2006

TR-2006003: Explicit Proofs in Formal Provability Logic

Evan Goris

Explicit Proofs in Formal Provability Logic

Evan Goris

March 19, 2006

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$\cap$GL and equals the fragment that can be realized by proof-terms of LP. Additionally we show that the problem of determining which implicit provability assertions in a given modal formula can be made explicit is decidable. In the final sections of this paper we establish the disjunction property for GLA and give an axiomatization for GL $\cap$ 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'. As a most simple and clear example of a modal formula with an intuitively clear 'provable in PA' interpretation we have for example the normality axiom:

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

Which expresses the rule of modus ponens. The project of studying metamathematics using modal logic, originally suggested by Gödel, really came to flourish after the arithmetical completeness theorem of Solovay [Sol76]. This theorem identifies the logic GL as the logic of provability, see also [Boo93]. GL is a remarkable system of modal logic that not only expresses Gödel's second incompleteness 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. Originally Gödel 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)

Roughly the reason why S4 doesn't work as a logic of provability in the sense of Solovay's theorems is that when reading the $\Box$ as formal provability the proofs don't need to be real proofs, just objects that behave like proofs. Just like infinite numbers in a non-standard model of Peano Arithmetic are not real numbers but mere objects that satisfy the familiar properties of numbers. Artemov's Logic of Proofs LP was invented to tackle this problem [AS92, Art95]. In LP the $\Box$'s are replaced by proof-terms that stand for 'real' proofs. 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 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 direct 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 [Yav02] and [Nog06] (cf. also [AN04]) the two above mentioned approaches to model provability propositionally are combined in a single logic that contains both the $\Box$ for formal provability and proof-terms for explicit proofs. The logic LPP form [Yav02] contains a richer language of proof-terms than LP. In [Nog06] 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, although true as we will see below, is not immediate. For even though the proof-term language of GLA is the same as it is in LP and both logics are arithmetical complete, the presence in GLA of proof-terms for statements involving provability assertions that cannot be made explicit allows so to say for $\Box$'s to occur implicitly in a $\Box$ free formula. For example for any formula B there exists a proof term t such that

$$t{:}(\Box(\Box B \to B) \to \Box B)$$

is a theorem of GLA. Such a t then may occur in a $\Box$ free theorem of GLA.

The main contribution of this paper is the theorem that GLA does not realize more modal formulas than LP. But we do a little more. Since formulas of GLA can contain both proof-terms and $\Box$'s, we can equally ask for a given modal formula, in case not all the $\Box$'s can be realized, whether then at least some of them can. During the process of answering the first question we will define a

[1] GLA was first introduced (under the name LPGL) supplied with Kripke-style semantics and proved to be arithmetically complete in Nogina's part of the technical report [AN04].

(decidable) logic that exactly characterizes the $\Box$'s in a modal formula that can be realized in GLA.

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 and Section 5 we give answers to these questions. In the final sections of this paper we consider some related issues and give some directions for further research.

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

2 Logic of Proofs

See [AB04] 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 $x, y, z, \dots$ and countably many axiom constants $a, b, c, \dots$

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 $!t$.

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 2.1 (Artemov[Art95]). *S4 $\vdash G$ iff there exists a normal F such that LP $\vdash F$ and $F^\circ \equiv G$*

Anther fundamental theorem concerning LP is its arithmetical completeness theorem [Art95]. See also [Art01, Gor05]. In the spirit of the arithmetical reading of modal formulas $\Box F$ as 'F is provable' ([Sol76, Boo93]), formulas of the form $t{:}F$ are read as 't is a proof of F'. By Theorem 2.1 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 [Yav02, Nog06]. However the natural lifting of Theorem 2.1 has not been addressed yet and is the core of this paper.

3 The system GLA

In this section we present the logic GLA from [Nog06] 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 [Yav02]. The logic there however has a richer language of explicit proofs than LP. In [Nog06] (cf. also [AN04]) 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' (with Modus Ponens).
- 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 two questions about GLA will be addressed.

1. For which modal formulas A can we find LP formulas B with $B^\circ \equiv A$ and $\mathsf{GLA} \vdash B$.

2. For which modal formulas A can we find 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 in solving these questions. But before we continue with that we finish this section with a few lemmata from [Nog06] 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 3.1. *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 3.2 (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 3.1 we that have for some s that $\mathsf{GLA} \vdash s{:}\Box B$. ◻

Lemma 3.3 (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 3.2. The inductive case when Y is obtained by modes ponens from previously obtained formulas is similar as in Lemma 3.2. ◻

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 2.1 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 3.4. *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 $\mathsf{S4}$. Clearly to show this it suffices to show the the other direction of Theorem 3.4, this however is less straightforward then in the $\mathsf{S4}/\mathsf{LP}$ 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 theorem 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 a 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 image of the following generalization of forgetful projection to GLA formulas.

Definition 4.1 (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' (with Modus Ponens),

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 4.2. $\mathsf{GLA} \vdash A$ *implies* $\mathsf{EI} \vdash A^\circ$

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. ☐

Definition 4.3 (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 that 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 we will see later, EI is decidable and can be embedded in a sub-logic that does have finite models and is complete for a class of finite frames.

Lemma 4.4 (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 $\mathsf{S4}$ 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 □-free fragment of EI coincides with S4. One direction, namely that S4 is a subset of the □-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 [BdRV01]. We will use bounded morphisms to connect these frames with our EI-frames.

Definition 4.5 (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 [BdRV01].

Lemma 4.6. *If f is a bounded morphism from M to M' then for all $w \in M$, M, w is bisimilar with $M', f(w)$. Consequently for any formula A, $M \models A$ iff $M' \models A$.*

Proposition 4.7. *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 ω 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 4.8. *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 ([BdRV01]). 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 4.7. By Lemma 4.4 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 4.6 that $M \models A$. □

Theorem 4.9. *Any modal formula that is realizable in* GLA *is a theorem of* S4

Proof. Let B be a realization of A (that is $B^\circ \equiv A$) such that $\mathsf{GLA} \vdash B$. By Lemma 4.2 $\mathsf{EI} \vdash B^\circ$ and thus by Theorem 4.8 $\mathsf{S4} \vdash B^\circ$. □

4.1 Modal Completeness

In this section we will show the modal completeness of EI with respect to EI frames. This can be done directly but we will take a little detour via a sub-logic EI^- of EI. This will be useful later on when we characterize what □'s of a given modal formula are realizable in GLA.

Let EI^- be the system obtained from EI by dropping the axiom scheme **C3**. For a set X of formulas let $\mathbb{B}(X)$ be the set of boolean combinations of formulas in X. Notice that $\mathbb{B}(X)$ can be taken finite when X is finite. For any modal formula A let

$$\mathrm{wr}(A) = \bigwedge\{\boxtimes(\boxtimes\Box B \to B) \mid B \in \mathbb{B}(\mathrm{Sub}(A))\} \ .$$

Theorem 4.10. *The following are equivalent.*

1. $\mathsf{EI}^- \vdash \mathrm{wr}(A) \to A$
2. $\mathsf{EI} \vdash A$
3. *A is valid in all* EI*-frames*

The implications $1 \Rightarrow 2$ is clear since EI is an extension of EI^- and $\mathsf{EI} \vdash \mathrm{wr}(A)$. The implication $2 \Rightarrow 3$ was shown in Lemma 4.4 above. We will show that $3 \Rightarrow 1$. Assume that $\mathsf{EI}^- \nvdash \mathrm{wr}(A) \to A$. Let Φ be a finite set of formulas that is subformula closed, contains A and is closed under single negation. We say that a set $\Gamma \subseteq \Phi$ is *maximal* wr(A)-*consistent* when $\Gamma + \{\mathrm{wr}(A)\}$ is consistent in EI^- and no set $\Gamma' \subseteq \Phi$, properly extending Γ is. Put

$$W' = \{\Gamma \mid \Gamma \text{ is a maximal wr}(A)\text{-consistent subset of } \Phi\} \ .$$

As in the proof of Proposition 4.7 we let $W_0, W_1, \ldots$ be countably many disjoint copies of W'. With Γ_i we denote the copy of Γ in W_i. Put

$$W = \bigcup_{i \geq 0} W_i \ .$$

Define $\Gamma_i R^{\boxtimes} \Delta_j$ iff

- $\boxtimes A \in \Gamma_i$implies $\boxtimes A, A \in \Delta_j$.

And $\Gamma_i R^{\Box} \Delta_j$ iff

- $\boxtimes A \in \Gamma_i$ iff $\boxtimes A \in \Delta_j$,
- $\Box A \in \Gamma_i$ implies $\Box A, A \in \Delta_j$,
- $j < i$ or, $i = j$ and there exist $\Box C \in \Delta_j$ with $\Box C \notin \Gamma_i$.

Lemma 4.11. *$\langle W, R^{\boxtimes}, R^{\Box} \rangle$ is an* EI *frame*

Proof. Obviously $R^{\boxtimes}$ is transitive and reflexive.

Transitivity of $R^{\Box}$: Suppose $\Gamma_i R^{\Box} \Delta_j R^{\Box} \Theta_k$. The first two properties that should hold between Γ_i and Θ_k for us to conclude $\Gamma_i R^{\Box} \Theta_k$ are easily verified. We now verify the third one. In case $k < j$ then also $k < i$. In case $k = j$ we have some $\Box C \in \Theta_k$ such that $\Box C \notin \Delta_j$. But then also $\Box C \notin \Gamma_i$.

Conversely well-foundedness of $R^{\Box}$: Suppose that there exists an infinite sequence

$$\Gamma_{i_0} R^{\Box} \Gamma_{i_1} R^{\Box} \Gamma_{i_2} \cdots$$

Since for $m > n$ we have $i_n \geq i_m$ there exists some $k \geq 0$ such that for all $l \geq k$, $i_l = i_k$. But then for all $n > m \geq k$, Γ_{i_n} contains strictly more $\Box$-formulas than Γ_{i_m}. Since Φ is finite and each $\Gamma_i \subseteq \Phi$ this leads to a contradiction.

So properties 1 and 2 of Definition 4.3 hold. Properties 3 and 4 are easily checked. We now show property 5.

Fix Γ_i. We have to find some Δ_j with $\Gamma_i R^{\boxtimes} \Delta_j R^{\Box} \Gamma_i$. Let

$$\Delta' = \{\boxtimes B, \neg \boxtimes C \mid \boxtimes B, \neg \boxtimes C \in \Gamma_i\} + \{\Diamond D \in \Phi \mid \Diamond D \in \Gamma_i \text{ or } D \in \Gamma_i\} \ .$$

We claim that Δ' is wr(A)-consistent. For suppose not. Then

$$\bigwedge \boxtimes B, \mathrm{wr}(A) \vdash \bigvee \Box \neg D \vee \bigvee \boxtimes C \ .$$

We have $\vdash \Box \neg D \to \Box(\Box \neg D \wedge \neg D)$ and $\vdash \boxtimes C \to \Box \boxtimes C$ and thus

$$\bigwedge \boxtimes B, \mathrm{wr}(A) \vdash \Box \left(\bigvee (\Box \neg D \wedge \neg D) \vee \bigvee \boxtimes C \right) \ .$$

So

$$\bigwedge \boxtimes B, \mathrm{wr}(A) \vdash \boxtimes\Box \left(\bigvee(\Box\neg D \wedge \neg D) \vee \bigvee \boxtimes C\right) \ .$$

Since $\bigvee(\Box\neg D \wedge \neg D) \vee \bigvee \boxtimes C$ is a boolean combination of formulas in Φ, and thus a boolean combination of sub-formulas of A we have

$$\mathrm{wr}(A) \vdash \boxtimes\Box \left(\bigvee(\Box\neg D \wedge \neg D) \vee \bigvee \boxtimes C\right) \to \bigvee(\Box\neg D \wedge \neg D) \vee \bigvee \boxtimes C \ .$$

And thus by the fact that $\Gamma \vdash \bigwedge \boxtimes B$ and $\Gamma \vdash \bigwedge \neg \boxtimes C$ we obtain

$$\Gamma, \mathrm{wr}(A) \vdash \bigvee(\Box\neg D \wedge \neg D) \ .$$

But for each of those D's, $\Gamma \vdash \Diamond D \vee D$. Contradicting the $\mathrm{wr}(A)$-consistency of Γ. Now let $j = i + 1$ and Δ_j be some maximal $\mathrm{wr}(A)$-consistent subset of Φ extending Δ'. It checks out easily that $\Gamma R^{\boxtimes} \Delta_j R^{\Box} \Gamma_i$. $\Box$

To turn $\langle W, R^{\boxtimes}, R^{\Box}\rangle$ into a model put $\Gamma \Vdash p$ iff $p \in \Gamma$.

Lemma 4.12 (Truth lemma)**.** *For all $A \in \Phi$ and all Γ we have that $\Gamma \Vdash A \Leftrightarrow A \in \Gamma$*

Proof. Induction on A. If A is a propositional variable the lemma holds by definition of $\Vdash$. The cases for the boolean connectives are trivial.

Case $A \equiv \Box B$. ($\Leftarrow$) Suppose $\Box B \in \Gamma$ and $\Gamma R^{\Box} \Delta$ then $B \in \Delta$ and by (IH) we get $\Delta \Vdash B$. ($\Rightarrow$) Suppose $\Box B \notin \Gamma$. We will show that

$$\Delta' = \{\boxtimes C, \neg \boxtimes D \mid \boxtimes C, \neg \boxtimes D \in \Gamma\} + \{\Box E, E \mid \Box E \in \Gamma\} + \{\neg B, \Box B\}$$

is $\mathrm{wr}(A)$-consistent. For suppose not. Then

$$\bigwedge \boxtimes C, \bigwedge \neg \boxtimes D, \bigwedge(\Box E \wedge E), \mathrm{wr}(A) \vdash \Box B \to B \ .$$

Thus

$$\bigwedge \boxtimes C, \bigwedge \neg \boxtimes D, \bigwedge \Box E, \mathrm{wr}(A) \vdash \Box(\Box B \to B) \ .$$

By **L3** we thus get

$$\bigwedge \boxtimes C, \bigwedge \neg \boxtimes D, \bigwedge \Box E, \mathrm{wr}(A) \vdash \Box B \ .$$

But the left hand side of $\vdash$ is all provable from $\Gamma + \mathrm{wr}(A)$ and thus so is $\Box B$, a contradiction. Now for any Δ with $\Delta' \subseteq \Delta \subseteq \Phi$ we have $\Gamma R^{\Box} \Delta$ and by (IH) we have $\Delta \Vdash \neg B$.

Suppose $A \equiv \boxtimes B$. ($\Leftarrow$) Suppose $\boxtimes B \in \Gamma$ and $\Gamma R^{\boxtimes} \Delta$. Then $B \in \Delta$ and by (IH) $\Delta \Vdash B$. ($\Rightarrow$) Suppose $\boxtimes B \notin \Gamma$. Let $\Delta' = \{C, \boxtimes C \mid \boxtimes C \in \Gamma\} + \{\neg B\}$. Δ' is easy seen to be $\mathrm{wr}(A)$-consistent. Any Δ with $\Delta' \subseteq \Delta \subseteq \Phi$ satisfies $\Gamma R^{\boxtimes} \Delta \Vdash \neg B$. $\Box$

Since $\neg A$ is contained in some $\Gamma \in W$ we thus have an EI model M, $w \in M$ and $w \Vdash \neg A$.

5 The System GEI^-

In this section we will define a cut-free Gentzen system GEI^- for EI^-. The existence of such a system is the reason for considering EI^-, since for EI such a system does not seem to exist. In Section 5.1 below we will use this system to realize theorems of both EI^- and EI in GLA. GEI^- is defined by the following axioms and rules. Axioms:

$$\text{Ax}\ \frac{}{p \vdash p} \qquad \frac{}{\bot \vdash}\ \bot$$

Weakening:

$$\text{W}\ \frac{\Gamma \vdash \Delta}{\Gamma', \Gamma \vdash \Delta, \Delta'}$$

Contraction:

$$\text{LC}\ \frac{A, A, \Gamma \vdash \Delta}{A, \Gamma \vdash \Delta} \qquad \frac{\Gamma \vdash \Delta, A, A}{\Gamma \vdash \Delta, A}\ \text{RC}$$

Propositional:

$$\text{L}\rightarrow\ \frac{\Gamma \vdash A, \Delta \qquad \Gamma, B \vdash \Delta}{\Gamma, A \rightarrow B \vdash \Delta} \qquad \frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \rightarrow B, \Delta}\ \text{R}\rightarrow$$

GL:

$$\frac{\boxtimes\Delta_0, \neg\boxtimes\Delta_1, \Box\Gamma, \Gamma, \Box A \vdash A}{\boxtimes\Delta_0, \neg\boxtimes\Delta_1, \Box\Gamma \vdash \Box A}\ \text{R}\Box$$

$\mathsf{S4}$:

$$\text{L}\boxtimes\ \frac{\Gamma, A \vdash \Delta}{\Gamma, \boxtimes A \vdash \Delta} \qquad \frac{\boxtimes\Gamma \vdash A}{\boxtimes\Gamma \vdash \boxtimes A}\ \text{R}\boxtimes$$

We will write $\mathsf{GEI}^- : \Gamma \vdash \Delta$ for 'the sequent $\Gamma \vdash \Delta$ is derivable in GEI^-' and $\mathsf{GEI}^- : \Gamma \nvdash \Delta$ for the negation of that assertion.

We define an EI^--frame similarly as an EI-frame (Definition 4.3) but without condition 5. In what follows we establish the equivalence of the following.

1. $\mathsf{GEI}^- : \Gamma \vdash \Delta$,
2. $\mathsf{EI}^- \vdash \bigwedge\Gamma \rightarrow \bigvee\Delta$,
3. $\bigwedge\Gamma \rightarrow \bigvee\Delta$ is valid on all finite EI^--frames.

The implications $1 \Rightarrow 2$ is an easy induction and $2 \Rightarrow 3$ is clear given our experience with EI (see the proof of Lemma 4.4). We show $3 \Rightarrow 1$. Assume $\Gamma \nvdash \Delta$. Let Φ be the set of sub-formulas of formulas in $\Gamma \cup \Delta$ and their single negations. We say that a pair $\langle\Gamma, \Delta\rangle$ is maximally consistent in Φ when $\Gamma \cup \Delta \subseteq \Phi$, $\Gamma \nvdash \Delta$ and for all $A \in \Phi - \Gamma$ we have $\Gamma, A \vdash \Delta$. And for all $A \in \Phi - \Delta$ we have $\Gamma \vdash \Delta, A$. Let

$$W = \{\langle\Gamma, \Delta\rangle \mid \langle\Gamma, \Delta\rangle \text{ maximally consistent in } \Phi\}\ .$$

If $w \in W$ then we write $w = \langle\Gamma_w, \Delta_w\rangle$. Define $xR^{\boxtimes}y$ iff

- $\boxtimes A \in \Gamma_x$ iff $\boxtimes A, A \in \Gamma_y$.

And $xR^{\Box}y$ iff

- $\Box A \in \Gamma_x$ implies $\Box A, A \in \Gamma_y$,
- $\boxtimes B \in \Gamma_x$ iff $\boxtimes B \in \Gamma_y$,
- for some $\Box C \in \Gamma_y$ we have $\Box C \notin \Gamma_x$.

Lemma 5.1. *$\langle W, R^{\boxtimes}, R^{\Box}\rangle$ is an EI^--frame*

Proof. Clearly both $R^{\Box}$ and $R^{\boxtimes}$ are transitive. Also clearly, since Φ is finite, $R^{\Box}$ is conversely well-founded.

We show that $R^{\boxtimes}$ is reflexive. Suppose that for some $w \in W$ we have $\boxtimes B \in \Gamma_w$. If $B \notin \Gamma$ then $B, \Gamma_w \vdash \Delta_w$ and thus also $\boxtimes B, \Gamma_w \notin \Delta_w$. But then since $\boxtimes B \in \Gamma_w$ we thus have $\Gamma_w \vdash \Delta_w$. A contradiction.

We show that $wR^{\Box}x$ and $wR^{\boxtimes}y$ implies $xR^{\boxtimes}y$. Let $\boxtimes B \in \Gamma_x$. Then $\boxtimes B \in \Gamma_w$ and thus $\boxtimes B, B \in \Gamma_y$.

We show $xR^{\Box}y$ implies $xR^{\boxtimes}y$. Let $\boxtimes B \in \Gamma_x$. Then $\boxtimes B \in \Gamma y$. ☐

Now to turn $\langle W, R^{\boxtimes}, R^{\Box}\rangle$ into a model define

$$w \Vdash p \Leftrightarrow p \in \Gamma_w \quad .$$

Lemma 5.2 (Truth lemma)**.** *For all $A \in \Phi$ we have that for all $w \in W$*

1. *$A \in \Gamma_w$ implies $w \Vdash A$ and*
2. *$A \in \Delta_w$ implies $w \nVdash A$.*

Proof. We show both items simultaneously with induction on in A.

Case $A \equiv p$. Item 1 is clear by definition. Suppose $A \in \Delta_w$. Since $\Gamma_w \nvdash \Delta_w$, $A \notin \Gamma_w$ and thus $w \nVdash A$.

Case $A \equiv B \to C$. Suppose $B \to C \in \Gamma_w$. Then $B \in \Delta_w$ or $C \in \Gamma_w$. In the first case (IH) give $w \nVdash B$ and in the second case $w \Vdash C$. Suppose $B \to C \in \Delta_w$. Then $B \in \Gamma_w$ and $C \in \Delta_w$. For if not then $\Gamma_w, B \vdash \Delta_w$ or $\Gamma_w \vdash C, \Delta_w$. Therefor in either case by weakening we get $\Gamma_w, B \vdash C, \Delta_w$. Thus $\Gamma_w \vdash B \to C, \Delta_w$ and by contraction $\Gamma_w \vdash \Delta_w$. So by (IH) we get $w \Vdash B$ and $w \nVdash C$.

Case $A \equiv \Box B$. Item 1 is immediate. Suppose $\Box B \in \Delta_w$. We show that

$$\{\Box C, C \mid \Box C \in \Gamma_w\}, \{\boxtimes D \mid \boxtimes D \in \Gamma_w\}, \{\neg \boxtimes E \mid \neg\boxtimes \in \Gamma_w\}, \Box B \nvdash B \quad .$$

For if not then

$$\{\Box C \mid \Box C \in \Gamma_w\}, \{\boxtimes D \mid \boxtimes D \in \Gamma_w\}, \{\neg \boxtimes E \mid \neg\boxtimes \in \Gamma_w\} \vdash \Box B \quad .$$

And thus $\Gamma_w \vdash \Delta_w$ as well. A contradiction. Clearly now we can find some x with $wR^{\Box}x$ and $B \in \Delta_x$. By (IH) we see $x \nVdash B$.

Case $A \equiv \boxtimes B$. Item 1 is immediate. Suppose $\boxtimes B \in \Delta_w$. We show that

$$\{\boxtimes B, B \mid \boxtimes B \in \Gamma_w\} \nvdash B \ .$$

For if not then

$$\{\boxtimes B, \boxtimes B \mid \boxtimes B \in \Gamma_w\} \vdash B$$

and thus also

$$\{\boxtimes B, \boxtimes B \mid \boxtimes B \in \Gamma_w\} \vdash \boxtimes B \ .$$

By a couple of contractions we obtain

$$\{\boxtimes B \mid \boxtimes B \in \Gamma_w\} \vdash \boxtimes B$$

and thus by weakening $\Gamma_w \vdash \Delta_w$, a contradiction. □

Corollary 5.3. Both EI^- and EI are decidable

Proof. Decidability of EI^- follows from the above cut-free Gentzen formulation. Decidability of EI follows then from Theorem 4.10. □

As a corollary to the above corollary we obtain the following theorem.

Theorem 5.4. *Given a modal formula A, determining what $\Box$'s in A can be realized by proof terms such that the result is a theorem of* GLA *is decidable. In particular it is decidable what $\Box$'s in a theorem of* GL *can be seen as explicit proofs.*

Proof. Consider the set of formulas X obtainable from A by replacing some $\Box$'s by $\boxtimes$'s. The formulas from X that are theorems of EI are exactly the answers to the problem and are effectively computable by Corollary 5.3. □

5.1 Realizing EI^- in GLA

In this section we will show the following.

Theorem 5.5. *Suppose* $\mathsf{EI}^- \vdash A$*. Then for some normal B with $B^\circ \equiv A$ we have* $\mathsf{GLA} \vdash B$

In the proof of this theorem below we will constantly substitute proof-terms for proof-variables. So with a *substitution* we will always mean a mapping from proof-variables to proof-terms. If α and β are substitutions then with $\alpha \circ \beta$ we denote the substitution σ defined by $\sigma(x) = \alpha(\beta(x))$. If Γ is a multi-set of formulas then we write $\Gamma[\sigma]$ for the result of applying σ to all the formulas in Γ.

Lemma 5.6. *If* $\mathsf{GLA} : \Gamma \vdash \Delta$ *and σ is a substitution then*

$$\mathsf{GLA} : \Gamma[\sigma] \vdash \Delta[\sigma].$$

Proof. Clear. □

Proof of Theorem 5.5. Consider a GEI^- derivation of A. We picture this derivation as a tree where all the nodes are labeled with sequents, the root node is labeled with the conclusion of the derivation and the leafs with axioms. We will realize all the sequents in this derivation in two steps. In step one we replace each GEI^- sequent in the derivation tree with a GLA sequent. These sequents are not derivable in GLA yet. In step two we will construct for each of those GLA sequents $\Gamma \vdash \Delta$ a substitution σ such that

$$\mathsf{GLA} : \Gamma[\sigma] \vdash \Delta[\sigma] \ .$$

(Step 1) All the occurrences of $\boxtimes$ in this derivation naturally split up into disjoint families as follows. We say that an occurrence of a $\boxtimes$ in a side formula in the conclusion of a rule-application is a *direct descendant* of another if the latter is a corresponding occurrence in (one of the) the premise(ses). So for example let $X(\boxtimes)$ be a formula where we have 'indicated' an occurrence of $\boxtimes$ and consider an application of the L$\rightarrow$ rule.

$$\frac{\Gamma \vdash A, \Delta, X(\boxtimes) \qquad \Gamma, B \vdash \Delta, X(\boxtimes)}{\Gamma, A \rightarrow B \vdash \Delta, X(\boxtimes)}$$

Then the two indicated occurrences of $\boxtimes$ in the premise are direct descendants of the one in the conclusion. As another example consider and application of the R$\Box$ rule.

$$\frac{\boxtimes\Delta_0, \neg\boxtimes\Delta_1, \Box\Gamma, \Box X(\boxtimes), \Gamma, X(\boxtimes), \Box A \vdash A}{\boxtimes\Delta_0, \neg\boxtimes\Delta_1, \Box\Gamma, X(\boxtimes) \vdash \Box A}$$

Again, the indicated occurrences of $\boxtimes$ in the premise are direct descendants of the one in the conclusion. These are the only two examples in which an occurrence of $\boxtimes$ in a side formula has two direct descendants.

Similarly we define direct descendants of occurrences of $\boxtimes$'s in principal formulas in a rule application. For example consider an application of the RW rule.

$$\frac{\Gamma \vdash \Delta, A(\boxtimes), A(\boxtimes)}{\Gamma \vdash \Delta, A(\boxtimes)}$$

The two indicated occurrences of $\boxtimes$ in the premise are direct descendants of the one in the conclusion This and the analog for the LC rule are the only examples in which an occurrence of $\boxtimes$ in a principal formula has two direct descendants.

Now we say that two occurrences are *directly related* if one of them is a direct descendant of the other and the relation *related* is the transitive closure direct related. Since the system GEI^- respects polarities, the collection of $\boxtimes$'s in a derivation split up into disjoint families of related $\boxtimes$'s of equal polarity.

Lets say there are k families and number them from 1 to k. In every GEI^- sequent $\Gamma \vdash \Delta$ do the following to obtain a GLA sequent. Replace each negative $\boxtimes$ that belongs to family i with a fresh proof variable x_i. For a positive $\boxtimes$ that belongs to family j, let n be the number of $\boxtimes$ introduced by a R$\boxtimes$ rule and replace this $\boxtimes$ with $u_1^j + \cdots + u_k^j$. All the variables $x_1, \ldots, u_1^1, \ldots, u_i^j, \ldots$ are taken to be pairwise distinct. This completes step 1.

(Step 2) We define with induction the depth of a sequent $\Gamma \vdash \Delta$ (the depth of a sequent is the maximal distance to an axiom) a substitution σ such that

$$\mathsf{GLA} : \Gamma[\sigma] \vdash \Delta[\sigma] \enspace .$$

Additionally we will assure that if the r'th R$\boxtimes$ rule in family s does not occur in the derivation above the sequent $\Gamma \vdash \Delta$ then

$$\sigma(u^s_r) = u^s_r \enspace . \tag{2}$$

In the base case of the induction we can simply take $\sigma = \mathrm{id}$. For all the rules but the L$\rightarrow$, R$\Box$, L$\boxtimes$ and the R$\boxtimes$ we clearly can simply take the same substitution for the conclusion as for the premise. In what follows we write out the remaining rules.

We first do the L$\rightarrow$ rule. So suppose

$$\mathsf{GLA} : \Gamma[\alpha] \vdash A[\alpha], \Delta[\alpha] \quad \text{and} \quad \mathsf{GLA} : \Gamma[\beta], B[\beta] \vdash \Delta[\beta] \enspace .$$

By (2) we have

$$\alpha \circ \beta = \beta \circ \alpha \enspace .$$

Thus if we define σ as $\alpha \circ \beta$ then by Lemma 5.6 we have that

$$\mathsf{GLA} : \Gamma[\sigma] \vdash A[\sigma], \Delta[\sigma] \quad \text{and} \quad \mathsf{GLA} : \Gamma[\sigma], B[\sigma] \vdash \Delta[\sigma] \enspace .$$

Thus

$$\mathsf{GLA} : \Gamma[\sigma], (A \rightarrow B)[\sigma] \vdash \Delta[\sigma] \enspace .$$

Now we consider the R$\Box$ case. Thus suppose we have

$$\mathsf{GLA} : x{:}\Delta_0[\sigma], \neg t{:}\Delta_1[\sigma], \Box\Gamma[\sigma], \Gamma[\sigma] \vdash (\Box A \rightarrow A)[\sigma] \enspace .$$

Doing the very same proof under the $\Box$ gives us

$$\mathsf{GLA} : \Box x{:}\Delta_0[\sigma], \Box\neg t{:}\Delta_1[\sigma], \Box\Box\Gamma[\sigma], \Box\Gamma[\sigma] \vdash \Box(\Box A \rightarrow A)[\sigma] \enspace .$$

Thus

$$\mathsf{GLA} : x{:}\Delta_0, \neg t{:}\Delta_1, \Box\Gamma, \vdash \Box(\Box A \rightarrow A) \enspace .$$

And thus

$$\mathsf{GLA} : x{:}\Delta_0, \neg t{:}\Delta_1, \Box\Gamma, \vdash \Box A \enspace .$$

So we simply take the same substitution σ for the conclusion of these rules as for the premise.

Now let us consider the R$\boxtimes$ rule. Let this be the r'th rule in family s. By (IH) we have

$$\mathsf{GLA} : x{:}\Gamma[\sigma] \vdash A[\sigma] \enspace .$$

By lifting we find some t not containing any of the u's such that

$$\mathsf{GLA} : x{:}\Gamma[\sigma] \vdash t{:}A[\sigma] \enspace .$$

Now by (2) we have that $\sigma(u^s_r) = u^s_r$, thus if we put $\sigma' = \sigma[u^s_r/t]$ we have

$$\mathsf{GLA} : \ x{:}\Gamma[\sigma'] \vdash ((u^s_1 + \cdots + t + \cdots + u^s_n){:}A)\,[\sigma'] \ .$$

And since t does not contain u^s_r we thus conclude

$$\mathsf{GLA} : \ x{:}\Gamma[\sigma'] \vdash ((u^s_1 + \cdots + u^s_r + \cdots + u^s_k){:}A)\,[\sigma'] \ .$$

Finally we consider the case L$\boxtimes$. So we have

$$\mathsf{GLA} : \ \Gamma[\sigma], A[\sigma] \vdash \Delta[\sigma] \ .$$

Let the L$\boxtimes$ rule introduce a $\boxtimes$ from the family with number i. Then clearly also

$$\mathsf{GLA} : \ \Gamma[\sigma], x_i{:}A[\sigma] \vdash \Delta[\sigma] \ .$$

$\square$

Corollary 5.7. Suppose $\mathsf{EI} \vdash A$. Then for some normal B with $B^\circ \equiv A$ we have $\mathsf{GLA} \vdash B$

Proof. Suppose $\mathsf{EI} \vdash A$. By Theorem 4.10 we have $\mathsf{EI}^- \vdash \mathrm{wr}(A) \to A$. By Theorem 5.5 we find a normal B with $B^\circ \equiv \mathrm{wr}(A) \to A$ and $\mathsf{GLA} \vdash B$. Now B is of the form $C \to D$ where $D^\circ \equiv A$ and C° is a conjunction of formulas of the form $\boxtimes(\boxtimes\Box X \to X)$. By normality of $C \to D$, C is a conjunction of formulas of the form $x{:}(t{:}\Box X \to X)$. Let $x_1, \ldots, x_k$ be all the proof variables that occur in C. Let a be an axiom constant. Then $\mathsf{GLA} \vdash D[x_1/a, \ldots, x_k/a]$, by using the axiom necessitation scheme $(x{:}(t{:}\Box X \to X))\,[x_1/a, \ldots, x_k/a]$. $\square$

6 The Disjunction Property for GLA

In this section we will prove the disjunction property for GLA. The analog for LP was first established in [Kru03] 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 [AN04].

Definition 6.1 (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. 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 [AN04].

Theorem 6.2 (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

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

for which

- $*(c) = \{A \mid \langle c, A\rangle \in \mathcal{CS}\}$,
- $F \to G * (s)$ 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 6.3. *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 6.4. If $F \in *(t)$ then $\mathsf{GLA}(\mathcal{CS}) \vdash t{:}F$

Proof. Induction on the complexity of t using Lemma 6.3. ☐

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 6.5. *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 6.2 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 6.6. *Let $X = \{\Box F_i \to F_i \mid 0 \le i < n\}$. There exists some $k \le n$ such that $w_k \Vdash \bigwedge X$.*

Proof. If not then for some $i < n$ and $r < s \le n$ we have $r \Vdash \Box A_i \wedge \neg A_i$ and $s \Vdash \Box A_i \wedge \neg A_i$. But $w_s R w_r$. A contradiction. □

Theorem 6.7 (Disjunction property)**.** *If* $\mathsf{GLA}(\mathcal{CS}) \vdash t{:}A \vee s{:}B$ *then*

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

Proof. Suppose $\mathsf{GLA}(\mathcal{CS}) \vdash t{:}A \vee s{:}B$. Let M be the model defined above. For any $i \ge 0$ let M_i be the sub-model of M generated by w_i. Since $\mathcal{CS}$ is finite by Lemma 6.6 there exists an $i \ge 0$ such that M_i is an $(t{:}A \vee s{:}B)$-sound $\mathcal{CS}$-model. By Theorem 6.2 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 6.4 we get $\mathsf{GLA}(\mathcal{CS}) \vdash t{:}A$ and in the second case $\mathsf{GLA}(\mathcal{CS}) \vdash s{:}B$. □

Notice that Theorem 6.7 generalizes to arbitrary constant specifications.

7 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 [Seg72]. 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 7.1. 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 7.2. *GL is the smallest modal logic that contains all the theorems of $\mathsf{K4}$ 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 7.3. $\mathsf{S4} \vdash \neg\mathrm{L}(\bot)$ *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. □

Let GR be the smallest normal modal logic that contains all the instances of

4 $\Box A \to \Box\Box A$,

G $\mathrm{L}(\bot) \to \boxdot\mathrm{L}(A)$,

R $\neg\mathrm{L}(\bot) \to \boxdot\mathrm{R}(A)$.

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

Theorem 7.4. $\mathsf{S4} \cap \mathsf{GL} \vdash A$ *iff* $\mathsf{GR} \vdash A$

Proof. The right to left direction is immediate from Lemma 7.3. To show the other direction let A be a theorem of both $\mathsf{S4}$ and GL. Then by Lemma 7.1 we get some $X_1, \dots X_k$ such that

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

And by Lemma 7.2 we get some $Y_1, \dots, Y_n$ 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 $\mathsf{K4} \subseteq \mathsf{GR}$ and

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

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

Theorem 7.5. GR *enjoys the Craig-interpolation property*

Proof. Suppose $\mathsf{GR} \vdash A \to B$. Then both $\mathsf{GL} \vdash A \to B$ and $\mathsf{S4} \vdash A \to B$. By the interpolation theorems for GL ([Boo93]) and $\mathsf{S4}$ ([BdRV01]) 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 S4 with GL is of interest when studying combined logics of explicit and formal proofs. Therefor 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 [Sch86]. Apparently, by Theorem 7.5 with GL and 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 GR?

Question 2. What is the explicit version of GR?

Question 3. What is the closed fragment of GR?

7.1 Post completeness

Above we have seen one way the intersection of GL with S4 naturally comes up. Another way this might be the case is as follows. In [Seg72] a modal logic is called *post complete* when it has no proper (non-trivial) extensions. It is known that there are exactly two normal post complete modal logics. Namely Tr: the smallest normal modal logic containing all instances of $A \leftrightarrow \Box A$. And Ns: the smallest normal modal logic containing $\Box\bot$.

Every normal modal logic is contained in Tr or Ns. Also S4 is not a sub-logic of Ns, GL not a sub-logic of Tr but, obviously, GR is a sub-logic of both. If L_1 and L_2 are normal modal sub-logics of S4 and of Ns, then so is the least logic extending $L_1 \cup L_2$. Thus the following question is well defined.

Question 4. What is the largest normal modal sub-logic of S4 that is contained in Ns?

Obviously the answer is $\mathsf{S4} \cap \mathrm{Ns}$

Question 5. Is $\mathsf{S4} \cap \mathrm{Ns} = \mathsf{GR}$?

Since in fact Tr is the only logic (not necessarily normal) extending S4, the following might be easier.

Question 6. Is $\mathsf{GL} \cap \mathrm{Tr} = \mathsf{GR}$?

8 Further Directions

In this final section we discuss some further directions for further research.

8.1 Conservativity

One could still ask whether GLA allows for a more efficient realization of S4 then LP. A negative answer to this question is clearly implied by a positive answer to the following one.

Question 7. Is GLA conservative over LP?

8.2 Further Relations with GL

One of the most striking features of the provability logic GL is the De Jongh-Sambin fixed-point theorem [Boo93].

Question 8. Does the fixed-point theorem hold for EI?

The answer is almost certainly yes. The axiom $\boxtimes A \to \Box \boxtimes A$ is probably enough, so the fixed-point theorem would probably even hold in a much weaker system.

Since the formulas $\boxtimes A$ represent decidable statements, one expects that the calculated fixed points can be simplified. Assuming that we do have a fixed point theorem for EI, then for the version of the fixed point theorem for the fragment of EI with only one propositional variable this is the case: in fixed-points we can eliminate all occurrences of $\boxtimes$. This immediately follows from what we discus next.

We say that a closed formula F is in *normal form* when it is a truth functional combination of formulas of the form $\Box^i\bot$. We show that any closed formula is equivalent to one in normal form. From the proof of the analog for GL one can obtain the following ([Boo93]).

Lemma 8.1. *If F is a closed and $\boxtimes$ free. Then $\mathsf{EI} \vdash \Box F$ or for some i we have $\mathsf{EI} \vdash \Box F \leftrightarrow \Box^i\bot$.*

Theorem 8.2. *Any closed formula is equivalent, in* EI*, to a formula in normal form.*

Proof. By the normal form theorem for sentences in GL it is enough to show that any formula $\boxtimes F$ can be written in normal form whenever F is in normal form. We have

$$\mathsf{EI} \vdash \boxtimes F \leftrightarrow \boxtimes\Box F \ .$$

By Lemma 8.1 we thus have that either

$$\mathsf{EI} \vdash \boxtimes F \leftrightarrow \top$$

or

$$\mathsf{EI} \vdash \boxtimes F \leftrightarrow \bot \ .$$

□

(As a side remark note that this theorem obviously transfers to GLA.)

Nevertheless the following is still unclear.

Question 9. If we do have a general fixed-point theorem for EI, can we then eliminate all occurrences of $\boxtimes$ in the fixed-points?

I would conjecture no but maybe something weaker is true.

8.3 New Operations on Proofs

An interesting modal formula in the language of EI is the following.

$$\boxtimes(\Box A \vee \Box B) \to \boxtimes A \vee \boxtimes B \ . \tag{3}$$

Contrary to the two variations

- $\boxtimes\Box A \to \boxtimes A$
- $\boxtimes(\Box A \vee \Box B) \to A \vee B$

this formula is not derivable in EI. An EI counter-model is shown in Figure 1. There the solid edges denote $R^{\Box}$ relations and the dashed ones $R^{\boxtimes}$ relations and we have omitted the reflexive $R^{\boxtimes}$ relations. One easily checks that

$$\boxtimes(\Box p \vee \Box q) \to \boxtimes p \vee \boxtimes q$$

does not hold in the bottom node.

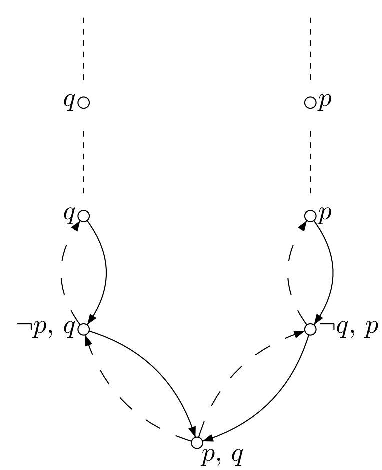

Figure 1: Counter Model

Nevertheless in arithmetic a computable operation on proofs for this scheme is easily defined and thus a logic that somehow contains such an operation would be a natural thing to study.

A drawback of such a hypothetical logic is that if it does have the internalization property, then it lacks the disjunction property (the disjunction property for LP was established in [Kru03] and for GLA it is shown in Section 6 above). For we have $\vdash \Box x{:}p \vee \Box\neg x{:}p$. Thus by internalization for some closed t we get

$$\vdash t{:}(\Box x{:}A \vee \Box\neg x{:}A).$$

Using a explicit version of (3) we then get for some r, $\vdash r{:}(x{:}A) \vee r{:}(\neg x{:}A)$. And a disjunction property would give $\vdash x{:}p$ or $\vdash \neg x{:}p$. Which is clearly absurd.

Interesting enough, the scheme 3 also pops-up when studying realizations in LPS4.

References

[AB04] Sergei N. Artemov and Lev D. Beklemishev. Provability logic. In D. Gabbay and F. Guenthner, editors, *Handbook of Philosophical Logic*, volume 13, pages 229–403. Kluwer, 2nd edition, 2004.

[AN04] S. Artemov and E. Nogina. Logic of knowledge with justifications from the provability perspective. Technical Report TR-2004011, CUNY Ph.D. Program in Computer Science, 2004.

[Art95] Sergei N. Artemov. Operational modal logic. Technical Report MSI 95-29, Cornell University, 1995.

[Art01] Sergei N. Artemov. Explicit provability and constructive semantics. *Bulletin of Symbolic Logic*, 7(1):1–36, 2001.

[AS92] Sergei Artëmov and Tyko Straßen. The basic logic of proofs. In E. Börger and G. Jäger and H. Kleine Büning and S. Martini and M.M. Richter, editor, *Computer Science Logic. 6th Workshop, CSL'92. San Miniato, Italy, September/October 1992. Selected Papers*, volume 702 of *Lecture Notes in Computer Science*, pages 14–28. Springer-Verlag, 1992.

[BdRV01] P. Blackburn, M. de Rijke, and Y. Venema. *Modal logic*. Cambridge University Press, New York, NY, USA, 2001.

[Boo93] G. Boolos. *The Logic of Provability*. Cambridge University Press, Cambridge, 1993.

[Gor05] Evan Goris. Logic of Proofs for bounded arithmetic. Technical Report TR-2005011, CUNY Ph.D. Program in Computer Science, 2005.

[Kru03] N. Krupski. On the complexity of the reflected logic of proofs. Technical Report TR-2003007, CUNY Ph.D. Program in Computer Science, 2003.

[Nog06] E. Nogina. On Logic of Proofs and Provability. *Bulletin of Symbolic Logic*, 12, 2006. in: *2005 Summer Meeting of the ASL*.

[Sch86] George F. Schumm. Some failures of interpolation on modal logic. *Notre Dame Journal of Formal Logic*, 27(1):108–110, 1986.

[Seg72] K. Segerberg. Post completeness in modal logic. *Journal of Symbolic Logic*, 37:711–715, 1972.

[Sol76] R. M. Solovay. Provability Interpretations of Modal Logic. *Israel Journal of Mathematics*, 25:287–304, 1976.

[Yav02] T. Yavorskaya. Logic of Proofs and Provability. *Annals of Pure and Applied Logic*, 113(1–3):345–372, 2002.