Derivability in the Logic of Proofs is Π_2^p-complete

Robert Milnikel
Department of Mathematics
Kenyon College, Gambier, OH 43022
milnikelr@kenyon.edu

July 29, 2005

Abstract

The Logic of Proofs realizes the modalities from traditional modal logics with *proof polynomials*, so an expression $\Box F$ becomes $t : F$ where t is a proof polynomial representing a proof of or evidence for F. The pioneering work on explicating the modal logic $\mathcal{S}4$ is due to S. Artemov and was extended to several subsystems by V. Brezhnev. In 2000, R. Kuznets presented a Π_2^p algorithm for deducibility in these logics; in the present paper we will show that the deducibility problem is Π_2^p-complete. (The analogous problem for traditional modal logics is PSPACE-complete.) Both Kuznets' work and the present results make assumptions on the values of proof constants.

1 Introduction

In a series of papers beginning in 1992, Sergei Artemov developed the Logic of Proofs ($\mathcal{LP}$), a realization of the modal logic $\mathcal{S}4$ in which the modality $\Box$ (often interpreted as provability) is replaced with explicit terms representing proofs. (See, for example, [1], [2], [3], and [4].) $\mathcal{LP}$ and its arithmetic interpretation provide answers to questions about the intended semantics of intuitionistic logic and $\mathcal{S}4$ asked by Gödel ([5], [6]) and provide a unified semantics for modality and the typed lambda-calculus. More recently, $\mathcal{LP}$ has found application as a paradigm for the logic of knowledge. *Evidence-based knowledge* is a constructive version of common knowledge, making problems involving the notion of common knowledge amenable to automated proof search and verification ([7]).

A. Mkrytchev ([8]) showed the decidability of $\mathcal{LP}$, and his algorithm for satisfiability was adapted and shown to be in Σ_2^p by R. Kuznets ([9]). As the satisfiability problem for classical $\mathcal{S}4$ is PSPACE-complete ([10]), $\mathcal{LP}$ has a clear advantage.

In this paper, we will show that deciding derivability in $\mathcal{LP}$ is Π_2^p-hard by encoding QBF-2 as a formula of $\mathcal{LP}$ which can be derived only if the quantified

boolean formula is true. This will show derivability in $\mathcal{LP}$ to be Π_2^p-complete (and satisfiability, of course, to be Σ_2^p-complete).

2 Preliminaries

We will begin with a formal definition of $\mathcal{LP}$ and statements of some previous results. Except as noted, the definitions and results will be drawn from [2].

2.1 The Language

Definition 2.1. The language of the Logic of Proofs ($\mathcal{LP}$) contains

- the language of classical propositional logic which includes propositional variables, truth constants $\top$, $\bot$, and boolean connectives
- proof variables $x_0, \ldots, x_n, \ldots$, proof constants $a_0, \ldots, a_n, \ldots$
- function symbols: unary !, binary $\cdot$ and $+$.
- operator symbol of the type "*proof polynomial: formula*".

Definition 2.2 (Proof polynomial). Proof polynomials are defined inductively:

- Proof variables and proof constants are proof polynomials.
- If t_1 and t_2 are proof polynomials, so are $!t_1$, $t_1 \cdot t_2$, and $t_1 + t_2$.

In general, $r \cdot s \cdot t \ldots$ should be read $(\ldots((r \cdot s) \cdot t)\ldots)$ and similarly for $r + s + t$. Proof polynomials built up entirely of constants are called *ground*.

Definition 2.3 ($\mathcal{LP}$ Formula). Formulas are defined just as for propositional logic, with one added inductive case for the operator :.

- Propositional letters, $\top$, and $\bot$ are formulas.
- If F_1 and F_2 are formulas, so are $F_1 \to F_2$, $F_1 \wedge F_2$, $F_1 \vee F_2$, $\neg F_1$.
- If F is a formula and t is a proof polynomial, $t : F$ is a formula.

We will generally use F, G, H for formulas in this language. The intended semantics for $t : F$ is "t is a proof of F". This intended semantics is made explicit via an arithmetic provability interpretation in [2] and a Kripke frame interpretation in [11]. Note that proof systems for $t : F$ are multi-conclusion ones, so t may represent a proof of several different F's.

2.2 Syntax

Definition 2.4 (Axioms and rules of $\mathcal{LP}_0$). We will begin by defining the system $\mathcal{LP}_0$ in the language of $\mathcal{LP}$. $\mathcal{LP}_0$ has the following axiom schemes:

A0. A finite set of axiom schemes of classical propositional logic

A1. $t : F \to F$ *reflection*

A2. $t : (F \to G) \to (s : F \to (t \cdot s) : G)$ *application*

A3. $t : F \to !t : (t : F)$ *proof checker*

A4. $s : F \to (s + t) : F$, $t : F \to (s + t) : F$ *sum*

and the single rule of inference modus ponens: $\dfrac{F \to G \qquad F}{G}$.

The deduction theorem $\Gamma, A \vdash B \iff \Gamma \vdash A \to B$ can be proven for $\mathcal{LP}_0$ by an easy inductive argument.

The following lemma will see much use in the present paper:

Lemma 2.5 (Lifting Lemma). *If $\vec{s} : \Gamma, \Delta \vdash F$, then there is a proof polynomial $t(\vec{x}, \vec{y})$ such that $\vec{s} : \Gamma, \vec{y} : \Delta \vdash t(\vec{s}, \vec{y}) : F$.*

While it is necessary (for reasons to be explicated in Section 2.4) to set out a Hilbert-style axiomatization for $\mathcal{LP}$, it will often be more convenient for us to use a sequent formulation.

Definition 2.6. By a *sequent* we mean a pair $\Gamma \Longrightarrow \Delta$ where Γ and Δ are finite multisets of $\mathcal{LP}$-formulas. The axioms of $\mathcal{LPG}_0$ are sequents of the form $\Gamma, F \Longrightarrow F, \Delta$ and $\Gamma, \bot \Longrightarrow \Delta$. Along with the usual Gentzen sequent rules of classical propositional logic, including the cut and contraction rules (see for example **G2c** from [12]), $\mathcal{LPG}_0$ contains the rules

$$\frac{A, \Gamma \Longrightarrow \Delta}{t : A, \Gamma \Longrightarrow \Delta}(:\Longrightarrow) \qquad \frac{\Gamma \Longrightarrow \Delta, t : A}{\Gamma \Longrightarrow \Delta, !t : t : A}(\Longrightarrow !)$$

$$\frac{\Gamma \Longrightarrow \Delta, t : A}{\Gamma \Longrightarrow \Delta, (t + s) : A}(\Longrightarrow +) \qquad \frac{\Gamma \Longrightarrow \Delta, t : A}{\Gamma \Longrightarrow \Delta, (s + t) : A}(\Longrightarrow +)$$

$$\frac{\Gamma \Longrightarrow \Delta, s : (A \to B) \qquad \Gamma \Longrightarrow \Delta, t : A}{\Gamma \Longrightarrow \Delta, (s \cdot t) : B}(\Longrightarrow \cdot).$$

By $\mathcal{LPG}_0^-$ we will mean the corresponding system without the rule Cut.

It is a theorem from [2] that the following are equivalent:

1. $\mathcal{LPG}_0^- \vdash \Gamma \Longrightarrow \Delta$
2. $\mathcal{LPG}_0 \vdash \Gamma \Longrightarrow \Delta$
3. $\mathcal{LP}_0 \vdash \bigwedge \Gamma \to \bigvee \Delta$

This, in conjunction with the deduction theorem, means that the deducibility of the sequent $\Gamma \Longrightarrow \varphi$ in a cut-free sequent calculus and the statement $\Gamma \vdash \varphi$ about the Hilbert-style $\mathcal{LP}_0$ are equivalent. I will often use the latter notation but rely on the existence of a cut-free sequent proof in arguing that if something was provable, it could only have been because a particular other formula was provable.

2.3 Semantics

There are several semantics for the language of $\mathcal{LP}$ for which the above axiomatization is sound and complete. In Artemov's original work ([2]), the formulas were interpreted as arithmetic sentences with a provably Δ_1 predicate $\mathrm{Prf}(x, y)$ ("x represents a proof of the formula encoded by y") playing a central role. In his paper proving the decidability of $\mathcal{LP}$ ([8]), Mkrtychev introduced a semantics based on a combination of classical truth assignments and *proof-theorem assignments*. This system was adapted by Kuznets ([9]) when he analyzed the complexity of the decidability problem, and by Fitting ([11]), who expanded it to a full Kripke-style semantics for LP. In Fitting's framework, Mkrtychev's models correspond to one-world models.

Mkrtychev's semantics is the most succinctly stated, and so we will use that in the present paper:

Definition 2.7 (Models of $\mathcal{LP}$ formulas). Suppose $*(\cdot)$ is a function mapping $\mathcal{LP}$ proof polynomials to sets of $\mathcal{LP}$ formulas. We will call $*$ a *proof-theorem assignment* for $\mathcal{LP}$ if it satisfies the following conditions:

- If $(G \to F) \in *(s)$ and $G \in *(t)$ then $F \in *(s \cdot t)$
- $*(s) \cup *(t) \subseteq *(s + t)$

A proof-theorem assignment is called *transitive* if in addition $F \in *(t)$ implies $t : F \in *(!t)$.

A *truth assignment* is a mapping v from the set of propositional letters to the set $\{True, False\}$. Given a truth assignment v and a proof-theorem assignment $*$, we define an interpretation $\mathcal{I}$ of the language of $\mathcal{LP}$ to be a triple $(v, *, \vDash)$ where $\vDash$ is a truth relation on formulas:

- For any propositional variable P, $\vDash P$ if and only if $v(P) = True$
- $\vDash t : F$ if and only if $F \in *(t)$
- $\vDash$ is defined inductively for boolean connectives in the usual manner.

We write $\mathcal{I} \vDash F$ to denote that $\vDash F$ holds for interpretation $\mathcal{I}$. An interpretation $\mathcal{I}$ is called *reflexive* if $F \in *(t)$ implies $\mathcal{I} \vDash F$ for any formula F and any proof polynomial t.

The system $\mathcal{LP}_0$ enjoys soundness and completeness with respect to reflexive and transitive interpretations in this semantics:

Theorem 2.8. *$\mathcal{LP}_0 \vdash F$ if and only if $\mathcal{I} \vDash F$ for all reflexive and transitive interpretations $\mathcal{I}$ of the language of $\mathcal{LP}$.*

2.4 Proof Constants

We turn now to proof constants, mentioned in the definition of the language of $\mathcal{LP}$ and not since. It turns out that the rules and semantics of proof constants, while simple, are "surprisingly central" ([11]). Continuing to quote Fitting, "proof constants are intended to represent evidence for elementary truths—those truths we know for reasons we do not further analyze." In our context, proof constants will represent the proofs of axioms. We will define several flavors of *constant specification* and will associate these with both the syntax and the semantics of $\mathcal{LP}$.

Definition 2.9. A *constant specification* is a mapping $\mathcal{C}$ from the set of proof constants to sets of formulas (possibly empty). A formula X has a proof constant with respect to $\mathcal{C}$ if $X \in \mathcal{C}(c)$ for some proof constant c. It is required that any formula having a proof constant with respect to $\mathcal{C}$ must be valid in $\mathcal{LP}_0$.

A constant specification $\mathcal{C}$ is called:

- *axiomatically appropriate* if the range of $\mathcal{C}$ is exactly the instances of axiom schemes A0-A4.
- *injective* if $\mathcal{C}$ associates each proof constant with either a single formula or no formulas at all.
- *schematic* if each proof constant c is associated with some number (possibly zero) of axiom schemes from A0-A4 and $\mathcal{C}(c)$ consists of exactly the instances of those schemes.
- *schematically injective* if $\mathcal{C}$ is schematic and no constant corresponds to more than one axiom scheme.
- *maximal* if each constant is associated with all instances of all axiom schemes A0-A4. Note that the maximal specification is both axiomatically appropriate and schematic.
- *finite* if $\mathcal{C}(c) = \emptyset$ for all but a finite number of proof constants c and furthermore $\mathcal{C}(c)$ is a finite set of specific formulas for each proof constant c.

A note on the terminology: In Artemov's original formulation of $\mathcal{LP}$ [2], "constant specification" referred to what was defined above as a finite constant specification. The particular definitions of "constant specification" and "axiomatically appropriate" just cited are Fitting's from [11]. The term "maximal constant specification" is from Kuznets ([9]). The use of the term "schematic" is new in the present paper, but the idea is present in both [13] and [9]. The notion of an "schematically injective" constant specification is new. Note that a

"injective" means "one formula per constant" whereas "schematically injective" means "one axiom scheme per constant," with the result that schematically injective constant specifications are not injective.

Let us now incorporate constant specifications into the syntax and semantics of $\mathcal{LP}$.

The syntactic rule of necessitation from classical modal logic (from F infer $\Box F$) is replaced in its explicit counterparts by necessitation on axioms, with the $\Box$ operator made explicit by proof constants.

Definition 2.10 ($\mathcal{C}$ Axiom Necessitation). Let $\mathcal{C}$ be a constant specification. Then the rule of $\mathcal{C}$ *Axiom Necessitation* is the rule $\dfrac{}{c : A}$ where A is an instance of an $\mathcal{LP}$ axiom A0-A4 and $A \in \mathcal{C}(c)$.

If we add the rule of C Axiom Necessitation to $\mathcal{LP}_0$ (whose only rule of inference, recall, is modus ponens) we get $\mathcal{LP}_{\mathcal{C}}$. Thus, $\mathcal{LP}_0$ is $\mathcal{LP}_{\mathcal{E}}$ where $\mathcal{E}$ is the constant specification with $\mathcal{E}(c) = \emptyset$ for all proof constants c. We will denote deduction in $\mathcal{LP}_{\mathcal{C}}$ by $\vdash_{\mathcal{C}}$.

What Artemov ([1], [2], [3]), Mkrtychev ([8]), and Kuznets ([9]) refer to simply as $\mathcal{LP}$ would be $\mathcal{LP}_{\mathcal{M}}$ under the present terminology, where $\mathcal{M}$ is the maximal constant specification defined above.

We can also add $\mathcal{C}$ Axiom Necessitation to the sequent calcului $\mathcal{LPG}_0$ and $\mathcal{LPG}_0^-$ by adding the sequent rule

$$\frac{\Gamma \Longrightarrow A, \Delta}{\Gamma \Longrightarrow c : A, \Delta}(\Longrightarrow c)$$

where A is an instance of an $\mathcal{LP}$ axiom A0-A4 and $A \in \mathcal{C}(c)$. The equivalences of $\mathcal{LP}_{\mathcal{C}}$, $\mathcal{LPG}_{\mathcal{C}}$, and $\mathcal{LPG}_{\mathcal{C}}^-$ continue to hold.

To incorporate constant specifications into the semantics is equally straightforward.

Definition 2.11 ($\mathcal{C}$ Model). A reflexive and transitive interpretation $\mathcal{I}$ of the language of $\mathcal{LP}$ is called a *$\mathcal{C}$-model* if $\mathcal{I} \vDash c : F$ for proof constant c and formula F exactly if $F \in \mathcal{C}(c)$.

All of the previously cited results for $\mathcal{LP}_0$ carry over to $\mathcal{LP}_{\mathcal{C}}$ (with reasonable restrictions on the $\mathcal{C}$'s involved).

Theorem 2.12. *Let $\mathcal{C}$ be a constant specification.*

- *The Deduction Theorem and Lifting Lemma (Lemma 2.5) hold for $\mathcal{LP}_{\mathcal{C}}$.*
- *Assuming $\mathcal{C}$ is axiomatically appropriate, $\mathcal{LP}_{\mathcal{C}}$ is sound and complete for $\mathcal{C}$-models.*
- *Assuming $\mathcal{C}$ is both axiomatically appropriate and schematic, $\mathcal{LP}_{\mathcal{C}}$ is decidable.*

2.5 Subsystems of $\mathcal{LP}$

Just as $\mathcal{LP}$ is an explicit version of the modal logic S4, there are systems closely related to $\mathcal{LP}$ which realize some well-known subsystems of S4: K, T, and K4[1]. These explicit versions of sublogics of S4 were defined, axiomatized, and proved sufficient to realize proofs in the corresponding modal logics by V. Brezhnev in [13] and were provided with a Mkrtychev-style semantics by Kuznets ([9]). Of particular interest is $\mathcal{LP}(\mathrm{K4})$, also called the *Logic of Beliefs*, but we will treat K and T also.

Most definitions and results carry through for explicit versions of K, T, and K4. Leaving aside the matter of constant specifications for the moment, let us define the explicit versions of these logics.

Definition 2.13. We continue to work in the language of $\mathcal{LP}$. Let the axiom schemes A0-A4 and modus ponens be as in Definition 2.4.

- $\mathcal{LP}(\mathrm{K})_0$ is the system consisting of axiom schemes A0, A2, and A4, plus the rule modus ponens.
- $\mathcal{LP}(\mathrm{T})_0$ is the system $\mathcal{LP}(\mathrm{K})_0$ plus the axiom scheme A1.
- $\mathcal{LP}(\mathrm{K4})_0$ is the system $\mathcal{LP}(\mathrm{K})_0$ plus the axiom scheme A3.

The sequent versions of these logics can also be obtained by eliminating the rules $(:\Longrightarrow)$, yielding $\mathcal{LP}(\mathrm{K4})_0$; $(\Longrightarrow!)$, yielding $\mathcal{LP}(\mathrm{T})_0$; or both of the just-mentioned rules, yielding $\mathcal{LP}(\mathrm{K})_0$.

For $\mathcal{LP}(\mathrm{K4})$, the definitions of constant specification and $\mathcal{C}$-model carry through unchanged, simply dropping references to axiom scheme A1. For $\mathcal{LP}(\mathrm{K})$ and $\mathcal{LP}(\mathrm{T})$, we require something more:

Definition 2.14. A constant specification $\mathcal{C}$ is *strongly $\mathcal{LP}$ appropriate* if $X \in \mathcal{C}(c)$ if and only if one of the following two conditions is met:

- X is an instance of an axiom scheme
- X is $d : Y$ where d is a proof constant and $Y \in \mathcal{C}(d)$.

In $\mathcal{LP}(\mathrm{K})$ and $\mathcal{LP}(\mathrm{T})$, we replace "axiomatically appropriate" with "strongly $\mathcal{LP}$ appropriate" where needed, and replace $\mathcal{C}$ axiom necessitation with the following recursive variant:

$\mathcal{C}$-Axiom Necessitation for $\mathcal{LP}(\mathrm{K})$ and $\mathcal{LP}(\mathrm{T})$: $\dfrac{}{c : A}$ where $A \in \mathcal{C}(c)$ and either A is an instance of an axiom or A can be inferred using $\mathcal{C}$-Axiom Necessitation.

[1] A very small amount of background: In addition to propositional axiom schemes, modus ponens, and necessitation, S4 has the three axiom schemes corresponding to application ($\Box(A \to B) \to (\Box A \to \Box B)$), reflection ($\Box A \to A$), and proof checker ($\Box A \to \Box\Box A$). The modal logic K has only application, T has application and reflection, and K4 has application and proof checker. For much more information see [14].

3 Complexity

In [9], R. Kuznets showed that the problem of derivability in $\mathcal{LP}$ is in Π_2^p, at the second level of the polynomial-time hierarchy. (See [15] or any standard text on complexity theory for definitions and background.) Kuznets was working in $\mathcal{LP}_{\mathcal{M}}$, where $\mathcal{M}$ is the maximal constant specification, but his proof does not rely on the maximality of the constant specification.

Theorem 3.1 ([9]). *Given a schematic constant specification $\mathcal{C}$ and a formula F in the language of $\mathcal{LP}$, the problem of deciding whether $\vdash_{\mathcal{C}} F$ is in Π_2^p.*

Proof. The following is only a very rough outline: Kuznets worked on the dual problem, showing that satisfiability is in Σ_2^p. He took a semantic approach and worked with sequents $\Gamma \Rightarrow \Delta$ made up of both formulae and proof-theorem assignment requirements of the form $F \in *(t)$.

A sequent $\Gamma \Rightarrow \Delta$ is *reflexively saturated* if the following four conditions are met:

1. If $A \to B \in \Gamma$ then either $A \in \Delta$ or $B \in \Gamma$
2. If $A \to B \in \Delta$ then $A \in \Gamma$ and $B \in \Delta$
3. If $(t : A) \in \Gamma$ then $A \in \Gamma$ and $A \in *(t)$
4. If $(t : A) \in \Delta$ then either $A \in \Delta$ or $A \in *(t) \in \Delta$

Kuznets' saturation algorithm starts with a sequent and non-deterministically finds a saturated sequent which is falsifiable exactly if the original sequent was. The algorithm operates in NP time.

The next step is to turn a sequent consisting of formulae and proof-theorem assignment requirements into a $\mathcal{C}$-model. The challenging part of this is not the propositional valuation, but extending the set of proof-theorem assignment requirements into a full proof-theorem assignment. Kuznets has an algorithm for this, and by a clever use of the Robinson graph algorithm shows that the problem of realizing whether a given sequent containing only atomic formulae and proof-theorem assignment requirements is refutable is a co-NP problem.

The saturation and completion problems taken together show that satisfiability for $\mathcal{LP}_{\mathcal{C}}$ is in Σ_2^p.

□

Kuznets ([9]) also showed that derivability for the explicit versions of K, T, and K4 is in Π_2^p.

We will show that the problem of derivability in $\mathcal{LP}$(K4) is Π_2^p-hard for any schematic, axiomatically appropriate constant specification, and that derivability is Π_2^p-hard in full $\mathcal{LP}$ under any schematically injective, axiomatically appropriate constant specification.

In both proofs, the following technical lemma about proof polynomials for a particular form of propositional tautology will be useful.

Lemma 3.2. *Let a propositional formula ψ in 3-CNF*[2] *built up out of propositional variables $p_1,\ldots, p_n$ and an axiomatically appropriate constant specification $\mathcal{C}$ be given. There is a single ground proof polynomial g_ψ such that $\vdash_{\mathcal{C}} g_\psi : (\hat{p_1} \to \cdots \to \hat{p_n} \to \psi)$ for all assignments of the $\hat{p_i}$ to either p_i or $\neg p_i$ which make $\hat{p_1} \to \cdots \to \hat{p_n} \to \psi$ a tautology. Furthermore, if $\mathcal{C}$ is schematic, then g_ψ is of size $O(n^2 \cdot |\psi|)$.*

Of course, this presumes a relatively standard axiomatization of propositional logic. One might dream up an axiomatization of propositional logic which would expand the size of g_ψ, but it would remain polynomial in the length of ψ, which is all that matters to us for the present. (See [16] for conservation of the lengths of proofs under different axiomatizations.)

The portion of the lemma that will be of use to us, and the only portion that is at all surprising, is that we can lift the proofs corresponding to the various valuations which make ψ true into the same proof polynomial in each case if the constant specification $\mathcal{C}$ is schematic. If we had an injective constant specification instead, for example, the length of g_ψ would be exponentially long in the length of ψ.

Let us now work through the details of building g_ψ.

Proof. Let a formula ψ with m 3-clauses $C_1,\ldots,C_m$ built up out of propositional variables $p_1,\ldots,p_n$ be given. We wish to show that there is a single ground proof term g_ψ of size $O(n^2 \cdot m)$ such that for any assignment of the $\hat{p_i}$'s to p_i or $\neg p_i$ such that $\hat{p_1} \to \cdots \to \hat{p_n} \to \psi$, $g_\psi : (\hat{p_1} \to \cdots \to \hat{p_n} \to \psi)$

Let us establish our propositional axiom schemes and associate proof constants with them:

1. $a_1 : \varphi \to (\psi \to \varphi)$
2. $a_2 : (\varphi \to \psi) \to (\varphi \to (\psi \to \theta)) \to (\varphi \to \theta)$
3. $a_3 : \varphi \to (\varphi \vee \psi)$
4. $a_4 : \psi \to (\varphi \vee \psi)$
5. $a_5 : \varphi \to \psi \to \varphi \wedge \psi$

We will begin by finding a proof term g_j for a single clause C_j such that for any assignment of the $\hat{p_i}$'s to p_i or $\neg p_i$ such that $\hat{p_1} \to \cdots \to \hat{p_n} \to C_j$, $g_j : (\hat{p_1} \to \cdots \to \hat{p_n} \to C_j)$

To simplify notation, let us assume that the clause C_j is $(p_{j_1} \vee \neg p_{j_2} \vee p_{j_3})$. Identical arguments and proof constants would work with different combinations of positives and negatives in front of the three atoms.

Let us note that in any assignment of the $\hat{p_i}$'s to p_i or $\neg p_i$ such that $\hat{p_1} \to \cdots \to \hat{p_n} \to C_j$, at least one of $\hat{p_{j_1}} = p_{j_1}$, $\hat{p_{j_2}} = \neg p_{j_2}$, and $\hat{p_{j_3}} = p_{j_3}$ is true. Assume for the moment that we could come up with proof constants g_{j_1}, g_{j_2} and

[2] A formula is in *conjunctive normal form* (CNF) if it is a conjunction of clauses of the form $(L_1 \vee \cdots \vee L_m)$ where each L_i is a literal. If $m = 3$ in each clause, ψ is in 3-CNF.

g_{j_3} such that for any assignment of the $\hat{p_i}$'s to p_i or $\neg p_i$ such that if $\hat{p_{j_1}} = p_{j_1}$ then $g_{j_1} : (\hat{p_1} \to \cdots \to \hat{p_n} \to C_j)$ (and similarly for g_{j_2} and g_{j_3}). Under this assumption, the g_j we are looking for will be $(g_{j_1} + g_{j_2} + g_{j_3})$.

While it is not always trivial to find an explicit proof of clearly valid propositional formulas, the task is made much simpler if an outline is given which lists the order in which the axiom schemes and the rule *modus ponens* are to be invoked without explicating the particular instances of the schemes. This is, in effect, what explicit proof terms do under a schematically injective constant specification.

We will attempt to balance explicitness with succinctness by presenting explicit proof terms which encode proofs of various valid schemes under the above axiomatization/constant specification, but relegating the proofs themselves to an appendix.

With this understanding, a few facts:

- $((a_2 \cdot a_3) \cdot (a_1 \cdot a_3)) : p_{j_1} \to (p_{j_1} \vee \neg p_{j_2} \vee p_{j_3})$.
- $((a_2 \cdot a_4) \cdot (a_1 \cdot a_3)) : \neg p_{j_2} \to (p_{j_1} \vee \neg p_{j_2} \vee p_{j_3})$.
- $a_3 : p_{j_3} \to (p_{j_1} \vee \neg p_{j_2} \vee p_{j_3})$.
- If $x : \varphi \to \theta$, then $((a_2 \cdot x) \cdot (a_1 \cdot a_1)) : \varphi \to \psi \to \theta$ for any ψ.
- If $x : \varphi \to \theta$, then $(a_1 \cdot x) : \psi \to \varphi \to \theta$ for any ψ.

By beginning the first of these facts and then applying the last-but-one formula $n - j_1$ times (with $\psi = \hat{p_i}$ for each $i > j_1$) and finishing with $j_1 - 1$ applications of the final formula (with $\psi = \hat{p_i}$ for each $i < j_1$), we generate exactly the desired g_{j_1} as described above.

Note that g_{j_1} is independent of the assignments of the $\hat{p_i}$'s to p_i or $\neg p_i$. (It doesn't even matter whether our root was p_{j_1} or $\neg p_{j_1}$. The proof outline as encoded in the proof term will be identical.) Note also that the length of g_{j_1} is exactly $4 + 3(n - j_1) + (j_1 - 1) \leq 3n + 1$.

Exactly parallel constructions beginning with the second and third facts generate g_{j_2} and g_{j_3}, each of which is also independent of the particular assignment of the $\hat{p_i}$'s and which have length at most $3n + 1$ and $3n - 2$ respectively. Thus, g_j has length at most $9n$.

We now have m proof variables g_j each of size linear in n such that $g_j : (\hat{p_1} \to \cdots \to \hat{p_n} \to C_j)$ is valid for all assignments of the $\hat{p_i}$'s to p_i or $\neg p_i$ such that $\hat{p_1} \to \cdots \to \hat{p_n} \to C_j$.

Before we proceed, a last fact, this one involving a particularly ugly proof polynomial:

- If $x : (\theta_1 \to (\theta_2 \to \psi))$ then $(a_2 \cdot [a_2 \cdot [a_1 \cdot (a_1 \cdot x)] \cdot a_2] \cdot (a_1 \cdot [a_2 \cdot (a_1 \cdot a_2) \cdot (a_2 \cdot a_1 \cdot (a_1 \cdot a_2))])) : (\varphi \to \theta_1) \to [(\varphi \to \theta_2) \to (\varphi \to \psi)]$

Let $\hat{\varphi_1}, \ldots, \hat{\varphi_n}$ be, as usual, some assignment such that $\hat{\varphi_1} \to \cdots \to \hat{\varphi_n} \to \psi$. Apply the above fact n times to the formula $a_5 : C_1 \to C_2 \to (C_1 \wedge C_2)$, with

φ as $\hat{\varphi_n}$, then as $\hat{\varphi_{n-1}}$, etc., to obtain a ground proof polynomial of length $13n+1$, call it b_2. We see that $b_2 : (\hat{\varphi_1} \to \cdots \to \hat{\varphi_n} \to C_1) \to (\hat{\varphi_1} \to \cdots \to \hat{\varphi_n} \to C_2) \to (\hat{\varphi_1} \to \cdots \to \hat{\varphi_n} \to (C_1 \wedge C_2))$. Now the proof polynomial $(b_2 \cdot g_1 \cdot g_2) : (\hat{\varphi_1} \to \cdots \to \hat{\varphi_n} \to (C_1 \wedge C_2))$. Call this proof polynomial d_2 and note that its length is at most $((13n+1)+9n+9n)$.

We can repeat the above process beginning with the formula $a_5 : (C_1 \wedge C_2) \to C_3 \to (C_1 \wedge C_2 \wedge C_3)$ to obtain $b_3 : (\hat{\varphi_1} \to \cdots \to \hat{\varphi_n} \to (C_1 \wedge C_2)) \to (\hat{\varphi_1} \to \cdots \to \hat{\varphi_n} \to C_3) \to (\hat{\varphi_1} \to \cdots \to \hat{\varphi_n} \to (C_1 \wedge C_2 \wedge C_3))$. Again, b_3 has length $13n+1$. We define d_3 as $b_3 \cdot d_2 \cdot g_3$ and note that $d_3 : (\hat{\varphi_1} \to \cdots \to \hat{\varphi_n} \to (C_1 \wedge C_2 \wedge C_3))$.

Proceeding similarly, we see that d_m will be the desired g_ψ and will have length at most $9n + (m-1) \cdot (22n+1) < 22nm$, clearly in the promised $O(n \cdot m)$ complexity class.

□

3.1 The Logic of Beliefs

We will show that deducibility in the Logic of Beliefs (explicit K4) is Π_2^p-hard be encoding a $\forall\exists$-quantified boolean formula into the language of $\mathcal{LP}$ so that it is valid exactly if $\mathcal{LP}$(K4) proves it. This case is much simpler than that of the full $\mathcal{LP}$ and serves as a good introduction to the ideas involved.

Theorem 3.3. *Given a quantified boolean formula $\varphi = \forall p_1 \cdots \forall p_n \exists q_1 \cdots \exists q_m \psi$ with $m, n \geq 0$ and ψ a quantifier-free 3-CNF boolean combination of p_1, …, p_n, q_1,…, q_m, and given any axiomatically appropriate and schematic constant specification $\mathcal{C}$ there is a formula F in the language of $\mathcal{LP}$ such that $\vdash_{\mathcal{C}} F$ in $\mathcal{LP}$(K4) exactly if φ is valid.*

Proof. Let φ be as in the statement of the theorem. Let $\mathcal{C}$ be any schematic, axiomatically appropriate constant specification.

Let g_ψ be as in Lemma 3.2 (noting that we now have propositional atoms p_1,…,p_n and q_1,…,q_m) and let F be the following:

$[(x_1 : p_1 \vee x_1 : \neg p_1) \wedge \cdots \wedge (x_n : p_n \vee x_n : \neg p_n) \wedge (y_1 : q_1) \wedge (z_1 : \neg q_1) \wedge \cdots \wedge (y_m : q_m) \wedge (z_m : \neg q_m)] \to (g_\psi \cdot x_1 \cdot x_2 \cdot \ldots \cdot x_n \cdot (y_1 + z_1) \cdot (y_2 + z_2) \cdot \ldots \cdot (y_m + z_m)) : \psi$

By the deduction theorem, we can say that $\mathcal{LP}(K4)$ proves F if and only if

$(x_1 : p_1 \vee x_1 : \neg p_1), \cdots, (x_n : p_n \vee x_n : \neg p_n), (y_1 : q_1), (z_1 : \neg q_1), \cdots, (y_m : q_m), (z_m : \neg q_m) \vdash_{\mathcal{C}} (g_\psi \cdot x_1 \cdot x_2 \cdot \ldots \cdot x_n \cdot (y_1 + z_1) \cdot (y_2 + z_2) \cdot \ldots \cdot (y_m + z_m)) : \psi$

Let $\hat{p_i}$ be either p_i or $\neg p_i$. Because propositional connectives are handled in both the syntax and semantics in a purely classical manner, the above will hold exactly if for each possible assignment of the $\hat{p_i}$'s to p_i or $\neg p_i$

$(x_1 : \hat{p_1}), \cdots, (x_n : \hat{p_n}), (y_1 : q_1), (z_1 : \neg q_1), \cdots, (y_m : q_m), (z_m : \neg q_m) \vdash_{\mathcal{C}} (g_\psi \cdot x_1 \cdot x_2 \cdot \ldots \cdot x_n \cdot (y_1 + z_1) \cdot (y_2 + z_2) \cdot \ldots \cdot (y_m + z_m)) : \psi$

As the conclusion of this deduction is, propositionally speaking, an atom, the only rules which might have been used in the last step of a sequent deduction were the $\mathcal{LP}$ rules ($\Longrightarrow +$), ($\Longrightarrow \cdot$), and ($\Longrightarrow !$). Since the proof polynomial involved is a product, the rule must have been ($\Longrightarrow \cdot$). This means that there must be some formula H so that both $(x_1 : \hat{p_1}), \cdots, (x_n : \hat{p_n}), (y_1 : q_1), (z_1 : \neg q_1), \cdots, (y_m : q_m), (z_m : \neg q_m) \vdash_{\mathcal{C}} (y_m + z_m) : H$ and $(x_1 : \hat{p_1}), \cdots, (x_n :$

$\hat{p_n}), (y_1 : q_1), (z_1 : \neg q_1), \cdots, (y_m : q_m), (z_m : \neg q_m) \vdash_{\mathcal{C}} (g_\psi \cdot x_1 \cdot x_2 \cdot \ldots \cdot x_n \cdot (y_1 + z_1) \cdot (y_2 + z_2) \cdot \ldots \cdot (y_{m-1} + z_{m-1}) : H \to \psi$.

Let us concentrate on the former first. If our premises prove $(y_m + z_m) : H$, the last rule used must have been $(\Longrightarrow +)$, and we must have a deduction either $(x_1 : \hat{p_1}), \cdots, (x_n : \hat{p_n}), (y_1 : q_1), (z_1 : \neg q_1), \cdots, (y_m : q_m), (z_m : \neg q_m) \vdash_{\mathcal{C}} y_m : H$ or $(x_1 : \hat{p_1}), \cdots, (x_n : \hat{p_n}), (y_1 : q_1), (z_1 : \neg q_1), \cdots, (y_m : q_m), (z_m : \neg q_m) \vdash_{\mathcal{C}} z_m : H$. Clearly H is either q_m or $\neg q_m$. Whichever one holds, call it $\hat{q_m}$.

Now we know that $(x_1 : \hat{p_1}), \cdots, (x_n : \hat{p_n}), (y_1 : q_1), (z_1 : \neg q_1), \cdots, (y_m : q_m), (z_m : \neg q_m) \vdash_{\mathcal{C}} (g_\psi \cdot x_1 \cdot x_2 \cdot \ldots \cdot x_n \cdot (y_1 + z_1) \cdot (y_2 + z_2) \cdot \ldots \cdot (y_{m-1} + z_{m-1})) : \hat{q_m} \to \psi$.

Proceed similarly to show that $(x_1 : \hat{p_1}), \cdots, (x_n : \hat{p_n}), (y_1 : q_1), (z_1 : \neg q_1), \cdots, (y_m : q_m), (z_m : \neg q_m) \vdash_{\mathcal{C}} (g_\psi \cdot x_1 \cdot x_2 \cdot \ldots \cdot x_n) : \hat{q_1} \to \cdots \to \hat{q_m} \to \psi$ for some assignment of the $\hat{q_j}$'s to either q_j or $\neg q_j$.

Once again, the last rule used in such a deduction must have been $(\Longrightarrow \cdot)$, so there must be a formula H such that $(x_1 : \hat{p_1}), \cdots, (x_n : \hat{p_n}), (y_1 : q_1), (z_1 : \neg q_1), \cdots, (y_m : q_m), (z_m : \neg q_m) \vdash_{\mathcal{C}} x_n : H$ and $(x_1 : \hat{p_1}), \cdots, (x_n : \hat{p_n}), (y_1 : q_1), (z_1 : \neg q_1), \cdots, (y_m : q_m), (z_m : \neg q_m) \vdash_{\mathcal{C}} (g_\psi \cdot x_1 \cdot \ldots \cdot x_{n-1}) : H \to \hat{q_1} \to \cdots \to \hat{q_m} \to \psi$. Clearly, H must be $\hat{p_n}$.

Again, we proceed similarly and show that if the original F was deducible, then for each assignment of the $\hat{p_i}$'s to either p_i or $\neg p_i$, we know that $(x_1 : \hat{p_1}), \cdots, (x_n : \hat{p_n}), (y_1 : q_1), (z_1 : \neg q_1), \cdots, (y_m : q_m), (z_m : \neg q_m) \vdash_{\mathcal{C}} g_\psi : (\hat{p_1} \to \cdots \to \hat{p_n} \to \hat{q_1} \to \cdots \hat{q_m} \to \psi)$ for some assignment of the $\hat{q_j}$'s to either q_j or $\neg q_j$.

However, as the premises make no reference to any proof constants, this will only be so if $\vdash_{\mathcal{C}} g_\psi : \hat{p_1} \to \cdots \to \hat{p_n} \to \hat{q_1} \to \cdots \hat{q_m} \to \psi$. (This is not immediate, but follows from a disassembly of g_ψ into its constituent proof constants and the fact that $(x_1 : \hat{p_1}), \cdots, (x_n : \hat{p_n}), (y_1 : q_1), (z_1 : \neg q_1), \cdots, (y_m : q_m), (z_m : \neg q_m) \vdash_{\mathcal{C}} c : A$ for a purely propositional formula A only if A is an instance of a propositional axiom scheme corresponding to the proof constant c.)

It follows that for each assignment of the $\hat{p_i}$'s to p_i or $\neg p_i$ there is an assignment of the $\hat{q_j}$'s to q_j or $\neg q_j$ which makes $\hat{p_1} \to \cdots \to \hat{p_n} \to \hat{q_1} \to \cdots \hat{q_m} \to \psi$ a tautology, and φ is valid.

We have really tackled only one direction the proof. We have shown that if F was deducible, then φ was valid. However, the proof in the other direction is much more straightforward. If φ is valid, then given any assignment of the $\hat{p_i}$'s to p_i or $\neg p_i$ there is an assignment of the $\hat{q_j}$'s to q_j or $\neg q_j$ so that $\hat{p_1} \to \cdots \to \hat{p_n} \to \hat{q_1} \to \cdots \hat{q_m} \to \psi$ is a propositional tautology. Going from this fact to a deduction of F is simple and straightforward.

□

Corollary 3.4. *The deducibility problem is Π_2^p-complete for $\mathcal{LP}$(K4) under any schematic, axiomatically appropriate constant specification. The dual problem of satisfiability is Σ_2^p-complete.*

A close examination of the above proof will show that it goes through for $\mathcal{LP}$)(K) as well, as long as the constant specification is strongly axiomatically appropriate.

3.2 The Full Logic of Proofs

For those familiar with the Logic of Proofs or with modal logic generally, the impossibility of using the above proof in a system with reflection (the axiom $(t : F) \to F$) will be clear. We had as premises both $y : q$ and $z : \neg q$, and these together with reflection axioms prove anything. Our task in bringing the above proof to the full logic of proofs will be to insist not only that a certain formula be provable, but that it be provable without reflection. To do that, we will capture the proof we want as a proof polynomial, but we will need to be able to distinguish within that proof polynomial which axioms each constant refers to. Thus, we will specify a constant specification in which different axioms are associated with different constants, and prove that we can encode our quantified boolean formula under that constant specification.

Theorem 3.5. *Given a quantified boolean formula $\varphi = \forall p_1 \cdots \forall p_n \exists q_1 \cdots \exists q_m \psi$ with $m, n \geq 0$ and ψ a quantifier-free 3-CNF boolean combination of p_1, ..., p_n, q_1,..., q_m and an axiomatically appropriate schematically injective constant specification $\mathcal{C}$, one can find a formula F in the language of $\mathcal{LP}$ such that $\vdash_{\mathcal{C}} F$ exactly if φ is valid.*

Proof. Let φ be as in the statement of the theorem. Let $\mathcal{C}$ be a schematically injective axiomatically appropriate constant specification. We will select three proof constants c_2, c_L, and c_R such that:

- $c_2 : A$ exactly if A is an instance of application (axiom scheme A2)
- $c_L : A$ exactly if A is an instance of the left sum rule for proof polynomials
- $c_R : A$ exactly if A is an instance of the right sum rule for proof polynomials

The formula F will be quite long, so let us introduce one abbreviation, once again making use of the g_ψ from Lemma 3.2:

We will define the proof polynomial k_n built out of proof constants and the variables x_1,..., x_n by induction. Let $k_0 = !g_\psi$, and let $k_n = c_2 \cdot k_{n-1} \cdot !x_n$.

Let us note some facts about k_n. Since g_ψ had length quadratic in the length of ψ, so will k_n. We know that that if $\hat{p_1} \to \hat{p_2} \to \cdots \hat{p_n} \to \hat{q_1} \to \cdots \hat{q_m} \to \psi$ is valid, then $\vdash_{\mathcal{C}} g_\psi : \hat{p_1} \to \hat{p_2} \to \cdots \hat{p_n} \to \hat{q_1} \to \cdots \hat{q_m} \to \psi$ and that $x_1 : \hat{p_1}, x_2 : \hat{p_2}, \ldots, x_n : \hat{p_n} \vdash_{\mathcal{C}} g_\psi \cdot x_1 \cdot x_2 \cdot \ldots \cdot x_n : \hat{q_1} \to \cdots \to \hat{q_m} \to \psi$. By Lemma 2.5, we are guaranteed a proof polynomial k so that $x_1 : \hat{p_1}, x_2 : \hat{p_2}, \ldots, x_n : \hat{p_n} \vdash_{\mathcal{C}} k : (g_\psi \cdot x_1 \cdot x_2 \cdot \ldots \cdot x_n : \hat{q_1} \to \cdots \to \hat{q_m} \to \psi)$. This k which is guaranteed is, in fact, the k_n defined above. Furthermore, under the constant specification $\mathcal{C}$, it turns out that k_n uniquely identifies this proof, to the extent that if $x_1 : \hat{p_1}, \ldots, x_n : \hat{p_n} \vdash_{\mathcal{C}} k_n : H$ for some formula H, then H must be of the form $g_\psi \cdot x_1 \cdot \ldots x_n : G$, with $\vdash_{\mathcal{C}} g_\psi : \hat{p_1} \to \cdots \to \hat{p_n} \to G$.

Let us prove this assertion by induction. We will abbreviate $x_1 : \hat{p_1}, x_2 : \hat{p_2}, \ldots x_n : \hat{p_n}$ by Γ_n. Now to be more explicit about the inductive statement: We will assert that for $i \leq n$, $\Gamma_n \vdash_{\mathcal{C}} k_i : H$ if and only if H is of the form $g_\psi \cdot x_1 \cdot \ldots \cdot x_i : G$ and $\Gamma_n \vdash_{\mathcal{C}} g_\psi : \hat{p_1} \to \hat{p_2} \to \cdots \hat{p_i} \to G$. In the case $i = 0$, the

assertion simply states that $\Gamma_n \vdash_{\mathcal{C}} !g_\psi : H$ if and only if H is of the form $g_\psi : G$ and $\Gamma_n \vdash_{\mathcal{C}} g_\psi : G$. Given that from our particular Γ_n no propositional rule or use of the rule $(:\!\Longrightarrow)$ could have yielded $!g_\psi : H$, it must have resulted from use of the rule $(\Longrightarrow !)$, and the conclusion follows.

Now let us assume that the assertion holds for i and prove it for $i+1$. $\Gamma_n \vdash_{\mathcal{C}} c_2 \cdot k_i \cdot !x_{i+1} : H$. Again, there is no propositional rule or use of the rule $(:\!\Longrightarrow)$ which could yield this result, given our particular Γ_n, so it must have been a result of the rule $(\Longrightarrow \cdot)$. That means that there must have been a formula F so that $\Gamma_n \vdash_{\mathcal{C}} !x_{i+1} : F$ and $\Gamma_n \vdash_{\mathcal{C}} c_2 \cdot k_i : F \to H$. Clearly $!x_{i+1}$ is the result of an application of $(\Longrightarrow !)$ to a formula of the form $x_{i+1} : F'$ with $\Gamma_n \vdash_{\mathcal{C}} x_{i+1} : F'$. An examination of Γ_n shows us that F' could only be $\hat{p_{i+1}}$. So it must be that $\Gamma_n \vdash_{\mathcal{C}} c_2 \cdot k_i : (x_{i+1} : \hat{p_{i+1}}) \to H$. Again, this could not have resulted from any propositional rules or use of $(:\!\Longrightarrow)$ and must be a result of $(\Longrightarrow \cdot)$. There must be a formula H_i so that $\Gamma_n \vdash_{\mathcal{C}} k_i : H_i$ and $\Gamma_n \vdash_{\mathcal{C}} c_2 : H_i \to (x_{i+1} : \hat{p_{i+1}} \to H)$. By induction, we know H_i to be of the form $g_\psi \cdot x_1 \cdot \ldots \cdot x_i : G$ and that $\Gamma_n \vdash_{\mathcal{C}} g_\psi : \hat{p_1} \to \hat{p_2} \to \cdots \hat{p_i} \to G$. Thus, we know that $\Gamma_n \vdash_{\mathcal{C}} c_2 : (g_\psi \cdot x_1 \cdot \ldots \cdot x_i : G) \to (x_{i+1} : \hat{p_{i+1}} \to H)$. This must mean that $(g_\psi \cdot x_1 \cdot \ldots \cdot x_i : G) \to (x_{i+1} : \hat{p_{i+1}} \to H)$ is an instance of axiom scheme A2, and G must have been of the form $\hat{p_{i+1}} \to G'$ with H of the form $x_1 \cdot \ldots \cdot x_i \cdot x_{i+1} : G'$. Furthermore, since we know that $\Gamma_n \vdash_{\mathcal{C}} g_\psi : \hat{p_1} \to \hat{p_2} \to \cdots \hat{p_i} \to G$, we know that $\Gamma_n \vdash_{\mathcal{C}} g_\psi : \hat{p_1} \to \hat{p_2} \to \cdots \hat{p_i} \to \hat{p_{i+1}} \to G'$ because G is exactly $\hat{p_{i+1}} \to G'$. This completes the inductive argument about k_n.

Clearly, for any assignment of $\hat{p_i}$'s which has a corresponding set of $\hat{q_j}$'s which make ψ true,

$x_1 : \hat{p_1}, \ldots x_n : \hat{p_n} \vdash_{\mathcal{C}} ((y_1 : q_1 \wedge z_1 : \neg q_1) \wedge \cdots \wedge (y_m : q_m \wedge z_m : \neg q_m)) \to (g_\psi \cdot x_1 \cdot x_2 \cdot \ldots \cdot x_n \cdot (y_1 + z_1) \cdot (y_2 + z_2) \cdot \ldots \cdot (y_m + z_m)) : \psi$

Moreover, this can be proved in a variety of ways. One would be to make use of reflection and the premises $y_1 : q_1$ and $z_1 : \neg q_1$. However, from our work with the Logic of Beliefs in the previous section, we know that there is also a proof which uses the premises "as intended" and makes no use of reflection. By applying the Lifting Lemma we are guaranteed a proof term t (which might refer to the x_i's) such that

$x_1 : \hat{p_1}, \ldots x_n : \hat{p_n} \vdash_{\mathcal{C}} t : [((y_1 : q_1 \wedge z_1 : \neg q_1) \wedge \cdots \wedge (y_m : q_m \wedge z_m : \neg q_m)) \to (g_\psi \cdot x_1 \cdot x_2 \cdot \ldots \cdot x_n \cdot (y_1 + z_1) \cdot (y_2 + z_2) \cdot \ldots \cdot (y_m + z_m)) : \psi]$

It turns out that for the "intended" proof, one possible t is of the form $(g_0 \cdot \overbrace{(c_L + c_R) \cdot c_2 \cdot (c_L + c_R) \cdot c_2 \cdot \ldots (c_L + c_R) \cdot c_2)}^{m \text{ times}} \cdot k_n$ where g_0 is a ground term consisting only of constants corresponding to propositional axioms and k_n is the proof polynomial discussed a few paragraphs ago. It is somewhat surprising that we can engineer g_0 to be both quadratic in the size of ψ and independent of the particular assignment of the $\hat{q_j}$'s. This is tedious but not difficult to show, very much along the lines of Lemma 3.2.[3] Let us denote the

[3]This is the place that the grouping into pairs of $(y_1 : q_1 \wedge z_1 : \neg q_1) \wedge \cdots \wedge (y_m : q_m \wedge z_m : \neg q_m)$ comes into play. If we were to let $a_6 : \varphi \wedge \psi \to \varphi$ and $a_7 : \varphi \wedge \psi \to \psi$, it turns out that $(a_6 + a_7) : (y_1 : q_1 \wedge z_1 : \neg q_1) \to y_1 : q_1$ and $(a_6 + a_7) : (y_1 : q_1 \wedge z_1 : \neg q_1) \to z_1 : \neg q_1$,

full t by t_ψ. Again, the length of t_ψ is quadratic in the length of ψ.

Let F be the following:

$[(x_1 : p_1 \vee x_1 : \neg p_1) \wedge \cdots \wedge (x_n : p_n \vee x_n : \neg p_n)] \rightarrow t_\psi : [((y_1 : q_1 \wedge z_1 : \neg q_1) \wedge \cdots \wedge (y_m : q_m \wedge z_m : \neg q_m)) \rightarrow (g_\psi \cdot x_1 \cdot x_2 \cdot \ldots \cdot x_n \cdot (y_1 + z_1) \cdot (y_2 + z_2) \cdot \ldots \cdot (y_m + z_m)) : \psi]$

First of all, let us invoke the deduction theorem and similar arguments to those in the case of $\mathcal{LP}$(K4) to note that $\vdash_{\mathcal{C}} F$ if and only if for each possible assignment of the $\hat{p_i}$'s to p_i or $\neg p_i$

$x_1 : \hat{p_1}, \ldots, x_n : \hat{p_n} \vdash_{\mathcal{C}} t_\psi : [((y_1 : q_1 \wedge z_1 : \neg q_1) \wedge \cdots \wedge (y_m : q_m \wedge z_m : \neg q_m)) \rightarrow (g_\psi \cdot x_1 \cdot x_2 \cdot \ldots \cdot x_n \cdot (y_1 + z_1) \cdot (y_2 + z_2) \cdot \ldots \cdot (y_m + z_m)) : \psi]$

This observation alone takes care of the universal quantifiers in the original quantified boolean formula $\forall p_1 \cdots \forall p_n \exists q_1 \cdots \exists q_m \psi$. As before, let use abbreviate $x_1 : \hat{p_1}, \ldots, x_n : \hat{p_n}$ by Γ_n.

Now all we need to do is show that

$\Gamma_n \vdash_{\mathcal{C}} t_\psi : [((y_1 : q_1 \wedge z_1 : \neg q_1) \wedge \cdots \wedge (y_m : q_m \wedge z_m : \neg q_m)) \rightarrow (g_\psi \cdot x_1 \cdot x_2 \cdot \ldots \cdot x_n \cdot (y_1 + z_1) \cdot (y_2 + z_2) \cdot \ldots \cdot (y_m + z_m)) : \psi]$

if and only if ψ with the p_i's replaced by truth values determined by whether $\hat{p_i}$ is p_i or $\neg p_i$ is satisfiable.

The following lemma will get us much of the way there:

Lemma 3.6. *Let $\mathcal{C}$, c_2, c_L, c_R, t_ψ and k_n be as defined above, and let t be some proof polynomial. Then*

$\Gamma_n \vdash_{\mathcal{C}} t_\psi : [((y_1 : q_1 \wedge z_1 : \neg q_1) \wedge \cdots \wedge (y_m : q_m \wedge z_m : \neg q_m)) \rightarrow (t \cdot (y_1 + z_1) \cdot (y_2 + z_2) \cdot \ldots \cdot (y_m + z_m)) : \psi]$

if and only if

$\Gamma_n \vdash_{\mathcal{C}} k_n : t : (\hat{q_1} \rightarrow \cdots \rightarrow \hat{q_m} \rightarrow \psi)$

for some assignment of the $\hat{q_j}$'s to either q_j or $\neg q_j$ respectively.

Proof. This is the messiest part of the argument, and for the sake of simplicity and readability, we will restrict ourselves to the case $m = 2$. This approach generalizes quite naturally.

Thus, we wish to prove that $\Gamma_n \vdash_{\mathcal{C}} (g_0 \cdot (c_L + c_R) \cdot c_2 \cdot (c_L + c_R) \cdot c_2) \cdot k_n : [((y_1 : q_1 \wedge z_1 : \neg q_1) \wedge (y_2 : q_2 \wedge z_2 : \neg q_2)) \rightarrow (t \cdot (y_1 + z_1) \cdot (y_2 + z_2)) : \psi]$ implies $\Gamma_n \vdash_{\mathcal{C}} k_n : t : (\hat{q_2} \rightarrow \hat{q_1} \rightarrow \psi)$ where $\hat{q_1}$ is either q_1 or $\neg q_1$ and $\hat{q_2}$ is either q_2 or $\neg q_2$. (The implication in the other direction is much more straightforward and will be easy to reconstruct from the argument in the present direction.)

We begin with

$\Gamma_n \vdash_{\mathcal{C}} (g_0 \cdot (c_L + c_R) \cdot c_2 \cdot (c_L + c_R) \cdot c_2) \cdot k_n : [((y_1 : q_1 \wedge z_1 : \neg q_1) \wedge (y_2 : q_2 \wedge z_2 : \neg q_2)) \rightarrow (t \cdot (y_1 + z_1) \cdot (y_2 + z_2)) : \psi]$.

As the conclusion of this sequent is atomic as far as propositional logic is concerned and no application of $(:\Longrightarrow)$ would have been of any use, the final rule used to obtain this sequent must have been $(\Longrightarrow \cdot)$. Thus there must be a formula F_n with

$\Gamma_n \vdash_{\mathcal{C}} k_n : F_n$

and

---

so the left/right or positive/negative choices made later in the argument do not affect the construction of g_0.

$\Gamma_n \vdash_{\mathcal{C}} (g_0 \cdot (c_L + c_R) \cdot c_2 \cdot (c_L + c_R) \cdot c_2) : (F_n \to [((y_1 : q_1 \wedge z_1 : \neg q_1) \wedge (y_2 : q_2 \wedge z_2 : \neg q_2)) \to (t \cdot (y_1 + z_1) \cdot (y_2 + z_2) : \psi)])$.

Let us leave $\Gamma_n \vdash_{\mathcal{C}} k_n : F_n$ alone for the moment and concentrate on the latter formula. Again, it must have been proven using $(\Longrightarrow \cdot)$. Thus, there is a formula A_1 such that $\Gamma_n \vdash_{\mathcal{C}} c_2 : A_1$ and $\Gamma_n \vdash_{\mathcal{C}} g_0 \cdot (c_L + c_R) \cdot c_2 \cdot (c_L + c_R) : (A_1 \to F_n \to [((y_1 : q_1 \wedge z_1 : \neg q_1) \wedge (y_2 : q_2 \wedge z_2 : \neg q_2)) \to (t \cdot (y_1 + z_1) \cdot (y_2 + z_2) : \psi)])$. Again, the last step in a proof of the latter formula must have used $(\Longrightarrow \cdot)$, so there is formula A_2 so that $\Gamma_n \vdash_{\mathcal{C}} (c_L + c_R) : A_2$ and $\Gamma_n \vdash_{\mathcal{C}} g_0 \cdot (c_L + c_R) \cdot c_2 : (A_2 \to A_1 \to F_n \to [((y_1 : q_1 \wedge z_1 : \neg q_1) \wedge (y_2 : q_2 \wedge z_2 : \neg q_2)) \to (t \cdot (y_1 + z_1) \cdot (y_2 + z_2) : \psi)])$.

If we continue in this way twice more, we see that there must also be formulas A_3 and A_4 so that $\Gamma_n \vdash_{\mathcal{C}} c_2 : A_3$, $\Gamma_n \vdash_{\mathcal{C}} (c_L + c_R) : A_4$, and $\Gamma \vdash_{\mathcal{C}} g_0 : (A_4 \to A_3 \to A_2 \to A_1 \to F_n \to [((y_1 : q_1 \wedge z_1 : \neg q_1) \wedge (y_2 : q_2 \wedge z_2 : \neg q_2)) \to (t \cdot (y_1 + z_1) \cdot (y_2 + z_2) : \psi)])$.

Now since $\Gamma_n \vdash_{\mathcal{C}} c_2 : A_1$ and $\Gamma_n \vdash_{\mathcal{C}} c_2 : A_3$, it must be that both A_1 and A_3 are instances of axiom scheme A2, the Application rule. Thus, each has the form $t : (F \to G) \to (s : F \to (t \cdot s) : G)$. It is also clear that, since $\Gamma_n \vdash_{\mathcal{C}} (c_L + c_R) : A_2$ and $\Gamma_n \vdash_{\mathcal{C}} (c_L + c_R) : A_4$, each of A_2 and A_4 must be instances of axiom scheme A4, the Sum rule, either the left or right version. This leads us to four possibilities, based on two choices of c_L versus c_R. (In general, of course, we would have 2^m possibilities, but we are looking specifically at the case $m = 2$.) For now, let us assume that A_2 is of the form $u : H \to (u + v) : H$ and that A_4 is of the form $v : H \to (u + v) : H$. Each of the other three cases would be dealt with essentially identically to this one.

Note that at least one of these four (in general, 2^m) cases must hold, but we have no way of knowing which. This collection of left/right decisions will correspond to the true/false decisions of the existentially quantified q_j's from our original quantified boolean formula.

Now that we know the form A_1, A_2, A_3, and A_4 must take, we can restate what we know. It must be that $\Gamma_n \vdash_{\mathcal{C}} k_n : F_n$ and that

$\Gamma_n \vdash_{\mathcal{C}} g_0 : ((v_2 : H_2 \to (u_2 + v_2) : H_2) \to (t_2 : (F_2 \to G_2) \to (s_2 : F_2) \to (t_2 \cdot s_2) : G_2) \to (u_1 : H_1 \to (u_1 + v_1) : H_1) \to (t_1 : (F_1 \to G_1) \to (s_1 : F_1) \to (t_1 \cdot s_1) : G_1) \to F_n \to [((y_1 : q_1 \wedge z_1 : \neg q_1) \wedge (y_2 : q_2 \wedge z_2 : \neg q_2)) \to (t \cdot (y_1 + z_1) \cdot (y_2 + z_2) : \psi)])$

for some formulas F_1, G_1, F_2, G_2, H_1, H_2, and F_n and some proof polynomials s_1, t_1, s_2, t_2, u_1, u_2, v_1, and v_2.

Further, since it is of the form $\Gamma_n \vdash_{\mathcal{C}} g_0 : \ldots$, it must be that the formula with the g_0 stripped off is a propositional tautology. (Recall that g_0 consists entirely of proof constants corresponding to propositional axioms.) However, as written, in contains many provisional formula and polynomial variables.

Upon close examination, we see that the formula could be rewritten as a conjunction of the following premises

- $y_1 : q_1$
- $z_1 : \neg q_1$

- $y_2 : q_2$
- $z_2 : \neg q_2$
- $t_1 : (F_1 \to G_1) \to (s_1 : F_1) \to (t_1 \cdot s_1) : G_1$
- $u_1 : H_1 \to (u_1 + v_1) : H_1$
- $t_2 : (F_2 \to G_2) \to (s_2 : F_2) \to (t_2 \cdot s_2) : G_2$
- $v_2 : H_2 \to (u_2 + v_2) : H_2$
- F_n

implying the conclusion $(t \cdot (y_1 + z_1) \cdot (y_2 + z_2)) : \psi$. The task that now faces us is a PROLOG-style unification problem. We need to unify these provisional formula and proof polynomial variables (the F's, G's, H's, s's, t's, u's, and v's) in such a way that the desired conclusion follows tautologically from them. Note here that the y's, z's, and q's are elementary and may not be unified out. Note as well that we have two pairs of essentially identical schemes. The choice of which to use at a particular point in unification is arbitrary and will not affect the outcome. (In fact, the choices might be dictated by the precise form of g_0, but that does not affect the current argument.)

One further thing to note is that from what we know about F_n, namely that $\Gamma_n \vdash_{\mathcal{C}} k_n : F_n$, we can not unify F_n with any of the first four premises nor with the desired conclusion at any stage of the unification before the final one. (Otherwise, the unification would be trivial.) This is the only place in the proof of this lemma that the premises Γ_n come into play.

We begin with our conclusion: $(t \cdot (y_1 + z_1) \cdot (y_2 + z_2) : \psi)$. This must be the consequence of one of our premises, and the only one that fits the bill is $t_1 : (F_1 \to G_1) \to (s_1 : F_1) \to (t_1 \cdot s_1) : G_1$ (or its identical twin scheme). Thus, we will unify t_1 with $(t \cdot (y_1 + z_1))$, s_1 with $(y_2 + z_2)$, and G_1 with ψ.

We now wish to prove $(t \cdot (y_1 + z_1) : (F_1 \to \psi)$ and $(y_2 + z_2) : F_1$ from

- $y_1 : q_1$
- $z_1 : \neg q_1$
- $y_2 : q_2$
- $z_2 : \neg q_2$
- $u_1 : H_1 \to (u_1 + v_1) : H_1$
- $t_2 : (F_2 \to G_2) \to (s_2 : F_2) \to (t_2 \cdot s_2) : G_2$
- $v_2 : H_2 \to (u_2 + v_2) : H_2$
- F_n

To prove $(y_2 + z_2) : F_1$, we will have to unify F_1 either with H_1 or H_2 (this involves a left/right decision). Let us choose H_2 to keep our subscripts straight. This also unifies u_2 with y_2 and v_2 with z_2. We also pick up the subgoal of proving $z_2 : H_2$. This clearly identifies H_2 (and hence F_1) with $\neg q_2$. Our new goal is to prove $(t \cdot (y_1 + z_1)) : \neg q_2 \to \psi$ propositionally from:

- $y_1 : q_1$
- $z_1 : \neg q_1$
- $y_2 : q_2$
- $u_1 : H_1 \to (u_1 + v_1) : H_1$
- $t_2 : (F_2 \to G_2) \to (s_2 : F_2) \to (t_2 \cdot s_2) : G_2$
- F_n

This step and the next are very similar to the previous two. We unify t with t_2, $(y_1 + z_1)$ with s_2, and G_2 with $\neg q_2 \to \psi$. This creates the subgoal of proving $(y_1 + z_1) : F_2$. This can only be achieved by unifying u_1 with y_1, v_1 with z_1, and F_2 with H_1. Again, we create the subgoal of proving $y_1 : H_1$, which clearly unifies H_1 (and F_2) with q_1.

Finally, we are left having to prove $t : q_1 \to (\neg q_2) \to \psi$ propositionally from

- $z_1 : \neg q_1$
- $y_2 : q_2$
- F_n

Clearly the only way to do this is to unify F_n with $t : q_1 \to (\neg q_2) \to \psi$, and at this point, we are free to do this (assuming the t is suitable). Remember that the only criterion we had for F_n was that $\Gamma_n \vdash_{\mathcal{C}} k_n : F_n$, so we have shown that, given the left/right choices we made $\Gamma_n \vdash_{\mathcal{C}} k_n : t : \neg q_2 \to q_1 \to \psi$. What we have shown in general is that for some assignment of $\hat{q_1}$ to q_1 or $\neg q_1$ and $\hat{q_2}$ to q_2 or $\neg q_2$, $\Gamma \vdash_{\mathcal{C}} k_n : t : \hat{q_2} \to \hat{q_1} \to \psi$.

This is exactly what we wished to show, at least for the case $m = 2$. The way to generalize this is clear. This completes the proof of the lemma.

□

Now let the assignments of $\hat{p_i}$ to p_i and $\neg p_i$ be arbitrary and the assignments of $\hat{q_j}$ to q_j and $\neg q_j$ be those guaranteed by the above lemma in the context of the given $\hat{p_i}$'s. Under these circumstances, we have reduced our task to showing that $x_1 : \hat{p_1}, \ldots, x_n : \hat{p_n} \vdash_{\mathcal{C}} k_n : (g_\psi \cdot x_1 \cdot \ldots \cdot x_n) : \hat{q_1} \to \cdots \to \hat{q_m} \to \psi$ if and only if ψ is true under the valuation of the p_i's and q_j's specified by the choices of $\hat{p_i}$ and $\hat{q_j}$.

Based on what we discovered about k_n at the beginning of the proof, $x_1 : \hat{p_1}, \ldots, x_n : \hat{p_n} \vdash_{\mathcal{C}} k_n : (g_\psi \cdot x_1 \cdot \ldots \cdot x_n) : \hat{q_1} \to \cdots \to \hat{q_m} \to \psi$ if and only

if $\vdash_{\mathcal{C}} g_\psi : \hat{p_1} \to \cdots \to \hat{p_n} \to \hat{q_1} \to \cdots \to \hat{q_m} \to \psi$. This is true only if $\hat{p_1} \to \cdots \to \hat{p_n} \to \hat{q_1} \to \cdots \to \hat{q_m} \to \psi$ is a tautology.

Thus, our task has finally been reduced to the trivial: Show that $\hat{p_1} \to \cdots \to \hat{p_n} \to \hat{q_1} \to \cdots \to \hat{q_m} \to \psi$ is a tautology if and only if ψ is true under the valuation of the p_i's and q_j's specified by the choices of $\hat{p_i}$ and $\hat{q_j}$. Since the choices of $\hat{p_i}$ and $\hat{q_j}$ specify a complete valuation as far as ψ is concerned, we are done.

□

Corollary 3.7. *Given a formula F in the language of $\mathcal{LP}$, the problem of whether F can be derived under a schematically injective, axiomatically appropriate constant specification is Π_2^p-complete. The dual problem of satisfiability is Σ_2^p-complete.*

4 Future Work

Several issues relating to the complexity of $\mathcal{LP}$ remain unanswered. First, does deducibility remain Π_2^p-hard if the condition of schematic injectivity is dropped? In particular, is deducibility under the maximal constant specification Π_2^p-hard? Secondly, what is the computability-theoretic complexity of deduction from an infinite recursive set of premises? Some further research into the complexity of $\mathcal{LP}$ has already been done. It is a folk result following from [2] and [9] that derivability in $\mathcal{LP}_0$ is co-NP complete, and it follows that it is also co-NP complete for finite constant specifications (and hence for fixed injective constant specifications, as a particular formula mentions only finitely many constants). Kuznets has also shown that decidable constant specifications can be designed which lead to satisfiability being undecidable. ([17])

There are many variations and extensions of $\mathcal{LP}$ not mentioned in the present paper, and of course another direction for research is to pursue complexity questions for these.

Finally, there are many Σ_2^p-complete and Π_2^p-complete problems in other areas of computer science. (For example, the problems of credulous/skeptical reasoning in default logic fall into this category.) Are there natural translations between $\mathcal{LP}$ and structures in these other areas of study?

Acknowledgement

Thanks to Prof. Sergei Artemov and to Roman Kuznets for encouragement and many helpful suggestions.

References

[1] Artemov, S.N., Strassen, T.: The basic logic of proofs. In Börger, E., Jäger, G., Büning, H.K., Martini, S., Richter, M., eds.: Computer Science Logic,

6th Workshop, Selected Papers. Volume 702 of Lecture Notes in Computer Science., San Miniato, Italy (1992) 14–28

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

[3] Artemov, S.N.: Unified semantics for modality and lambda-terms via proof polynomials. In Vermulen, K., Copestake, A., eds.: Algebras, Diagrams and Decisions in Language, Logic and Computation, Stanford, CA (2002)

[4] Artemov, S.N.: Back to the future: Explicit logic for computer science. In Baaz, M., Makowsky, J., eds.: Computer Science Logic, Proceedings of the 12th annual workshop. Volume 2803 of Lecture Notes in Computer Science., Springer (2003) 43

[5] Gödel, K.: Eine interpretation des intuitionistischen aussagenkalkuls. Ergebnisse Math. Colloq. **4** (1933) 39–40

[6] Gödel, K.: Vortrag bei zilsel, 1938. In Feferman, S., ed.: Kurt Godel Collected Works, vol. III. Oxford University Press, Oxford (1995) 86–113

[7] Artemov, S.N.: Evidence-based common knowledge. Technical Report TR-2004018, City University of New York (2004)

[8] Mkrtychev, A.: Models for the logic of proofs. In Adain, S., Nerode, A., eds.: Logical Foundations of Computer Science '97, Berlin, Springer Verlag (1997) 266–277 Lecture Notes in Computer Science vol. 1234.

[9] Kuznets, R.: On the complexity of explicit modal logics. In: Proceedings of the 14^{th} International Wokrshop on Computer Science Logic, Berlin, Springer Verlag (2000) 371–383

[10] Ladner, R.: The computational complexity of provability in systems of modal propositional logic. SIAM Journal of Computing **6** (1977) 467–480

[11] Fitting, M.: The logic of proofs, semantically. Annals of Pure and Applied Logic **125** (2005) 1–25

[12] Troelstra, A., Schwichtenburg, H.: Basic Proof Theory. Cambridge University Press, Cambridge (1996)

[13] Brezhnev, V.: On the logic of proofs. In: Proceedings of the Sixth ESSLLI Student Session, Helsinki. (2001) 35–46

[14] Hughes, G.E., Cresswell, M.J.: A New Introduction to Modal Logic. Routledge, Oxford (1996)

[15] Papadimitriou, C.H.: Computational Complexity. Addison Wesley, Boston, MA (1993)

[16] Pudlák, P.: The lengths of proofs. In Buss, S.R., ed.: The Handbook of Proof Theory. Elsevier, Amsterdam (1998) 547–637

[17] Kuznets, R.: On decidability of the logic of proofs with arbitrary constant specifications. Bulletin of the Association for Symbolic Logic **11** (2005) 114 Abstract only.

Appendix

As an aid to those who wish to confirm the technical details involved in the proof terms from Lemma 3.2, here are some of the deductions alluded to in the proof.

Proposition 4.1. *$\varphi \to \psi, \psi \to \theta \vdash \varphi \to \theta$ invoking each premise only once and invoking two axioms.*

Proof. The deduction is as follows:

$\psi \to \theta$	Premise
$(\psi \to \theta) \to \varphi \to (\psi \to \theta)$	Axiom 1
$\varphi \to \psi \to \theta$	Modus Ponens
$\varphi \to \psi$	Premise
$(\varphi \to \psi) \to (\varphi \to \psi \to \theta) \to (\varphi \to \theta)$	Axiom 2
$(\varphi \to \psi \to \theta) \to (\varphi \to \theta)$	Modus Ponens
$\varphi \to \theta$	Modus Ponens

□

Corollary 4.2. *$A \to (A \vee B \vee C)$ with four calls to axioms.*

Apply Proposition 4.1 with premises $A \to (A \vee B)$ (Axiom 3) and $(A \vee B) \to (A \vee B \vee C)$ (Axiom 3 again).

Corollary 4.3. *$B \to (A \vee B \vee C)$ with four calls to axioms.*

Apply Proposition 4.1 with premises $B \to (A \vee B)$ (Axiom 4) and $(A \vee B) \to (A \vee B \vee C)$ (Axiom 3).

Proposition 4.4. *$\varphi \to \theta \vdash \varphi \to \psi \to \theta$ invoking the premise only once and invoking three axioms.*

Proof. Here is the deduction:

$\theta \to \psi \to \theta$	Axiom 1
$(\theta \to \psi \to \theta) \to \varphi \to (\theta \to \psi \to \theta)$	Axiom 1
$\varphi \to \theta \to \psi \to \theta$	Modus Ponens
$[\varphi \to \theta] \to [\varphi \to \theta \to \psi \to \theta] \to [\varphi \to \psi \to \theta]$	Axiom 2
$\varphi \to \theta$	Premise
$[\varphi \to \theta \to \psi \to \theta] \to [\varphi \to \psi \to \theta]$	Modus Ponens
$\varphi \to \psi \to \theta$	Modus Ponens

□

Proposition 4.5. *$\varphi \to \theta \vdash \psi \to \varphi \to \theta$ invoking the premise only once and invoking one axiom.*

Proof. The deduction is as follows:

$\varphi \to \theta$	Premise
$(\varphi \to \theta) \to \psi \to (\varphi \to \theta)$	Axiom 1
$\psi \to \varphi \to \theta$	Modus Ponens

□

Proposition 4.6. *$A \to B \to C \vdash B \to A \to C$ invoking the premise only once and invoking 6 axioms.*

Proof. Here is the deduction:

$(A \to B) \to (A \to B \to C) \to (A \to C)$	Axiom 2
$[(A \to B) \to (A \to B \to C) \to (A \to C)] \to$ $\quad B \to [(A \to B) \to (A \to B \to C) \to (A \to C)]$	Axiom 1
$B \to (A \to B) \to (A \to B \to C) \to (A \to C)$	Modus Ponens
$B \to (A \to B)$	Axiom 1
$[B \to (A \to B)] \to$ $\quad [B \to (A \to B) \to (A \to B \to C) \to (A \to C)] \to$ $\quad [B \to (A \to B \to C) \to (A \to C)]$	Axiom 2
$[B \to (A \to B) \to (A \to B \to C) \to (A \to C)] \to$ $\quad [B \to (A \to B \to C) \to (A \to C)]$	Modus Ponens
$B \to (A \to B \to C) \to (A \to C)$	Modus Ponens
$A \to B \to C$	Premise
$(A \to B \to C) \to B \to (A \to B \to C)$	Axiom 1
$B \to (A \to B \to C)$	Modus Ponens
$[B \to (A \to B \to C)] \to$ $\quad [B \to (A \to B \to C) \to (A \to C)] \to$ $\quad [B \to A \to C]$	Axiom 2
$[B \to (A \to B \to C) \to (A \to C)] \to [B \to A \to C]$	Modus Ponens
$B \to A \to C$	Modus Ponens

□

Corollary 4.7. *$[\varphi \to (\theta_2 \to \psi)] \to [(\varphi \to \theta_2) \to (\varphi \to \psi)]$ can be proved with seven axiom invocations.*

Proof. Proposition 4.6 with Axiom 2 as premise. □

Proposition 4.8. *$\theta_1 \to \theta_2 \to \psi \vdash (\varphi \to \theta_1) \to (\varphi \to \theta_2) \to (\varphi \to \psi)$ invoking the premise only once and invoking 13 axioms.*

Proof. Here is the deduction:

$\theta_1 \to (\theta_2 \to \psi)$	Premise
$(\theta_1 \to (\theta_2 \to \psi)) \to \varphi \to (\theta_1 \to (\theta_2 \to \psi))$	Axiom 1
$\varphi \to \theta_1 \to (\theta_2 \to \psi)$	Mod. Pon.
$(\varphi \to \theta_1 \to (\theta_2 \to \psi)) \to (\varphi \to \theta_1) \to (\varphi \to \theta_1 \to (\theta_2 \to \psi))$	Axiom 1
$(\varphi \to \theta_1) \to (\varphi \to \theta_1 \to (\theta_2 \to \psi))$	Mod. Pon.
$(\varphi \to \theta_1) \to (\varphi \to \theta_1 \to (\theta_2 \to \psi)) \to (\varphi \to (\theta_2 \to \psi))$	Axiom 2
$[(\varphi \to \theta_1) \to (\varphi \to \theta_1 \to (\theta_2 \to \psi))]$ $\quad \to [(\varphi \to \theta_1) \to (\varphi \to \theta_1 \to (\theta_2 \to \psi)) \to (\varphi \to (\theta_2 \to \psi))]$ $\quad \to [(\varphi \to \theta_1) \to (\varphi \to (\theta_2 \to \psi))]$	Axiom 2
$[(\varphi \to \theta_1) \to (\varphi \to \theta_1 \to (\theta_2 \to \psi)) \to (\varphi \to (\theta_2 \to \psi))]$ $\quad \to [(\varphi \to \theta_1) \to (\varphi \to (\theta_2 \to \psi))]$	Mod. Pon.
$(\varphi \to \theta_1) \to (\varphi \to (\theta_2 \to \psi))$	Mod. Pon.
$[\varphi \to (\theta_2 \to \psi)] \to [(\varphi \to \theta_2) \to (\varphi \to \psi)]$	Cor. 4.7
$(\varphi \to \theta_1) \to (\varphi \to \theta_2) \to (\varphi \to \psi)$	Prop. 4.1

Note that the use of Corollary 4.7 adds seven axiom invocations and the use of Proposition 4.1 adds two.

□