aligned}$$

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, \dots by the boolean connectives \neg , \wedge as usual, and by the unary modal operators $\Box_{p_0}(\cdot)$, $\Box_{p_1}(\cdot)$, \dots 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 \perp (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, \dots are used for proof variables, capital letters S, T, \dots for sentence variables and A, B, C, \dots for modal formulas.

1.2 Arithmetic, proof predicates

In order to allow iterations of modalities, which is an essential principle of the Basic 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 *arithmetical interpretation* of the modal language.

1.2 Definition Let the theory T be Primitive Recursive Arithmetic PRA, or let T be a recursive extension of $I\Sigma_1$ which is valid in the standard model of arithmetic, e.g. let T be Peano Arithmetic PA.

Greek letters φ, ψ, \dots denote arithmetical formulas. In this text we do not distinguish between the number n and its numeral \overline{n} .

In the sequel, by *formula* we always mean *modal formula*.

1.3 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 an expression t occurs in the formula φ then $\ulcorner t \urcorner < \ulcorner \varphi \urcorner$,

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

- $Prf(x, y)$ is (provably-in- \mathbb{T} equivalent to) a recursive formula in x and y ,
- $\mathbb{T} \vdash \varphi \iff \exists n \in \mathbb{N}: Prf(n, \ulcorner \varphi \urcorner)$ 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 $n \geq k$.

A proof predicate is thus nothing but a recursive enumeration of the theorems of \mathbb{T} , and a functional proof predicate is additionally injective. The following definition gives some examples of such proof predicates.

1.5 Definition Let $proof(x)$ be a standard arithmetical term for the recursive predicate “ x is the Gödel number of a proof in \mathbb{T} ”. A formal description of $proof(\cdot)$ can be found for example in [5] or [10]. Let $lh(s)$ and $(s)_i$ be primitive recursive terms which compute the length and the i 'th component of a sequence s , respectively.

1. The *Gödel proof predicate* $\widetilde{Prf}(\cdot, \cdot)$ is defined as usual by

$$\widetilde{Prf}(x, y) := proof(x) \wedge (x)_{lh(x)} = y$$

i.e. $\widetilde{Prf}(x, y)$ holds iff y is the Gödel number of the last formula of the proof with Gödel number x .

2. The *nonfunctional Gödel proof predicate* $\overline{Prf}(\cdot, \cdot)$ is defined by

$$\overline{Prf}(x, y) := \text{proof}(x) \wedge \exists i \leq lh(x) : (x)_i = y$$

i.e. $\overline{Prf}(x, y)$ holds iff x is the Gödel number of a proof which contains a formula with Gödel number y .

Note that with respect to $\widetilde{Prf}(\cdot, \cdot)$ and $\overline{Prf}(\cdot, \cdot)$ each theorem has infinitely many proofs.

3. 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 \mathbb{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 1.3). On the other side, short programs can compute long theorems in such a way that $Prf_1(x, y)$ does not necessarily imply $x \geq y$.
4. 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 $\varphi_1, \varphi_2, \dots$ such that $Prf_2(n, \ulcorner \varphi_i \urcorner)$ is true for a fixed n .

It is not difficult to see that the Gödel proof predicate $\widetilde{Prf}(\cdot, \cdot)$ is both functional and monotonic, the nonfunctional Gödel proof predicate $\overline{Prf}(\cdot, \cdot)$ is monotonic but not functional, $Prf_1(\cdot, \cdot)$ is functional but not monotonic, and that $Prf_2(\cdot, \cdot)$ is an arbitrary proof predicates. Moreover, the corresponding provability predicates $\widetilde{Pr}(y) := \exists x \widetilde{Prf}(x, y)$ and $\overline{Pr}(y) := \exists x \overline{Prf}(x, y)$ are provably-in- \mathbb{T} equivalent (cf. [5], [10]).

1.3 Semantics

The semantics of the Basic Logic of Proofs is based on arithmetical interpretations:

1.6 Definition Let $Prf(\cdot, \cdot)$ be a proof predicate in \mathbb{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 \mathbb{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:

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

1.7 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. $\varphi \equiv \varphi$, but $\varphi \wedge \varphi \not\equiv \varphi$, $S_0 \not\equiv S_1$ and $\Box_{p_0} \top \not\equiv \Box_{p_1} \top$).

1.8 Example Consider the formula $\neg \Box_p \neg \Box_p \top$. Its arithmetical interpretation is $\neg Prf(p^*, \ulcorner \neg Prf(p^*, \ulcorner \top^* \urcorner) \urcorner)$, depending on $Prf(\cdot, \cdot)$ and the interpretation of the proof variable p . Assume first that $Prf(\cdot, \cdot)$ is a monotonic proof predicate, for example the Gödel one $\widetilde{Prf}(\cdot, \cdot)$. As p^* occurs in $\neg Prf(p^*, \ulcorner \top^* \urcorner)$ and by the convention on Gödel numbering (remark 1.3), it follows that $p^* < \ulcorner \neg Prf(p^*, \ulcorner \top^* \urcorner) \urcorner$. Hence by the monotonicity property $Prf(p^*, \ulcorner \neg Prf(p^*, \ulcorner \top^* \urcorner) \urcorner)$ cannot be true. As this is a recursive sentence, $\neg Prf(p^*, \ulcorner \neg Prf(p^*, \ulcorner \top^* \urcorner) \urcorner)$ is provable. So $\neg \Box_p \neg \Box_p \top$ is provable (thus true) under every monotonic interpretation. Assume next that $Prf(\cdot, \cdot)$ is defined by the following fixed point equation, i.e. \mathbb{T} proves the following equivalence:

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

Still, $Prf(\cdot, \cdot)$ is a proof predicate: It is recursive and enumerates all theorems by $\widetilde{Prf}(\cdot, \cdot)$, and additionally the sentence $\neg Prf(0, \ulcorner \top^* \urcorner)$ which is according to the fixed point equation provable in \mathbb{T} , too. Now by

the fixed point equation, $Prf(0, \ulcorner \neg Prf(0, \ulcorner \top^* \urcorner) \urcorner)$ is true, and so with $p^* = 0$, $\neg Prf(p^*, \ulcorner \neg Prf(p^*, \ulcorner \top^* \urcorner) \urcorner)$ is false. So there exists an interpretation which makes $\neg \Box_p \neg \Box_p \top$ false, but this interpretation is no longer monotonic.

1.4 Main results

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

1.9 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))

$$\begin{array}{ll}
 \text{(A1)} & \text{All (boolean) tautologies} \\
 \text{(A2)} & \Box_p A \longrightarrow A \\
 \text{(R1)} & \frac{A \quad A \rightarrow B}{B} \\
 \text{(A3)} & \Box_p A \wedge \Box_p B \wedge F \longrightarrow G \quad (F = G \pmod{A = B}) \\
 \text{(A3')} & \neg(\Box_p A \wedge \Box_p B) \quad (A \neq B) \\
 \text{(A4)} & \neg[\Box_{q_1} A_2(q_2) \wedge \Box_{q_2} A_3(q_3) \wedge \dots \wedge \Box_{q_n} A_1(q_1)]
 \end{array}
 \left. \vphantom{\begin{array}{l} \text{(A1)} \\ \text{(A2)} \\ \text{(R1)} \end{array}} \right\} \mathcal{P}$$

$$\left. \begin{array}{l} \text{(A3)} \\ \text{(A3')} \end{array} \right\} \mathcal{U}$$

$$\left. \begin{array}{l} \text{(A4)} \end{array} \right\} \mathcal{M}$$

where A , B , F , G are formulas, p, q_1, \dots, q_n are proof variables, and $A_i(q_i)$ is a 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 $\forall \theta : (A\theta \equiv B\theta \rightarrow F\theta \equiv G\theta)$, where θ denotes a substitution which substitutes proof variables for proof variables and formulas for sentence variables. (A2) is the *Reflexivity Axiom*, (A3) the *Unification Axiom*, (A3') the *Functionality Axiom* and (A4) the *Monotonicity Axiom*.

1.10 Remark Due to lemma 2.9 the axiom (A3) can also be replaced by the two following axioms:

$$\begin{array}{ll}
 \text{(A3}_1\text{)} & \neg(\Box_p A \wedge \Box_p B) \quad (A, B \text{ are not unifiable}) \\
 \text{(A3}_2\text{)} & \Box_p A \wedge \Box_p B \wedge F \longrightarrow G \quad (A, B \text{ unifiable and } F_{\tau_{A,B}} \equiv G_{\tau_{A,B}})
 \end{array}$$

where $\tau_{A,B}$ is an idempotent most general unifier of A and B which is obtained by a fixed but arbitrary unification algorithm (e.g. algorithm 2.6). So it is decidable whether a formula is an instance of (A3). For technical reasons we will often use (A3₁)+(A3₂) instead of (A3).

The main result of this text is that for each modal formula A the following hold:

$$\begin{aligned} \mathcal{P} \vdash A &\iff \top \vdash A^* \text{ for every interpretation } (\cdot)^*, \\ \mathcal{PF} \vdash A &\iff \top \vdash A^* \text{ for every i-functional } (\cdot)^*, \\ \mathcal{PM} \vdash A &\iff \top \vdash A^* \text{ for every monotonic } (\cdot)^*, \\ \mathcal{PFM} \vdash A &\iff \top \vdash A^* \text{ for every i-functional, monotonic } (\cdot)^*, \\ \mathcal{PU} \vdash A &\iff \top \vdash A^* \text{ for every functional } (\cdot)^*, \\ \mathcal{PUM} \vdash A &\iff \top \vdash A^* \text{ for every functional, monotonic } (\cdot)^*. \end{aligned}$$

Furthermore, in each assertion above one may replace “ $\top \vdash A^*$ ” by “ A^* is true”. E.g. for \mathcal{P} that means

$$\mathcal{P} \vdash A \iff \forall^* : \top \vdash A^* \iff \forall^* : A^* \text{ is true}$$

where “ $\forall^* : S$ ” is used as usual (cf. [5], [10], [11]) as an abbreviation for the fact that S holds for every interpretation $(\cdot)^*$.

The proof of the completeness provides semantical cut elimination for sequential versions of these logics. We get decidability as a consequence.

Moreover, for each of these completeness theorems a proof predicate can uniformly be chosen. \mathcal{PUM} even is complete with respect to all interpretations which use a fixed functional and monotonic proof predicate, for example the Gödel one $\overline{Prf}(\cdot, \cdot)$. The same is true for \mathcal{PM} and a certain nonfunctional proof predicate which is based on $\overline{Prf}(\cdot, \cdot)$. Thereby, \mathcal{PUM} is the logic of the functional Gödel proof predicate. If we use this specific interpretation in the case of \mathcal{PM} and \mathcal{PUM} , then it is not required any more to interpret the proof variables as Gödel numbers of proofs instead of the proofs themselves; we may change the following two items in the definition 1.6 of arithmetical interpretation:

- $\phi(p_i)$ is a proof in \top .
- $(\Box_p A)^* := Prf(\ulcorner p_i^* \urcorner, \ulcorner A^* \urcorner)$.

None of the logics can be regarded as a *normal* modal logic as neither the necessitation rule

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

nor substitution rule

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

are valid under arithmetical interpretations.

1.11 Example Some consequences of the Reflexivity Axiom (A2) are

$$\begin{aligned} \mathcal{P} &\vdash \neg \Box_p \perp \\ \mathcal{P} &\vdash \neg \Box_p \Box_q \perp \\ \mathcal{P} &\vdash \Box_p \neg A \rightarrow \neg \Box_q A \\ \mathcal{P} &\vdash (\Box_p A \wedge \Box_p B) \rightarrow (A \leftrightarrow B) \\ &(\text{even: } \mathcal{P} \vdash (\Box_p A \wedge \Box_p B) \rightarrow (A \wedge B)) \end{aligned}$$

From the Unification Axiom (A3) follow theorems like the following, which are not provable in \mathcal{P}

$$\begin{aligned} \mathcal{P}\mathcal{U} &\vdash \Box_p A \rightarrow \neg \Box_p (A \wedge A) \\ \mathcal{P}\mathcal{U} &\vdash \Box_p S_0 \wedge \Box_p S_1 \wedge S_0 \longrightarrow S_1 \\ \mathcal{P}\mathcal{U} &\vdash \Box_p S_0 \wedge \Box_p S_1 \longrightarrow (\Box_q S_0 \leftrightarrow \Box_q S_1) \\ \mathcal{P}\mathcal{U} &\vdash \neg (\Box_p S_0 \wedge \Box_p \Box_q S_0) \\ \mathcal{P}\mathcal{U} &\vdash \Box_p S_0 \wedge \Box_p S_1 \wedge \Box_q S_0 \longrightarrow \neg \Box_q (S_1 \vee \perp) \end{aligned}$$

Each theorem of $\mathcal{P}\mathcal{U}$ is also a theorem of $\mathcal{P}\mathcal{F}$ (cf. theorem 2.13). The converse is not true; consequences of the Functionality Axiom (A3') which are not theorems of $\mathcal{P}\mathcal{U}$ are e.g.

$$\begin{aligned} \mathcal{P}\mathcal{F} &\vdash \neg (\Box_p S_0 \wedge \Box_p S_1) \\ \mathcal{P}\mathcal{F} &\vdash \Box_q \Box_{p_0} \top \rightarrow \neg \Box_q \Box_{p_1} \top \end{aligned}$$

In the sequel we will see that none of our logics proves any formula of the form $\Box_p A$. But $\mathcal{P}\mathcal{U}$ proves $\neg \Box_p A$ for some formulas A . For example, $\Box_p \Box_p \top \rightarrow \Box_p \top$ is an instance of (A2), and $\neg (\Box_p \Box_p \top \wedge \Box_p \top)$ is an instance of (A3₁), hence it follows that $\mathcal{P}\mathcal{U} \vdash \neg \Box_p \Box_p \top$. The formula $\neg \Box_p \Box_p \top$ is also an instance of the Monotonicity Axiom (A4), i.e. $\mathcal{P}\mathcal{M} \vdash \neg \Box_p \Box_p \top$. Another consequence of this axiom is that $\mathcal{P}\mathcal{M} \vdash \neg \Box_p \neg \Box_p \top$ (cf. example 1.8).

In section 2 the soundness, and in section 3 the completeness of the proof systems with respect to arithmetical interpretations are proved. Section 4 is devoted to uniform proof predicates. In section 5 syntactical models are defined and shown to be sound and complete with respect to the proof systems. Section 6 then investigates some principles of the Basic Logic of Proofs, mainly concerning fixed points. And finally, in section 7 possible extensions of the Basic Logic of Proofs are discussed.

2 Soundness

In this section we prove soundness of the modal systems \mathcal{P} , \mathcal{PF} , \mathcal{PU} , \mathcal{PM} , \mathcal{PFM} and \mathcal{PUM} with respect to arithmetical interpretations.

2.1 Soundness without unification

In this subsection we deal with the logics that do not make use of the Unification Axiom.

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

$$\mathcal{P} \vdash A \quad \Longrightarrow \quad \begin{array}{l} \forall^* : \top \vdash A^*, \quad \text{and therefore} \\ \forall^* : A^* \text{ is true} \end{array}$$

Here, \forall^* quantifies arbitrary arithmetical interpretations.

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

(A1) and (R1) straightforward.

(A2) 1st case: $\top \vdash \text{Prf}(p^*, \ulcorner A^* \urcorner)$. It follows by definition 1.4 that $\top \vdash A^*$, hence $\top \vdash \text{Prf}(p^*, \ulcorner A^* \urcorner) \rightarrow A^*$.

2nd case: $\top \not\vdash \text{Prf}(p^*, \ulcorner A^* \urcorner)$. As $\text{Prf}(\cdot, \cdot)$ is recursive (definition 1.4), $\top \vdash \neg \text{Prf}(p^*, \ulcorner A^* \urcorner)$, thus $\top \vdash \text{Prf}(p^*, \ulcorner A^* \urcorner) \rightarrow A^*$.

■

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

$$\mathcal{PF} \vdash A \quad \Longrightarrow \quad \begin{array}{l} \forall^* : \top \vdash A^*, \quad \text{and therefore} \\ \forall^* : A^* \text{ is true} \end{array}$$

Here, \forall^* quantifies i-functional interpretations.

Proof In view of theorem 2.1 it remains to verify the soundness of the Functionality Axiom:

(A3') 1st case: $\top \vdash \text{Prf}(p^*, \ulcorner A^* \urcorner)$. As $\ulcorner A^* \urcorner \neq \ulcorner B^* \urcorner$ ($A \not\equiv B$) and by the functionality of the proof predicate (definition 1.4), $\top \vdash \neg \text{Prf}(p^*, \ulcorner B^* \urcorner)$, hence $\top \vdash \neg(\text{Prf}(p^*, \ulcorner A^* \urcorner) \wedge \text{Prf}(p^*, \ulcorner B^* \urcorner))$.

2nd case: $\top \not\vdash \text{Prf}(p^*, \ulcorner A^* \urcorner)$. Then $\top \vdash \neg \text{Prf}(p^*, \ulcorner A^* \urcorner)$, since $\text{Prf}(\cdot, \cdot)$ is recursive, thus $\top \vdash \neg(\text{Prf}(p^*, \ulcorner A^* \urcorner) \wedge \text{Prf}(p^*, \ulcorner B^* \urcorner))$.

■

2.3 Soundness of \mathcal{PM} Let A be a modal formula. Then

$$\mathcal{PM} \vdash A \quad \Longrightarrow \quad \begin{array}{l} \forall^* : \top \vdash A^*, \quad \text{and therefore} \\ \forall^* : A^* \text{ is true} \end{array}$$

Here, \forall^* quantifies monotonic interpretations.

Proof In view of theorem 2.1 it remains to verify the soundness of the Monotonicity Axiom:

(A4) Assume that \top does not prove

$$(\neg[\Box_{q_1} A_2(q_2) \wedge \Box_{q_2} A_3(q_3) \wedge \dots \wedge \Box_{q_n} A_1(q_1)])^*$$

It follows that the sentences

$$\begin{array}{l} Prf(q_1^*, \ulcorner(A_2(q_2))^*\urcorner), Prf(q_2^*, \ulcorner(A_3(q_3))^*\urcorner), \dots \\ \dots, Prf(q_n^*, \ulcorner(A_1(q_1))^*\urcorner) \end{array}$$

are true. $Prf(q_i^*, \ulcorner(A_j(q_j))^*\urcorner)$ implies by the monotonicity of the proof predicate (definition 1.4) that $q_i^* \geq \ulcorner(A_j(q_j))^*\urcorner$. By the convention on Gödel numbering (remark 1.3), and since 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

$$\begin{array}{l} q_1^* \geq \ulcorner(A_2(q_2))^*\urcorner > q_2^* \geq \ulcorner(A_3(q_3))^*\urcorner > \dots \\ \dots > q_n^* \geq \ulcorner(A_1(q_1))^*\urcorner > q_1^* \end{array}$$

which is a contradiction.

■

The soundness of \mathcal{PFM} follows from the three previous theorems.

2.2 Soundness with unification

The goal of this subsection is to investigate the close relationship between arithmetical interpretations and substitutions, and to prove the soundness of \mathcal{PU} with respect to arithmetical interpretations. We consider only \mathcal{PU} , the definitions and proofs for \mathcal{PUM} are analogous.

First, we make some modifications of the common unification technique to our language of labeled modalities. A well-written overview of this topic is [8], where the notations used in this text are taken from. Those readers who are familiar with substitutions, composition of substitutions, and most general unifiers, can go directly to definition 2.8.

2.4 Definition A *substitution* θ is a finite set of the form $\{T_1 \leftarrow A_1, \dots, T_n \leftarrow A_n, q_1 \leftarrow r_1, \dots, q_m \leftarrow r_m\}$, where the T_i are distinct sentence variables, the q_j are distinct proof variables, and each A_i is a modal formula different from T_i , and each r_j is a proof variable different from q_j . In the following an *expression* is a modal formula or a proof variable. If E is an expression, then we write $E\theta$ for the result of simultaneously replacing each occurrence of T_i in E by A_i and each occurrence of q_j in E by r_j for $i \leq n$ and $j \leq m$, respectively. If θ and θ' are substitutions, then obviously $\theta = \theta'$ iff $E\theta \equiv E\theta'$ for every expression E . The *composition* of substitutions $\theta = \{T_1 \leftarrow A_1, \dots, q_1 \leftarrow r_1, \dots\}$ and $\theta' = \{T'_1 \leftarrow A'_1, \dots, q'_1 \leftarrow r'_1, \dots\}$, denoted by $\theta \circ \theta'$ ($\theta\theta'$ for short) is the substitution obtained by removing elements of the form $T'_i \leftarrow A'_i$ where $T'_i \in \{T_1, \dots\}$ and $q'_j \leftarrow r'_j$ where $q'_j \in \{q_1, \dots\}$, and those of the form $T_i \leftarrow T_i$ and $q_j \leftarrow q_j$ from the set $\{T_1 \leftarrow A_1\theta', \dots, q_1 \leftarrow r_1\theta', \dots\} \cup \theta'$. Notice that composition is defined in such a way that $(E\theta)\sigma \equiv E(\theta\sigma)$ and $(\mu\theta)\sigma = \mu(\theta\sigma)$ for any expression E and substitutions μ, θ and σ .

2.5 Definition An *equation set* S is a (possibly empty) set $\{E_1 = E'_1, \dots, E_n = E'_n\}$ of equations of expressions. A substitution θ is called a *unifier* of S iff $E_1\theta \equiv E'_1\theta, \dots, E_n\theta \equiv E'_n\theta$. Two modal formulas A and B are called *unifiable* iff the equation set $\{A = B\}$ has a unifier. An equation set is in *solved form* if it is of the form $\{T_1 = A_1, \dots, T_n = A_n, q_1 = r_1, \dots, q_m = r_m\}$ where A_1, \dots, A_n are formulas, r_1, \dots, r_m are proof variables, and the T_1, \dots, T_n and q_1, \dots, q_m are distinct sentence and proof variables, respectively, which do not occur on the right hand side of any equation. Such an equation set in solved form defines the substitution $\{T_1 \leftarrow A_1, \dots, T_n \leftarrow A_n, q_1 \leftarrow r_1, \dots, q_m \leftarrow r_m\}$, which clearly is a unifier of the set. Equation sets are called *equivalent* if they have the same unifiers.

The following algorithm transforms any unifiable equation set S in an equivalent equation set, which is in solved form. For any equation set S that is not unifiable, the algorithm halts with failure.

2.6 Unification Algorithm Non-deterministically choose an equation from the equation set to which a numbered step applies:

1. $\neg A = \neg B$: replace by the equation $A = B$.
2. $(A_1 \wedge A_2) = (B_1 \wedge B_2)$: replace by the equations $A_1 = B_1$ and $A_2 = B_2$.

3. $\Box_p A = \Box_q B$: replace by the equations $p = q$ and $A = B$.
4. $p_i = p_i$ or $S_i = S_i$: delete the equation.
5. $A = B$ where A and B are both one of $\neg C$, $C \wedge D$ or $\Box_p C$ but have different principal connectives: halt with failure.
6. $A = S_i$ where A is not a sentence variable: replace by the equation $S_i = A$.
7. $S_i = A$ where A is not the sentence variable S_i and S_i has another occurrence in the set of equations: if S_i appears in A then halt with failure (occurs check) otherwise replace S_i by A in every other equation.
8. $p_i = p_j$ where $i \neq j$ and p_i has another occurrence in the set of equations: replace p_i by p_j in every other equation.

The algorithm terminates when no step can be applied or when failure has been returned.

2.7 Lemma

- (i) If the Unification Algorithm terminates by failure, then the equation set S has no unifier,
- (ii) If the Unification Algorithm does not terminate by failure, then it terminates with an equivalent equation set S' in solved form, and if θ is the substitution determined by S' then
 - (a) θ is a unifier of S ,
 - (b) θ is idempotent, i.e. $\theta\theta = \theta$,
 - (c) θ is the *most general unifier (mgu)* of S , i.e. if μ is another unifier of S then there exists a substitution λ with $\mu = \theta\lambda$.

Proof (cf. [8])

■

For convenience we fix some arbitrary but deterministic variant of the Unification Algorithm. Let $\tau_{A,B}$ be the mgu of A and B obtained by this deterministic algorithm starting with the equation set $\{A = B\}$.

2.8 Definition Let A, B, C, D be formulas. Then

$$C = D \pmod{A = B} \quad : \iff \quad \forall \theta : (A\theta \equiv B\theta \rightarrow C\theta \equiv D\theta)$$

Note that, if A, B are not unifiable then $C = D \pmod{A = B}$ holds for all C and B .

2.9 Lemma Let A, B, C, D be formulas such that A and B are unifiable. Then

$$C = D \pmod{A = B} \iff C_{\tau_{AB}} \equiv D_{\tau_{AB}}$$

Proof Let $C = D \pmod{A = B}$. Then $C_{\tau_{A,B}} \equiv D_{\tau_{A,B}}$ since $\tau_{A,B}$ unifies A and B . Conversely if $C_{\tau_{A,B}} \equiv D_{\tau_{A,B}}$ and θ is an arbitrary unifier A and B then for some substitution λ , $C\theta \equiv C_{\tau_{A,B}}\lambda \equiv D_{\tau_{A,B}}\lambda \equiv D\theta$. ■

2.10 Corollary The relation $C = D \pmod{A = B}$ is decidable. ■

2.11 Definition If $(\cdot)^* = (Prf(\cdot, \cdot), \phi)$ is an arithmetical interpretation and if θ is a substitution, then their composition $((\cdot)\theta)^*$ is defined to be the arithmetical interpretation $(Prf(\cdot, \cdot), \phi')$ where $\phi'(x) := \phi(x\theta)$.

Arithmetical interpretations and substitutions are compatible in the following sense:

2.12 Lemma Let $(\cdot)^*$ be an arithmetical interpretation and let θ be a substitution. If $(\cdot)^{**} := ((\cdot)\theta)^*$ then $D^{**} \equiv (D\theta)^*$ for all formulas D .

Proof Induction on the complexity of D :

- D is a sentence variable: By definition.
- $D = \neg A$: By the induction hypothesis $A^{**} \equiv (A\theta)^*$, so $(\neg A)^{**} \equiv \neg A^{**} \equiv \neg(A\theta)^* \equiv (\neg A\theta)^* \equiv ((\neg A)\theta)^*$.
- $D = A \wedge B$: By the induction hypothesis $A^{**} \equiv (A\theta)^*$ and $B^{**} \equiv (B\theta)^*$, hence $(A \wedge B)^{**} \equiv A^{**} \wedge B^{**} \equiv (A\theta)^* \wedge (B\theta)^* \equiv (A\theta \wedge B\theta)^* \equiv ((A \wedge B)\theta)^*$.
- $D = \Box_p A$: By the induction hypothesis $A^{**} \equiv (A\theta)^*$, therefore $(\Box_p A)^{**} \equiv Prf(p^{**}, \ulcorner A^{**} \urcorner) \equiv Prf((p\theta)^*, \ulcorner (A\theta)^* \urcorner) \equiv (\Box_{p\theta}(A\theta))^*$, which is the same as $((\Box_p A)\theta)^*$.

■

2.13 Theorem Let A be a formula. Then

$$\mathcal{P}\mathcal{U} \vdash A \quad \Longrightarrow \quad \mathcal{P}\mathcal{F} \vdash A$$

Proof It suffices to show that $\mathcal{P}\mathcal{F}$ proves the axioms (A3₁) and (A3₂):

(A3₁) If A and B are not unifiable, then they are not syntactically identical, thus $\mathcal{P}\mathcal{F} \vdash \neg(\Box_p A \wedge \Box_p B)$.

(A3₂) Let A and B be unifiable.

1st case: $A \equiv B$, thus $\tau_{A,B} = \varepsilon$, and so $F \equiv G$.

Trivially, $\mathcal{P}\mathcal{F} \vdash \Box_p A \wedge \Box_p A \wedge F \rightarrow F$.

2nd case: $A \not\equiv B$. We get $\mathcal{P}\mathcal{F} \vdash \neg(\Box_p A \wedge \Box_p B)$,

and so $\mathcal{P}\mathcal{F} \vdash \Box_p A \wedge \Box_p B \wedge F \rightarrow G$.

Of course, after the soundness and completeness results are established, this theorem is a direct consequence of the fact that the theorems of $\mathcal{P}\mathcal{F}$ are all those formulas which are true under functional interpretations that are injective, and the theorems of $\mathcal{P}\mathcal{U}$ are the formulas which are true under all functional interpretations.

■

2.14 Lemma Let A, B be modal formulas and let $(\cdot)^*$ be an arithmetical interpretation. If $A^* \equiv B^*$ then

(a) A and B are unifiable,

(b) $(\cdot)^* = ((\cdot)\tau_{A,B})^*$.

Proof Run the Unification Algorithm 2.6 starting with the equation set $\{A = B\}$ and observe that

– if the equation set S is reduced to S' in one step then

$$\bigwedge_{(E_1=E_2) \in S} E_1^* \equiv E_2^* \quad \text{iff} \quad \bigwedge_{(E_1=E_2) \in S'} E_1^* \equiv E_2^*,$$

(where E_1 and E_2 are expressions)

– if the algorithm terminates by failure with the equation set S then

$$\bigwedge_{(E_1=E_2) \in S} E_1^* \equiv E_2^* \quad \text{is false.}$$

It follows by induction that

- (i) if the algorithm terminates by failure then $A^* \not\equiv B^*$,
- (ii) if the algorithm terminates successfully then $A^* \equiv B^*$.

As (i) can not occur it follows that A and B are unifiable and for all sentence variables S_i and proof variables p_j :

$$\begin{aligned} S_i^* &\equiv (S_i\tau_{A,B})^* \\ p_j^* &\equiv (p_j\tau_{A,B})^* \end{aligned}$$

Finally, it follows by lemma 2.12 that $E^* \equiv (E\tau_{A,B})^*$ for an arbitrary expressions E .

■

2.15 Lemma Let A, B be formulas and σ a substitution such that $A\sigma \equiv B\sigma$. Then there exists an interpretation $(\cdot)^*$ such that $A^* \equiv B^*$.

Proof Let the interpretation $(\cdot)^{**}$ be defined as $S_i^{**} := \forall x_i(x_i = x_i)$, and $p_i^{**} := i$. Then $(\cdot)^*$ defined as $S_i^* := (S_i\sigma)^{**}$, $p_i^* := (p_i\sigma)^{**}$, and using the same proof predicate as $(\cdot)^{**}$, has the desired property, which follows from lemma 2.12. Notice that $(\cdot)^*$ is defined independently of A and B , and that $(\cdot)^{**}$ is injective, hence for for arbitrary formulas F and G , $F\sigma \equiv G\sigma$ iff $(F\sigma)^{**} \equiv (G\sigma)^{**}$ iff $F^* \equiv G^*$.

■

The previous lemmas disclose a major difference between “i-functional interpretations and syntactical identity” where we have

$$\forall^* : A^* \equiv B^* \iff A, B \text{ are identical}$$

and “functional interpretations and unifiability” where we have

$$\exists^* : A^* \equiv B^* \iff A, B \text{ are unifiable}$$

2.16 Soundness of \mathcal{PU} Let A be a modal formula. Then

$$\mathcal{PU} \vdash A \implies \begin{aligned} \forall^* : \top \vdash A^*, \quad \text{and therefore} \\ \forall^* : A^* \text{ is true} \end{aligned}$$

Here, \forall^* quantifies functional interpretations.

The soundness of \mathcal{PUM} is proved in a similar way, using theorem 2.3.

Proof It remains to show that (A3₁) and (A3₂) are sound, so let $(\cdot)^*$ be a functional interpretation.

(A3₁) As A and B are not unifiable, it follows by lemma 2.14 that $A^* \not\equiv B^*$, so by the functionality of $Prf(\cdot, \cdot)$, $Prf(p^*, \ulcorner A^* \urcorner) \wedge Prf(p^*, \ulcorner B^* \urcorner)$ is false, hence, as this formula is recursive, $\top \vdash \neg(Prf(p^*, \ulcorner A^* \urcorner) \wedge Prf(p^*, \ulcorner B^* \urcorner))$.

(A3₂) 1st case: $\top \vdash Prf(p^*, \ulcorner A^* \urcorner) \wedge Prf(p^*, \ulcorner B^* \urcorner)$. By the functionality $A^* \equiv B^*$, thus by lemma 2.14 A and B are unifiable and $F^* \equiv (F_{\tau_{A,B}})^* \equiv (G_{\tau_{A,B}})^* \equiv G^*$. So $\top \vdash F^* \leftrightarrow G^*$, and finally $\top \vdash Prf(p^*, \ulcorner A^* \urcorner) \wedge Prf(p^*, \ulcorner B^* \urcorner) \wedge F^* \rightarrow G^*$.

2nd case: $\top \not\vdash Prf(p^*, \ulcorner A^* \urcorner) \wedge Prf(p^*, \ulcorner B^* \urcorner)$. As $Prf(\cdot, \cdot)$ is recursive, $\top \vdash \neg(Prf(p^*, \ulcorner A^* \urcorner) \wedge Prf(p^*, \ulcorner B^* \urcorner))$, so again we get $\top \vdash Prf(p^*, \ulcorner A^* \urcorner) \wedge Prf(p^*, \ulcorner B^* \urcorner) \wedge F^* \rightarrow G^*$.

■

3 Completeness

The main aim of this section is to prove the arithmetical completeness of our logics (i.e. the converse of theorems 2.1, 2.2, 2.3 and 2.16). In the following subsection 3.1 the sequential versions $\mathcal{P}_{\mathcal{G}}$, $\mathcal{PF}_{\mathcal{G}}$, $\mathcal{PU}_{\mathcal{G}}$, $\mathcal{PM}_{\mathcal{G}}$, $\mathcal{PFM}_{\mathcal{G}}$ and $\mathcal{PUM}_{\mathcal{G}}$ (the \mathcal{G} stands for Gentzen) of our logics are presented. In subsection 3.2 it is shown that these logics are sound w.r.t. their Hilbert style versions, and in subsection 3.3 these logics are analyzed in a structural way (Saturation Lemma). Subsections 3.4 – 3.7 then deal with the arithmetical part of the completeness proof by constructing arithmetical interpretations (countermodels).

The proofs for all systems go along the lines of the following diagram (here for \mathcal{P}):

$$\begin{array}{ccc}
 \forall^* : (\bigwedge \Gamma \rightarrow \bigvee \Delta)^* \text{ is true} & \stackrel{(1)}{\longleftarrow} & \forall^* : \top \vdash (\bigwedge \Gamma \rightarrow \bigvee \Delta)^* \\
 \begin{array}{c} \Downarrow \\ (2) \end{array} & & \begin{array}{c} \Uparrow \\ (5) \end{array} \\
 \mathcal{P}_{\mathcal{G}}^- \vdash \Gamma \supset \Delta & \stackrel{(3)}{\implies} & \mathcal{P}_{\mathcal{G}} \vdash \Gamma \supset \Delta & \stackrel{(4)}{\implies} & \mathcal{P} \vdash \bigwedge \Gamma \rightarrow \bigvee \Delta
 \end{array}$$

Here $\mathcal{P}_{\mathcal{G}}^-$ denotes the Gentzen style system $\mathcal{P}_{\mathcal{G}}$ without the cut-rule. Now, (1) is valid by the consistency of \top , (3) holds by definition, and (5) is the main result of the previous section. What remains to show are (4) in subsection 3.2, and (2) in subsection 3.4 for \mathcal{P} , in subsection 3.5 for \mathcal{PF} , in subsection 3.6 for \mathcal{PU} , and in subsection 3.7 for the logics containing the Monotonicity Axiom.

As an immediate consequence of the relations shown in the diagram we get the soundness and completeness of the proof systems with respect to arithmetical interpretations:

3.1 Main Theorem for \mathcal{P} , \mathcal{PF} , \mathcal{PU} , \mathcal{PM} , \mathcal{PFM} and \mathcal{PUM}

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

$$\begin{array}{ccc}
 \mathcal{P} \vdash A & \iff & \forall^* : \top \vdash A^* & \text{and moreover} \\
 & & \forall^* : A^* \text{ is true} &
 \end{array}$$

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

And in consequence of the cut elimination theorem,

- \mathcal{P} is decidable.

The same is true for \mathcal{PF} , \mathcal{PU} , \mathcal{PM} , \mathcal{PFM} and \mathcal{PUM} , as well.

3.1 Gentzen style systems

In the following, a *sequent* is a formal expression $\Gamma \supset \Delta$, where Γ and Δ are finite sets of modal formulas. If $\Gamma = A_1, \dots, A_k$, then $\bigwedge \Gamma := A_1 \wedge \dots \wedge A_k$, and if $\Delta = B_1, \dots, B_l$, then $\bigvee \Delta := B_1 \vee \dots \vee B_l$.

3.2 Definition \mathcal{P}_G , \mathcal{PF}_G , \mathcal{PU}_G , \mathcal{PM}_G , \mathcal{PFM}_G and \mathcal{PUM}_G are the sequent calculi with axioms and rules of inference as follows:

- Sequent calculus for classical propositional logic including the cut-rule. }
- $\frac{A, \Gamma \supset \Delta}{\Box_p A, \Gamma \supset \Delta} \text{I}\Box$ } \mathcal{P}
- $\Box_p A, \Box_p B \supset$ (A, B not unifiable) }
- $\frac{(\Box_p A, \Gamma \supset \Delta)\tau_{A,B}}{\Box_p A, \Box_p B, \Gamma \supset \Delta} \tau_{A,B}$ (A, B unifiable) } \mathcal{U}
- $\Box_p A, \Box_p B \supset$ ($A \neq B$) } \mathcal{F}
- $\Box_{q_1} A_2(q_2), \Box_{q_2} A_3(q_3), \dots, \Box_{q_n} A_1(q_1) \supset$ } \mathcal{M}

As usual, $A_i(q_i)$ is a formula in which q_i occurs, and the scheme \mathcal{M} includes the axiom $\Box_{q_1} A_1(q_1) \supset$. Again, $\tau_{A,B}$ is an idempotent most general unifier of A and B which is obtained by a fixed but arbitrary unification algorithm (e.g. algorithm 2.6). We call the new rule in \mathcal{P} the *Reflexivity Rule*, \mathcal{U} the *Unification Axiom* and the *Unification Rule*, \mathcal{F} the *Functionality Axiom* and \mathcal{M} the *Monotonicity Axiom*.

\mathcal{P}_G^- is the system \mathcal{P}_G without the cut rule; we use analogous definitions for \mathcal{PF}_G^- , \mathcal{PU}_G^- , \mathcal{PM}_G^- , \mathcal{PFM}_G^- and \mathcal{PUM}_G^- .

3.3 Example The following is a \mathcal{PU}_G^- -proof of $\neg \Box_p \Box_p \top$ for some

proof variable p , starting with an instance of the Unification Axiom:

$$\frac{\frac{\frac{\Box_p \top, \Box_p \Box_p \top \supset}{\Box_p \Box_p \top, \Box_p \Box_p \top \supset} l\Box}{\Box_p \Box_p \top \supset} lC}{\supset \neg \Box_p \Box_p \top} r\neg$$

3.2 Soundness w.r.t. Hilbert style systems

3.4 Soundness of \mathcal{P}_G , \mathcal{PF}_G , \mathcal{PM}_G and \mathcal{PFM}_G For each sequent $\Gamma \supset \Delta$:

$$\mathcal{P}_G \vdash \Gamma \supset \Delta \quad \Longrightarrow \quad \mathcal{P} \vdash \bigwedge \Gamma \rightarrow \bigvee \Delta$$

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

Proof Straightforward induction on the length of the proof of $\Gamma \supset \Delta$. ■

3.5 Soundness of \mathcal{PU}_G and \mathcal{PUM}_G For each sequent $\Gamma \supset \Delta$:

$$\mathcal{PU}_G \vdash \Gamma \supset \Delta \quad \Longrightarrow \quad \mathcal{PU} \vdash \bigwedge \Gamma \rightarrow \bigvee \Delta$$

The same holds for \mathcal{PUM}_G and \mathcal{PUM} .

Proof Using remark 1.10 it remains to show that the Unification Rule is sound with respect to \mathcal{PU} : Let $\mathcal{PU} \vdash (\Box_p A \wedge \bigwedge \Gamma \rightarrow \bigvee \Delta)_{\tau_{A,B}}$. As $\tau_{A,B}$ is idempotent (lemma 2.7), $(\Box_p A \wedge \Box_p B \wedge \bigwedge \Gamma \rightarrow \bigvee \Delta)_{\tau_{A,B}\tau_{A,B}}$ and $(\Box_p A \wedge \Box_p B \wedge \bigwedge \Gamma \rightarrow \bigvee \Delta)_{\tau_{A,B}}$ are identical, so

$$\Box_p A \wedge \Box_p B \wedge (\Box_p A \wedge \Box_p B \wedge \bigwedge \Gamma \rightarrow \bigvee \Delta)_{\tau_{A,B}} \longrightarrow (\Box_p A \wedge \Box_p B \wedge \bigwedge \Gamma \rightarrow \bigvee \Delta)$$

is an instance of (A3₂). As a consequence we get

$$\mathcal{PU} \vdash \Box_p A \wedge \Box_p B \longrightarrow (\Box_p A \wedge \Box_p B \wedge \bigwedge \Gamma \rightarrow \bigvee \Delta)$$

which is equivalent to

$$\mathcal{PU} \vdash \Box_p A \wedge \Box_p B \wedge \bigwedge \Gamma \rightarrow \bigvee \Delta$$

■

3.3 Saturations

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

1. $\neg A \in \Gamma$ implies $A \in \Delta$,
2. $\neg A \in \Delta$ implies $A \in \Gamma$,
3. $A \wedge B \in \Gamma$ implies $A \in \Gamma$ and $B \in \Gamma$,
4. $A \wedge B \in \Delta$ implies $A \in \Delta$ or $B \in \Delta$,
5. $\Box_p A \in \Gamma$ implies $A \in \Gamma$.

3.7 Saturation Lemma for $\mathcal{P}_G, \mathcal{PF}_G, \mathcal{PM}_G$ and \mathcal{PFM}_G Let $\Gamma \supset \Delta$ be a sequent such that $\mathcal{P}_G^- \not\vdash \Gamma \supset \Delta$. 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) $\mathcal{P}_G^- \not\vdash \Gamma' \supset \Delta'$.

The same holds for $\mathcal{PF}_G, \mathcal{PM}_G$ and \mathcal{PFM}_G in place of \mathcal{P}_G , too. 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 provable, otherwise the algorithm fails.

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

- if $S = \neg A \in \Gamma$ and $A \notin \Delta$, then $\Delta := \Delta \cup \{A\}$.
- if $S = \neg A \in \Delta$ and $A \notin \Gamma$, then $\Gamma := \Gamma \cup \{A\}$.
- if $S = A \wedge B \in \Gamma$ and $A \notin \Gamma$ or $B \notin \Gamma$, then $\Gamma := \Gamma \cup \{A, B\}$.

- if $S = A \wedge B \in \Delta$ and $A \notin \Delta$ and $B \notin \Delta$, then $\Delta := \Delta \cup \{A\}$ and branch, or $\Delta := \Delta \cup \{B\}$ and branch.
- if $S = \Box_p A \in \Gamma$ and $A \notin \Gamma$, then $\Gamma := \Gamma \cup \{A\}$.
- if $\Gamma \supset \Delta$ is a propositional axiom (i.e. if $\Gamma \cap \Delta \neq \emptyset$), then backtrack.

In the case of \mathcal{PF} and \mathcal{PFM} :

- if $\Gamma \supset \Delta$ is an instance of the Functionality Axiom (i.e. if there are formulas $\Box_p A, \Box_p B \in \Gamma$ and $A \neq B$), then backtrack.

In the case of \mathcal{PM} and \mathcal{PFM} :

- if $\Gamma \supset \Delta$ is an instance of the Monotonicity Axiom (i.e. if there are formulas $\Box_{q_1} A_2(q_2), \Box_{q_2} A_3(q_3), \dots, \Box_{q_n} A_1(q_1) \in \Gamma$, where in $A_i(q_i)$ the proof variable q_i occurs), 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.
- If the algorithm fails then each branch in the computation contains an axiom, and so one can readily construct a proof of $\Gamma \supset \Delta$.
- If the algorithm succeeds then the resulting sequent $\Gamma' \supset \Delta'$ is saturated and not provable. Otherwise, assume that $\Gamma' \supset \Delta'$ is provable and thus, as it is saturated, an axiom. Starting with $\Gamma' \supset \Delta'$, and according to the saturation process, construct a proof of $\Gamma \supset \Delta$.

■

3.9 Saturation Lemma for \mathcal{PU}_G and \mathcal{PUM}_G Let $\Gamma \supset \Delta$ be a sequent such that $\mathcal{PU}_G^- \not\vdash \Gamma \supset \Delta$. Then there exists a saturated sequent $\Gamma' \supset \Delta'$ and a substitution σ , such that

- (i) $\Gamma\sigma \subset \Gamma', \Delta\sigma \subset \Delta'$,
- (ii) $\mathcal{PF}_G^- \not\vdash \Gamma' \supset \Delta'$.

The same holds for $\mathcal{PUM}_{\mathcal{G}}$ and $\mathcal{PFM}_{\mathcal{G}}$, respectively. Furthermore $\Gamma' \supset \Delta'$ is effectively computable from $\Gamma \supset \Delta$.

Proof The Saturation Algorithms for $\mathcal{PU}_{\mathcal{G}}$ and $\mathcal{PUM}_{\mathcal{G}}$ work similarly to that for $\mathcal{PF}_{\mathcal{G}}$ and $\mathcal{PFM}_{\mathcal{G}}$, the only new steps that have to be added are:

- if $\Box_p A, \Box_p B \in \Gamma$ and A, B are not unifiable, then backtrack.
- if $\Box_p A, \Box_p B \in \Gamma$ ($A \not\equiv B$) and A, B are unifiable, then apply $\tau_{A,B}$ to $\Gamma \supset \Delta$.

Additional properties of the Saturation Algorithm for $\mathcal{PU}_{\mathcal{G}}$ and $\mathcal{PUM}_{\mathcal{G}}$:

- Termination: Each substitution τ_{A_i, B_i} replaces at least one proof or sentence variable, therefore there are only finitely many substitutions possible during the algorithm. After each substitution there are only finitely many other saturation steps possible, too.
- If $\tau_{A_1, B_1}, \dots, \tau_{A_k, B_k}$ are the substitutions applied during the saturation algorithm (in that order), then let $\sigma := \tau_{A_1, B_1} \circ \tau_{A_2, B_2} \circ \dots \circ \tau_{A_k, B_k}$. As each substitution τ_{A_i, B_i} is applied to the whole sequent, clearly $\Gamma\sigma \subset \Gamma'$ and $\Delta\sigma \subset \Delta'$.
- $\mathcal{PF}_{\mathcal{G}}^- \not\vdash \Gamma' \supset \Delta'$: Apply the Saturation Algorithm 3.8 for $\mathcal{PF}_{\mathcal{G}}$ to $\Gamma' \supset \Delta'$. The algorithm succeeds immediately since $\Gamma' \supset \Delta'$ is already saturated: It is not possible that $\Box_p A, \Box_p B \in \Gamma'$ with $A \not\equiv B$ as both cases (A, B unifiable, and A, B not unifiable) are treated by the Saturation Algorithm for $\mathcal{PU}_{\mathcal{G}}$. Hence $\Gamma' \supset \Delta'$ is not $\mathcal{PF}_{\mathcal{G}}^-$ -provable.

■

3.4 The general case

In this subsection, $(\cdot)^*$ denotes an arbitrary arithmetical interpretation.

3.10 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.

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

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.

We 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) we define a predicate $Prf(\cdot, \cdot)$ – and this $Prf(\cdot, \cdot)$ completes the interpretation $(\cdot)^*$ – which solves the following fixed point equation:
 \top proves

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

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 \top .

Our first task is to show that $Prf(\cdot, \cdot)$ can be constructed in this way. Let the formula F be defined as

$$F(x, y, z_{0,0}, z_{0,1}, \dots, z_{m,J_m}) \iff \forall r \leq x \left[\right.$$

the proof is completed by the observation that $Prf(\cdot, \cdot)$ really is a proof predicate.

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

$$\begin{aligned} D^* \text{ is true} &\iff \top \vdash D^* \\ D^* \text{ is false} &\iff \top \vdash \neg D^* \end{aligned}$$

By induction on the complexity of D it follows that:

$$\begin{aligned} D \in \Gamma' &\implies D^* \text{ is true} \\ D \in \Delta' &\implies D^* \text{ is false} \end{aligned}$$

- $D = S_j \in \Gamma'$: $D^* = \forall x_i(x_i = x_i)$ is true.
- $D = S_j \in \Delta'$: $D^* = \forall x_i(x_i \neq x_i)$ is false.
- $D = \neg A \in \Gamma'$: As $\Gamma' \supset \Delta'$ is saturated, $A \in \Delta'$. By the induction hypothesis A^* is false, hence $(\neg A)^*$ is true.
- $D = \neg A \in \Delta'$: As $\Gamma' \supset \Delta'$ is saturated, $A \in \Gamma'$. By the induction hypothesis A^* is true, hence $(\neg A)^*$ is false.
- $D = (A \wedge B) \in \Gamma'$: As $\Gamma' \supset \Delta'$ is saturated, $A \in \Gamma'$ and $B \in \Gamma'$. By the induction hypothesis both A^* and B^* are true, hence $(A \wedge B)^*$ is true.
- $D = (A \wedge B) \in \Delta'$: As $\Gamma' \supset \Delta'$ is saturated, $A \in \Delta'$ or $B \in \Delta'$. By the induction hypothesis A^* is false or B^* is false, hence $(A \wedge B)^*$ is false.
- $D = \Box_{p_i} A_{i,j} \in \Gamma'$: $(\Box_{p_i} A_{i,j})^* = Prf(2i, \ulcorner A_{i,j} \urcorner)$ 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 since there exists no modal formula C such that $\ulcorner C \urcorner = \ulcorner \forall x_0 \forall x_0 (x_0 = x_0) \urcorner$.

It remains to show that $Prf(\cdot, \cdot)$ can be used as a proof predicate in \top :

$$\top \vdash \varphi \iff \exists n \in \mathbb{N} : Prf(n, \ulcorner \varphi \urcorner) \text{ is true}$$

Let $\mathbb{T} \vdash \varphi$. 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, thus by the fixed point equation

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

Conversely, if $Prf(n_0, \ulcorner \varphi \urcorner)$ is true for some $n_0 \in \mathbb{N}$, we consider the following 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 $\mathbb{T} \vdash \varphi$.

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 \mathbb{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 $\mathbb{T} \vdash \varphi$.

So $Prf(\cdot, \cdot)$ is a proof predicate for \mathbb{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.

$$\mathbb{T} \vdash \neg(\bigwedge \Gamma \rightarrow \bigvee \Delta)^*$$

■

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

$$\forall^* : (\bigwedge \Gamma \rightarrow \bigvee \Delta)^* \text{ is true} \quad \implies \quad \mathcal{P}_{\mathcal{G}}^- \vdash \Gamma \supset \Delta$$

Proof Assume that $\mathcal{P}_{\mathcal{G}}^- \not\vdash \Gamma \supset \Delta$. By the Saturation Lemma 3.8 there exists a saturated sequent $\Gamma' \supset \Delta'$ which is not $\mathcal{P}_{\mathcal{G}}^-$ -provable. Hence by the Main Lemma 3.10 for \mathcal{P} there exists an arithmetical interpretation $(\cdot)^*$ which makes $\bigwedge \Gamma' \rightarrow \bigvee \Delta'$ false. But as $\Gamma \subset \Gamma'$ and $\Delta \subset \Delta'$, this interpretation falsifies also $\bigwedge \Gamma \rightarrow \bigvee \Delta$.

■

So the last gap in the diagram at the beginning of this subsection has been filled, and thereby all claims of the Main Theorem 3.1 for \mathcal{P} are proved. For the decidability of a formula A , apply the saturation algorithm 3.8 for \mathcal{P} 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.

Notice that the Reflexivity Rule cannot be replaced by the logically equivalent axiom $\Box_p A \supset A$ while preserving the cut-elimination theorem. It would not be possible to eliminate the cut in the following proof:

$$\frac{\Box_p \Box_p A \supset \Box_p A \quad \Box_p A \supset A}{\Box_p \Box_p A \supset A} \text{cut}$$

3.5 Completeness with i-functionality

This subsection is devoted to the modal system \mathcal{PF} which corresponds to i-functional arithmetical interpretations. In this subsection, $(\cdot)^*$ always denotes such an interpretation. The proofs go along the lines of the previous subsection on the basic system \mathcal{P} .

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

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

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 saturation and non-provability of $\Gamma' \supset \Delta'$, there exists no proof variable p such that both $\Box_p A$ and $\Box_p B$ are contained in Γ' for distinct formulas A and B .

The fixed point equation for $Prf(\cdot, \cdot)$ is a special case of that for \mathcal{P} : \top proves

$$Prf(u, v) \iff \forall r \leq u \left[\begin{array}{l} u = 2r + 1 \rightarrow \widetilde{Prf}(r, v) \quad \wedge \\ u = 2r \rightarrow \left[\begin{array}{l} r = 0 \rightarrow v = \ulcorner A_0 \urcorner \quad \wedge \\ \vdots \\ r = m \rightarrow v = \ulcorner A_m \urcorner \quad \wedge \\ r > m \rightarrow v = \ulcorner \forall x_0 \forall x_0 (x_0 = x_0) \urcorner \end{array} \right] \end{array} \right]$$

Obviously, $Prf(\cdot, \cdot)$ 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

$$\top \vdash \neg(\bigwedge \Gamma \rightarrow \bigvee \Delta)^*$$

■

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

$$\forall^* : (\bigwedge \Gamma \rightarrow \bigvee \Delta)^* \text{ is true} \iff \mathcal{PF}_G^- \vdash \Gamma \supset \Delta$$

■

So we have proved the Main Theorem 3.1 for \mathcal{PF} . For the decidability of a formula A , again, $\mathcal{PF} \vdash A$ iff the Saturation Algorithm 3.8 for \mathcal{PF} fails to find a saturation of $\supset A$.

3.6 Completeness with unification

The goal of this subsection is to show that \mathcal{PU} is complete with respect to functional arithmetical interpretations that are not necessarily injective. The proof is based on the Main Lemma 3.12 for \mathcal{PF} . Up to the end of this subsection, $(\cdot)^*$ denotes a functional interpretation.

3.14 Main Lemma for \mathcal{PU} Let $\Gamma \supset \Delta$ be a sequent. Then

$$\forall^* : (\bigwedge \Gamma \rightarrow \bigvee \Delta)^* \text{ is true} \quad \Longrightarrow \quad \mathcal{PU}_{\mathcal{G}}^- \vdash \Gamma \supset \Delta$$

Proof Let $\mathcal{PU}_{\mathcal{G}}^- \not\vdash \Gamma \supset \Delta$. According to the Saturation Lemma 3.9 for $\mathcal{PU}_{\mathcal{G}}$ there exists a saturated sequent $\Gamma' \supset \Delta'$ which is not $\mathcal{PF}_{\mathcal{G}}^-$ -provable, and a substitution σ such that $\Gamma\sigma \subset \Gamma'$ and $\Delta\sigma \subset \Delta'$ (i.e. if $D \in \Gamma$ then $D\sigma \in \Gamma'$, and if $D \in \Delta$ then $D\sigma \in \Delta'$).

From the Main Lemma 3.12 for \mathcal{PF} it follows that there exists an injective interpretation $(\cdot)^*$ such that:

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

Let $(\cdot)^{**} := ((\cdot)\sigma)^*$. Notice that $(\cdot)^{**}$ is not necessarily injective. Now if $D \in \Gamma$ then $D^{**} \equiv (D\sigma)^*$ is true since $D\sigma \in \Gamma'$, and if $D \in \Delta$ then $D^{**} \equiv (D\sigma)^*$ is false since $D\sigma \in \Delta'$. Therefore $(\bigwedge \Gamma \rightarrow \bigvee \Delta)^{**}$ is false, and again it is clear that even $\top \vdash \neg(\bigwedge \Gamma \rightarrow \bigvee \Delta)^{**}$.
■

The following theorem is another consequence of the Completeness Theorem and the Saturation Lemma for $\mathcal{PU}_{\mathcal{G}}$:

3.15 Theorem Let A be a formula, then:

$$\mathcal{PU} \vdash A \quad \Longleftrightarrow \quad \forall \sigma : \mathcal{PF} \vdash A\sigma$$

Proof Let $\mathcal{PU} \vdash A$ and let σ be a substitution. Consider $(\cdot)^{**} := ((\cdot)\sigma)^*$ where $(\cdot)^*$ is an arbitrary arithmetical interpretation. From $\mathcal{PU} \vdash A$ it follows that A^{**} thus $(A\sigma)^*$ is true for each interpretation $(\cdot)^*$. As \mathcal{PU} is arithmetically complete it follows $\mathcal{PU} \vdash A\sigma$, and so by theorem 2.13, $\mathcal{PF} \vdash A\sigma$. Conversely, if $\mathcal{PU} \not\vdash A$ then $\mathcal{PU}_{\mathcal{G}}^- \not\vdash A$, and therefore by the Saturation Lemma 3.9 for $\mathcal{PU}_{\mathcal{G}}$ there exists a sequent $\Gamma' \supset \Delta'$ with $\mathcal{PF}_{\mathcal{G}}^- \not\vdash \Gamma' \supset \Delta'$ and a substitution σ such that $A\sigma \in \Delta'$. By weakening $\mathcal{PF}_{\mathcal{G}}^- \not\vdash A\sigma$, thereby $\mathcal{PF} \not\vdash A\sigma$.
■

Notice that $\forall \sigma : \mathcal{PF} \vdash A\sigma$ is not equivalent to $\mathcal{PF} \vdash A$ since \mathcal{PF} is not closed under substitutions:

$$\mathcal{PF} \vdash \neg(\Box_p S_0 \wedge \Box_p S_1),$$

but

$$\mathcal{PF} \not\vdash \neg(\Box_p \top \wedge \Box_p \top).$$

So the theorems of \mathcal{PU} are exactly the theorems of \mathcal{PF} for which the substitution property holds.

But also the system \mathcal{PU} has a peculiarity: the subformula property does not hold for it. The formula $\Box_q \top$ in the following proof is such an example:

$$\frac{\Box_p \top, \Box_q \top \supset \Box_q \top}{\Box_p S_0, \Box_p \top, \Box_q S_0 \supset \Box_q S_0} \{S_0 \leftarrow \top\}$$

3.7 Completeness with monotonicity

In this subsection we first prove the Main Lemma for $\mathcal{PFM}/\mathcal{PUM}$ and then for \mathcal{PM} . As a further consequence of the completeness proofs we get that for $\mathcal{PFM}/\mathcal{PUM}$ an arbitrary functional and monotonic proof predicate can be fixed, and $\mathcal{PFM}/\mathcal{PUM}$ 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. The same is true for \mathcal{PM} and a special monotonic proof predicate, which is based on the nonfunctional Gödel proof predicate. So \mathcal{PM} and $\mathcal{PFM}/\mathcal{PUM}$ are not only some other specializations in the studies of proof predicates, but they differ in a fundamental property from \mathcal{P} , \mathcal{PF} and \mathcal{PU} .

We prove completeness only for \mathcal{PFM} and not for \mathcal{PUM} .

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

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

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} , \mathcal{PF} and \mathcal{PU} : The \Box is interpreted independently from $\Gamma' \supset \Delta'$ as a fixed functional and monotonic proof predicate. On the contrary, the proof variables cannot be interpreted in a fixed way any more as section 4 about uniformity 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:

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

This relation is a strict, well-founded ordering on the proof variables:

It is irreflexive, since if $\Box_{q_1} A_2(q_2), \dots, \Box_{q_{n-1}} A_1(q_1) \in \Gamma'$, then $\mathcal{PFM}_{\bar{g}} \vdash \Gamma' \supset \Delta'$. 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:

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

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 formulas A occurring in $\Gamma' \cup \Delta'$:

$$s(A) := \begin{cases} 0, & \text{if no proof variable occurs in } A, \\ \max\{s(p) \mid p \text{ is a proof variable which occurs in } A\}, & \text{else.} \end{cases}$$

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:

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

So the interpretation of a modal formula is recursive. As mentioned before, the \Box is interpreted as an arbitrary functional and monotonic proof predicate, for example the Gödel one:

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

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

- (i) we define D^* , i.e. we fix the interpretation for all proof variables occurring in D ,
- (ii) we prove that D has the following property:

$$\begin{aligned} D \in \Gamma' &\implies D^* \text{ is true} \\ D \in \Delta' &\implies D^* \text{ is false} \end{aligned}$$

If D is a sentence variable or a boolean combination of formulas then (i) and (ii) are proved by straightforward induction on the complexity of D , using that $\Gamma' \supset \Delta'$ is saturated and not an axiom.

induction base: $s(D) = 0$, so D is \Box -free and D^* is independent from the interpretation of the proof variables, thus 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 not provable hence not an axiom, 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 $\top \vdash A^*$. Let p_i^* be the Gödel number of a proof of A^* in \top . 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, since $\widetilde{Prf}(\cdot, \cdot)$ is functional (lemma 1.5) 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 \top . So $(\Box_{p_i} A)^* = \widetilde{Prf}(p_i^*, \ulcorner A^* \urcorner)$ is defined and false, as $\widetilde{Prf}(\cdot, \cdot)$ is functional (lemma 1.5) 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 we have shown that for every modal formula D contained in $\Gamma' \cup \Delta'$, if $D \in \Gamma'$ then D^* is true, and if $D \in \Delta'$ then D^* is false. Therefore $(\bigwedge \Gamma' \rightarrow \bigvee \Delta')^*$ is a false recursive formula and thus not provable in \top .

■

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

and monotonic one. So additionally to the Main Theorem 3.1 for \mathcal{PFM} we have proved the following uniformity result:

3.17 Theorem Let $\widehat{Prf}(\cdot, \cdot)$ be a functional and monotonic proof predicate. Then for every formula A :

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

The same also holds for \mathcal{PUM} , if $(\cdot)^*$ is not required to be injective.

The last goal in this subsection (and section) is to prove completeness for \mathcal{PM} , too. The proof is very similar to that for \mathcal{PFM} , but we have to solve a problem related to the following observation: The language of labeled modalities under the interpretation of $\Box_p A$ as “ p is a proof containing A ” is powerful enough to express certain details of proofs in \mathbb{T} . For example the formula $\Box_p(A \wedge A) \rightarrow \Box_p A$ states under non-functional interpretations that each proof of $A \wedge A$ contains a proof of A . Even though there exist particular axiom systems for \mathbb{T} for which this principle is valid, it is in general not true. So for the completeness proof for \mathcal{PM} we have to consider proof predicates, which have no such special properties. In [4] it is demonstrated that for this purpose it is possible to use an ordinary Hilbert style proof system in \mathbb{T} , provided that we make some weak assumptions. In this text we suggest a more general solution for this problem, without having to be concerned with the structure of proofs in \mathbb{T} .

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

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

Proof The proof is essentially the same as the proof of the Main Lemma 3.16 for \mathcal{PFM} . The only difference is that due to the lack of functionality, Γ' may contain several distinct formulas $\Box_p A_1, \dots, \Box_p A_m$. So p^* must be chosen to be the Gödel number of a proof which contains A_1^*, \dots, A_m^* but no B^* if $\Box_p B \in \Delta'$. Again, define

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

3.19 Lemma Let $\varphi_1, \dots, \varphi_m$ be provable in \mathbb{T} . Then there exist a monotonic proof predicate $Prf(\cdot, \cdot)$ and infinitely many (Gödel number of) proofs, such that for each (Gödel number of a) proof n :

- $Prf(n, \ulcorner \varphi_i \urcorner)$ is true for each φ_i ($1 \leq i \leq m$).
- $Prf(n, \ulcorner A^* \urcorner)$ is false for each modal formula A and interpretation $(\cdot)^*$ based on $Prf(\cdot, \cdot)$, such that $A^* \not\equiv \varphi_i$ ($1 \leq i \leq m$).

Proof Let $\langle x_1, \dots, x_k \rangle$ and $(x)_y$ be primitive recursive terms for pairing (for an arbitrary number of arguments) and projection. Remind that $\overline{Prf}(\cdot, \cdot)$ is the nonfunctional Gödel proof predicate (definition 1.5), and let $n \in \mathbb{N}$ be such that $\overline{Prf}(n, \ulcorner \varphi_1 \urcorner), \dots, \overline{Prf}(n, \ulcorner \varphi_m \urcorner)$ hold. Clearly, there exist infinitely many such numbers n .

We regard now $\langle n, m, \langle \ulcorner \varphi_1 \urcorner, \dots, \ulcorner \varphi_m \urcorner \rangle \rangle$ as a proof for $\varphi_1, \dots, \varphi_m$ (and only for $\varphi_1, \dots, \varphi_m$), by defining the recursive predicate $Prf(\cdot, \cdot)$ as

$$Prf(x, y) := \exists n', m', c' < x \left[\begin{array}{l} n' = (x)_1 \wedge m' = (x)_2 \wedge c' = (x)_3 \wedge \\ \overline{Prf}(n', y) \wedge \\ \exists i \leq m' : y = (c')_i \end{array} \right]$$

Obviously, $Prf(\cdot, \cdot)$ has the desired properties, i.e.

- $Prf(\cdot, \cdot)$ is monotonic as $\langle n, m, \langle \ulcorner \varphi_1 \urcorner, \dots, \ulcorner \varphi_m \urcorner \rangle \rangle > n$ (cf. remark 1.3), and $\overline{Prf}(\cdot, \cdot)$ is monotonic,
- for each φ_i ($1 \leq i \leq m$), $Prf(\langle n, m, \langle \ulcorner \varphi_1 \urcorner, \dots, \ulcorner \varphi_m \urcorner \rangle \rangle, \ulcorner \varphi_i \urcorner)$ is true,
- if $A^* \not\equiv \varphi_i$ ($1 \leq i \leq m$), then $Prf(\langle n, m, \langle \ulcorner \varphi_1 \urcorner, \dots, \ulcorner \varphi_m \urcorner \rangle \rangle, \ulcorner \varphi_i \urcorner)$ is false.

It remains to show that $Prf(\cdot, \cdot)$ is a proof predicate in \mathbb{T} :

$$\mathbb{T} \vdash \varphi \iff \exists k \in \mathbb{N} : Prf(k, \ulcorner \varphi \urcorner) \text{ is true}$$

Let $Prf(k, \ulcorner \varphi \urcorner)$ be true for some $k \in \mathbb{N}$. By the definition of $Prf(\cdot, \cdot)$, $\overline{Prf}(n', \ulcorner \varphi \urcorner)$ holds for some $n' \in \mathbb{N}$, thus, as $\overline{Prf}(\cdot, \cdot)$ is a proof predicate, $\mathbb{T} \vdash \varphi$.

Conversely, if $\mathbb{T} \vdash \varphi$ then let n be the Gödel number of a proof of φ by means of $\overline{Prf}(\cdot, \cdot)$, i.e. $\overline{Prf}(n, \ulcorner \varphi \urcorner)$ is true. Let $k := \langle n, 1, \ulcorner \varphi \urcorner \rangle$. Clearly, $Prf(k, \ulcorner \varphi \urcorner)$ holds.

■

To continue the proof of the Main Lemma 3.18, we define D^* by induction on $s(D)$ and prove that if $D \in \Gamma'$ then D^* is true, and if $D \in \Delta'$ then D^* is false.

The interpretation of the proof variables has to be done in a way, such that injectivity is guaranteed. This can always be achieved as each provable formula has infinitely many proofs by lemma 3.19. So together with the interpretation of the sentence variables, $(\cdot)^*$ is an injective interpretation.

The cases where D is a sentence variable or a boolean combination of formulas are straightforward. For the induction step let $D = \Box_{p_i} A$ with $s(D) = k$.

- If $\Box_{p_i} A_1, \dots, \Box_{p_i} A_m \in \Gamma'$ then for each j , $A_j \in \Gamma'$ and $s(A_j) < k$. Hence A_j^* is a true recursive formula and so $\top \vdash A_j^*$. Let p_i^* be a Gödel number of a proof of A_1^*, \dots, A_m^* by lemma 3.19. So $(\Box_{p_i} A_j)^* = \text{Prf}(p_i^*, \ulcorner A_j^* \urcorner)$ is true.
- If $\Box_{p_i} A \in \Delta'$ and there exist formulas $\Box_{p_i} B_1, \dots, \Box_{p_i} B_m$ in Γ' . Then p_i^* is already defined and A^* is different from each B_j due to the injectivity of $(\cdot)^*$. Hence by lemma 3.19, $(\Box_{p_i} A)^* = \text{Prf}(p_i^*, \ulcorner A^* \urcorner)$ is false.
- 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 a Gödel number of a proof of the sentence $\forall x_i \forall x_i (x_i = x_i)$ by lemma 3.19. As there exists no modal formula A such that $\ulcorner A^* \urcorner = \ulcorner \forall x_i \forall x_i (x_i = x_i) \urcorner$, it follows that $(\Box_{p_i} A)^* = \text{Prf}(p_i^*, \ulcorner A^* \urcorner)$ is false.

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

■

Again, the Main Theorem 3.1 for \mathcal{PM} is proved, and a fixed monotonic proof predicate was used. So we get the following uniformity result:

3.20 Theorem There exists a monotonic proof predicate $\widehat{\text{Prf}}(\cdot, \cdot)$ such that for every formula A :

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

4 Uniformity

With respect to the uniformity theorems 3.17 and 3.20 for \mathcal{PM} , \mathcal{PFM} and \mathcal{PUM} , it is a natural question whether there exist uniform proof predicates for \mathcal{P} , \mathcal{PF} and \mathcal{PU} too, i.e. whether there exists a fixed proof predicate $Prf(\cdot, \cdot)$ under which for every modal formula A (here for \mathcal{P})

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

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 such uniform proof predicates do exist. The construction of a uniform proof predicate for \mathcal{PF} is described in the following; the cases of \mathcal{P} and \mathcal{PU} can be treated in a similar way.

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

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

Proof If $\mathcal{PF} \vdash A$ then it follows by theorem 2.2 that $\top \vdash A^*$ for each i-functional interpretation $(\cdot)^*$. Trivially $\top \vdash A^*$ 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 3.10 and 3.12, 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 algorithm for \mathcal{PF} is primitive recursive, i.e. that \mathcal{PF} is primitive recursive. Let A_0, A_1, \dots be a primitive recursive list of all formulas not provable in \mathcal{PF} , and let $\Gamma_0 \supset \Delta_0, \Gamma_1 \supset \Delta_1, \dots$ 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 $\langle \cdot, \cdot \rangle$ 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 such a formula B is unique since $\Gamma_{(r)_1} \supset \Delta_{(r)_1}$ is \mathcal{PF} -saturated. Moreover, $C(x)$ is primitive recursive, since the existential quantifier

occurring in it can be bounded primitive recursively in x (cf. remark 1.3). The construction of Lemma 3.12 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:

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

$$\phi_n(p_i) := 2 \cdot \langle n, i \rangle$$

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: \top proves

$$\begin{aligned} \widehat{Prf}(u, v) \iff & \forall r \leq u \left[\right. \\ & u = 2r + 1 \rightarrow \widehat{Prf}(r, v) \quad \wedge \\ & u = 2r \rightarrow \left[\begin{array}{l} C(r) \rightarrow v = \ulcorner B^* \urcorner \text{ for the formula } B \\ \text{such that } \Box_{p(r)_2} B \in \Gamma_{(r)_1} \text{ and the inter-} \\ \text{pretation } (\cdot)^* = (\widehat{Prf}(\cdot, \cdot), \phi_{(r)_1}). \\ \neg C(r) \rightarrow v = \ulcorner \forall x_0 \forall x_0 (x_0 = x_0) \urcorner \end{array} \right] \right] \end{aligned}$$

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

$$\begin{aligned} D \in \Gamma_n & \implies D^* \text{ is true} \\ D \in \Delta_n & \implies D^* \text{ is false} \end{aligned}$$

Proof Induction on the complexity of D :

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

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

is true according to the fixed point equation.

- $D = \Box_{p_i} B \in \Delta_n$. Then $C(< n, i >)$ is violated, and $\lceil B^* \rceil = \lceil \forall x_0 \forall x_0 (x_0 = x_0) \rceil$ is also false as there exists no formula B such that $B^* \equiv \forall x_0 \forall x_0 (x_0 = x_0)$. Therefore $\widehat{Prf}(2 \cdot < n, i >, \lceil B^* \rceil)$ is false, too.

■

4.3 Lemma

- (a) $\widehat{Prf}(\cdot, \cdot)$ is primitive recursive and functional.
- (b) $\top \vdash \varphi \iff \widehat{Prf}(n, \lceil \varphi \rceil)$ for some $n \in \mathbb{N}$.

Proof

- (a) Observe 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. Clearly, $\widehat{Prf}(\cdot, \cdot)$ is also functional.
- (b) Let $\top \vdash \varphi$ and let m be the Gödel number of a proof of φ in \top . Then $\widehat{Prf}(m, \lceil \varphi \rceil)$ holds and thus $\widehat{Prf}(2m + 1, \lceil \varphi \rceil)$. Conversely, let $\widehat{Prf}(k, \lceil \varphi \rceil)$ for some k .

If $k = 2m + 1$ then $\widehat{Prf}(m, \lceil \varphi \rceil)$ holds, so m is the Gödel number of a proof of φ , hence $\top \vdash \varphi$.

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 4.2, D^* is a true primitive recursive formula; again $\top \vdash \varphi$.

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

■

Thus theorem 4.1 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 :

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

After the uniformization of the proof predicate in \mathcal{P} , \mathcal{PF} and \mathcal{PU} , the 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], [6], [9] and [12]. This question will be answered up to the end of this section.

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

- (i) a (functional and/or monotonic) proof predicate $Prf(\cdot, \cdot)$ for \mathbb{T} ,
- (ii) an evaluation α of proof variables as natural numbers,
- (iii) an evaluation β of sentence variables as sentences of \mathbb{T} .

So the completeness theorem 3.1 states among others that

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

Theorem 4.1 shows that also

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

The proofs of theorems 3.10 and 3.12 show that the interpretation α of the proof variables alone is uniformizable in \mathcal{P} , \mathcal{PF} and \mathcal{PU} (e.g. $p_i^* = 2i$). The completeness theorems can therefore be formulated as

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

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

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

and let $\hat{\alpha}$ be such an α and $\widehat{Prf}(\cdot, \cdot)$ be such a $Prf(\cdot, \cdot)$. As $\mathcal{P}/\mathcal{PF}/\mathcal{PU} \not\vdash \Box_{p_0} \top$ it follows that $\mathbb{T} \not\vdash \widehat{Prf}(p_0^{\hat{\alpha}}, \ulcorner \top^* \urcorner)$ and then $\mathbb{T} \vdash \neg \widehat{Prf}(p_0^{\hat{\alpha}}, \ulcorner \top^* \urcorner)$. But this is equivalent to $\mathcal{P}/\mathcal{PF}/\mathcal{PU} \vdash \neg \Box_{p_0} \top$, which is known to be false.

The interpretation α of the proof variables is not uniformizable in the case of the monotonic logics \mathcal{PM} , \mathcal{PFM} and \mathcal{PUM} . Assume that

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

and let $\hat{\alpha}$ be such a fixed α . Let A be a formula $\neg \Box_{p_0} B$ with $B := \top \wedge \top \wedge \dots \wedge \top$ such that $\ulcorner B^* \urcorner > p_0^{\hat{\alpha}}$. As $\mathcal{PM}/\mathcal{PFM}/\mathcal{PUM} \not\vdash \neg \Box_{p_0} B$,

it follows that there exists a monotonic proof predicate $Prf(\cdot, \cdot)$ such that $\top \not\vdash \neg Prf(p_0^\alpha, \ulcorner B^* \urcorner)$ which is equivalent to $\top \vdash Prf(p_0^\alpha, \ulcorner B^* \urcorner)$. But a consequence of $Prf(p_0^\alpha, \ulcorner B^* \urcorner)$ is that $p_0^\alpha \geq \ulcorner B^* \urcorner$, which is a contradiction.

The interpretation β of the sentence variables is not uniformizable at all. To avoid repetitions, we present the proofs only for \mathcal{P} . The arguments and results remain the same for the other logics, too.

Assume that

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

and let $\widehat{\beta}$ be such a fixed β . As $\mathcal{P} \not\vdash \neg \Box_{p_0} S_0$, this implies that

$$\exists \alpha, Prf(\cdot, \cdot) : \top \not\vdash \neg Prf(p_0^\alpha, \ulcorner S_0^{\widehat{\beta}} \urcorner)$$

which is equivalent to

$$\exists \alpha, Prf(\cdot, \cdot) : \top \vdash Prf(p_0^\alpha, \ulcorner S_0^{\widehat{\beta}} \urcorner)$$

from which follows that $\top \vdash S_0^{\widehat{\beta}}$. As a consequence,

$$\forall \alpha, Prf(\cdot, \cdot) : \top \not\vdash Prf(p_0^\alpha, \ulcorner \neg S_0^{\widehat{\beta}} \urcorner)$$

hence

$$\forall \alpha, Prf(\cdot, \cdot) : \top \vdash \neg Prf(p_0^\alpha, \ulcorner \neg S_0^{\widehat{\beta}} \urcorner)$$

which implies $\mathcal{P} \vdash \neg \Box_{p_0} \neg S_0$, but again this is known to be false.

The situation can therefore be summarized as follows:

In the cases of \mathcal{P} , \mathcal{PF} and \mathcal{PU} 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 the last section.

In the cases of \mathcal{PFM} and \mathcal{PUM} every functional and monotonic proof predicate is a uniform one, and in the case of \mathcal{PM} such a predicate exists. But due to the Monotonicity Axiom the uniformization of the proof variables is not possible.

All other combinations of uniformization, including those of the sentence variables, are not possible.

5 Syntactical models

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

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.

5.1 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 $q_1 < q_2 : \Leftrightarrow \Box_{q_2} A_1(q_1) \in w$ (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. Note 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}).

5.2 Example

- (i) $\mathcal{P} \models \Box_p A \rightarrow A$ for every formula A : Let w be an arbitrary model. Then $w \models \Box_p A \rightarrow A$, as from $w \models \Box_p A$ follows $\Box_p A \in w$, hence $w \models A$.
- (ii) $\mathcal{P} \not\models S_0 \rightarrow \Box_p S_0$: 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 $w := \emptyset$.

5.3 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 aim of the next two subsections is to show that for each formula A :

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

Soundness and completeness for \mathcal{P} , \mathcal{PF} , \mathcal{PM} and \mathcal{PFM} are proved using the technique of canonical models in subsection 5.1, the systems \mathcal{PU} and \mathcal{PUM} are handled separately in subsection 5.2 .

5.1 Models without unification

The following definitions and results are fairly standard (cf. [7], pp. 9-12), so the proofs are not given in all details.

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:

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

■

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

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 $\mathcal{P} \vdash A \rightarrow B$, and $A \in M$, then $B \in M$. (4) and (5) are shown in a similar way.

■

5.6 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 $\mathcal{P} \not\vdash A$, 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. $\mathcal{P} \not\vdash A$. The same argument is valid for \mathcal{PF} , \mathcal{PM} and \mathcal{PFM} , too.

■

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

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

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

Proof If w is a model, then let $\bar{w} := \{A \mid w \models A\}$. We show first, that if w is a \mathcal{P} -model such that $w \models A$, then \bar{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, \bar{w} is maximal, and \bar{w} contains A . Now assume that \bar{w} is not \mathcal{P} -consistent, i.e. there exist formulas $A_1, \dots, A_n \in \bar{w}$ in such a way that $\mathcal{P} \vdash \neg(A_1 \wedge \dots \wedge A_n)$. From $A_1, \dots, A_n \in \bar{w}$ follows that $w \models A_1 \wedge \dots \wedge A_n$, i.e. $w \not\models \neg(A_1 \wedge \dots \wedge A_n)$. 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 5.2 (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 $\mathcal{P} \not\vdash A$, i.e. there exists a \mathcal{P} -model w , such that $w \models \neg A$. Thus \bar{w} is a \mathcal{P} -MCS which contains $\neg A$, and so \bar{w} does not contain A . By lemma 5.6, $\mathcal{P} \not\vdash A$. The same argument is valid for \mathcal{PF} , \mathcal{PM} and \mathcal{PFM} , too.

■

Notice that in the proof of lemma 5.7, if w is a model then \bar{w} contains the same quasiatomic formulas as w . 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. From this follows that \prec defined on \bar{w} is well-founded, too. This observation can be used for constructing arithmetical interpretations in the cases of \mathcal{PM} , \mathcal{PFM} and \mathcal{PUM} (cf. lemma 3.16).

5.8 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 . Clearly, 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 5.5) $C \notin M$ 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 5.5), 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. ■

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

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

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

Proof Let $\mathcal{P} \not\models A$, i.e. by lemma 5.6, there exists a \mathcal{P} -MCS M which does not contain A , thus by lemma 5.5 contains $\neg A$. By lemma 5.8 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. ■

5.2 Models with unification

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 (theorem 3.15), 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. [8]).

5.10 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:

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

We will use this definition mainly to get a more convenient description of functional models (lemma 5.13). The following lemma is purely technical, and it will help us to shorten several proofs.

5.11 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.

5.12 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 ,

$$\sigma w' \models A \iff w' \models A\sigma$$

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 5.10, for all quasiatomic formulas A , $\sigma w' \models A$ iff $w' \models A\sigma$. Therefore, by lemma 5.11, 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 5.12) 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 5.12 enables us to give another definition of \mathcal{PU} -model and \mathcal{PUM} -model:

5.13 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 5.10, $w = \sigma w'$. ■

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 $S_1 \rightarrow S_1$).

5.14 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 5.12 and 5.13. ■

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

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

Proof $\mathcal{PU} \vdash A$ iff (theorem 3.15) $\forall \sigma: \mathcal{PF} \vdash A\sigma$ 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 listed for the completeness of the discussion on functional interpretations.

5.16 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 ,

First we 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 .

5.18 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. $S \in \text{dom}(\sigma) \setminus w$ implies $w' \not\models S\sigma$.

If w is a \mathcal{PU} -model based on w' and σ , then clearly 1.-3. hold. 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 5.11 it follows that for all formulas A , $w \models A$ iff $w' \models A\sigma$. Let A be quasiatomic. If $w \models A$, thus $A \in w$ 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 $S \notin \text{dom}(\sigma)$, 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 $S \in \text{dom}(\sigma)$, 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 5.18.

5.19 Definition Let w be a finite set of quasiatomic formulas. A *w-chain* is a (finite or infinite) sequence $(\varepsilon, w) = (\sigma_0, w_0), (\sigma_1, w_1), \dots$, 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 $w_{k+1} := w'$.

5.20 Lemma Let w be a model, and let $(\varepsilon, w), \dots, (\sigma_k, w_k)$ be the initial elements of a w -chain. Then $w = \sigma_k w_k$, 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 $w_k \models B\mu$, thus $w_k \models A$, 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, $w_{k+1} \models A$. ■

5.21 Lemma Let w be a model, and let $(\varepsilon, w), \dots, (\sigma_k, w_k)$ 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 5.19. 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 by the idempotence of σ_k , $\text{var}(w_k) \cap \text{dom}(\sigma_k) = \emptyset$, and as μ is an idempotent unifier of formulas in w_k , $\text{dom}(\mu) \subset \text{var}(w_k)$, and $\text{ran}(\mu) \subset \text{var}(w_k)$. As a consequence, $\text{dom}(\mu) \cap \text{dom}(\sigma_k) = \emptyset$, and $\text{ran}(\mu) \cap \text{dom}(\sigma_k) = \emptyset$.

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, thus 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 $\text{dom}(\sigma_k)$: if F_1 contains no variable of $\text{dom}(\sigma_k)$, then $F_1 \equiv F_1\sigma_k$. From this follows that $F_1\mu$ contains a variable of $\text{dom}(\sigma_k)$, thus $F_2\mu$ contains a variable of $\text{dom}(\sigma_k)$, thus F_2 contains a variable of $\text{dom}(\sigma_k)$. Consequently, F_2 is not of the form $D_2\sigma_k$, too. According to definition 5.19, $w_k := \{A \mid \exists B \in w : A \equiv B\sigma_k, \text{ and } A \text{ is quasiatomic}\}$, hence $F_1, F_2 \notin w_k$. So finally we get $w_k \models \neg F_1$ and $w_k \models \neg F_2$, thus $w_k \models F_1 \leftrightarrow F_2$. 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 $\neg B \equiv A\mu \equiv A\mu\mu \equiv \neg B\mu$, thus $B \equiv B\mu$. 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: Clearly, 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 $w' \models A\mu$, and thereby $w' \models A$.

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 $w_k \not\models (D_1 \leftrightarrow D_2)\sigma_k$. 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 pairs $\Box_p A, \Box_p B \in w$ ($A \not\equiv B$), 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 $w_k \models (D_1 \leftrightarrow D_2)\sigma_k$; contradiction. ■

5.22 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 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 than the number of variables in w_k , as μ is idempotent and $\mu \neq \varepsilon$. 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, thus 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 5.21, w is not a \mathcal{PU} -model. ■

5.23 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 5.22.

■

5.24 Remark In the decision procedure above we have used only idempotent unifiers. It is possible to restrict the definition 5.1 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 in such a way that $\sigma = \mu\alpha$. Let $w'' := w'\alpha^{-1}$. Clearly, w'' again 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 $w \models A$.

6 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. [5] and [10]). Among other things we show that: In \mathcal{P} and \mathcal{PF} fixed points do not always exist (theorem 6.4), but in \mathcal{PM} and \mathcal{PFM} they do (theorem 6.6). There are formulas, which have logically unique fixed points as usual (e.g. theorem 6.5), i.e. if A is a fixed point and A is logically equivalent to B , then B is a fixed point, too. But there are also formulas, which have syntactically unique fixed points (theorem 6.9). Finally, there are formulas which have logically different fixed points (last example at the end of this section).

According to definition 5.1, 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 $\text{subf}(A)$ be the set of all subformulas of a formula A .

6.1 Lemma Let w be a \mathcal{P} -model and A a formula such that $w \models A$, and let $w_A := w \cap \text{subf}(A)$. 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 5.3).

Proof Clearly w_A is a finite set of quasiatomatic formulas. By straightforward induction on the complexity of a formula B it follows that if $B \in \text{subf}(A)$, then $w \models B$ iff $w_A \models B$ (cf. proof of lemma 5.8). 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. ■

6.2 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 $A := \neg \Box_p \perp$).

Proof

- a) Let w be a model such that $w \models A$, and let $w_A := w \cap \text{subf}(A)$. According to lemma 6.1, $w_A \models A$, 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.

■

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

- a) $\mathcal{P} \models A \rightarrow \Box_p A$ 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 $A = \neg \Box_p \perp$).

■

First note 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 in such a way 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:

6.4 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 6.3. 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 6.3 is the following:

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

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 6.3 item a) equivalent to $\mathcal{P} \models \neg A$. The same holds for \mathcal{PF} , \mathcal{PM} and \mathcal{PFM} , too.
■

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

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

$$\begin{aligned} \mathcal{PM} \models A &\leftrightarrow D(\Box_{q_1} \perp, \dots, \Box_{q_k} \perp) \\ &\leftrightarrow D(\Box_{q_1} C_1(A), \dots, \Box_{q_k} C_k(A)) \\ &\leftrightarrow D(A) \end{aligned}$$

■

6.7 Example According to the construction in the proof above, the formula $D(x) := \neg\Box_p(x)$ has the fixed point $A = \neg\Box_p\perp$; indeed, $\mathcal{PM} \models (\neg\Box_p\perp) \leftrightarrow \neg\Box_p(\neg\Box_p\perp)$. Notice that $\neg\Box_p\perp$ 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 5.2 (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 6.3 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.

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

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

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

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

Proof The only case from the right to the left which has to be explained is that if $\mathcal{PF} \models A \rightarrow (\Box_p \bar{B}_1 \vee \dots \vee \Box_p \bar{B}_k)$, 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 $w_A := w \cap \text{subf}(A)$. By lemma 6.1, $w_A \models A$. 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, $\mathcal{PF} \not\models A \rightarrow (\Box_p \bar{B}_1 \vee \dots \vee \Box_p \bar{B}_k)$.

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

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

where w is a \mathcal{PFM} -model, and $\Box_p \bar{B}_1, \dots, \Box_p \bar{B}_k$ 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 $\bar{w}_A := \bar{w} \cap \text{subf}(A)$. Still, \bar{w}_A is a \mathcal{PFM} -model and $\bar{w}_A \models A$, according to lemma 6.1. 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 . ■

Notice that in the right hand side of the preceding lemma the disjunction must contain in general more than one formula of the form $\Box_p B$. It is not true that $\mathcal{PF} \models \neg \Box_p A$ iff $\mathcal{PF} \models A \rightarrow \Box_p B$ for a formula B : Let $A := \Box_p \top \vee \Box_p (\top \wedge \top)$. Then $\mathcal{PF} \models \neg \Box_p (\Box_p \top \vee \Box_p (\top \wedge \top))$, but there is no formula B such that $\mathcal{PF} \models (\Box_p \top \vee \Box_p (\top \wedge \top)) \rightarrow \Box_p B$.

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:

6.9 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 $\tilde{w} := \{\Box_p A\}$. Clearly, \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 $\tilde{w} \not\models \Box_p \top$ since $A \not\equiv \top$. 2nd case: If there exists a \mathcal{P} -model (\mathcal{PF} -model) w_0 such that $w_0 \models \neg A$, then let $\tilde{w} := w_0 \cap \text{subf}(\neg A)$. By lemma 6.1, \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

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

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:

6.10 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} in such a way 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 6.9; all formulas equivalent to \top are fixed points, but \top itself is not. 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.

7 Extensions

Extensions of the Basic Logic of Proofs are suggested by different people. In most cases it is criticized that the formulas $\Box_p A$ admit nested modalities in the argument A , but the proof variables p have no structure at all.

A first attempt is to introduce propositional connectives on the proof variables as it is done e.g. in *dynamic logic*. Doing this, one has to make some assumptions on the structure of the proofs in \mathbb{T} . This can make sense in many cases, but clearly is not in the line of the Basic Logic of Proofs. So we will not discuss this approach.

Another possibility is to introduce quantifiers for proof variables, i.e. to extend the definition 1.1 of the modal language as follows:

- We still have symbols p, q, r, \dots which are intended to range over proofs (we call p, q, r, \dots now *proof constants*), and additionally we have free and bound variables x, y, z, \dots for proofs (now called *proof variables*).
- If A is a formula then also $\Box_x A$ is a formula.
- If A is a formula then $\exists x A$ is a formula ($\forall x A$ is defined as $\neg \exists x \neg A$).

Then we extend the definition 1.6 of an arithmetical interpretation by:

- $(\Box_x A)^* := \text{Prf}(x, \ulcorner A^* \urcorner)$, and
- $(\exists x A)^* := \exists x A^*$.

The very first observation is that we can now define

$$\Box A := \exists x \Box_x A.$$

As mentioned at the end of subsection 1.2, $\exists x \Box_x A$ behaves like the ordinary provability predicate under arithmetical interpretations. Thus, we can formulate all theorems of the Provability Logic GL.

Some examples of formulas in this extended language are:

- (1) $\Box_p A \longrightarrow \Box A$,
- (2) $\neg \Box \Box_p A \longrightarrow \Box \neg \Box_p A$ (Decidability of $\Box_p A$),
- (3) $\Box_p \Box^k A \longrightarrow \Box^l A$ ($k, l \in \mathbb{N}$, and $\Box^n A := \underbrace{\Box \dots \Box}_n A$),
- (4) $\neg \Box_p \Box \perp$,
- (5) $\Box(\Box_p A \rightarrow A) \longrightarrow \Box A$ (Modification of Löb's theorem),

- (6) $\Box\forall xA(x) \longrightarrow \forall x\Box A(x)$ (Converse of the Barcan formula), and similarly,
 (7) $\exists x\Box A(x) \longrightarrow \Box\exists xA(x)$,
 (8) $\forall x(\Box_x A \longrightarrow \Box\Box_x A)$ (Demonstrable Σ_1 -completeness),
 (9) $\forall x\Box(\Box_x A \longrightarrow A)$.

7.1 Example The formula $\exists x\neg\Box_x\top$ can be read as “there exists a proof that does not derive \top ”. Its arithmetical interpretation is $\exists x\neg Prf(x, \ulcorner\top\urcorner)$.

If we consider only functional interpretations $(\cdot)^*$, then $\exists x\neg Prf(x, \ulcorner\top\urcorner)$ is a true Σ_1 -sentence, hence provable in \top . So $\exists x\neg\Box_x\top$ holds under functional interpretations.

Assume next that $Prf(\cdot, \cdot)$ is defined by:

$$Prf(x, y) := \widetilde{Prf}(x, y) \vee y = \ulcorner\top\urcorner$$

Clearly, $Prf(\cdot, \cdot)$ is a nonfunctional proof predicate, and $\forall x Prf(x, \ulcorner\top\urcorner)$ is a true sentence. So $\exists x\neg Prf(x, \ulcorner\top\urcorner)$ is false, hence not provable in \top . Therefore, $\exists x\neg\Box_x\top$ does not hold under arbitrary interpretations.

A modification of this formula is

$$\neg\Box A \longrightarrow \exists x\neg\Box_x A$$

Let $(\cdot)^*$ be an arbitrary interpretation. From $\top \vdash \exists x\neg Prf(x, \ulcorner A^*\urcorner)$ follows that $\top \vdash \neg Pr(\ulcorner A^*\urcorner) \longrightarrow \exists x\neg Prf(x, \ulcorner A^*\urcorner)$, so assume that $\top \not\vdash \exists x\neg Prf(x, \ulcorner A^*\urcorner)$. As this is a Σ_1 -sentence, we get that $Prf(n, \ulcorner A^*\urcorner)$ is true for all numbers n , hence $\top \vdash Pr(\ulcorner A^*\urcorner)$, and so again $\top \vdash \neg Pr(\ulcorner A^*\urcorner) \longrightarrow \exists x\neg Prf(x, \ulcorner A^*\urcorner)$. Thus, $\neg\Box A \longrightarrow \exists x\neg\Box_x A$ holds under arbitrary interpretations.

A remarkable step into this direction of an extension of the Basic Logic of Proofs has been done by S.N. Artëmov. His language does not contain quantifiers, but the labeled modalities $\Box_p A$ of the Basic Logic of Proofs as well as the modalities $\Box A$ of GL. He interprets this formulas in a straightforward manner as

$$\begin{aligned} (\Box_p A)^* &:= Prf(p^*, \ulcorner A^*\urcorner) \\ (\Box A)^* &:= Pr(\ulcorner A^*\urcorner) \end{aligned}$$

So w.r.t. the extended language as it is described at the beginning of this section, Artëmov allows only existential quantifiers of the form $\exists x \Box_x A$. His sound and complete proof system consists of the axioms and rules of GL as presented at the beginning of subsection 1.1, as well as the axioms and rules for the Basic Logic of Proofs, and in addition of

$$\begin{array}{ll} \Box_p A \longrightarrow \Box \Box_p A & \text{(stability)} \\ \neg \Box_p A \longrightarrow \Box \neg \Box_p A & \text{(stability)} \\ \frac{\Box A}{A} & \text{(converse necessitation)} \end{array}$$

Examples of theorems of this logic are examples (1) – (4) above. (1) is just the introduction of an existential quantifier. (2) is a direct consequence of the two stability schemes. For (3) let $(\cdot)^*$ be an arithmetical interpretation, and let us consider two cases. 1st case: If $\top \vdash \text{Prf}(p^*, \text{Pr}(\ulcorner \dots \text{Pr}(\ulcorner A^* \urcorner) \dots \urcorner))$ (k times), then we get by the Reflexivity Axiom $\top \vdash \text{Pr}(\ulcorner \dots \text{Pr}(\ulcorner A^* \urcorner) \dots \urcorner)$ (k times), and then by necessitation and converse necessitation, $\top \vdash \text{Pr}(\ulcorner \dots \text{Pr}(\ulcorner A^* \urcorner) \dots \urcorner)$ (l times). 2nd case: If $\top \not\vdash \text{Prf}(p^*, \text{Pr}(\ulcorner \dots \text{Pr}(\ulcorner A^* \urcorner) \dots \urcorner))$ (k times), then the claim follows immediately as this is a recursive formula. The theorem (4) is a special case of (3): Let $A := \perp$, $k := 1$ and $l := 0$. The modification of Löb's theorem (5) is not valid: Assume that (5) is a theorem. As $\Box_p A \rightarrow A$ is an axiom, one can derive $\Box(\Box_p A \rightarrow A)$ by necessitation, hence $\Box A$, hence A for every formula A .

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] 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.
- [4] 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.
- [5] G. Boolos, *The unprovability of consistency: an essay in modal logic*. Cambridge: Cambridge University Press, 1979.
- [6] G. Boolos, “Extremely undecidable sentences,” *Journal of Symbolic Logic*, vol. 47, pp. 191–196, Mar. 1982.
- [7] 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.
- [8] 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.
- [9] F. Montagna, “On the diagonalizable algebra of Peano arithmetic,” *Bollettino della Unione Matematica Italiana*, vol. 16-B, no. 5, pp. 795–812, 1979.

- [10] C. Smoryński, “The incompleteness theorems,” in *Handbook of Mathematical Logic* (J. Barwise, ed.), ch. D.1, pp. 821–865, North-Holland, Amsterdam, 1977.
- [11] R. M. Solovay, “Provability interpretations of modal logic,” *Israel Journal of Mathematics*, vol. 25, pp. 287–304, 1976.
- [12] A. Visser, *Aspects of Diagonalization and Provability*. PhD thesis, University of Utrecht, 1981.

Index

\perp, \top	2
\equiv	4
\models	45
\forall^*	7
$\Box A$	1, 67, 68
$\Box_p A$	2, 67
$F = G \pmod{A = B}$	6, 14, 15
$\tau_{A,B}$	7, 14, 15, 20, 24
$\Gamma \supset \Delta, \bigwedge \Gamma, \bigvee \Delta$	20
$\sigma w'$	49
arithmetical interpretation	2, 4, 67
Barcan formula	68
based	45
chain	53
compatibility (interpretations — substitutions)	15
completeness (w.r.t. arithmetical interpretations)	
\mathcal{P}	19, 24, 42
\mathcal{PF}	19, 29, 42
\mathcal{PU}	19, 30, 42
\mathcal{PM}	19, 35, 48
$\mathcal{PFM}, \mathcal{PUM}$	19, 32, 48
completeness (w.r.t. syntactical models)	
$\mathcal{P}, \mathcal{PF}, \mathcal{PM}, \mathcal{PFM}$	49
$\mathcal{PU}, \mathcal{PUM}$	51
composition (interpretation and substitution)	15
consistent, consistency	46, 61
cut elimination	7, 19
decidability	
$F = G \pmod{A = B}$	15
models	52, 53, 56
theories	7, 20, 29, 30, 67
Unification Axiom	7
diagonalization	25
dynamic logic	67

equation set	13
expression	13
fixed points	1, 59
existence	1, 59, 61, 64
uniqueness	1, 64
logically	59, 61
syntactically	59, 63
fixed point equation	25
fixed point theorem	64
Functionality Axiom	6, 8, 11, 20
Gödel numbering	3
Gödel's incompleteness theorem	1, 61
Gödel proof predicate $\widetilde{Prf}(\cdot, \cdot)$	3, 7, 25, 32
Gödel proof predicate (nonfunctional) $\overline{Prf}(\cdot, \cdot)$	4, 7, 32, 36
idempotent	14, 54, 57
injectivity	3, 5
interpretation	
arithmetical	2, 4, 11, 25, 42, 46
functional	5, 17, 31, 46
i-functional	5, 11, 17, 29, 31, 46
monotonic	5, 12, 33, 35, 46
Kripke model	45
language, modal and arithmetical	2, 67
Lindenbaum's Lemma	47
Löb's theorem	1, 67
Main Theorem	19
maximal, maximal consistent set (MCS)	47
models (syntactical)	
\mathcal{P}	45, 46
$\mathcal{PF}, \mathcal{PFM}$	45
$\mathcal{PU}, \mathcal{PUM}$	45, 46, 50, 52, 57, 59
\mathcal{PM}	45, 46
Monotonicity Axiom	6, 8, 12, 20

most general unifier (mgu)	14, 49
necessitation	7, 45, 69
numeral	3
Peano Arithmetic PA	1, 2
Primitive Recursive Arithmetic PRA	2
proof predicate	3, 27
functional	3, 30
monotonic	3, 36
proof variable	2, 42, 67
Provability Logic GL	1, 42, 59, 61, 63, 67, 68
provability predicate	1, 4, 67
quantifiers	67
quasiatomic	2, 45
Reflexivity Axiom	6, 8, 11
Reflexivity Rule	20, 29
saturation, saturated	22
saturation algorithm	22, 39
saturation lemma	
$\mathcal{P}_G, \mathcal{PF}_G, \mathcal{PM}_G, \mathcal{PFM}_G$	22, 39
$\mathcal{PU}_G, \mathcal{PUM}_G$	23
sentence variable	2, 42
sequent	20
Σ_1 -completeness	68
Solovay, R.M.	1, 2
solved form	13
soundness (w.r.t. arithmetical interpretations)	
$\mathcal{P}, \mathcal{PF}$	11
$\mathcal{PM}, \mathcal{PFM}$	12
$\mathcal{PU}, \mathcal{PUM}$	17
soundness (w.r.t. syntactical models)	
$\mathcal{P}, \mathcal{PF}, \mathcal{PM}, \mathcal{PFM}$	48
$\mathcal{PU}, \mathcal{PUM}$	51
soundness (Gentzen style w.r.t. Hilbert style)	21
subformula property	32
substitution	12, 13, 31, 49, 59

composition	13
substitution lemma and rule	1, 8, 31, 45, 49
syntactically identical	5, 17
T	2
theories (Hilbert style)	
\mathcal{P}	6, 8, 24
\mathcal{PF}	6, 8, 29, 31, 39
\mathcal{PU}	6, 8, 20, 31, 32
\mathcal{PM}	6, 7, 8, 32
\mathcal{PFM}	6, 32
\mathcal{PUM}	6, 7, 32
theories (Gentzen style) $\mathcal{P}_g, \mathcal{PF}_g, \mathcal{PU}_g, \mathcal{PM}_g, \mathcal{PFM}_g,$ $\mathcal{PUM}_g, \mathcal{P}_g^-, \mathcal{PF}_g^-, \mathcal{PU}_g^-, \mathcal{PM}_g^-, \mathcal{PFM}_g^-, \mathcal{PUM}_g^-$	19, 20
Unification Algorithm	13
Unification Axiom	6, 8, 17, 20
Unification Rule	20, 21
unifier, unifiable	13, 17, 49
uniformity	
$\mathcal{P}, \mathcal{PF}, \mathcal{PU}$	7, 39, 41
\mathcal{PM}	7, 37, 42
$\mathcal{PFM}, \mathcal{PUM}$	7, 35, 42
proof variables	42
sentence variables	42, 43

Curriculum vitae

I was born on March 11, 1963 in San Francisco. In 1968, my family moved to Zürich. From 1969 to 1982, I attended the primary schools and the high school (*Gymnasium Rämibühl*) in Zürich, and graduated in 1982 with the *Matura Typus C*.

I began my university studies at the Swiss Federal Institute of Technology (ETH) Zürich in the faculty of mathematics and physics in 1983. In 1983 and 1984, I also made my military service in the Swiss army. In 1986 and 1987, I studied topics related to *artificial intelligence* at the University of Kaiserslautern (FRG) for two semesters. I obtained the degree of a Dipl. Math. ETH with a master thesis on *constructive negation in logic programming* in 1989.

Subsequently, I worked for the seminar of applied mathematics at the ETH Zürich for one semester. Since then I have been scientific assistant and doctoral student of Prof. G. Jäger at the institute for computer science at the University of Berne.