2003

TR-2003012: A Semantics for the Logic of Proofs

Melvin Fitting

A Semantics for the Logic of Proofs

Melvin Fitting
Dept. Mathematics and Computer Science
Lehman College (CUNY), 250 Bedford Park Boulevard West
Bronx, NY 10468-1589
e-mail: fitting@lehman.cuny.edu
web page: comet.lehman.cuny.edu/fitting

September 19, 2003

1 Introduction

The intention of the present report is to provide a Kripke-style semantics for Artemov's Logic of Proofs, **LP**, [1, 2]. Of course additional machinery must be added to that which is standard in Kri[pke semantics. It takes the form of what we might call, informally, *possible justification*, or *possible evidence*. To take an intuitive example, what might serve as possible evidence for the statement, "George Bush is editor of the New York Times?" Clearly the editorial page of any copy of the New York Times would serve, while no page of Mad Magazine would do (although the magazine might very well contain the claim that George Bush does edit the Times). Note that possible evidence need not be evidence of a fact. Nor need it be decisive—it could happen that the New York Times decides to omit its editor's name. Nonetheless, what the Times prints on this subject would count as evidence, and what Mad prints would not. It is this notion of possible evidence that will be added to standard Kripke machinery, to produce a sound and strongly complete semantics for **LP**. I will also use this semantics to provide alternative proofs of two well-known results concerning **LP**.

2 Background

This report, in a sense, continues a previous technical report, "A Semantic Proof of the Realizability of Modal Logic in the Logic of Proofs," [3]. A certain amount of background material is duplicated from that report.

Proof polynomials are built from variables and constants by three operations "$\cdot$" (application), "!" (proof checker), and "+" (union), where proof checker is a unary operation and application and union are binary ones. Under the standard provability interpretation, proof polynomials denote the obvious computable operations on proofs.

The axioms and rules of **LP** are:

A0.	*classical axioms*	
A1.	$t{:}(F \supset G) \supset (s{:}F \supset (t\cdot s){:}G)$	*(application)*
A2.	$t{:}F \supset F$	*(explicit reflexivity)*
A3.	$t{:}F \supset\ !t{:}(t{:}F)$	*(proof checker)*
A4.	$s{:}F \supset (s+t){:}F, \quad t{:}F \supset (s+t){:}F$	*(sum, or union)*
R1.	*Modus Ponens*	
R2.	$\vdash c{:}A$, *where* $A \in$ *A0-A4,* *c is any proof constant.*	*(axiom necessitation)*

There is an analogue of the Necessitation Rule

$$\frac{\vdash F}{\vdash \Box F}$$

in **LP**. It has the form of an admissible rule of Explicit Necessitation ([1, 2]):

$$\frac{\vdash F}{\vdash p{:}F} \quad \textit{for some proof polynomial } p.$$

Rule *R2* needs some comment. A *constant specification* is a mapping from axioms to constants. It is *injective* if it is $1-1$. A proof using *R2* determines a constant specification—map axioms used in the proof to the constants assigned by *R2* applications, and axioms not used to arbitrary constants. Conversely, we can start with a constant specification, and insist that applications of *R2* introduce constants into proofs according to it. I will show soundness and completeness relative to an arbitrary constant specification.

The Logic of Proofs is an explicit version of **S4**: the "forgetful" projection of **LP**, where $t{:}F$ is systematically replaced by $\Box F$, coincides with **S4** ([2], Lemma 9.1). The key property of **LP** is its ability to emulate the whole of **S4**, the Realizability Theorem (Theorem 9.4 from [2]). This theorem states that if **S4** derives F then one can find an assignment r of proof polynomials to the $\Box$'s of F in such a way that the resulting formula F^r is derivable in **LP**. Artemov's proof of the Realization Theorem goes through cut-elimination for **S4**, which puts serious limits on finding explicit counterparts for other modal logics, since many of them do not enjoy cut-elimination. An alternative, semantic-based, proof was given in [3]. One of Artemov's problems (number 1 from the list of problems posted on `http://www.cs.gc.cuny.edu/~sartemov`) asks for a semantics for **LP**. The semantics presented here evolved out of the work in [3].

Any terminology or results not included here can be found in [2].

3 Presentation of an LP Semantics

Let C be a constant specification, an assignment of a proof constant to each axiom, *A0* - *A4*. Since this can be arbitrary, whether $c{:}X$ is provable or not, where c is a specific constant and X is an axiom, depends on C. Consequently the semantics will be relative to constant specification C.

$\mathcal{F} = \langle \mathcal{G}, \mathcal{R} \rangle$ is a *frame* in the usual sense, where $\mathcal{G}$ is a set of states and $\mathcal{R}$ is a binary relation on $\mathcal{G}$. It is assumed that $\mathcal{R}$ is reflexive and transitive, hence $\mathcal{F}$ is a frame for **S4**.

I next want to introduce a formal version of possible evidence. Now, if t is a proof polynomial and Γ is a state, intuitively t can serve as evidence for certain assertions in state Γ, and not for other assertions. Consequently we can identify the 'possible evidence' supplied by t at Γ with a set of formulas. Of course such a set must meet certain conditions—these will be given below.

Given a frame $\mathcal{F} = \langle \mathcal{G}, \mathcal{R} \rangle$, a *possible evidence* function $\mathcal{E}$ is a mapping from states and proof polynomials to sets of formulas. We can read $X \in \mathcal{E}(\Gamma, t)$ as "t is possible evidence for X in state Γ." Before stating the conditions the evidence function must satisfy, I need to introduce a few operations on formula sets.

1. If S and T are sets of formulas, $S \cdot T = \{Y \mid X \supset Y \in S \text{ and } X \in T \text{ for some formula } X\}$
2. If S is a set of formulas and $!t$ is a proof polynomial, $(!t)S = \{t{:}X \mid X \in S\}$

Now, here are the conditions that must be met by evidence function $\mathcal{E}$:

Monotonicity For each proof polynomial t, and for all $\Gamma, \Delta \in \mathcal{G}$,
$\Gamma \mathcal{R} \Delta$ implies $\mathcal{E}(\Gamma, t) \subseteq \mathcal{E}(\Delta, t)$

Constant Condition For each formula X, with $C(X) = c$,
$X \in \mathcal{E}(\Gamma, c)$, for each $\Gamma \in \mathcal{G}$.

Application For all proof polynomials s, t, and for each $\Gamma \in \mathcal{G}$,
$\mathcal{E}(\Gamma, s) \cdot \mathcal{E}(\Gamma, t) \subseteq \mathcal{E}(\Gamma, s \cdot t)$.

Proof Checker For each proof polynomial t, and for each $\Gamma \in \mathcal{G}$,
$(!t)\mathcal{E}(\Gamma, t) \subseteq \mathcal{E}(\Gamma, !t)$.

Sum For all proof polynomials s, t, and for each $\Gamma \in \mathcal{G}$,
$\mathcal{E}(\Gamma, s) \cup \mathcal{E}(\Gamma, t) \subseteq \mathcal{E}(\Gamma, s + t)$.

As usual, a forcing relation $\Vdash$ between states and formulas is introduced. At the atomic level, it is specified arbitrarily—this is part of the definition of a particular model. Then it is extended to arbitrary formulas according to the following rules. For each $\Gamma \in \mathcal{G}$:

1. $\Gamma \Vdash \bot$ never holds—written $\Gamma \nVdash \bot$.

2. $\Gamma \Vdash (X \supset Y)$ if and only if $\Gamma \nVdash X$ or $\Gamma \Vdash Y$.

3. $\Gamma \Vdash (t{:}X)$ if and only if $X \in \mathcal{E}(\Gamma, t)$ and, for every $\Delta \in \mathcal{G}$ with $\Gamma\mathcal{R}\Delta$, $\Delta \Vdash X$.

Item 3 above intuitively says, we have $t : X$ at a state provided X is necessarily the case at that state, and t can serve as possible evidence for X at that state.

Soundness and completeness can be shown for axiomatic **LP** relative to the semantics above. But with the same effort, it can be shown for a more restricted class of models, and this turns out to be of particular use. So, call models defined as above *weak* models for **LP**. The additional condition I want to impose might be summarized as "whatever must be so, must be so for a reason." The requirement is that of being

Fully Explanatory If $\Delta \Vdash X$ for every $\Delta \in \mathcal{G}$ such that $\Gamma\mathcal{R}\Delta$, then for some proof polynomial t we have $\Gamma \Vdash (t{:}X)$.

If the Fully Explanatory condition is also met, I say $\mathcal{M} = \langle \mathcal{G}, \mathcal{R}, \mathcal{E}, \Vdash \rangle$ is an **LP**-*model*. If it is necessary to be absolutely precise, it is a model relative to the constant specification C.

4 Soundness

The methodology for proving axiomatic soundness is the usual one—verify validity of the axioms, and show the rules preserve validity. I'll consider two axioms as representative.

First consider an application axiom—validity arguments for most other axioms follow a similar pattern. Suppose $\mathcal{M} = \langle \mathcal{G}, \mathcal{R}, \mathcal{E}, \Vdash \rangle$ is an **LP**-model,

$\Gamma \in \mathcal{G}$, and $\Gamma \Vdash t{:}(F \supset G)$ and $\Gamma \Vdash s{:}F$. It must be shown that $\Gamma \Vdash (t \cdot s){:}G$. Let $\Delta \in \mathcal{G}$ be an arbitrary state with $\Gamma \mathcal{R} \Delta$. Since $\Gamma \Vdash t{:}(F \supset G)$, $\Delta \Vdash (F \supset G)$, and $(F \supset G) \in \mathcal{E}(\Gamma, t)$. Likewise since $\Gamma \Vdash s{:}F$, $\Delta \Vdash F$ and $F \in \mathcal{E}(\Gamma, s)$. Then $\Delta \Vdash G$, of course. Also, $G \in \mathcal{E}(\Gamma, t) \cdot \mathcal{E}(\Gamma, s) \subseteq \mathcal{E}(\Gamma, t \cdot s)$, by the Application Condition on models. It follows that $\Gamma \Vdash (t \cdot s){:}G$.

Next, an intermediate result. I'll show that if $\Gamma \Vdash t{:}X$ and $\Gamma \mathcal{R} \Delta$, then $\Delta \Vdash t{:}X$ too. So, suppose $\Gamma \Vdash t{:}X$ and $\Gamma \mathcal{R} \Delta$. Let $\Omega \in \mathcal{G}$ be an arbitrary state such that $\Delta \mathcal{R} \Omega$. Since $\mathcal{R}$ is transitive, $\Gamma \mathcal{R} \Omega$, and so $\Omega \Vdash X$. Also, $X \in \mathcal{E}(\Gamma, t)$ so by the Monotonicity Condition for $\mathcal{E}$, $X \in \mathcal{E}(\Delta, t)$. It follows that $\Delta \Vdash t{:}X$.

Now I'll show the validity of a proof checker axiom, which needs the result just shown. Suppose $\Gamma \in \mathcal{G}$ and $\Gamma \Vdash t{:}X$. I'll show $\Gamma \Vdash !t{:}t{:}X$. Well, since $\Gamma \Vdash t{:}X$, $X \in \mathcal{E}(\Gamma, t)$, and hence $t{:}X \in (!t)\mathcal{E}(\Gamma, t) \subseteq \mathcal{E}(\Gamma, !t)$, using the Proof Checker condition on models. Also, by the previous paragraph $t{:}X$ is forced at every world accessible from Γ. It follows that $\Gamma \Vdash !t{:}t{:}X$.

We have assumed a constant specification C, and I'm assuming $\mathcal{M}$ is an **LP** model relative to C. If X is an axiom, we have now established that X is forced at each state of $\mathcal{M}$. If $\Gamma \in \mathcal{G}$, and $C(X) = c$, by the Constant Condition on models, $X \in \mathcal{E}(\Gamma, c)$. Also X is forced at every world accessible from Γ, so $\Gamma \Vdash c{:}X$.

The only other rule is modus ponens, and it is trivial that it preserves validity.

Note that we did not use the Fully Explanatory condition in this section.

5 Completeness

Completeness proceeds by a canonical model argument, adapted to **LP**. As above, a constant specification C is assumed fixed both for proofs and for the semantics, and it is used throughout what follows.

Call a set S of **LP** formulas *inconsistent* if there is some finite subset $\{X_1, \ldots, X_n\} \subseteq S$ such that $(X_1 \wedge \ldots \wedge X_n) \supset \bot$ is a theorem of **LP**. Call S *consistent* if it is not inconsistent. Let $\mathcal{G}$ be the set of all maximally consistent sets of **LP** formulas. If $\Gamma \in \mathcal{G}$, let $\Gamma^{\#} = \{X \mid (t{:}X) \in \Gamma, \text{ for some } t\}$, and set $\Gamma \mathcal{R} \Delta$ if $\Gamma^{\#} \subseteq \Delta$. This gives us a frame, $\langle \mathcal{G}, \mathcal{R} \rangle$. The 'explicit reflexivity' axiom scheme of **LP** implies the frame is reflexive, and the 'proof checker' axiom scheme implies it is transitive. Define a mapping $\mathcal{E}$ by setting $\mathcal{E}(\Gamma, t) = \{X \mid t{:}X \in \Gamma\}$. Finally, define a forcing relation by specifying that for an atomic formula P, $\Gamma \Vdash P$ if and only if $P \in \Gamma$. This gives us a structure $\mathcal{M} = \langle \mathcal{G}, \mathcal{R}, \mathcal{E}, \Vdash \rangle$.

First I show $\mathcal{M}$ is a weak **LP** model. I'll verify two of the conditions on the evidence function $\mathcal{E}$—other conditions are similar. To begin, I'll verify the Application Condition: for each $\Gamma \in \mathcal{G}$, $\mathcal{E}(\Gamma, s) \cdot \mathcal{E}(\Gamma, t) \subseteq \mathcal{E}(\Gamma, s \cdot t)$. Suppose $Y \in \mathcal{E}(\Gamma, s) \cdot \mathcal{E}(\Gamma, t)$. Then for some X we have $X \in \mathcal{E}(\Gamma, t)$ and $(X \supset Y) \in \mathcal{E}(\Gamma, s)$. By the present definition of $\mathcal{E}$, we must have $t{:}X \in \Gamma$ and $s{:}(X \supset Y) \in \Gamma$. Since $s{:}(X \supset Y) \supset (t{:}X \supset (s \cdot t){:}Y)$ is an **LP** axiom, and Γ is maximally consistent, it follows that $(s \cdot t){:}Y \in \Gamma$, and hence $Y \in \mathcal{E}(\Gamma, s \cdot t)$.

Next, I'll verify the Monotonicity Condition. Suppose $\Gamma, \Delta \in \mathcal{G}$ and $\Gamma\mathcal{R}\Delta$. Also assume $X \in \mathcal{E}(\Gamma, t)$. By definition of $\mathcal{E}$, we have $t{:}X \in \Gamma$. Since $t{:}X \supset !t{:}t{:}X$ is an **LP** axiom, we have $!t{:}t{:}X \in \Gamma$, and hence $t{:}X \in \Gamma^{\#}$. Since $\Gamma\mathcal{R}\Delta$ we have $\Gamma^{\#} \subseteq \Delta$, so $t{:}X \in \Delta$, and so $X \in \mathcal{E}(\Delta, t)$.

Other conditions are similar. Thus $\mathcal{M}$ is a weak **LP** model.

Now a Truth Lemma can be shown: for each formula X and each $\Gamma \in \mathcal{G}$

$$X \in \Gamma \Longleftrightarrow \Gamma \Vdash X.$$

Most of the cases are as usual. I'll verify only the modal one. Suppose the result is known for X, and we are considering the formula $t{:}X$.

Suppose first that $t{:}X \in \Gamma$. Then $X \in \Gamma^{\#}$, so if Δ is an arbitrary member of $\mathcal{G}$ with $\Gamma\mathcal{R}\Delta$, we have $\Gamma^{\#} \subseteq \Delta$ and hence $X \in \Delta$. By the induction hypothesis, $\Delta \Vdash X$. Also since $t{:}X \in \Gamma$, we have $X \in \mathcal{E}(\Gamma, t)$. It follows that $\Gamma \Vdash t{:}X$.

Next, suppose $\Gamma \Vdash t{:}X$. This case is trivial. By the present definition of $\Vdash$ we must have $X \in \mathcal{E}(\Gamma, t)$, and by definition of $\mathcal{E}$, we must also have $t{:}X \in \Gamma$.

Thus we have the Truth Lemma. At this point a completeness result relative to weak **LP** models has been established. But in fact $\mathcal{M}$ is a model, and not just a weak one. I show this next.

Suppose $\Gamma \in \mathcal{G}$ and, for every $\Delta \in \mathcal{G}$ with $\Gamma\mathcal{R}\Delta$ we have $\Delta \Vdash X$. I'll show $\Gamma \Vdash t{:}X$ for some t. Well, suppose not. Then for each proof polynomial t, $\Gamma \Vdash \neg(t{:}X)$ and so, by the Truth Lemma, $\neg(t{:}X) \in \Gamma$ for each t.

The key item to show is that $\Gamma^{\#} \cup \{\neg X\}$ is consistent. For then we can extend it to a maximal consistent set Δ. By definition, $\Gamma\mathcal{R}\Delta$, and by the Truth Lemma, $\Delta \not\Vdash X$, contradicting the assumption. So I now concentrate on showing this key item.

Suppose $\Gamma^{\#} \cup \{\neg X\}$ is not consistent. Then for some $Y_1, \ldots, Y_k \in \Gamma^{\#}$, **LP** proves $(Y_1 \wedge \ldots \wedge Y_k \wedge \neg X) \supset \bot$, and hence **LP** also proves $(Y_1 \wedge \ldots \wedge Y_k) \supset X$. For each $i = 1, \ldots, k$, since $Y_i \in \Gamma^{\#}$, there is some proof polynomial s_i such that $s_i{:}Y_i \in \Gamma$. Using the Lifting Lemma (5.4 in [2]) and the Substitution

Lemma, there is a proof polynomial t such that **LP** proves $(s_1{:}Y_1 \wedge \ldots \wedge s_k{:}Y_k) \supset t(s_1, \ldots, s_k){:}X$. Hence $t(s_1, \ldots, s_k){:}X \in \Gamma$, but this contradicts the original assumption that $\neg t{:}X \in \Gamma$ for each t.

Thus $\mathcal{M}$ is an **LP** model. Now strong completeness follows as usual: if S is consistent it is satisfiable. Extend S to a maximal consistent set Γ, $\Gamma \in \mathcal{G}$ and, using the Truth Lemma, $\Gamma \Vdash X$ for every $X \in \Gamma$, and hence S is satisfied at Γ. Ordinary completeness is immediate. If X is not provable, $\{\neg X\}$ is consistent, hence satisfiable, hence X is not valid.

6 Two Additional Results

In this section I use the semantics just introduced to give new proofs of two results of Artemov, one simple, the other a bit more complex.

Suppose $\langle \mathcal{G}, \mathcal{R}, \Vdash \rangle$ is an **S4** model—$\mathcal{R}$ is reflexive and transitive—and $\Vdash$ is defined for atoms. Define a mapping $\mathcal{E}$ by setting $\mathcal{E}(\Gamma, t)$ to be the entire set of **LP** formulas, for every $\Gamma \in \mathcal{G}$ and every proof polynomial t. It is easy to check that this makes $\langle \mathcal{G}, \mathcal{R}, \mathcal{E}, \Vdash \rangle$ into an **LP** model with respect to any constant specification (not just a weak model). Following notation of [2], if Y is a formula of **LP**, then Y° is the monomodal formula that results by replacing each subformula of the form $t{:}Z$ with $\Box Z$. It is easy to check that for each **LP** formula X, and for each $\Gamma \in \mathcal{G}$, $\Gamma \Vdash X$ in the **LP** model $\langle \mathcal{G}, \mathcal{R}, \mathcal{E}, \Vdash \rangle$ if and only if $\Gamma \Vdash X^\circ$ in the **S4** model $\langle \mathcal{G}, \mathcal{R}, \Vdash \rangle$. (The definition of $\Vdash$ is the same at the atomic level in the **S4** and **LP** models, but the extension to all formulas differs, because of the different languages involved.)

Theorem 6.1 *If X is a theorem of **LP**, then X° is a theorem of* **S4**.

Proof If X is a theorem of **LP**, then X is valid in all **LP** models, hence in all models converted from **S4** models, as outlined above. Since all **S4** models convert to **LP** models, it follows that X° is valid in all **S4** models, and hence X° is a theorem of **S4**. ■

Note that the argument above did not need that the models converted from **S4** models are **LP** models—that they are weak **LP** models is enough. The next result needs the stronger version.

Theorem 6.2 *Suppose X is an **LP** theorem. Then for some proof polynomial t, $t{:}X$ is also an **LP** theorem.*

Proof Suppose X is an **LP** theorem, and hence valid in all **LP** models. Also suppose that, for no proof polynomial t is $t{:}X$ provable. I show this leads to a contradiction.

First, I claim the set $\{\neg t_1{:}X, \neg t_2{:}X, \ldots\}$ is consistent, where $\{t_1, t_2, \ldots\}$ is the set of all proof polynomials. The argument is as follows. If the set were not consistent, there would be a finite subset $\{\neg t_{i_1}{:}X, \ldots, \neg t_{i_k}{:}X\}$ such that $(\neg t_{i_1}{:}X \wedge \ldots \wedge \neg t_{i_k}{:}X) \supset \bot$ is an **LP** theorem. Then $t_{i_1}{:}X \vee \ldots \vee t_{i_k}{:}X$ would be an **LP** theorem. It follows by using the Sum axiom that $(t_{i_1} + \ldots + t_{i_k}){:}X$ would also be an **LP** theorem, but this contradicts the assumption that for no proof polynomial t is $t{:}X$ provable.

Since the set $\{\neg t_1{:}X, \neg t_2{:}X, \ldots\}$ is consistent, there is an **LP** model in which it is satisfiable. Say that in $\langle \mathcal{G}, \mathcal{R}, \mathcal{E}, \Vdash \rangle$, for $\Gamma \in \mathcal{G}$, $\Gamma \nVdash t_i{:}X$ for each proof polynomial t_i. But since our assumption is that X is valid, for every $\Delta \in \mathcal{G}$ with $\Gamma \mathcal{R} \Delta$ we have $\Delta \Vdash X$. Then the Fully Explanatory condition says we must have $\Gamma \Vdash t{:}X$ for some proof polynomial t, and this is our contradiction. ■

References

[1] S. Artemov, "Operational Modal Logic," *Tech. Rep. MSI 95-29*, Cornell University, December 1995.

[2] S. Artemov, "Explicit provability and constructive semantics", The *Bulletin for Symbolic Logic*, v.7, No. 1, pp. 1-36, 2001 `http://www.cs.gc.cuny.edu/~sartemov/publications/BSL.ps`.

[3] M. Fitting, "A semantic proof of the realizability of modal logic in the logic of proofs", *Tech. Rep. TR-2003010*, `http://www.cs.gc.cuny.edu/tr/`, City University of New York, September 2003.