2003

TR-2003010: A Semantic Proof of the Realizability of Modal Logic in the Logic of Proofs

Melvin Fitting

A Semantic Proof of the Realizability of Modal Logic in 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 11, 2003

1 Introduction

The Logic of Proofs (**LP**) was introduced by Sergei Artemov in [1, 2] and answered a long standing question about the intended provability semantics for the modal logic **S4** and for intuitionistic propositional logic. In addition to classical propositional logic, **LP** contains new atoms of sort $t:F$, where F is a formula and t is a special proof term called a *proof polynomial*. The intended semantics of $t:F$ is *t is a proof of F*, and was formalized in [1, 2].

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]):

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

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** (actually, this is a weak version of the full result, which will be stated properly below). 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. One of Artemov's problems (number 14 from the list of problems posted on `http://www.cs.gc.cuny.edu/~sartemov`) asks for a proof of the realization theorem which does not depend on cut-elimination for **S4**.

In this paper I offer an alternative semantical proof of the Realization Theorem which does not rely on cut-free derivations thus solving the above problem. In addition, the proof presented here clarifies the role of the operation "+" in the realization of modal logic. I show that there is a realization of **S4** into the "+"-free fragment $\mathbf{LP}^-$ of **LP**, which then can be transformed into Artemov's realization by a limited use of "+" axioms of **LP**.

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

2 Statement of Results

Let φ be a monomodal formula, *fixed for the rest of this report*. I will make use of φ and its subformulas, but by subformula I mean subformula *occurrence*. Strictly speaking, I should be working with a parse tree for φ, but I am attempting to keep terminology as simple as possible. So in the following, for 'subformula' read 'subformula occurrence.'

Let A be an assignment of a proof polynomial variable to each subformula of φ of the form $\Box X$ that is in a negative position. I will assume that A

assigns different variables to different subformulas—this plays a role in the proof of Proposition 5.1. First, I define a mapping w_A, which was used in Artemov's Realization Theorem.

w_A assigns a set of **LP** formulas to each subformula of φ, as follows.

1. If P is an atomic subformula of φ, $w_A(P) = \{P\}$ (this includes the case that P is $\bot$).

2. If $X \supset Y$ is a subformula of φ, $w_A(X \supset Y) = \{X' \supset Y' \mid X' \in w_A(X)$ and $Y' \in w_A(Y)\}$.

3. If $\Box X$ is a negative subformula of φ, $w_A(\Box X) = \{x : X' \mid A(\Box X) = x$ and $X' \in w_A(X)\}$.

4. If $\Box X$ is a positive subformula of φ, $w_A(\Box X) = \{t : X' \mid X' \in w_A(X)$ and t is any proof polynomial$\}$.

I also define a similar mapping v_A from subformulas of φ to sets of **LP** formulas. Its definition is the same as that for w_A except for item 4, which reads as follows:

4. If $\Box X$ is a positive subformula of φ, $v_A(\Box X) = \{t : (X_1 \vee \ldots \vee X_n) \mid X_1, \ldots, X_n \in v_A(X)$ and t is any proof polynomial$\}$.

By $\mathbf{LP}^-$ I mean **LP** without the 'sum' axioms.

Theorem 2.1 *φ is a theorem of* **S4** *if and only if there are $\varphi_1, \ldots, \varphi_n \in v_A(\varphi)$ such that $\varphi_1 \vee \ldots \vee \varphi_n$ is a theorem of* $\boldsymbol{LP}^-$.

Theorem 2.2 *φ is a theorem of* **S4** *if and only if there is some $\varphi' \in w_A(\varphi)$ such that φ' is a theorem of* ***LP***. *(This is Corollary 9.5 from [2].)*

Both of the theorems above are actually shown in a stronger form than is stated. Proofs in $\mathbf{LP}^-$ and **LP** can be taken to be *injective*, meaning that each constant introduced by rule *R2* is unique—no proof constant serves to 'justify' more than one axiom. It is this stronger form of Theorem 2.2 that is proved in [2].

3 First Part of Proof

Following [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 $\Box Z$.

Lemma 3.1 *Let X be a subformula of φ, and let $Y \in v_A(X)$. Then $Y^\circ \equiv X$ is a theorem of* **S4**. *(In fact, the primary tool needed is the formula scheme $(A \vee A) \equiv A$.)*

Proof A straightforward induction on the degree of X. ■

Now it is easy to see (induction on proof length) that the forgetful projection, replacing $t : X$ by $\Box X$, turns an $\mathbf{LP}^-$ proof into a correct **S4** proof. This, and a little more work, gives us half of Theorem 2.1.

Proposition 3.2 *If there are $\varphi_1, \ldots, \varphi_n \in v_A(\varphi)$ such that $\varphi_1 \vee \ldots \vee \varphi_n$ is a theorem of $\boldsymbol{LP}^-$, then φ is a theorem of* **S4**.

Proof Using the observation above, provability of $\varphi_1 \vee \ldots \vee \varphi_n$ in $\mathbf{LP}^-$ implies provability of $\varphi_1^\circ \vee \ldots \vee \varphi_n^\circ$ in **S4**, and by the Lemma, this implies provability of φ in **S4**. ■

4 Second Part of Proof

This Section is devoted to showing that if φ is provable in **S4**, then $\varphi_1 \vee \ldots \vee \varphi_n$ is provable in $\mathbf{LP}^-$ for some $\varphi_1, \ldots, \varphi_n \in v_A(\varphi)$.

Once and for all, let us select a *constant specification* that is injective, that is, a $1-1$ assignment of a proof constant to each axiom of $\mathbf{LP}^-$. When rule *R2* is applied in a proof, adding $c : A$ where A is an axiom, it is assumed that c is the constant associated with A by this constant specification.

Call a set S of $\mathbf{LP}^-$ 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 $\mathbf{LP}^-$. Call S *consistent* if it is not inconsistent. Let $\mathcal{G}$ be the set of all maximally consistent sets of $\mathbf{LP}^-$ 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 $\mathbf{LP}^-$ implies the frame is reflexive, and the 'proof checker' axiom scheme implies it is transitive, hence it is an **S4** frame. Finally, define a forcing relation by specifying it at the atomic level: $\Gamma \Vdash P$ if and only if $P \in \Gamma$. This gives us an **S4** model $\mathcal{M} = \langle \mathcal{G}, \mathcal{R}, \Vdash \rangle$.

If X is a subformula of φ I will write $\neg v_A(X)$ for $\{\neg X' \mid X' \in v_A(X)\}$. Note that $\neg v_A(X)$ is very different in meaning from $v_A(\neg X)$.

Proposition 4.1 *In the* **S4** *model $\mathcal{M} = \langle \mathcal{G}, \mathcal{R}, \Vdash \rangle$, for each $\Gamma \in \mathcal{G}$:*

1. *If ψ is a positive subformula of φ and $\neg v_A(\psi) \subseteq \Gamma$ then $\Gamma \not\Vdash \psi$.*

2. *If ψ is a negative subformula of φ and $v_A(\psi) \subseteq \Gamma$ then $\Gamma \Vdash \psi$.*

Proof The proof, of course, is by induction on the complexity of ψ. The atomic case is trivial. I will cover the remaining cases in detail.

Positive Implication Suppose ψ is $(X \supset Y)$, ψ is a positive subformula of φ, $\neg v_A(X \supset Y) \subseteq \Gamma$, and the result is known for X and Y. Note that X occurs negatively in φ and Y occurs positively.

Let X' be an arbitrary member of $v_A(X)$, and Y' be an arbitrary member of $v_A(Y)$. Then $\neg(X' \supset Y') \in \neg v_A(X \supset Y)$. Since $\neg(X' \supset Y') \in \Gamma$, and Γ is maximally consistent, $X' \in \Gamma$ and $\neg Y' \in \Gamma$. Since X' and Y' were arbitrary, it follows that $v_A(X) \subseteq \Gamma$ and $\neg v_A(Y) \subseteq \Gamma$. Then by the induction hypothesis, $\Gamma \Vdash X$ and $\Gamma \nVdash Y$, hence $\Gamma \nVdash (X \supset Y)$.

Negative Implication Suppose ψ is $(X \supset Y)$, ψ is a negative subformula of φ, $v_A(X \supset Y) \subseteq \Gamma$, and the result is known for X and Y. In this case, X occurs positively in φ and Y occurs negatively.

If $\neg v_A(X) \subseteq \Gamma$, by the induction hypothesis $\Gamma \nVdash X$, and hence $\Gamma \Vdash (X \supset Y)$. So now suppose $\neg v_A(X) \not\subseteq \Gamma$. Then for some $X' \in v_A(X)$, $\neg X' \notin \Gamma$, hence by the maximal consistency of Γ, $X' \in \Gamma$. Now, let Y' be an arbitrary member of $v_A(Y)$. Then $(X' \supset Y') \in v_A(X \supset Y)$, hence $(X' \supset Y') \in \Gamma$. Since $X' \in \Gamma$, again by maximal consistency, $Y' \in \Gamma$. Since Y' was arbitrary, we have that $v_A(Y) \subseteq \Gamma$, so by the induction hypothesis, $\Gamma \Vdash Y$, and again $\Gamma \Vdash (X \supset Y)$.

Positive Necessity Suppose ψ is $\Box X$, ψ is a positive subformula of φ, $\neg v_A(\Box X) \subseteq \Gamma$, and the result is known for X (which also occurs positively in φ).

The key item to show is that $\Gamma^{\#} \cup \neg v_A(X)$ is consistent. For then we can extend it to a maximal consistent set Δ. By definition, $\Gamma \mathcal{R} \Delta$, and by the induction hypothesis, $\Delta \nVdash X$, hence $\Gamma \nVdash \Box X$. So I now concentrate on showing this key item.

Suppose $\Gamma^{\#} \cup \neg v_A(X)$ is not consistent. Then for some $Y_1, \ldots, Y_k \in \Gamma^{\#}$ and $X_1, \ldots, X_n \in v_A(X)$, $\mathbf{LP}^-$ proves $(Y_1 \wedge \ldots \wedge Y_k \wedge \neg X_1 \wedge \ldots \wedge \neg X_n) \supset \bot$, and hence $\mathbf{LP}^-$ also proves $(Y_1 \wedge \ldots \wedge Y_k) \supset (X_1 \vee \ldots \vee X_n)$. 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 analog of the Lifting Lemma (5.4 in [2]) and the Substitution Lemma, there is a proof polynomial t such that $\mathbf{LP}^-$ proves $(s_1 : Y_1 \wedge \ldots \wedge s_k : Y_k) \supset t(s_1, \ldots, s_k) : (X_1 \vee \ldots \vee X_n)$. Hence

$t(s_1, \ldots, s_k) : (X_1 \vee \ldots \vee X_n) \in \Gamma$, but this contradicts the original assumption that $\neg v_A(\Box X) \subseteq \Gamma$.

Negative Necessity Suppose ψ is $\Box X$, ψ is a negative subformula of φ, $v_A(\Box X) \subseteq \Gamma$, and the result is known for X (which also occurs negatively in φ).

Let X' be an arbitrary member of $v_A(X)$. Since $\Box X$ is a negative subformula of φ, $x : X' \in v_A(\Box X)$, where $x = A(\Box X)$. Hence $(x : X') \in \Gamma$. Now if Δ is an arbitrary member of $\mathcal{G}$ with $\Gamma \mathcal{R} \Delta$, by definition $\Gamma^{\#} \subseteq \Delta$, hence $X' \in \Delta$. Thus $v_A(X) \subseteq \Delta$, so by the induction hypothesis, $\Delta \Vdash X$. Since Δ was arbitrary, $\Gamma \Vdash \Box X$.

■

Proposition 4.2 *If, for every $\varphi_1, \ldots, \varphi_n \in v_A(\varphi)$, it is the case that $\varphi_1 \vee \ldots \vee \varphi_n$ is not a theorem of **LP**$^-$, then φ is not a theorem of* **S4**.

Proof Assume $\varphi_1 \vee \ldots \vee \varphi_n$ is not a theorem of **LP**$^-$ for every $\varphi_1, \ldots, \varphi_n \in v_A(\varphi)$. It follows that $\neg v_A(\varphi)$ is consistent. For otherwise there would be $\varphi_1, \ldots, \varphi_n \in v_A(\varphi)$ such that $(\neg\varphi_1 \wedge \ldots \wedge \neg\varphi_n) \supset \perp$ would be a theorem of **LP**$^-$, and hence so would $\varphi_1 \vee \ldots \vee \varphi_n$, contrary to assumption. Since $\neg v_A(\varphi)$ is consistent, extend it to a maximal consistent set Γ. $\Gamma \in \mathcal{G}$ and so, by the previous Proposition, $\Gamma \nVdash \varphi$, hence φ is not a theorem of **S4**. ■

5 Third Part of Proof

Half of Theorem 2.2 has an easy proof. If $\varphi' \in w_A(\varphi)$, and φ' has an **LP** proof, replacing each modality t : by $\Box$ throughout the proof converts it to a proof in **S4** of φ. It is the converse half that is difficult. In this section I provide a new proof for this.

A *substitution* is a mapping from a finite set of proof polynomial variables to proof polynomials. I denote the substitution that maps each x_i to t_i, $i = 1, \ldots, k$, by $\{x_1/t_1, \ldots, x_k/t_k\}$; it has *domain* $\{x_1, \ldots, x_n\}$. I will generally use σ, with and without subscripts, for substitutions. I will denote the result of applying the substitution σ to the **LP** formula Z by $Z\sigma$. If σ_1 and σ_2 are substitutions whose domains do not overlap, then $\sigma_1 \cup \sigma_2$ is again a substitution. Recall that I required the assignment A of variables to negative necessity subformulas of φ to associate distinct variables to different subformulas. Consequently, if X and Y are different subformulas of φ, and $X' \in v_A(X)$ and $Y' \in v_A(Y)$, and $\sigma_{X'}$ and $\sigma_{Y'}$ are substitutions whose domains are the variables of X' and Y' respectively, $\sigma_{X'}$ and $\sigma_{Y'}$ have non-overlapping domains, and hence $\sigma_{X'} \cup \sigma_{Y'}$ is again a substitution. This plays a role in the proof of the Proposition that follows.

Proposition 5.1 *For every ψ that is a subformula of φ, and for each ψ_1, …, $\psi_n \in v_A(\psi)$, there is a substitution σ and a formula $\psi' \in w_A(\psi)$ such that:*

1. *If ψ is a positive subformula of φ, $(\psi_1 \vee \ldots \vee \psi_n)\sigma \supset \psi'$ is a theorem of **LP**.*
2. *If ψ is a negative subformula of φ, $\psi' \supset (\psi_1 \wedge \ldots \wedge \psi_n)\sigma$ is a theorem of **LP**.*

Proof By induction on the complexity of ψ. If ψ is atomic the result is immediate, since $v_A(\psi)$ and $w_A(\psi)$ are both $\{\psi\}$, so we can take ψ' to be ψ, and use the empty substitution. I'll cover the non-atomic cases in detail.

Positive Implication Suppose ψ is $(X \supset Y)$, ψ is a positive subformula of φ, and the result is known for X and Y. Note that X occurs negatively in φ and Y occurs positively.

Say $\psi_i = (X_i \supset Y_i)$, where $X_i \in v_A(X)$ and $Y_i \in v_A(Y)$. By the induction hypothesis there are substitutions σ_X and σ_Y, and there are $X' \in w_A(X)$ and $Y' \in w_A(Y)$ such that $X' \supset (X_1 \wedge \ldots \wedge X_n)\sigma_X$ and $(Y_1 \vee \ldots \vee Y_n)\sigma_Y \supset Y'$ are both theorems of **LP**. Without loss of generality we can assume the domain of σ_X is exactly the set of variables of $X_1 \wedge \ldots \wedge X_n$, and similarly for σ_Y. Then, if we let σ be $\sigma_X \cup \sigma_Y$, by classical logic, the following is valid: $[(X_1 \supset Y_1) \vee \ldots \vee (X_n \supset Y_n)]\sigma \supset (X' \supset Y')$, which establishes this case.

Negative Implication Suppose ψ is $(X \supset Y)$, ψ is a negative subformula of φ, and the result is known for X and Y. Note that X occurs positively in φ and Y occurs negatively.

Again say $\psi_i = (X_i \supset Y_i)$, where $X_i \in v_A(X)$ and $Y_i \in v_A(Y)$. This time, by the induction hypothesis there are substitutions σ_X and σ_Y, and there are $X' \in w_A(X)$ and $Y' \in w_A(Y)$ such that $(X_1 \vee \ldots \vee X_n)\sigma_X \supset X'$ and $Y' \supset (Y_1 \wedge \ldots \wedge Y_n)\sigma_Y$ are theorems of **LP**. As in the previous case, we can assume σ_X and σ_Y have non-overlapping domains. Then again, if we set $\sigma = \sigma_X \cup \sigma_Y$, by classical logic the following is valid: $(X' \supset Y') \supset [(X_1 \supset Y_1) \wedge \ldots \wedge (X_n \supset Y_n)]\sigma$, establishing this case.

Positive Necessity Suppose ψ is $\Box X$, ψ is a positive subformula of φ, and the result is known for X (which also occurs positively in φ).

In this case $\psi_1, \ldots, \psi_n$ are of the form $t_1 : D_1, \ldots, t_n : D_n$, where each t_i is some proof polynomial and D_i is a disjunction of members of $v_A(X)$. Let $D = D_1 \vee \ldots \vee D_n$ be the disjunction of the D_i. By the induction hypothesis there is some substitution σ and some member $X' \in w_A(X)$ such that $D\sigma \supset X'$ is a theorem of **LP**. Consequently for each i, $D_i\sigma \supset X'$ is a theorem of **LP**, and hence there is a proof polynomial u_i such that $u_i : (D_i\sigma \supset X')$ is an **LP** theorem. But then, $(t_i : D_i)\sigma \supset (u_i \cdot t_i\sigma) : X'$ is also an **LP** theorem (application axiom, and the fact that $(t_i : D_i)\sigma = (t_i\sigma) : (D_i\sigma))$. Let s be the proof polynomial $(u_1 \cdot t_1\sigma) + \ldots + (u_n \cdot t_n\sigma)$. It follows from the sum axiom that **LP** proves $(t_i : D_i)\sigma \supset s : X'$, for each i, and hence that $(t_1 : D_1 \vee \ldots \wedge \vee_n : D_n)\sigma \supset s : X'$ is an **LP** theorem. Since $s : X' \in w_A(\Box X)$, this concludes the positive necessity case.

Negative Necessity Suppose ψ is $\Box X$, ψ is a negative subformula of φ, and the result is known for X (which also occurs negatively in φ).

In this case $\psi_1, \ldots, \psi_n$ are of the form $x : X_1, \ldots, x : X_n$, where $X_i \in v_A(X)$ and $x = A(\Box X)$. By the induction hypothesis there is some substitution σ and some $X' \in w_A(X)$ such that $X' \supset (X_1 \wedge \ldots \wedge X_n)\sigma$ is a theorem of **LP**. Without loss of generality, we can assuume x is not in the domain of σ. Now, for each $i = 1, \ldots, n$, the formula $X' \supset X_i\sigma$ is a theorem of **LP**, and so there is a proof polynomial t_i such that $t_i : (X' \supset X_i\sigma)$ is an **LP** theorem. Let s be the proof polynomial $t_1 + \ldots + t_n$. Then by the sum axiom, $s : (X' \supset X_i\sigma)$ is an **LP** theorem, for each i. It follows by the application axiom that $x : X' \supset (s \cdot x) : (X_i\sigma)$ is an **LP** theorem, for each i. If we let σ' be the substitution $\sigma \cup \{x/(s \cdot x)\}$, we have the **LP** provability of $x : X' \supset (x : X_i)\sigma'$ for each i, and hence of $x : X' \supset (x : X_1 \wedge \ldots \wedge x : X_n)\sigma'$, which establishes the result in this case.

This conclude the proof. ■

Now the hard half of Theorem 2.2 follows quickly. Suppose φ has an **S4** proof. By Theorem 2.1, there are $\varphi_1, \ldots, \varphi_n \in v_A(\varphi)$ such that $\varphi_1 \vee \ldots \vee \varphi_n$ is an $\mathbf{LP}^-$ theorem, and hence an **LP** theorem. By Proposition 5.1 there is a substitution σ and a formula $\varphi' \in w_A(\varphi)$ such that $(\varphi_1 \vee \ldots \vee \varphi_n)\sigma \supset \varphi'$ is an **LP** theorem. Since $\varphi_1 \vee \ldots \vee \varphi_n$ is provable in **LP**, so is $(\varphi_1 \vee \ldots \vee \varphi_n)\sigma$, by the Substitution Lemma, and the provability of φ' follows.

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`.