Explicit Proofs in Formal Provability Logic

Evan Goris

The Graduate Center of the City University of New York
365 Fifth Avenue, 10016 New York, NY, U.S.A.
evangoris@gmail.com

Abstract. In this paper we answer the question what implicit proof assertions in the provability logic GL can be realized by explicit proof terms. In particular we show that the fragment of GL which can be realized by generalized proof terms of GLA is exactly S4 ∩ GL and equals the fragment that can be realized by proof-terms of LP. In the final sections of this paper we establish the disjunction property for GLA and give an axiomatization for GL ∩ S4.

1 Introduction

One of the most striking applications of classical propositional modal logic to mathematics is without much doubt the interpretation of $\Box$ as 'provable in Peano Arithmetic PA' (for a neat introduction to the purpose of this see [6], we will aim here at a quick technical treatment). The normality axiom (1) below is a a most simple and clear example of a modal formula with an intuitively clear 'provable in PA' interpretation:

$$\Box(A \to B) \to (\Box A \to \Box B). \tag{1}$$

Clearly this scheme expresses the rule of modus ponens. The project of studying provability (and other meta-mathematical notions) in an axiomatic setting using modal logic, originally suggested by Gödel, really came to flourish after the arithmetical completeness theorem of Solovay [15]. This theorem identifies the logic GL as the logic of provability, see also [8]. GL is a remarkable system of modal logic that not only proofs Gödel's second incompleteness theorem, and more generally a formalized version of Löb's Theorem, but even satisfies a fixed-point theorem, very much in the spirit of Gödel's fixed-point lemma but in a purely propositional setting.

However, Gödel originally suggested the modal logic S4 as the logic of provability. This is indeed a most natural candidate for a provability logic but as it turns out incompatible with GL (the least normal modal logic extending both is the inconsistent one). Basically when the $\Box$ is read as *provable* the schemes expressed by S4 are both too strong (reflection) and too weak (no Löb's Theorem).

Artemov's Logic of Proofs LP was invented to tackle this problem [5,1]. In LP the $\Box$'s are replaced by proof-terms and the notion under study switched from *is provable* to *is proved by*. These proof-terms are build up from axiom-constants, proof-variables and function symbols that represent effective operations on proofs. For example there is a binary function symbol $\cdot$ that constructs

S. Artemov and A. Nerode (Eds.): LFCS 2007, LNCS 4514, pp. 241–253, 2007.

from a proof x of $A \to B$ and a proof y of A a proof $x{\cdot}y$ of B. Which gives a means to express the rule of modus ponens, just as (1) but now in an explicit way:

$$x{:}(A \to B) \to (y{:}A \to (x{\cdot}y){:}B).$$

There are natural translations between modal formulas and LP-formulas. In one direction we can 'forget' the proof-terms in an LP formula by substituting $\Box$'s for them (forgetful-projection) and in the other direction we can substitute proof-terms for the $\Box$'s in a modal formula (realizations). The link of LP with S4 is as follows. For any theorem F of LP, the forgetful projection of F is a theorem of S4 and for any theorem A of S4 there exists a realization of A that is a theorem of LP. The latter is nicely formulated as LP can *realize* all theorems of S4. This, together with the arithmetical completeness theorem for LP does give a provability reading to S4 for which S4 is complete.

In [16] and [12] (cf. also [4]) the axiomatic study of provability (Provability Logic) and the axiomatic study of proofs (Logic of Proofs) are combined in a single logic that contains both the $\Box$ for formal provability and proof-terms for explicit proofs. The logic LPP from [16] contains a richer language of proof-terms than LP. In [12] this is shown to be not necessary, there an arithmetically complete logic GLA [1] has been recovered that has exactly the same term language as LP.

Recently F. Montagna posed the question whether GLA allows for the realization of more modal formulas than just S4 (given what we know about LP it is immediate that GLA realizes at least S4). A negative answer to this question is the main contribution of this paper.

This paper is organized as follows. In Section 2 we define the Logic of Proofs LP. In Section 3 we define the Logic of Proofs and Formal Provability GLA and formulate the main research question addressed in this paper. In Section 4 we give an answer to these questions. In the final sections of this paper we consider some related issues and give some directions for further research.

2 Logic of Proofs

See [3] for an extensive overview of LP. Here we only state the basic definitions and theorems relevant to this paper. The language of LP is two-sorted. We have *proofs terms* that are build up using

- Countably many proofs variables $x, y, z, \ldots$ and countably many axiom constants $a, b, c, \ldots$

and two binary function symbols $+$, $\cdot$ and a unary one $!$:

- if t and s are proof terms then so are $t{+}s$, $t{\cdot}s$ and $!t$.

[1] GLA was first introduced (under the name LPGL) supplied with Kripke-style semantics and proved to be arithmetically complete in E. Nogina's part of [4].

And we have LP *formulas*, which are generated by the following clauses.

– 'Propositional Logic',
– If F is a formula and t a proof term then $t{:}F$ is a formula.

We say that an LP formula F is *normal* when all negative occurrences off subformulas $t{:}G$ of F are of the form $x{:}G$, where x is a proof variable.

The logic LP is axiomatized by the following schemata and rules.

A0 'Classical Propositional Logic' (with Modus Ponens),
A1 $t{:}A \to A$,
A2 $s{:}(A \to B) \to t{:}A \to (s{\cdot}t){:}B$,
A3 $s{:}A \to (s+t){:}A$, $s{:}A \to (t+s){:}A$,
A4 $t{:}A \to !t{:}(t{:}A)$,
A5 $c{:}A$, c an axiom constant and A an instance of **A0**-**A4**.

If F is an LP formula then its *forgetful projection* F° is obtained by replacing all the proof terms by $\Box$'s. More formally:

– $p^\circ \equiv p$ and $\bot^\circ \equiv \bot$,
– $(A \to B)^\circ \equiv (A^\circ \to B^\circ)$,
– $(t{:}A)^\circ \equiv \Box(A^\circ)$.

A *realization* of a modal formula F is an LP formula G for which $G^\circ \equiv F$.

One of the fundamental theorems concerning LP is the following.

Theorem 1 (Artemov[1]). $\mathsf{S4} \vdash G$ *iff there exists a normal* F *such that* $\mathsf{LP} \vdash F$ *and* $F^\circ \equiv G$.

Anther fundamental theorem concerning LP is its arithmetical completeness theorem [1]. See also [2,9]. In the spirit of the arithmetical reading of modal formulas $\Box F$ as 'F is provable' ([15,8]), formulas of the form $t{:}F$ are read as 't is a proof of F'. By Theorem 1 this provides us with a natural provability semantics for modal logic for which S4 is complete. Given this interpretation of LP it is natural to consider a system that includes both expressions of the form $\Box F$ and $t{:}F$. This has been done in detail in [16,12]. However natural liftings of Theorem 1 have not been addressed yet and one of those liftings is the main topic of this paper.

3 The System GLA

In this section we present the logic GLA from [12] and formulate two questions that will be answered in the remainder of the paper.

A joint logic of formal provability and explicit proofs has first been studied in [16]. The logic there however has a richer language of explicit proofs than LP. In [12] (cf. also [4]) a logic GLA, also a joint logic of formal provability and explicit proofs has been recovered in which the language of explicit proofs is exactly that of LP. This is the system we will study here.

The language of GLA is that of LP enriched with the modal operator $\Box$. The formulas of the system GLA are generated by the following rules.

- 'Propositional Logic',
- if A is a formula and t is a proof term then $t{:}A$ is a formula,
- if A is a formula then $\Box A$ is a formula.

The logic GLA is axiomatized by the following axiom schemata and rules.

- 'Classical Propositional Logic',
- Provability Logic GL:
  L1 $\Box(A \to B) \to (\Box A \to \Box B)$,
  L2 $\Box A \to \Box\Box A$,
  L3 $\Box(\Box A \to A) \to \Box A$,
  - $\vdash A$ implies $\vdash \Box A$.
- Logic of Proofs LP:
  A1 $t{:}A \to A$,
  A2 $s{:}(A \to B) \to t{:}A \to (s{\cdot}t){:}B$,
  A3 $s{:}A \to (s+t){:}A$, $s{:}A \to (t+s){:}A$,
  A4 $t{:}A \to !t{:}(t{:}A)$,
  A5 $c{:}A$, c an axiom constant and A an instance of **A0**-**A4**, **L1**-**L3** or **C1**-**C3**.
- Connecting principles:
  C1 $t{:}A \to \Box A$,
  C2 $\neg t{:}A \to \Box\neg t{:}A$,
  C3 $t{:}\Box A \to A$.

Notice that **A5** is richer than its analog in LP. The forgetful projection of an LP formula obviously generalizes to GLA formulas by setting $(\Box A)^\circ \equiv \Box A^\circ$. The following question about GLA will be addressed.

> For which modal formulas A can we find $\Box$-free GLA formulas B with $B^\circ \equiv A$ and $\mathsf{GLA} \vdash B$.

As we will argue in the next subsection, the obvious generalization of the forgetful projection to GLA formulas as given above does not give us much to work with for solving this question. But first we finish this section with a few lemmata from [12] that will be of interest later.

In what follows we write

$$\mathsf{GLA} : X_1, \ldots, X_n \vdash Y_1, \ldots, Y_k$$

for the assertion that $Y_1 \vee \cdots \vee Y_k$ is provable using modus ponens only from the theorems of GLA and $X_1, \ldots, X_n$.

Lemma 1. *For any formula A there exists a term t such that*

$$\mathsf{GLA} \vdash x{:}A \to t{:}\Box A$$

Proof. We have $\mathsf{GLA} \vdash c{:}(x{:}A \to \Box A)$ and $\mathsf{GLA} \vdash x{:}A \to !x{:}(x{:}A)$. Thus $\mathsf{GLA} \vdash x{:}A \to (c{\cdot}!x){:}\Box A$

Lemma 2 (Constructive necessitation). *If* $\mathsf{GLA} \vdash A$ *then for some ground term* t *we have* $\mathsf{GLA} \vdash t{:}A$.

Proof. Induction on a GLA derivation of A. If A is one of the axioms other than **A5** we can take any axiom constant for t. If A is an instance of **A5**, say $A \equiv a{:}B$, then we can take $!a$ for t. Suppose A is obtained by modus ponens from $B \to A$ and B. Thus $\mathsf{GLA} \vdash B \to A$ and $\mathsf{GLA} \vdash B$. By (IH) we have terms t_1 and t_2 such that $\mathsf{GLA} \vdash t_1{:}(B \to A)$ and $\mathsf{GLA} \vdash t_2{:}B$. And thus for t we can take $t_1{\cdot}t_2$. Suppose that A is obtained from B using necessitation. Thus $\mathsf{GLA} \vdash B$. By (IH) we have $\mathsf{GLA} \vdash t{:}B$ for some t. By Lemma 1 we that have for some s that $\mathsf{GLA} \vdash s{:}\Box B$.

Lemma 3 (Lifting lemma). *If*

$$\mathsf{GLA}: \; x_1{:}X_1, \ldots, x_n{:}X_n \vdash Y$$

then for some term t *we have*

$$\mathsf{GLA}: \quad x_1{:}X_1, \ldots, x_n{:}X_n \vdash t{:}Y.$$

Moreover the proof-variables in t *are all among* $\{x_1, \ldots, x_n\}$.

Proof. Induction on a derivation of Y from the $x_i{:}X_i$'s. If Y is one of the X_i's, say X_{i_0} then for t we can take x_{i_0}. If Y is a theorem of GLA the required t is given by Lemma 2. The inductive case when Y is obtained by modes ponens from previously obtained formulas is similar as in Lemma 2.

3.1 The Trouble with the Forgetful Projection in GLA

Obviously, since LP is a sub-system of GLA we have that $\mathsf{LP} \vdash A$ implies $\mathsf{GLA} \vdash A$. And thus in particular by Theorem 1 we have the following. (Recall that an LP formula is normal when all negative occurrences of proof-terms are variables, we use the same terminology for the more general formulas of GLA.)

Theorem 2. *If* $\mathsf{S4} \vdash A$ *then for some normal* B *with* $B^\circ \equiv A$ *we have* $\mathsf{GLA} \vdash B$.

It is also true that GLA does not realize all the theorems of GL. For suppose that for some terms t and r we have

$$\mathsf{GLA} \vdash x{:}(r{:}\bot \to \bot) \to t{:}\bot.$$

Since $\mathsf{GLA} \vdash c{:}(r{:}\bot \to \bot)$ we thus have $\mathsf{GLA} \vdash t[x/c]{:}\bot$ and by reflection $\mathsf{GLA} \vdash \bot$. A contradiction.

As we will see below the theorems of GL that can be realized in GLA are precisely those formulas that are also theorems of S4. Clearly to show this it suffices to show the the other direction of Theorem 2, this however is less straightforward then in the S4/LP case. One easily sees that if $\mathsf{LP} \vdash A$ then $\mathsf{S4} \vdash A^\circ$. If we however in the most straightforward way extend the definition of forgetful projection to formulas in the language of GLA, then the set of theorems of GLA

under this projection is not even closed under modus ponens. For the following three formulas are theorems of GLA.

- $\Box(\Box p \to p) \to \Box p$,
- $x{:}p \to p$,
- $\Box(x{:}p \to p)$.

Their forgetful projections are respectively

- $\Box(\Box p \to p) \to \Box p$,
- $\Box p \to p$,
- $\Box(\Box p \to p)$.

From which p follows using modus ponens. Obviously p is not the forgetful projection of any theorem of GLA. The trick is to not study the 'plain' forgetful projection but a variant that remembers which $\Box$'s came from proof terms and which where already there. This is what we will carry out in the coming sections.

4 The System EI

In this section we will show that only the theorems of S4 can be realized in GLA. The main tool is a modal propositional logic with two modalities $\Box$ and $\boxtimes$. In particular we will be interested in the modal formulas in this language that constitute images of the following generalization of forgetful projection to GLA formulas.

Definition 1 (Forgetful projection). *For an* GLA *formula A we define the* forgetful projection A° *with induction on A as follows.*

- $p^\circ \equiv p$ *and* $\bot^\circ \equiv \bot$,
- $(A \to B)^\circ \equiv (A^\circ \to B^\circ)$,
- $(\Box A)^\circ \equiv \Box(A^\circ)$,
- $(t{:}A)^\circ \equiv \boxtimes(A^\circ)$.

Let EI (for Explicit/Implicit) be the normal bi-modal logic axiomatized by the following axiom schemata and rules.

CP 'Classical Propositional Logic',
L1 $\Box(A \to B) \to (\Box A \to \Box B)$,
L2 $\Box A \to \Box\Box A$,
L3 $\Box(\Box A \to A) \to \Box A$,
S1 $\boxtimes(A \to B) \to (\boxtimes A \to \boxtimes B)$,
S2 $\boxtimes A \to \boxtimes\boxtimes A$,
S3 $\boxtimes A \to A$,
C1 $\boxtimes A \to \Box A$,
C2 $\neg\boxtimes A \to \Box\neg\boxtimes A$,
C3 $\boxtimes\Box A \to A$,
R $\vdash A$ implies $\vdash \boxtimes A$.

Lemma 4. GLA $\vdash A$ *implies* EI $\vdash A^\circ$.

Proof. Induction on a GLA derivation of A. If A is an instance of **A5** then A is of the form $c{:}B$, B° is an axiom of EI and $\boxtimes B^\circ (\equiv (c{:}B)^\circ)$ is derivable using $\boxtimes$ necessitation. If A is an instance of any of the other axiom schemata then A° is an axiom of EI. Suppose $A \equiv \Box B$, and the last step in the derivation of A is necessitation. By (IH) we obtain $\mathsf{EI} \vdash B^\circ$. By $\boxtimes$ necessitation we obtain $\mathsf{EI} \vdash \boxtimes B^\circ$ and by **C1** and modus ponens we get $\mathsf{EI} \vdash \Box B^\circ$. The case 'the last step is modus ponens' is trivial.

Next we formulate a Kripke semantics for EI. A binary relation R is *conversely well-founded* when every R *increasing path* $x_0 R x_1 R x_2 \cdots$ is finite.

Definition 2 (EI-frame). *A bi-modal Kripke frame* $\langle W, R^\Box, R^\boxtimes \rangle$ *is an* EI-frame *if*

1. $R^\Box$ *is transitive and conversely well-founded,*
2. $R^\boxtimes$ *is transitive and reflexive,*
3. $xR^\Box y$ *implies* $xR^\boxtimes y$,
4. $xR^\Box y$ *and* $xR^\boxtimes z$ *implies* $yR^\boxtimes z$,
5. *for all* x *there exists* y *such that* $xR^\boxtimes y$ *and* $yR^\Box x$.

Notice that no finite frames satisfying both 1 and 5 exist. For if 5 holds then one inductively constructs a sequence

$$x_1 R^\boxtimes x_2 R^\boxtimes x_3 \cdots$$

For which we in addition have $\cdots x_3 R^\Box x_2 R^\Box x_1$. Thus by transitivity of $R^\Box$ we have for all $i < j$

$$x_j R^\Box x_i.$$

But if the frame is finite then for some $i < j$ we must have $x_i = x_j$, contradicting the conversely well-foundedness of $R^\Box$.

Nevertheless, as is shown in [10], EI can be embedded in a sub-logic that does have finite models and is complete for a class of finite frames.

Lemma 5 (Modal soundness). *If* $\mathsf{EI} \vdash A$ *then* A *is valid on any* EI*-frame.*

Proof. As usual it suffices to show the lemma for A an axiom of EI. All instances of GL and S4 are well-known to hold because of properties 1 and 2 of EI-frames.

We show that $\boxtimes A \to \Box A$ is valid. Suppose $w \Vdash \boxtimes A$ and suppose $wR^\Box x$. By 3 we have $wR^\boxtimes x$ and thus $x \Vdash A$.

To show that also $\boxtimes A \to \Box \boxtimes A$ is valid, suppose that in addition $xR^\boxtimes y$ then by 2 $wR^\boxtimes y$ and thus $y \Vdash A$ as well.

Now we show that $\neg \boxtimes A \to \Box \neg \boxtimes A$ is valid. Suppose $w \Vdash \neg \boxtimes A$ and $wR^\Box x$. For some y with $wR^\boxtimes y$ we have $y \Vdash \neg A$. By 4 we have $xR^\boxtimes y$ and thus $x \Vdash \neg \boxtimes A$.

Finally we show that $\boxtimes \Box A \to A$ is valid. Suppose $w \Vdash \boxtimes \Box A$. By 5 there exists some x with $wR^\boxtimes x$ and $xR^\Box w$. We thus have $x \Vdash \Box A$ and thus $w \Vdash A$.

We aim at showing that the $\Box$-free fragment of EI coincides with S4. One direction, namely that S4 is a subset of the $\Box$-free fragment is obvious. For the other direction we will make use of the completeness of S4 with respect to transitive and reflexive Kripke frames [7]. We will use bounded morphisms to connect these frames with our EI-frames.

Definition 3 (Bounded morphism). *Let M and M' be two Kripke models. A* bounded morphism *from M to M' is a surjective mapping $M \longrightarrow M'$ such that for all $x, y \in M$ we have*

- $x \Vdash p$ *iff* $f(x) \Vdash' p$,
- xRy *implies* $f(x)R'f(y)$,
- *If* $f(x)R'y'$ *then for some* y *we have* $f(y) = y'$ *and* xRy.

The following lemma is well-known, see [7].

Lemma 6. *If f is a bounded morphism from M to M' then for all $w \in M$, M, w is bi-similar with $M', f(w)$. Consequently for any formula A, $M \models A$ iff $M' \models A$.*

Proposition 1. *For any transitive and reflexive Kripke model M there exists an* EI *model $M_\omega = \langle W_\omega, R^\Box, R^\boxtimes, \Vdash\rangle$ such that there exists a bounded morphism from $\langle W_\omega, R^\boxtimes, \Vdash\rangle$ to M.*

Proof. Let $M = \langle W, R, \Vdash\rangle$ be an S4 model. Let W_1, W_2, ... be countably many disjoint copies of W. For $x \in W$ we denote with x_i the copy of x in W_i. Define $M_\omega = \langle W_\omega, R^\boxtimes, R^\Box, \Vdash\rangle$ as follows.

- $W_\omega = \bigcup_{i \geq 1} W_i$,
- $x_i R^\boxtimes y_j$ iff xRy,
- $x_i R^\Box y_j$ iff $x = y$ and $j < i$,
- $x_i \Vdash p$ iff $x \Vdash p$.

First we will show that M_ω is based on an EI-frame. That $R^\boxtimes$ is transitive and reflexive is immediate. That $R^\Box$ is transitive and conversely well-founded is also easy to see. Suppose that $x_i R^\Box y_j$. Then we thus have in particular that $x = y$ and by reflexivity of R we get $x_i R^\boxtimes y_j$. Suppose that $x_i R^\Box y_j$ and $x_i R^\boxtimes z_k$. We have to show that yRz. But this follows immediately since from our assumptions it follows that $y = x$ and xRz. Let $x_i \in W_\omega$. We have to show that for some $y_j \in W_\omega$ we have $x_i R^\boxtimes y_j$ and $y_j R^\Box x_i$. Just take $y_j = x_{i+1}$. This completes the proof that M_ω is based on an EI-frame.

We show that the mapping f defined by $f(x_i) = x$ is a bounded morphism from $\langle W_\omega, R^\boxtimes, \Vdash\rangle$ to M. f is clearly surjective and by definition of $\Vdash$ we have $x_i \Vdash p$ iff $f(x_i) \Vdash p$. Suppose $x_i R^\boxtimes y_j$. Then xRy and thus $f(x_i)Rf(y_j)$. Suppose $f(x_i)Ry$. $f(x_i) = x$, thus xRy. By definition of $R^\boxtimes$ we have $x_i R^\boxtimes y_i$. And by definition of f we have $f(y_i) = y$.

Theorem 3. *If A is $\Box$-free and* $\mathsf{EI} \vdash A$ *then* $\mathsf{S4} \vdash A$.

Proof. We show that any A satisfying the assumptions of the theorem is valid on all transitive and reflexive frames. The theorem then follows from the modal completeness of S4 ([7]). So let F be some S4 frame and let M be a model based on F. Let M_ω be the EI-model from Proposition 1. By Lemma 5 of EI we have that $M_\omega \models A$. And since M is a bounded morphic image from M_ω we also have by Lemma 6 that $M \models A$.

Theorem 4. *Any modal formula that is realizable in* GLA *is a theorem of* S4*.*

Proof. Let B be a realization of A (that is B is $\Box$-free and $B^\circ \equiv A$) such that $\mathsf{GLA} \vdash B$. By Lemma 4 $\mathsf{EI} \vdash B^\circ$ and thus by Theorem 3 $\mathsf{S4} \vdash B^\circ$.

5 The Disjunction Property for GLA

In this section we will prove the disjunction property for GLA. The analog for LP was first established in [11] using a minimal model construction for LP and we will use the same technique here.

With a *constant specification* we mean a set $\mathcal{CS}$ of pairs $\langle c, A\rangle$ where $c{:}A$ is an instance of **A5**. With $\mathsf{GLA}(\mathcal{CS})$ we denote the fragment of GLA where **A5** is restricted to $c{:}A$ for $\langle c, A\rangle \in \mathcal{CS}$. For the sake of completeness we repeat some definitions from [4].

Definition 4 (GLA-model). *A* GLA-model *is a structure* $\langle W, R, \Vdash\rangle$ *where*

1. *R is a transitive conversely well-founded relation on W,*
2. *$\Vdash$ is a forcing relation satisfying for all $w, v \in W$,*
   (a) the usual constraint on boolean connectives and $\Box$,
   (b) for all $t{:}F$, $w \Vdash t{:}F$ iff $v \Vdash t{:}F$,
   (c) $w \Vdash t{:}F$ implies $w \Vdash F$,
   (d) $w \Vdash s{:}(F \to G)$ and $w \Vdash t{:}F$ implies $w \Vdash (s{\cdot}t){:}G$,
   (e) $w \Vdash t{:}F$ implies $w \Vdash (t + s){:}F$ and $w \Vdash (s + t){:}F$,
   (f) $w \Vdash t{:}F$ implies $w \Vdash !t{:}(t{:}F)$.

Let F be a formula and let $\mathrm{Sub}(F)$ be the set of sub-formulas of F. Put

$$\mathrm{S}(F) = \bigwedge\{\Box A \to A \mid \Box A \in \mathrm{Sub}(F)\}.$$

We say that a rooted GLA-model $\langle W, R, \Vdash\rangle$ with root r is *F-sound* when

$$r \Vdash \mathrm{S}(F).$$

A rooted GLA-model is a *$\mathcal{CS}$-model* when it is A-sound for all $\langle c, A\rangle \in \mathcal{CS}$ and $c{:}A$ holds in the whole model. The following theorem is shown in [4].

Theorem 5 (Modal completeness). $\mathsf{GLA}(\mathcal{CS}) \vdash A$ *iff A is valid in all A-sound $\mathcal{CS}$-models.*

For the remainder of this section we fix a finite constant specification $\mathcal{CS}$. Let $*$ be the least map

$$* : \text{GLA-terms} \longrightarrow \mathcal{P}(\text{GLA-formulas})$$

for which

- $*(c) = \{A \mid \langle c, A\rangle \in \mathcal{CS}\}$,
- $F \to G \in *(s)$ and $F \in *(t)$ implies $G \in *(s{\cdot}t)$,
- $F \in *(s)$ implies $F \in *(s + t)$ and $F \in *(t + s)$,
- $F \in *(t)$ implies $t{:}F \in *(!t)$.

The following lemma follows immediately from minimality of $*$.

Lemma 7. *1. For all variables x, $*(x) = \emptyset$,*
2. for all constants c, $*(c) = \{A \mid \langle c, A\rangle \in \mathcal{CS}\}$,
3. $F \in *(t + s)$ implies $F \in *(t)$ or $F \in *(s)$,
4. $F \in *(s{\cdot}t)$ implies that for some G, $G \in *(t)$ and $G \to F \in *(s)$,
5. $F \in *(!t)$ implies that for some $G \in *(t)$, $F \equiv t{:}G$.

Corollary 1. *If $F \in *(t)$ then $\mathsf{GLA}(\mathcal{CS}) \vdash t{:}F$.*

Proof. Induction on the complexity of t using Lemma 7.

Now given this map $*$ we define a GLA-model $M = \langle W, R \Vdash\rangle$ as follows.

- $W = \{w_0, w_1, w_2, \ldots\}$,
- $w_i R w_j$ iff $i > j$,
- $w \Vdash p$ for all $w \in W$ and all p,
- $w \Vdash t{:}A$ iff $A \in *(t)$ and for all $v \in W$, $v \Vdash A$.

Lemma 8. *M is a GLA-model. Moreover it is a GLA-model in which $c{:}A$ holds for all $\langle c, A\rangle \in \mathcal{CS}$.*

Proof. R is clearly transitive and conversely well-founded. All constraints on $\Vdash$ hold by definition and the properties of the map $*$. For $\langle c, A\rangle \in \mathcal{CS}$ we have by Theorem 5 that A holds in M. We also have that $A \in *(c)$ and thus $c{:}A$ holds in M.

The next lemma implies that for any F there exists some $w \in W$ such that w generates an F-sound $\mathcal{CS}$-model.

Lemma 9. *Let $X = \{\Box F_i \to F_i \mid 0 \leq i < n\}$. There exists some $k \leq n$ such that $w_k \Vdash \bigwedge X$.*

Proof. If not then by a pigeon hole argument it follows that for some $i < n$ and $r < s \leq n$ we have $w_r \Vdash \Box F_i \wedge \neg F_i$ and $w_s \Vdash \Box F_i \wedge \neg F_i$. But $w_s R w_r$. A contradiction.

Theorem 6 (Disjunction property). *If $\mathsf{GLA}(\mathcal{CS}) \vdash t{:}A \vee s{:}B$ then*

$$\mathsf{GLA}(\mathcal{CS}) \vdash t{:}A \quad \textit{or} \quad \mathsf{GLA}(\mathcal{CS}) \vdash s{:}B.$$

Proof. Suppose $\mathsf{GLA}(\mathcal{CS}) \vdash t{:}A \vee s{:}B$. Let M be the model defined above. For any $i \geq 0$ let M_i be the sub-model of M generated by w_i. Since $\mathcal{CS}$ is finite by Lemma 9 there exists an $i \geq 0$ such that M_i is an $(t{:}A \vee s{:}B)$-sound $\mathcal{CS}$-model. By Theorem 5 we have $w_i \Vdash t{:}A \vee s{:}B$. But then $w_i \Vdash t{:}A$ or $w_i \Vdash s{:}B$. In the first case by Corollary 1 we get $\mathsf{GLA}(\mathcal{CS}) \vdash t{:}A$ and in the second case $\mathsf{GLA}(\mathcal{CS}) \vdash s{:}B$.

Notice that Theorem 6 generalizes to arbitrary constant specifications.

6 The Intersection of S4 and GL

We give an axiomatization of all formulas in the intersection of S4 with GL. We show that this normal modal logic has the Craig-interpolation property.

We follow the terminology from [14]. That is, a *modal logic* is a proper subset of the set of all modal formulas closed under substitution and modes ponens. A modal logic is *normal* when it is also closed under necessitation and contains all instances of $\Box(A \to B) \to (\Box A \to \Box B)$. The following lemmata are folklore.

Lemma 10. S4 *is the smallest modal logic that contains all the theorems of* K4 *and all instances of* $\Box A \to A$ *and* $\Box(\Box A \to A)$.

Lemma 11. GL *is the smallest modal logic that contains all the theorems of* K4 *and all instances of* $\Box(\Box A \to A) \to \Box A$ *and* $\Box(\Box(\Box A \to A) \to \Box A)$.

In what follows we abbreviate

$$\mathrm{L}(p) \equiv \Box(\Box p \to p) \to \Box p,$$
$$\mathrm{R}(p) \equiv \Box p \to p.$$

Lemma 12. $\mathsf{S4} \vdash \neg\mathrm{L}(\bot)$ *and* $\mathsf{GL} \vdash \mathrm{L}(\bot)$.

Proof. We have $\mathsf{S4} \vdash \Box\Diamond\top$ and $\mathsf{S4} \vdash \Diamond\top$ and thus $\mathsf{S4} \vdash \neg\mathrm{L}(\bot)$. $\mathsf{GL} \vdash \mathrm{L}(\bot)$ is clear.

For F a formula we write $\boxdot F$ for $\Box F \wedge F$. Let $\mathsf{K4L_0T_0}$ be the smallest normal modal logic that contains all the instances of

$\mathsf{4}$ $\Box A \to \Box\Box A$,
$\mathsf{L_0}$ $\mathrm{L}(\bot) \to \boxdot\mathrm{L}(A)$,
$\mathsf{T_0}$ $\neg\mathrm{L}(\bot) \to \boxdot\mathrm{R}(A)$.

We write $\mathsf{S4} \cap \mathsf{GL} \vdash A$ for $\mathsf{S4} \vdash A$ and $\mathsf{GL} \vdash A$.

Theorem 7. $\mathsf{S4} \cap \mathsf{GL} \vdash A$ *iff* $\mathsf{K4L_0T_0} \vdash A$

Proof. The right to left direction is immediate from Lemma 12. To show the other direction let A be a theorem of both S4 and GL. Then by Lemma 10 we get some $X_1, \ldots X_k$ such that

$$\mathsf{K4} \vdash \bigwedge_{1 \le i \le k} \boxdot(\Box X_i \to X_i) \to A.$$

And by Lemma 11 we get some $Y_1, \ldots, Y_n$ such that

$$\mathsf{K4} \vdash \bigwedge_{1 \le i \le n} \boxdot(\Box(\Box Y_i \to Y_i) \to \Box Y_i) \to A.$$

As $\mathsf{K4} \subseteq \mathsf{K4L_0T_0}$ and

$$\mathsf{K4L_0T_0} \vdash \neg\mathrm{L}(\bot) \vee \mathrm{L}(\bot) \to \bigwedge_{1 \le i \le k} \boxdot(\Box X_i \to X_i) \vee \bigwedge_{1 \le i \le n} \boxdot(\Box(\Box Y_i \to Y_i) \to \Box Y_i)$$

we have $\mathsf{K4L_0T_0} \vdash \neg\mathrm{L}(\bot) \vee \mathrm{L}(\bot) \to A$ and thus $\mathsf{K4L_0T_0} \vdash A$.

Theorem 8. $\mathsf{K4L_0T_0}$ *enjoys the Craig-interpolation property.*

Proof. Suppose $\mathsf{K4L_0T_0} \vdash A \to B$. Then both $\mathsf{GL} \vdash A \to B$ and $\mathsf{S4} \vdash A \to B$. By the interpolation theorems for GL ([8]) and $\mathsf{S4}$ ([7]) we find I_1 and I_2, in the common language of A and B such that $\mathsf{GL} \vdash A \to I_1 \to B$ and $\mathsf{S4} \vdash A \to I_2 \to B$. Now put

$$I \equiv (I_1 \wedge \mathrm{L}(\bot)) \vee (I_2 \wedge \neg \mathrm{L}(\bot)).$$

Since $\mathsf{GL} \vdash \mathrm{L}(\bot)$ we have $\mathsf{GL} \vdash I \leftrightarrow I_1$ and since $\mathsf{S4} \vdash \neg \mathrm{L}(\bot)$ we have $\mathsf{S4} \vdash I \leftrightarrow I_2$. Thus I is an interpolant for $A \to B$ in both $\mathsf{S4}$ and GL.

We have shown in the main body of this paper that the intersection of $\mathsf{S4}$ with GL is of interest when studying combined logics of explicit and formal proofs. Therefore the standard questions in the studies of modal logic are in order. However, intersections of modal logics are in general not the nicest objects in existence [13]. Apparently, by Theorem 8 with GL and $\mathsf{S4}$ we might be more lucky and therefore desirable and well-behaved answers to the questions below are plausible.

Question 1. Is there a nice cut-free formulation of $\mathsf{K4L_0T_0}$?

Question 2. What is the explicit version of $\mathsf{K4L_0T_0}$?

Question 3. What is the closed fragment of $\mathsf{K4L_0T_0}$?

Acknowledgements

The author would like to thank Professor Sergei Artemov and the anonymous referees for useful comments and suggestions.

References

1. Artemov, S.N.: Operational modal logic. Technical Report MSI 95-29, Cornell University (1995)
2. Artemov, S.N.: Explicit provability and constructive semantics. Bulletin of Symbolic Logic **7**(1) (2001) 1–36
3. Artemov, S.N., Beklemishev, L.D.: Provability logic. In Gabbay, D., Guenthner, F., eds.: Handbook of Philosophical Logic. Volume 13. 2nd edn. Kluwer (2004) 229–403
4. Artemov, S.N., Nogina, E.: Logic of knowledge with justifications from the provability perspective. Technical Report TR-2004011, CUNY Ph.D. Program in Computer Science (2004)
5. Artemov, S.N., Straßen, T.: The basic logic of proofs. In Börger, E., Jäger, G., Kleine Büning, H., Martini, S., Richter, M.M., eds.: Selected papers of the 6th Workshop on Computer Science Logic (CSL-1992), San Miniato, Italy, September 28–October 2, 1992. Volume 702 of Lecture Notes in Computer Science., Springer-Verlag (1993) 14–28

6. Beklemishev, L.D., Visser, A.: Problems in the logic of provability. Technical Report Logic Group Preprint Series 235, Department of Philosophy of Utrecht University, Utrecht (2005)
7. Blackburn, P., de Rijke, M., Venema, Y.: Modal logic. Cambridge University Press, New York, NY, USA (2001)
8. Boolos, G.: The Logic of Provability. Cambridge University Press, Cambridge (1993)
9. Goris, E.: Logic of proofs for bounded arithmetic. In Dima Grigoriev, J.H., Hirsch, E.A., eds.: Computer Science - Theory and Applications: First International Computer Science Symposium in Russia, CSR 2006, St. Petersburg, Russia, June 8-12. 2006. Volume 3967 of Lecture Notes in Computer Science., Elsevier (2006) 191–201
10. Goris, E.: Explicit proofs in formal provability logic. Technical Report TR-2006003, CUNY Ph.D. Program in Computer Science (2006)
11. Krupski, N.V.: On the complexity of the reflected logic of proofs. Technical Report TR-2003007, CUNY Ph.D. Program in Computer Science (2003)
12. Nogina, E.: On logic of proofs and provability. Bulletin of Symbolic Logic **12** (2006) 2005 Summer Meeting of the ASL.
13. Schumm, G.F.: Some failures of interpolation in modal logic. Notre Dame Journal of Formal Logic **27**(1) (1986) 108–110
14. Segerberg, K.: Post completeness in modal logic. Journal of Symbolic Logic **37** (1972) 711–715
15. Solovay, R.M.: Provability interpretations of modal logic. Israel Journal of Mathematics **25** (1976) 287–304
16. Yavorskaya-Sidon, T.L.: Logic of proofs and provability. Annals of Pure and Applied Logic **113**(1–3) (2002) 345–372